Allegato 3

SERVIZIO SANITARIO REGIONALE
EMILIA-ROMAGNA
Azienda Unità Sanitaria Locale della Romagna

LINEE GUIDA FIRMA DIGITALE

Di seguito si riportano le indicazioni per firmare digitalmente i documenti con lo standard CADES (.p7m) e PADES (.pdf) utilizzando File Protector 6 o Dike 6

In caso di difficoltà

In caso di problemi nell'uso della Firma Digitale, potete chiedere assistenza aprendo un ticket telefonando al numero 89600 tasto 2.

In ogni caso è necessario fornire almeno le seguenti informazioni:

- tipo e versione di sistema operativo
- versione del software Java
- versione di File Protector o Dike o se il problema è legato alla firma dentro InterproFx

Actalis File Protector 6

Guida rapida all'uso

Concetti di base

Firma digitale

La firma digitale è un'operazione con la quale si genera un codice crittografico che dimostra l'**identità** e l'**integrità** di un documento. In altre parole, la firma digitale permette di verificare che il documento:

- è stato firmato da una ben precisa persona
- successivamente, non ha subito modifiche

La firma digitale si basa su algoritmi crittografici che richiedono il possesso, da parte dell'utente, di una **chiave privata** e di un corrispondente **certificato**. La chiave privata ed il certificato sono normalmente memorizzati su un dispositivo elettronico simile ad una carta di credito, chiamato **smartcard** (sono le nostre CNS), oppure su un **token USB** (non utilizzate dall'azienda):

Smartcard

Token USB

In fase di generazione della firma, è necessario digitare il **PIN** della propria smartcard o dispositivo USB.

Il certificato è un piccolo file contenente informazioni essenziali per la verifica della firma:

- il nome ed il codice fiscale dell'utente titolare (es. Mario Rossi)
- il nome dell'azienda di appartenenza, se applicabile
- il nome dell'ente certificatore (es. Actalis S.p.A.)
- la data di inizio e la data di fine validità
- la **chiave pubblica** del titolare
- altre informazioni di servizio

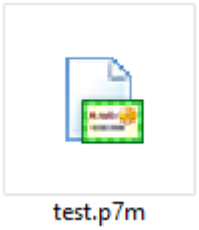
Il certificato viene rilasciato all'utente da un ente terzo fidato, detto **certificatore** (Certification Authority, CA).

Dopo aver generato una firma digitale, questa viene solitamente salvata in un file detto **busta crittografica**; la busta contiene normalmente anche il documento di partenza ed il certificato del firmatario, così da tenere insieme tutte le informazioni necessarie per la verifica.

Esistono diversi formati di busta crittografica; il più diffuso è quello conosciuto come PKCS#7 (in tal caso il file ha l'estensione **P7M**).

Affinché la firma digitale abbia un pieno valore legale (in tal caso si parla di firma **qualificata**), devono essere rispettate diverse norme di legge che stabiliscono requisiti relativi alle chiavi, al certificato, alla smartcard, al certificatore, al formato della busta crittografica, eccetera. Puoi trovare una rassegna delle principali norme di legge sul sito dei servizi di certificazione di Actalis: http://portal.actalis.it.

La icona di un documento firmato con File Protector assume il seguente aspetto:



Cifratura (crittografia)

La **cifratura** (detta anche crittografia) di un documento è un'operazione con la quale si rende quel documento completamente illeggibile per chiunque, ad eccezione di chi possiede la chiave che permette di decifrarlo, ossia riportarlo "in chiaro". La cifratura, dunque, permette di assicurare la confidenzialità di informazioni riservate.

Per cifrare un documento in modo che solo un particolare destinatario possa leggerlo, il mittente deve avere a disposizione il certificato di quel destinatario, poiché l'operazione di cifratura richiede l'uso della chiave pubblica.

Per poter **de**cifrare un documento, il destinatario deve avere a disposizione la propria smartcard, in quanto l'operazione di decifratura richiede l'uso della chiave privata.

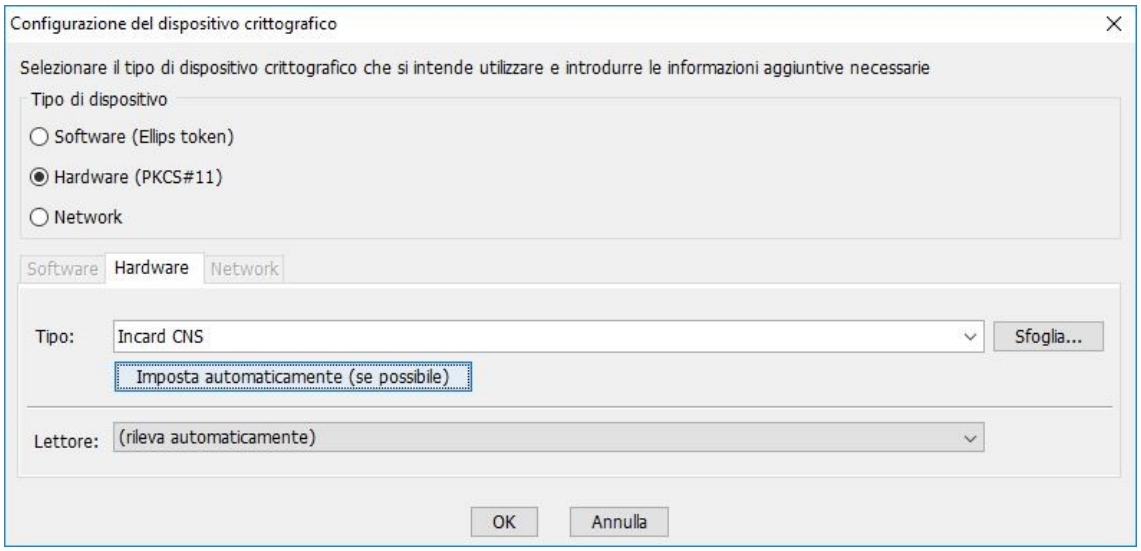
Le operazioni di firma digitale e cifratura possono essere combinate tra loro: in altre parole, un documento può essere firmato e successivamente cifrato, così da garantirne sia la paternità che la segretezza.

Per maggiori informazioni, si rimanda al Manuale Utente.

La icona di un documento cifrato con File Protector assume il seguente aspetto:

Configurare l'applicazione per l'accesso alla smartcard

Se avete ricevuto il software insieme alla smartcard, File Protector dovrebbe essere già pre-configurato in modo corretto. In ogni caso, per la configurazione si procede come segue. Avviare l'applicazione, inserire la smartcard nel lettore e quindi selezionare la voce "**Configurazione**" del menu "**Dispositivo**"; apparirà la seguente finestra di dialogo:



A questo punto cliccare sul bottone "**Imposta automaticamente**": se la smartcard vi è stata fornita da Actalis, essa sarà riconosciuta e configurata in modo automatico. Altrimenti, selezionare il tipo corretto di smartcard dal menu a discesa. Cliccare infine sul bottone "OK" per concludere. L'impostazione viene memorizzata, quindi in seguito non sarà più necessario svolgere questa operazione.

Per quanto riguarda il lettore di smartcard da usare, di norma è preferibile lasciare che File Protector lo determini in modo automatico (questo è l'effetto dell'impostazione iniziale "rileva automaticamente"). Altrimenti, selezionare il lettore desiderato dalla lista a discesa.

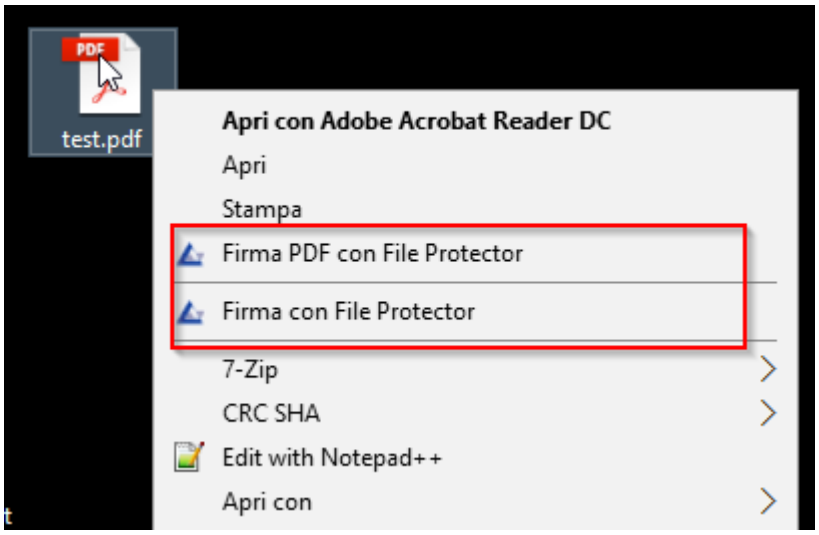
Firmare un file .p7m (Firma Cades)

Per poter firmare un file, **dovete avere almeno un certificato valido di firma sulla vostra smartcard**. Se ne avete più di uno, in fase di firma dovrete scegliere il certificato desiderato.

Si può avviare la firma digitale di un file in tre modi diversi, descritti di seguito:

- dall'esterno dell'applicazione, attraverso il menu contestuale di Windows Explorer
- dall'esterno dell'applicazione, mediante "drag-and-drop"
- dall'interno di File Protector

Il **primo metodo**, disponibile al momento solo in ambiente Windows, consiste nel cliccare sull'icona del file desiderato con il tasto destro del mouse, per visualizzare il menu contestuale; qui selezionare la voce "**Firma con File Protector**" per avviare l'applicazione e firmare il file. Vi verrà richiesto il PIN della smartcard. La firma digitale verrà salvata nella stessa cartella del documento di partenza, con estensione P7M. Per esempio, la firma del file contratto.pdf verrà salvata in un file di nome contratto.pdf.p7m.



Il **secondo metodo** è particolarmente comodo se l'applicazione File Protector è già avviata. In tal caso, la firma di un file si può avviare trascinando l'icona del file desiderato sopra l'area-bersaglio di File Protector:

Come **terzo metodo**, se l'applicazione File Protector è già avviata, per avviare la firma di un file si può anche:

- selezionare la voce "**Firma**" dal menu "**File**"
- oppure cliccare sul bottone "**Firma**" della toolbar

In entrambi i casi verrà visualizzata una finestra di selezione file per consentirvi di scegliere il file desiderato.

Tramite menu' File è possibile inoltre accedere ai vari tipi di firma (Cades di default, PDF-Pades e XML-Xades, e le relative versioni remote).

Avviando la firma dall'interno di File Protector, è possibile eseguire anche una *firma multipla* (vedere la sezione relativa).

Firmare una cartella

Con File Protector è possibile firmare tutti i file presenti in una cartella con una singola operazione.

Sono disponibili due modalità di firma di una cartella:

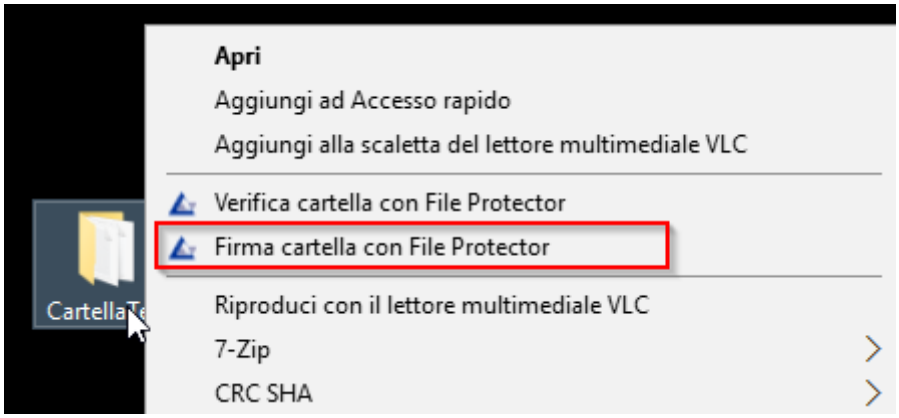
- firma individuale di ciascun file
- firma di un elenco delle impronte dei file

Nel primo caso vengono prodotte tante buste crittografiche P7M quanti sono i file presenti nella cartella di input. Nel secondo caso, invece, viene prodotta una singola busta crittografica in formato XML. Il secondo metodo è più veloce e consente un forte risparmio di spazio su disco, quando la cartella di input contiene molti documenti.

Come nel caso della firma di un singolo file, si può avviare la firma di una cartella in tre modi diversi:

- dall'esterno dell'applicazione, attraverso il menu contestuale di Windows Explorer
- dall'esterno dell'applicazione, mediante "drag-and-drop"
- dall'interno di File Protector

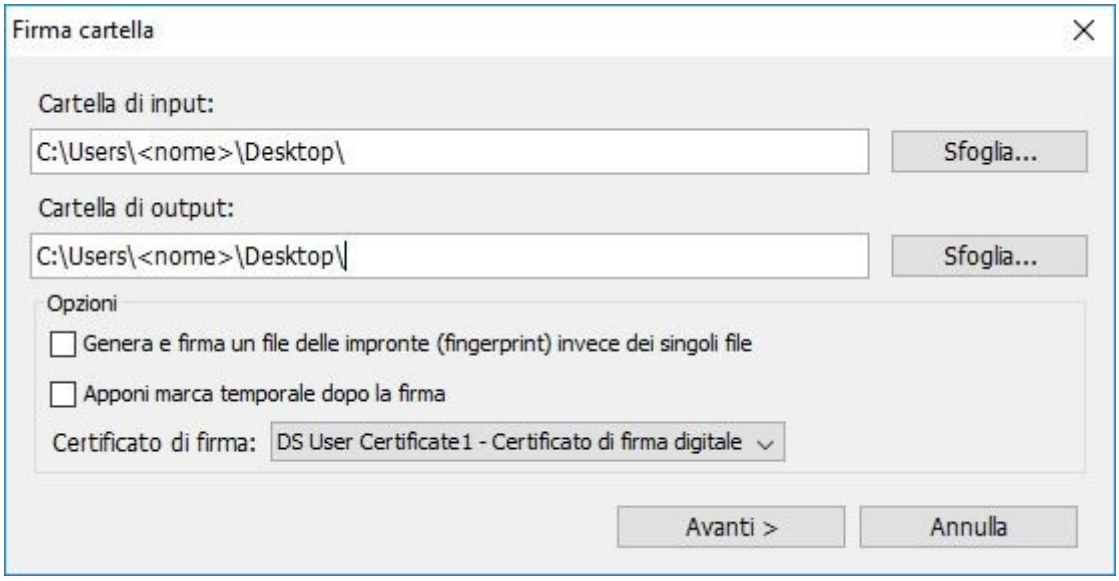
Il **primo metodo**, disponibile al momento solo in ambiente Windows, consiste nel cliccare sull'icona della cartella desiderata con il tasto destro del mouse, per visualizzare il menu contestuale; qui selezionare la voce "**Firma Cartella con File Protector**" per avviare l'applicazione ed avviare il processo di firma.



Il **secondo metodo** è particolarmente comodo se l'applicazione File Protector è già avviata. In tal caso, la firma di una cartella si può avviare trascinando l'icona della cartella desiderata sopra l'area-bersaglio di File Protector (vedere la figura).

Il **terzo metodo**, utilizzabile se l'applicazione File Protector è già avviata, consiste nel selezionare la voce "**Firma Cartella**" dal menu "**File**".

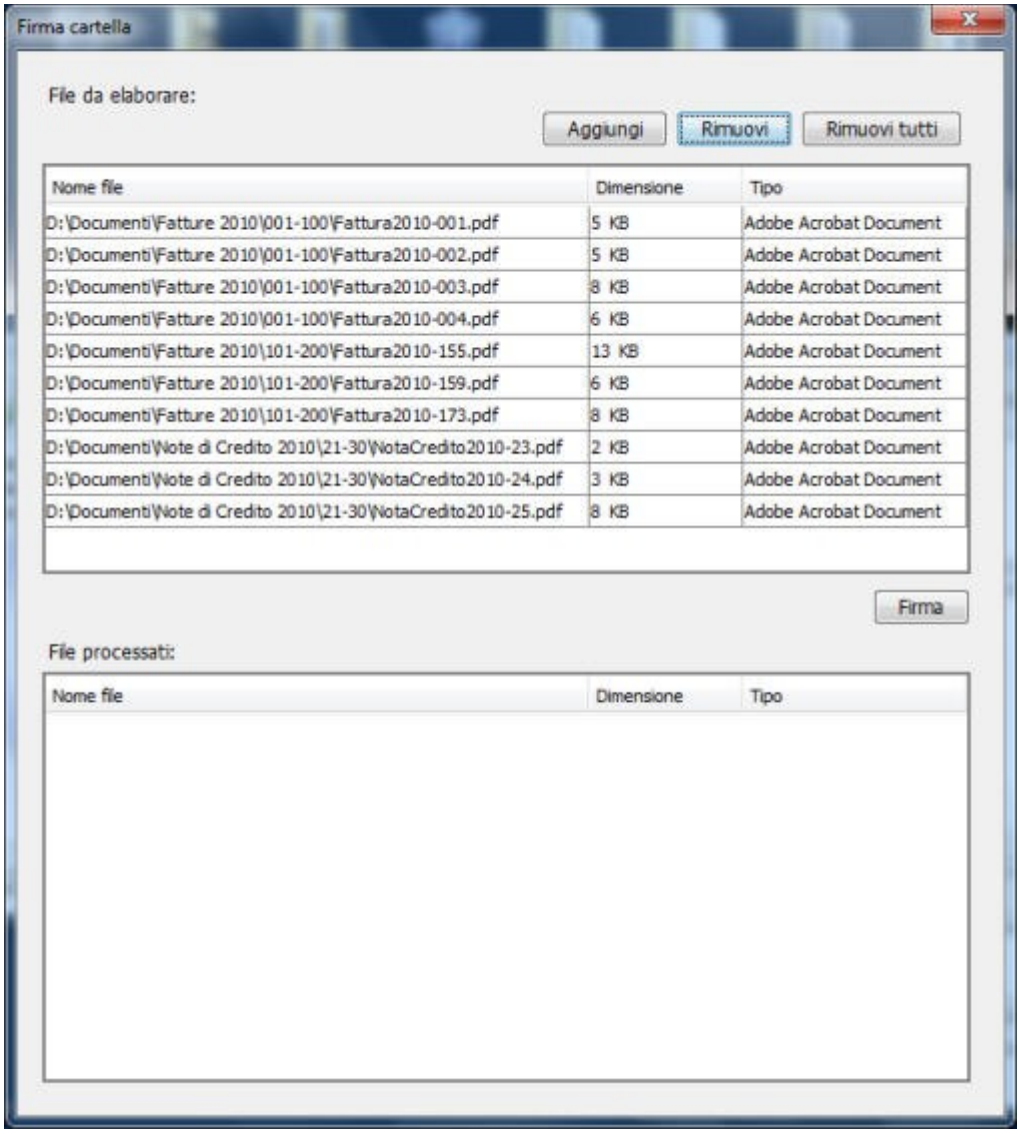
Qualunque sia il metodo scelto per avviare la firma di una cartella, apparirà la seguente finestra di dialogo:



In questa finestra occorre scegliere la modalità di firma desiderata e le relative opzioni. Dopodiché, cliccando sul bottone "**Avanti >**" il processo di firma avrà inizio.

Firma di un insieme di file

Selezionando la voce di menu "**Firma di un insieme di file**" appare una finestra di dialogo che permette di firmare un insieme qualsiasi di file, anche residenti in cartelle diverse:

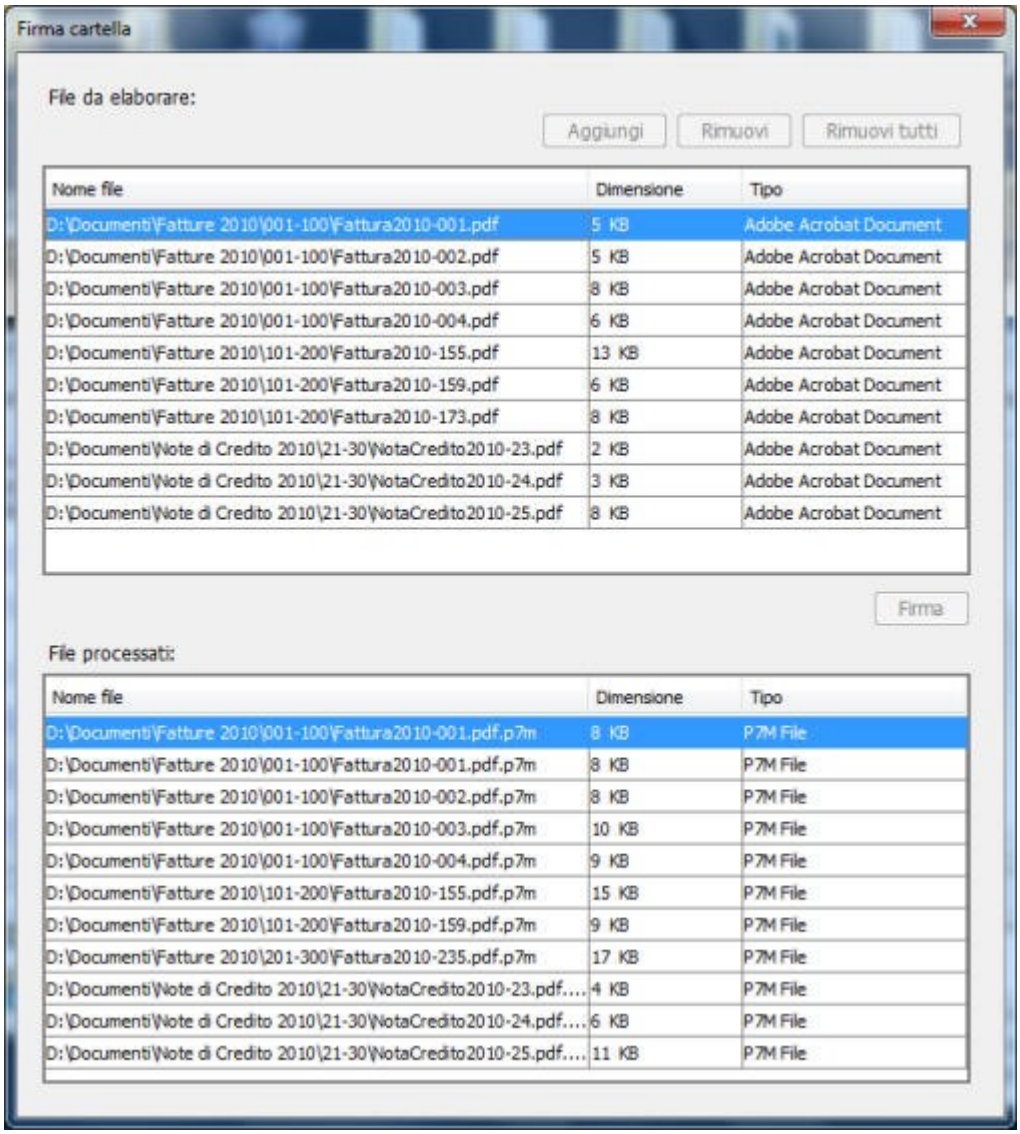


La parte superiore della finestra ("basket") elenca i file che verranno firmati. L'elenco può essere compilato sia cliccando sul bottone "**Aggiungi**" e selezionando un file, sia *trascinando* l'icona del file desiderato sull'elenco stesso (drag and drop). Possono essere aggiunti al basket anche file già firmati (in questo caso verrà aggiunta ad essi una ulteriore firma).

Come si può intuire, i bottoni "Rimuovi" e "Rimuovi tutti" permettono di eliminare dal basket il file selezionato oppure tutti quanti.

Volendo controllare un documento prima della firma, è sufficiente fare doppio-clic sulla voce corrispondente nell'elenco "da elaborare": il file sarà aperto nell'applicazione associata (per es. nel caso di un documento PDF si aprirà tipicamente Adobe Reader).

Cliccando infine sul bottone "**Firma**", verrà avviato il processo di firma digitale (in formato P7M) di tutti i file dell'elenco. Le buste P7M risultanti, elencate nella parte inferiore della finestra, vengono salvate nella stessa cartella del documento di origine:



Al termine, per dismettere la finestra premere il tasto OK oppure cliccare sull'icona di chiusura.

Firma un insieme di file PDF

In modo del tutto analogo alla "**Firma di un insieme di file**", è possibile eseguire la "**Firma di un insieme di file PDF**" che permette di eseguire drag'drop di un insieme qualsiasi di file PDF, anche residenti in cartelle diverse. La firma eseguita è la firma Adobe e quindi i documenti firmati sono ancora documenti PDF denominati con il suffisso: (firmato). Per esempio "pippo.pdf" una volta firmato si chiamerà "pippo(firmato).pdf.

Firmare in modalità PDF

In un documento PDF (Portable Document Format) è possibile inserire una o più firme digitali senza necessità di produrre una busta crittografica separata. File Protector è in grado di generare anche firme in standard PDF; l'utente può quindi scegliere tra la firma classica (P7M) oppure la firma PDF, secondo necessità.

La firma in standard PDF ha il vantaggio di poter essere verificata col visualizzatore Adobe Reader, di ampia diffusione, e di poter avere una rappresentazione grafica che la rende più facilmente confrontabile con la firma tradizionale (autografa). Per contro, la firma in standard

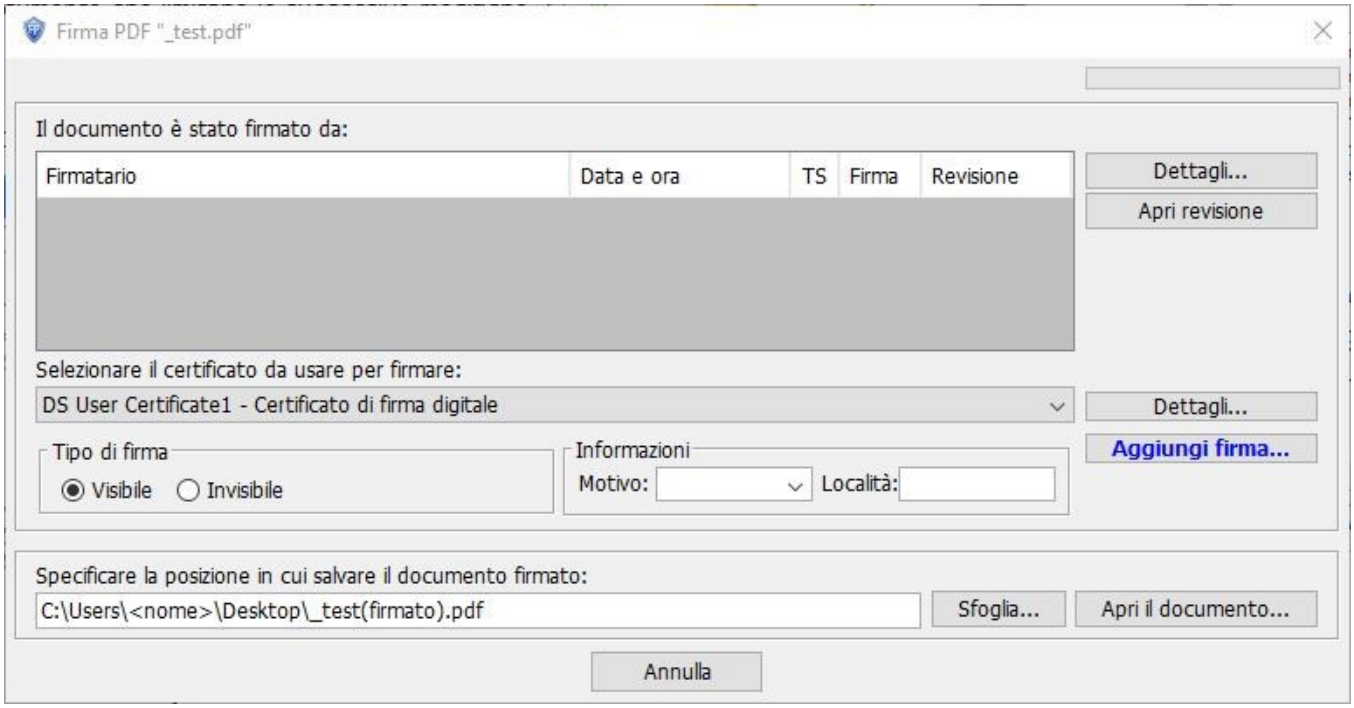
PDF è per adesso meno diffusa ed accettata della firma P7M, pur avendo lo stesso valore dal punto di vista tecnico e legale, ed è applicabile solo ai documenti in formato PDF.

Esistono due tipi di firma PDF dal punto di vista "grafico":

- firma *invisibile* (senza rappresentazione grafica)
- firma *visibile* (con rappresentazione grafica)

Nel caso della firma visibile normalmente il documento PDF contiene un **campo firma** apprositamente predisposto. Ad ogni firma apposta al documento corrisponde una nuova "revisione" del documento stesso.

Per firmare un documento in standard PDF si deve selezionare la voce "**Firma PDF**" dal menu "**File**". Dopo aver selezionato il documento desiderato, compare la seguente finestra di dialogo:



È possibile, opzionalmente, compilare i campi "Motivo" e "Località"; in tal caso, tali informazioni saranno anch'esse firmate e inserite tra i campi della firma.

Infine, per aggiungere una firma al documento basta scegliere il certificato desiderato e cliccare sul bottone "**Aggiungi firma**".

* * *

È anche possibile avviare il processo di firma PDF dal menu contestuale di Windows, cliccando col tasto destro del mouse sul documento desiderato e poi selezionando la voce di menu "**Firma PDF con File Protector**"

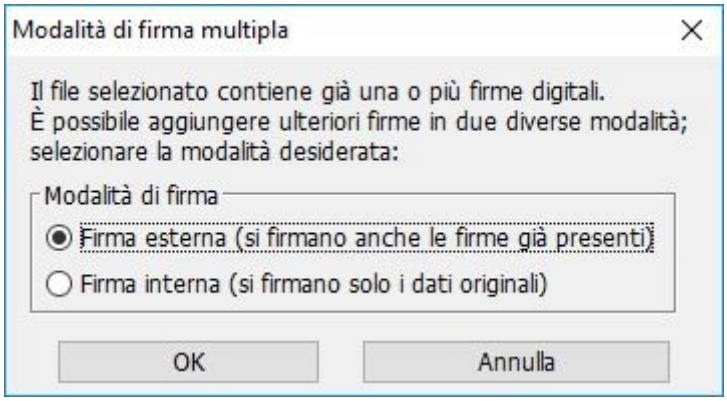
Eseguire firme multiple

Ad un medesimo documento possono essere apposte più firme digitali; si parla in tal caso di "firme multiple". Questo consente di dimostrare che più persone hanno assunto la paternità e/o la responsabilità del documento, eventualmente in momenti diversi, così come spesso avviene nel caso della tradizionale firma autografa (basti pensare ai contratti, ai bilanci, ecc).

Esistono tre tipologie di firme multiple:

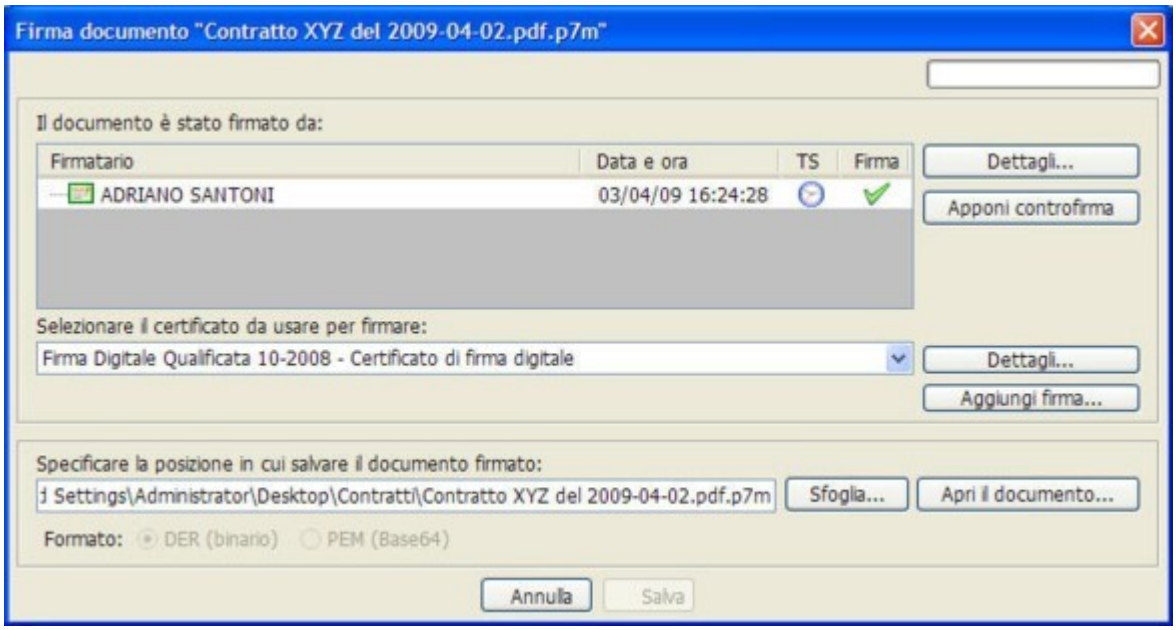
- firme "a matrioska"
- firme parallele (anche dette *indipendenti*)
- contro-firme (anche dette *annidate*)

Il primo tipo si ottiene semplicemente firmando una busta crittografica P7M (che contiene un documento già firmato). Questa operazione digitale equivale, nel mondo della carta, a firmare una busta che contiene un documento firmato, ciò che in effetti a volte viene fatto (si pensi alle buste che contengono le offerte in risposta a bandi di gara). Per effettuare una firma "a matrioska" con File Protector, occorre agire dall'interno dell'applicazione, cliccando sul bottone "**Firma**" oppure selezionando la corrispondente voce di menu. Quando File Protector si accorge che il documento selezionato è in effetti una busta P7M, visualizza la seguente finestra di dialogo:



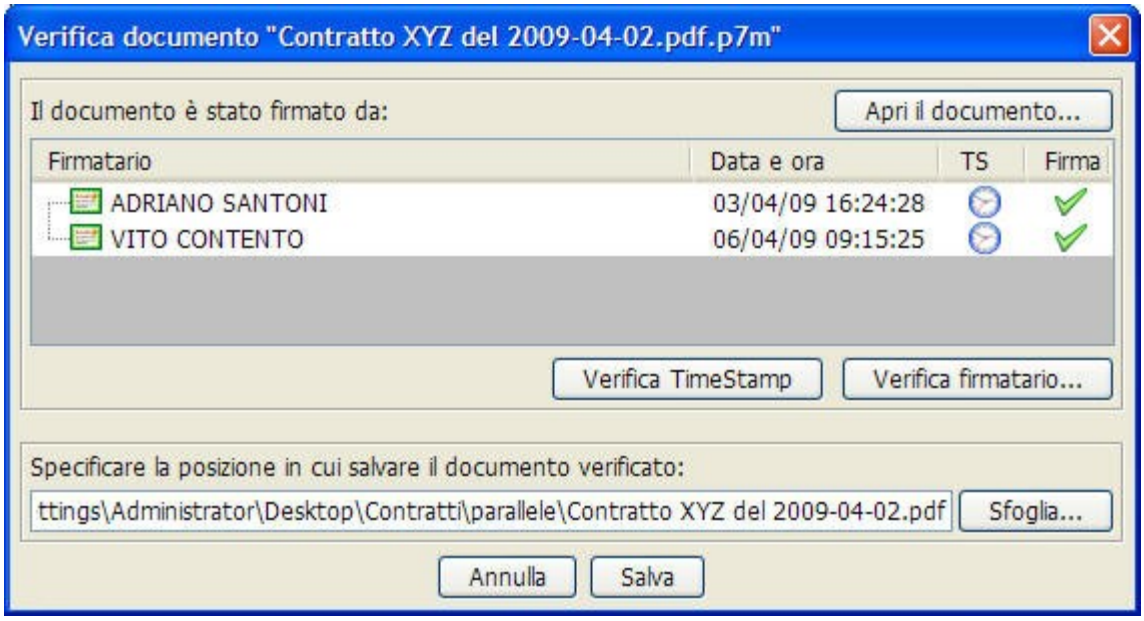
A questo punto, per fare una firma multipla "a matrioska" si deve selezionare la voce "**Firma esterna**".

Selezionando invece la voce "**Firma interna**", sarà possibile eseguire firme multiple del secondo e del terzo tipo; apparirà a questo punto la seguente finestra di dialogo:

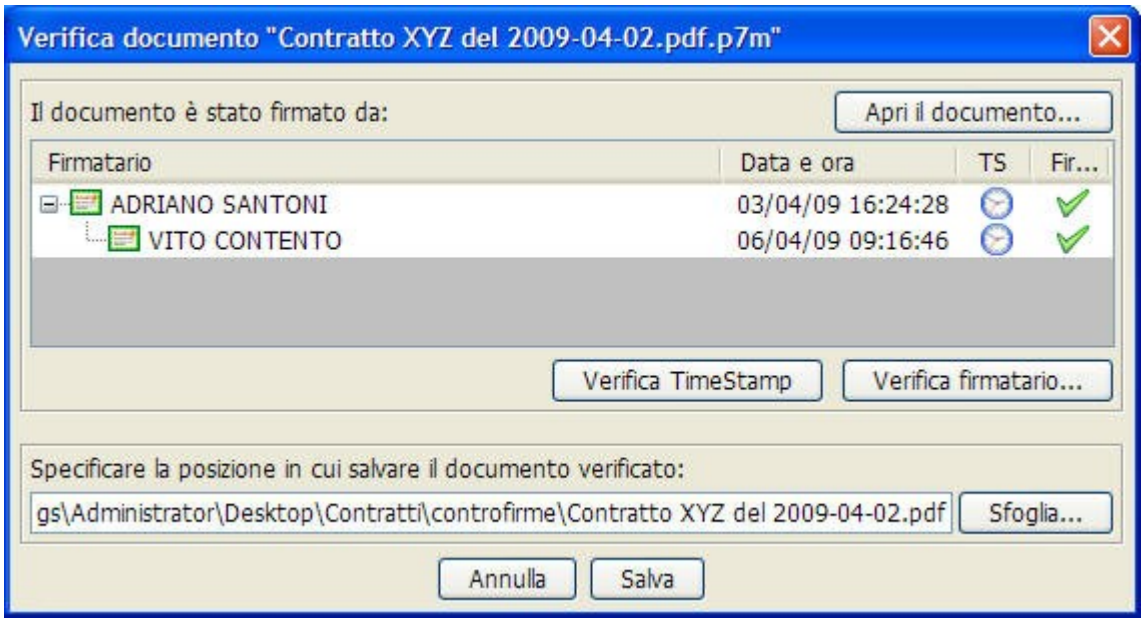


Il secondo tipo di firma multipla (detta *parallela* o *indipendente*) consiste nell'aggiungere ulteriori firme "a fianco" della prima, dove ciascuna firma mantiene la sua indipendenza (ogni firmatario firma gli stessi dati che firmano gli altri). Questa operazione digitale equivale, nel

mondo della carta, ad apporre più firme, da parte di persone diverse, in calce al medesimo documento. Per aggiungere una firma indipendente, cliccare sul bottone "**Aggiungi firma...**" nella finestra mostrata sopra. In fase di verifica, si potrà constatare che il documento contiene le firme aggiunte:



Il terzo tipo di firma multipla (detta *controfirma* o *annidata*) si ottiene firmando una firma già esistente, e conservando il risultato (detto contro-firma) all'interno della medesima busta. Facendo questo, il secondo firmatario in pratica approva o "convalida" la prima firma. A sua volta, la seconda firma può essere firmata da una terza persona, e così via. Per aggiungere una controfirma, selezionare la firma desiderata poi cliccare sul bottone "**Apponi controfirma**" nella finestra mostrata sopra. In fase di verifica, si potrà constatare che il documento contiene la contro-firma (notare la rappresentazione ad albero):



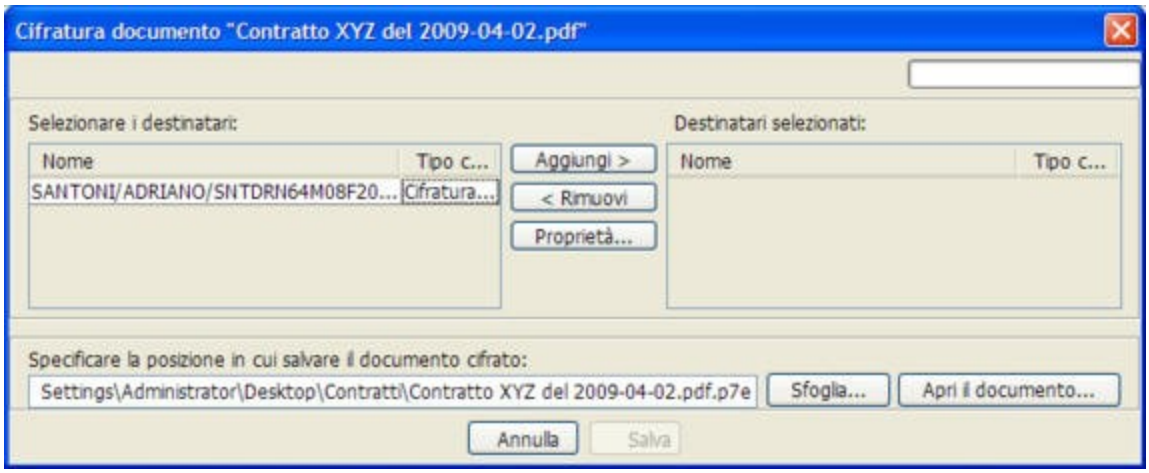
Cifrare (crittografare) un file

Ricordiamo anzitutto che per cifrare un documento è necessario possedere il certificato di cifratura del destinatario (ossia dell'utente che vogliamo sia l'unico a poter decifrare il documento).

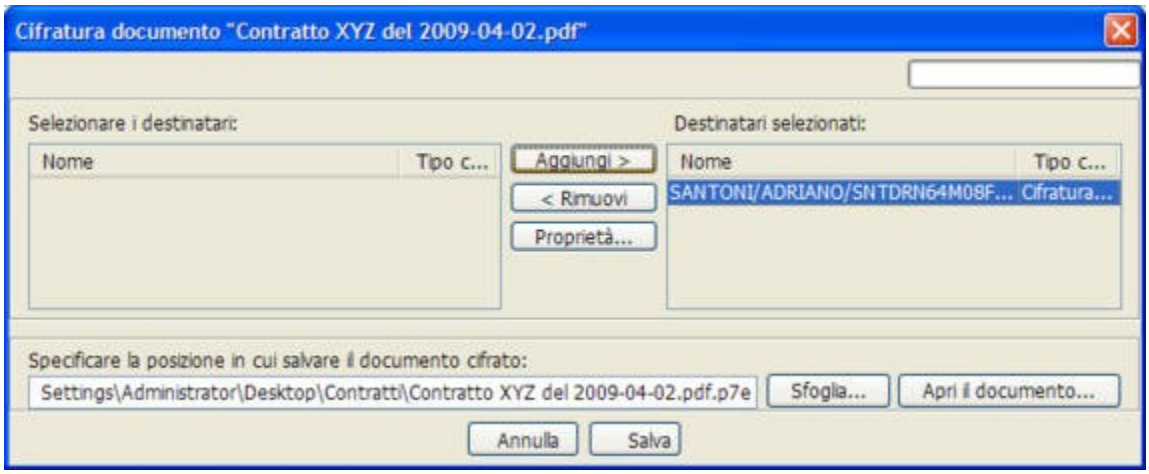
Nel caso in cui il certificato desiderato sia pubblicato su un directory server, è possibile scaricarlo ed importarlo nel proprio database di certificati direttamente dall'interno di File Protector (vedere la sezione relativa). Altrimenti, si può richiedere il certificato al destinatario e poi importarlo manualmente nel proprio database di certificati.

È possibile cifrare un documento per più utenti contemporeamente, ossia in modo tale che diverse persone - e solo loro - possano decifrarlo.

Per cifrare un documento, cliccare sul bottone "**Cifra**" nella finestra principale di File Protector, oppure selezionare la voce corrispondente nel menu "**File**". Dopo aver selezionato il documento desiderato, apparirà la seguente finestra:



Nella parte sinistra sono elencati i certificati di cifratura disponibili (ossia presenti nel proprio database dei certificati), mentre nella parte destra sono elencati i certificati dei destinatari. Si possono aggiungere e rimuovere a piacere i destinatari del documento cifrato:



Per completare l'operazione, cliccare sul bottone "**Salva**".

La firma digitale e la cifratura possono essere applicate in modo combinato ad un medesimo documento, in modo da assicurarne sia l'origine (ed integrità) sia la segretezza. Per fare

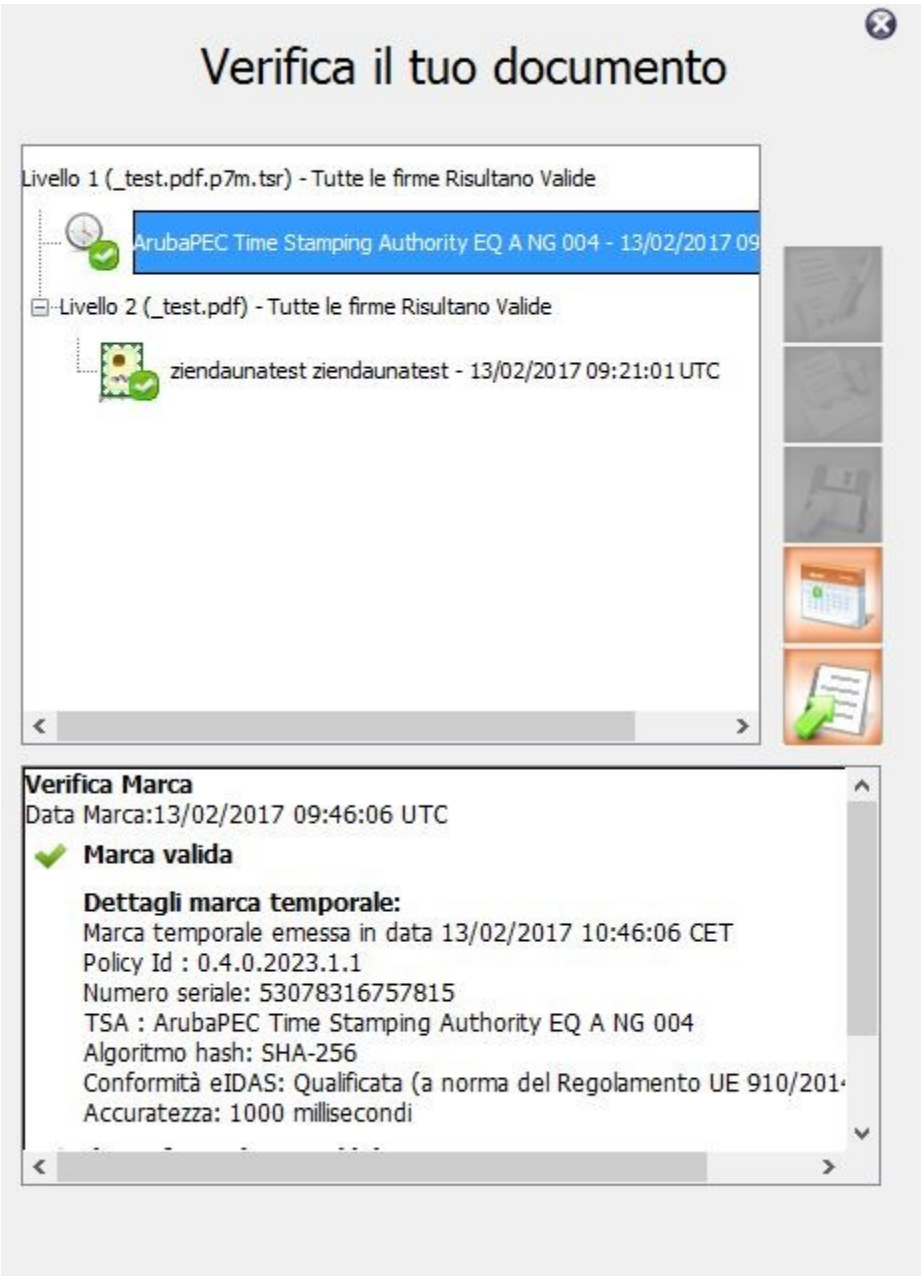
questo, cliccare sul bottone "**Firma e Cifra**" nella finestra principale di File Protector, oppure selezionare la voce corrispondente dal menu "File".

Verificare un documento firmato e/o marcato

La funzione di verifica è applicabile indistintamente a file firmati (P7M, PDF, XML) e marche temporali (TSR, TSD, TST) e si può avviare in quattro modi diversi:

- facendo "doppio-clic" sul file da verificare
- attraverso il menu contestuale di Windows Explorer (selezionare la voce "**Verifica con File Protector**")
- mediante "drag-and-drop" (trascinamento del documento sull'area bersaglio)
- cliccando sul bottone "**Verifica**" oppure selezionando la voce di menu "**File**" > "**Verifica**"

Al termine della verifica, apparirà la seguente finestra:



Da questa finestra è possibile:

- verificare la validità e il tipo della firma
- verificare la validità del certificato di ogni firmatario e di ogni marca
- visualizzare il documento fimato, estrarlo e salvarlo su file (tramite i pulsanti laterali)
- visualizzare e verificare la marca temporale (se presente) associata alla firma
- imporre la data e l'ora di verifica

La verifica *completa* di una firma digitale richiede due passi:

1. verifica della firma in se stessa (verifica di integrità)
2. verifica del certificato del firmatario

Nell'interfaccia ad albero sono mostrate contestualmente entrambe le infomazioni, mentre nel box sottostante è riportato il dettaglio di verifica.

È importante notare che la verifica del certificato viene sempre svolta alla data-ora corrente, la quale viene determinata nel modo seguente:

- la data-ora estratta dalla marca temporale associata alla firma (se presente)
- altrimenti, la data-ora estratta dall'attributo signingTime (se presente)
- altrimenti, la data-ora corrente del sistema operativo

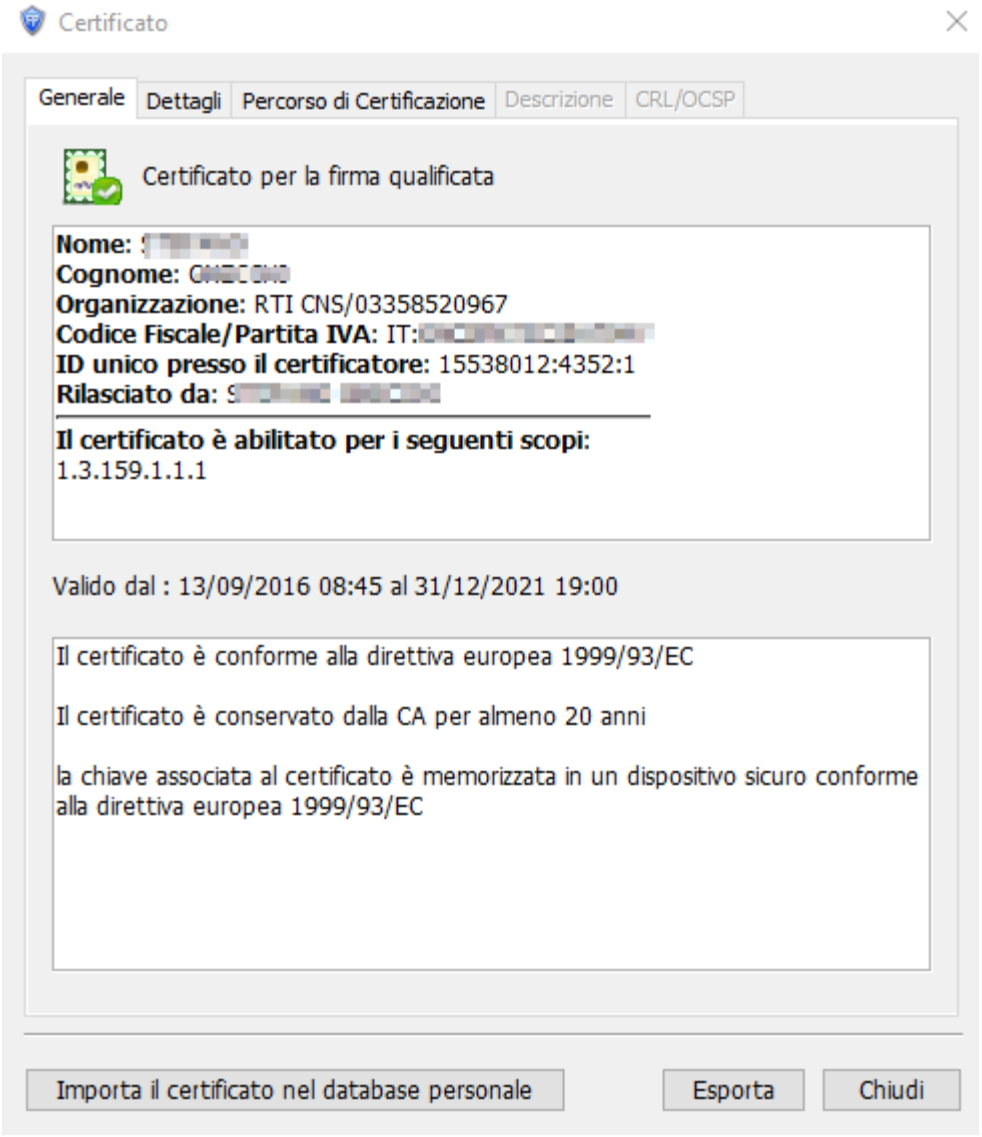
Per effettuare la verifica del certificato ad una data-ora diversa, di propria scelta, cliccare sul bottone

Da qui, usando gli appositi selettori, è possibile impostare la data e ora desiderate per la verifica del certificato.

Gli altri pulsanti laterali alla finestra si attivano contestualmente alla tipologia di file verificato, non essendo certe operazioni disponibili per qualunque formato di busta

1. aggiungi firma (interna o esterna)
2. aggiungi controfirma
3. apri il file contenuto nella busta
4. salva il file contenuto nella busta
5. verifica alla data
6. salva il report PDF di verifica

Tramite il doppio click del mouse su di un certificato di firma o di marca temporale (TSA) è possibile aprire il dialogo di dettaglio del certificato:



Nel dialogo che appare è possibile visualizzare, tra le altre cose, i dettagli relativi al possessore del certificato e il **periodo di validità** del certificato.

Il bottone "**Importa il certificato nel database personale**" consente di memorizzare il certificato in esame nel proprio database dei certificati, in modo da poterlo recuperare in seguito quando si debba fare una cifratura. Questo è utile solo per i certificati di cifratura (es. di tipo S/MIME o generico), mentre è inutile nel caso dei certificati qualificati in quanto questi ultimi non possono essere usati per operazioni di cifratura.

Decifrare un documento

Per decifrare un documento cifrato, si può procedere in cinque modi diversi:

- cliccare sul bottone "Verifica" nella finestra principale,
- oppure selezionare la voce "Verifica" dal menu "File",
- oppure trascinare il documento desiderato sull'area bersaglio,
- oppure fare doppio-clic sull'icona del documento desiderato,
- oppure cliccare sull'icona del documento col tasto destro del mouse, quindi selezionare la voce "**Decifra con File Protector**" dal menu contestuale.

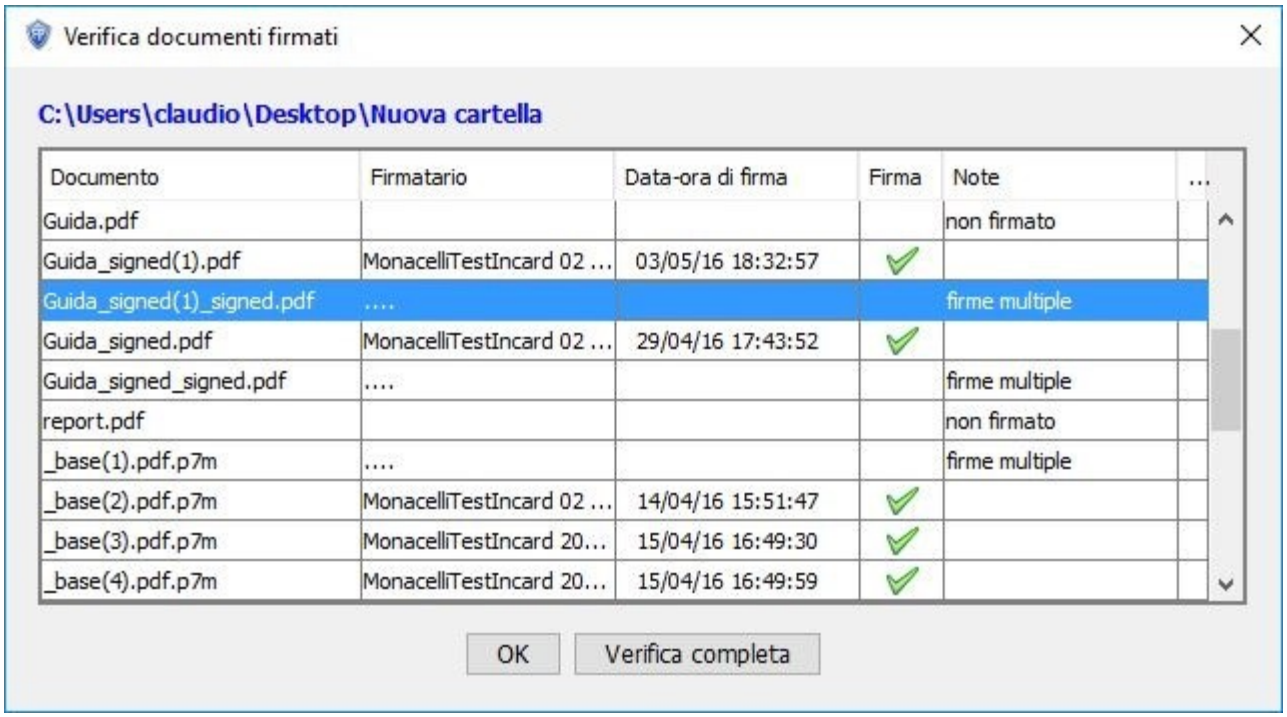
Se non si possiede la chiave privata necessaria per decifrare, apparirà un messaggio d'errore:

Altrimenti, apparirà il seguente dialogo che permette di visualizzare e salvare il documento "in chiaro":

Verificare una cartella

Se una cartella è stata firmata col metodo elenco delle impronte, per la verifica si procede come nel caso di una normale verifica di firma XML, avendo l'accortezza di selezionare il file di nome "**signature.xml**" presente nella cartella firmata.

Se invece sono stati firmati i singoli file contenuti in una cartella, è possibile svolgere una "verifica massiva" selezionando la voce "**Verifica cartella**" dal menu "File" dell'applicazione. Dopo aver selezionato la cartella di input (quella che contiene i documenti firmati da verificare) apparirà una finestra di dialogo di questo tipo:



Nel caso in cui il documento selezionato presenti una firma singola - come avviene di norma nel caso della firma cartella - la finestra mostra le informazioni principali risultanti dalla verifica: il nome del firmatario (estratto dal certificato), la data e ora di firma (se presente, eventualmente attestata da una marca temporale), la validità della firma e le eventuali note aggiuntive in caso di errore.

Nel caso in cui invece il file selezionato presenti più firme, apparirà la dicitura "firme multiple". In entrambi i casi ci si potrà ricondurre ai dettagli della verifica selezionando il file dall'elenco e cliccando sul bottone "**Verifica completa**".

La funzione di "verifica cartella" supporta tutti i tipi di firma gestiti dall'applicazione: P7M/CMS, PDF, XML.

Decifrare i file presenti in una cartella

Se i file presenti in una cartella (e nelle sottocartelle) sono stati cifrati con "**Cifra cartella**" (modalità disponibile solo per alcuni profili), è possibile svolgere la "decifratura massiva" selezionando la voce "**Decifra cartella**" dal menu "File" dell'applicazione. Dopo aver selezionato la cartella di input (quella che contiene i documenti da decifrare) viene richiesto l'inserimento del token ed il PIN. Quindi, se sono disponibili le credenziali per decifrare, ciascun file verrà decifrato.

La funzionalità è eseguita in modo ricorsivo sui file cifrati presenti nelle sottocartelle.

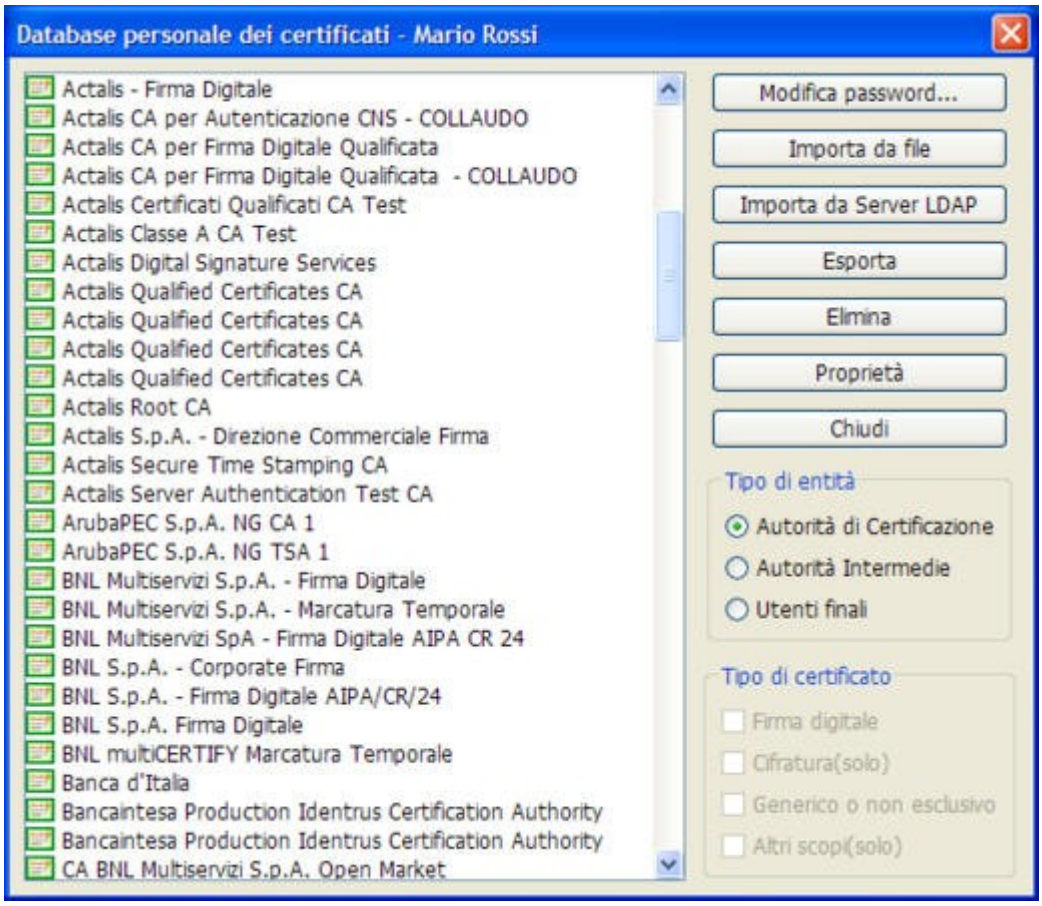
Gestione dei certificati

File Protector permette di gestire un database personale dei certificati delle CA e degli utenti;

- i certificati di CA sono necessari per verificare la validità dei certificati degli utenti;
- i certificati degli utenti finali sono necessari solo per le operazioni di cifratura.

Il database è protetto con la password di accesso al profilo.

È possibile aggiungere, rimuovere e visualizzare i certificati attraverso la finestra di gestione dei certificati, alla quale si accede selezionando la voce "**Database certificati**" dal menu "**Strumenti e opzioni**":



Da questa interfaccia è inoltre possibile importare nuovi anche tramite server LDAP precedentemente configurato da menu' **(Strumenti e Opzioni > Elenco server LDAP)**.

Gestione del dispositivo

File Protector permette una completa gestione del dispositivo di firma (es. smartcard o token USB), in termini di:

- visualizzazione delle informazioni principali sul dispositivo
- visualizzazione degli oggetti presenti sul dispositivo
- ridenominazione degli oggetti
- cancellazione degli oggetti
- importazione di certificati
- esportazione di certificati
- importazione di dati qualsiasi
- creazione di nuove coppie di chiavi
- richiesta di certificati, anche on-line
- cambio del PIN
- sblocco del PIN
- cambio del PUK

Per accedere a queste funzionalità, selezionare la voce "**Gestione del dispositivo**" dal menu "**Strumenti e opzioni**"; apparirà la seguente finestra di dialogo:

Avvertenze:

1. Actalis declina ogni responsabilità in caso di problemi derivanti da un uso non consapevole di queste funzionalità.
2. La cancellazione di oggetti (certificati, chiavi, ecc) è permanente; non c'è modo di recuperare le informazioni cancellate.
3. In generale una chiave privata non è esportabile, in quanto la smartcard lo impedisce; quand'anche fosse possibile, si rammenta che l'estrazione "in chiaro" di una chiave privata di firma costituisce un'infrazione alle norme vigenti.

Gestione del profilo

File Protector è un'applicazione multi-utente, ovvero permette a diversi utenti di utilizzare la medesima installazione, ciascuno conservando le proprie opzioni e preferenze. All'avvio di File Protector compare la seguente finestra di dialogo:

Da questa finestra è possibile la creazione di nuovi profili e la selezione di quello desiderato. Per accedere all'applicazione col profilo desiderato, occorre conoscere la password corrispondente, che viene decisa dall'utente al momento della creazione del profilo.

raccomandiamo di selezionare l'opzione "Memorizza la password" e **NON** l'opzione "Autologin". (questa seconda opzione fa in modo che File Protector non mostri più questa finestra, così da velocizzare la partenza dell'applicazione però con alcune versioni vecchie di Windows è stato

rilevato un problema per cui alla chiusura del programma non è più possibile riaprirlo se non si chiude la sessione utente nel pc.)

Gestione del PIN

Il dispositivo di firma (smartcard o altro dispositivo equivalente) è protetto da un codice segreto detto **PIN.** Durante una sessione di lavoro con File Protector, per poter svolgere operazioni di firma o decifratura dovete digitare il PIN della vostra smartcard almeno una volta (cliccare sul bottone "**Login**" nella finestra principale); in alcuni casi, File Protector vi chiede automaticamente di inserire il PIN se necessario:

Al termine di una sessione di lavoro File Protector, se preferite lasciare attiva l'applicazione, raccomandiamo di cliccare sul bottone "**Logout**" in modo da impedire ad altri l'uso indebito della vostra smartcard.

Senza conoscere il vostro PIN, non è possibile apporre la vostra firma digitale o decifrare un documento a voi riservato, perciò è molto importante che il vostro PIN sia noto solo a voi e che sia difficile da indovinare.

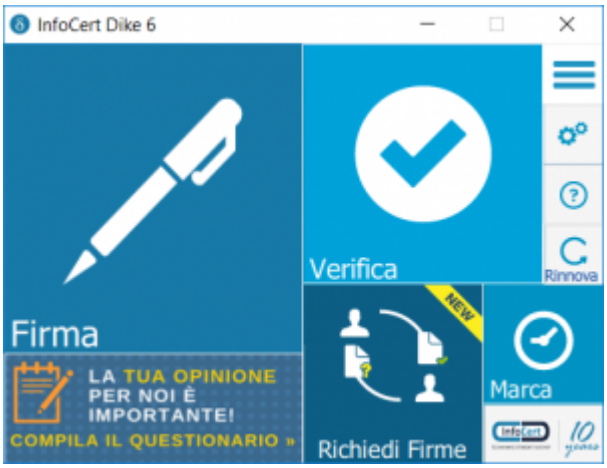
La smartcard viene di solito consegnata all'utente con un adeguato PIN preimpostato; tuttavia potete impostare il PIN al valore desiderato selezionando la voce "**Cambio PIN**" dal menu "**Dispositivo**", nella finestra principale.

Per ragioni di sicurezza, se si inserisce il PIN in modo errato più di un certo numero di volte (solitamente 3), la smartcard si blocca e non è più possibile utilizzarla fino a quando non viene sbloccata. Per **sbloccare** la vostra smartcard, dovete conoscere un secondo codice segreto detto **PUK**. In tal caso, selezionate la voce "**Sblocco PIN**" dal menu "**Dispositivo**", nella finestra principale.

Si faccia attenzione a digitare correttamente il PUK, perché anche questo è soggetto al blocco in caso di errori ripetuti. In caso di blocco del PUK, non è più possibile ripristinare il normale funzionamento della smartcard.

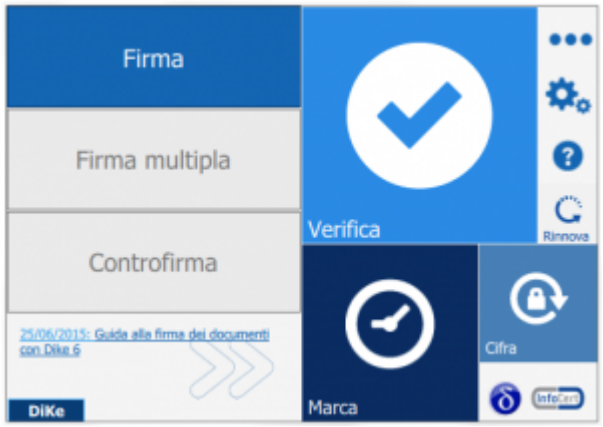
FIRMA DI DOCUMENTI UTILIZZANDO DIKE 6 (NON USARE VERSIONI PRECEDENTI)

Apro l'applicativo, nella schermata principale potrò firmare o verificare la firma apposta ad un documento.

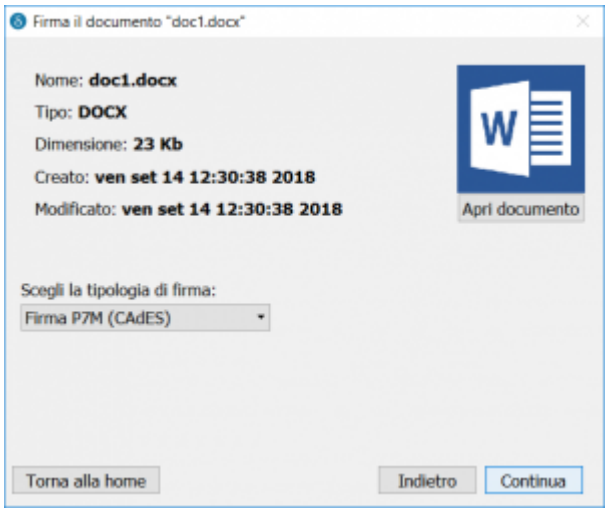


FIRMA DI UN DOCUMENTO

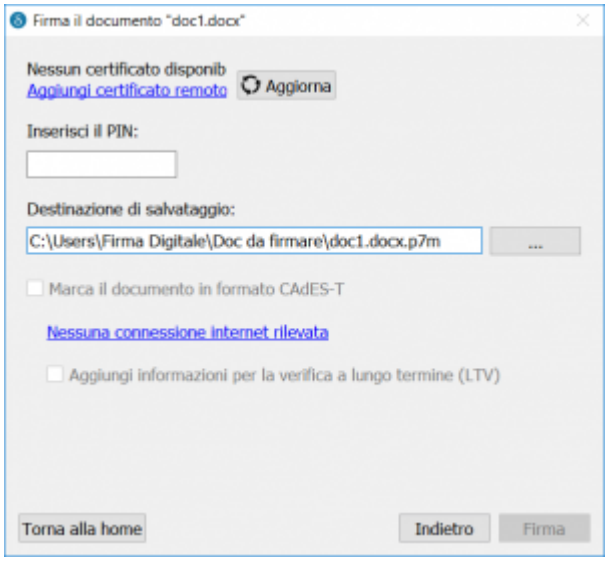
Passando il mouse sul riquadro *Firma* lo faccio ruotare e accedo all'elenco delle funzioni di firma.



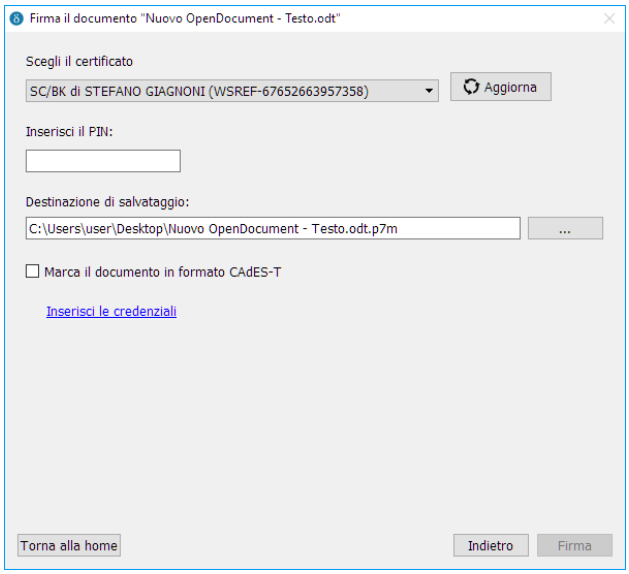
Poiché sto utilizzando Dike 6, ho a disposizione l'opzione *Firma* che mi permette di selezionare il documento da firmare e di richiamarlo all'interno del software.
Le opzioni *Firma multipla* e *Controfirma*, di colore grigio, sono disponibili nella versione PRO.
Dike 6 mi presenta gli estremi del documento (tipo, dimensione, ecc.) e, qualora lo ritenessi necessario, mi mette a disposizione il pulsante *Apri documento* per visualizzarlo.
Inoltre, Dike 6 evidenzia che sto per eseguire una firma che produrrà un documento con estensione **.p7m**, cioè a standard CAdES e mi fa procedere con un clic sul pulsante *Continua*.
(con questo formato si possono firmare qualsiasi file purchè sia nei formati consentiti per i documenti inseriti nell'applicativo di protocollo)



Prima di iniziare il processo di firma vero e proprio, Dike 6 verifica che io abbia a disposizione un certificato di sottoscrizione con il quale firmare.

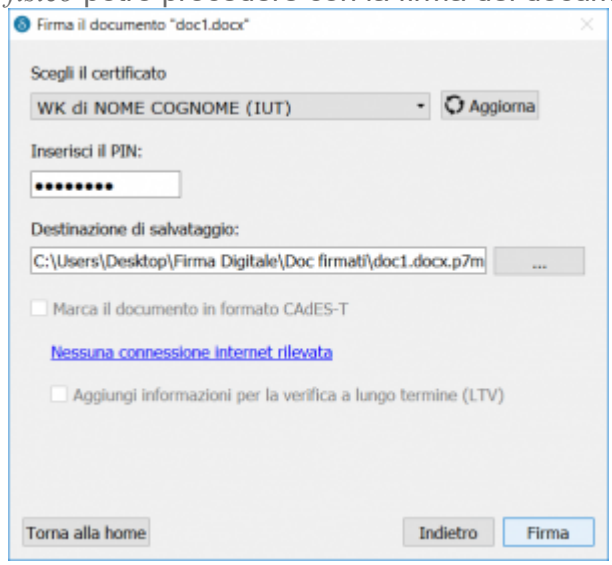


Un clic sul pulsante *Aggiorna* mi propone le possibili alternative collegate alla postazione di lavoro: noi usiamo solo smart card (CNS) però si potrebbero usare anche firme su supporti diversi (BusinessKey o una **Wireless Key**. Anche nel caso della **Wireless Key**).



Firma P7M con un certificato su dispositivo fisico

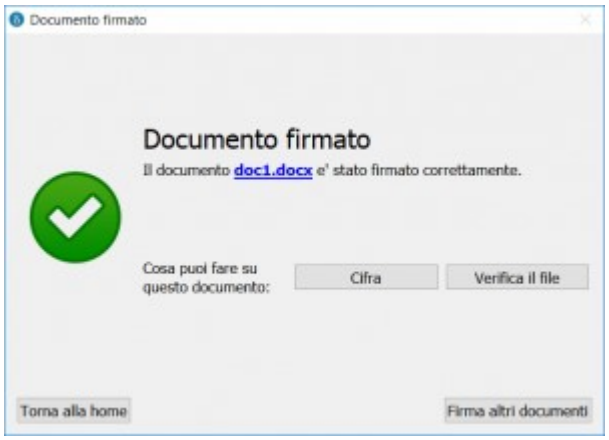
Dopo aver selezionato l'opzione *certificato di sottoscrizione supportato da un dispositivo fisico* potrò procedere con la firma del documento.



Inizierò a digitare il PIN di protezione della mio dispositivo fisico nel campo *Inserisci il PIN* proseguendo poi con l'indicazione della cartella all'interno della quale memorizzare il documento firmato.

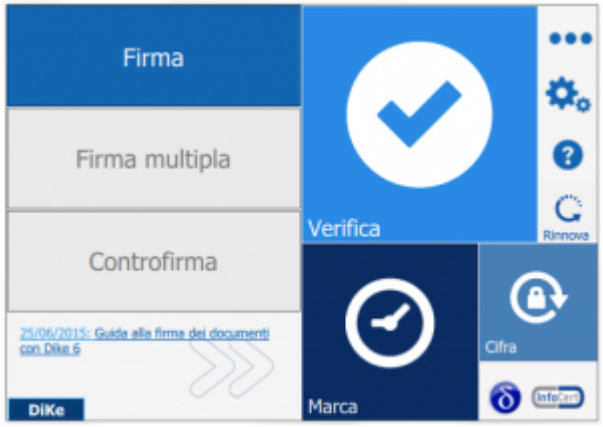
Dike 6 propone un possibile percorso nel campo *Destinazione di salvataggio*. Posso accettare quanto suggerito o apportare una modifica utilizzando il pulsante posto a fianco del campo.

Un clic sul pulsante *Firma* conclude il processo di sottoscrizione del documento; Dike 6 mi confermerà l'avvenuta firma con un messaggio.

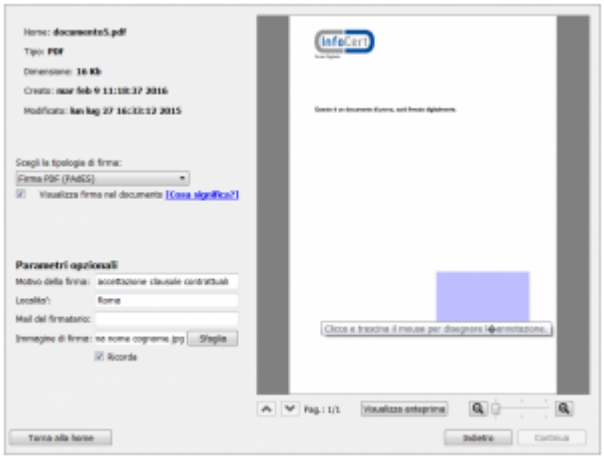

Documento firmato
Documento firmato
Il documento doc1.docx e' stato firmato correttamente.
Cosa puoi fare su questo documento:
Cifra
Verifica il file
Torna alla home
Firma altri documenti

FIRMA PDF DI UN DOCUMENTO

Passando il mouse sul riquadro *Firma* lo faccio ruotare e accedo all'elenco delle funzioni di firma.



Poiché sto utilizzando Dike 6, ho a disposizione l'opzione *Firma* che mi permette di selezionare il documento da firmare e di richiamarlo all'interno del software.
Le opzioni *Firma multipla* e *Controfirma*, di colore grigio, sono disponibili nella versione PRO.
Dike 6 mi presenta gli estremi del documento (tipo, dimensione, ecc.) nonché un riquadro di visualizzazione che lo contiene e che mi permette di scorrerlo, di ingrandirlo o di produrne un anteprima.
Dike 6 mi informa che il mio documento firmato manterrà l'estensione .pdf, cioè la firma sarà a standard PAdES.
Posso comunque firmare il documento in modalità CAdES ricorrendo all'opzione presente nel menu *Scegli la tipologia di firma*.
L'opzione *Visualizza firma nel documento* selezionata, mi segnala che la mia firma a standard PAdES sarà arricchita con un'annotazione grafica visibile, contenente gli estremi della firma stessa.
Qualora decidessi di eliminare l'annotazione grafica, otterrei comunque un documento con estensione .pdf firmato secondo lo standard PAdES, ma senza informazioni attinenti alla firma visibili sul documento.



I *Parametri opzionali*, infine, mi consentono di arricchire il processo di firma con informazioni riguardanti:

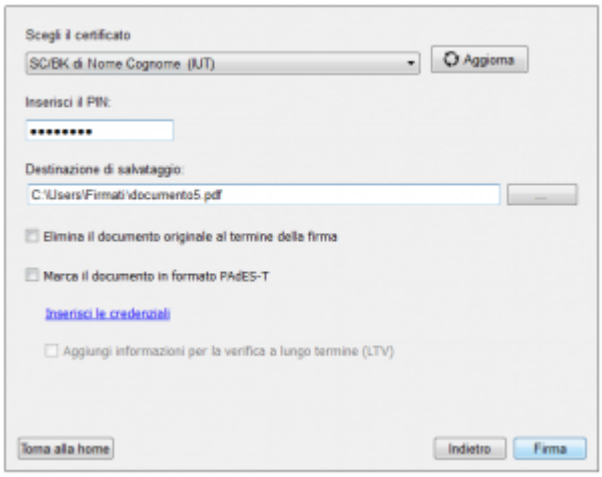
- il motivo per il quale sottoscriverò digitalmente il documento, ad esempio: accettazione delle clausole contrattuali, accettazione delle clausole vessatorie del contratto, espressione del mio consenso al trattamento dei dati personali ai sensi della L. 196/2003, ecc.;
- il luogo di apposizione della firma;
- un mio eventuale recapito e-mail;
- l'immagine della mia firma grafica, sempreché io l'abbia già scansionata e salvata come immagine nel mio computer. Il formato ammesso è il .jpg. E' molto importante tenere a mente che questo segno grafico **non ha alcun valore legale** e **non è** in alcun modo **la mia firma digitale**.

Trascinando il puntatore che mi appare sullo schermo, posso delimitare un'area di colore viola all'interno del documento. La scelta del suo posizionamento è lasciata all'iniziativa del firmatario: va da sé che se ho la necessità di firmare digitalmente un contratto, posizionerò l'area nella zona del documento in cui è prevista l'apposizione della firma del contraente.

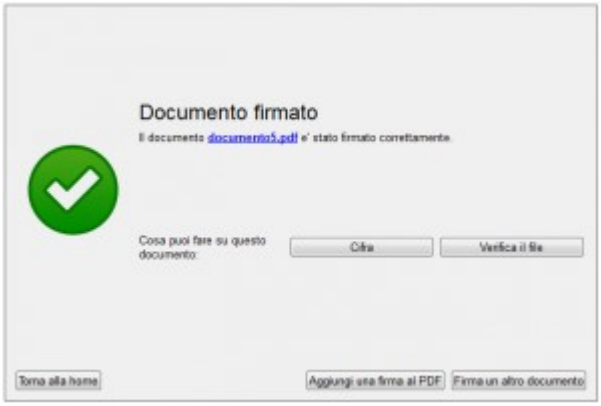
Procedo con un clic sul pulsante *Continua*.

Firma PDF con un certificato su dispositivo fisico

Dopo aver selezionato l'opzione *certificato di sottoscrizione supportato da un dispositivo fisico* potrò procedere con la firma del documento.



Inizierò a digitare il PIN di protezione della mio dispositivo fisico nel campo *Inserisci il PIN* proseguendo poi con l'indicazione della cartella all'interno della quale memorizzare il documento firmato.
Dike 6 propone un possibile percorso nel campo *Destinazione di salvataggio*. Posso accettare quanto suggerito o apportare una modifica utilizzando il pulsante posto a fianco del campo.
Un clic sul pulsante *Firma* conclude il processo di sottoscrizione del documento; Dike 6 mi confermerà l'avvenuta firma con un messaggio.



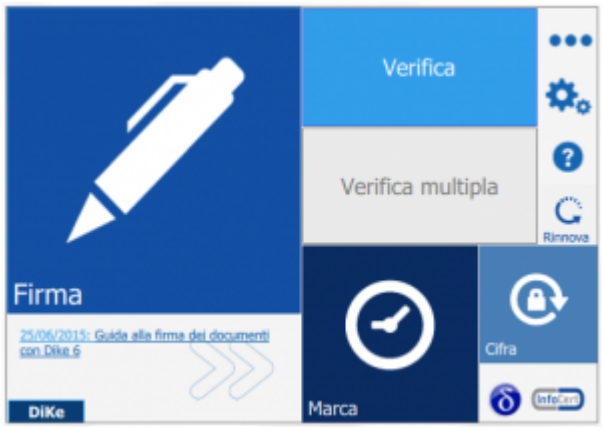
Un clic sul pulsante *Aggiungi una firma al PDF* mi permette di proseguire il processo di firma del documento, facendolo sottoscrivere da uno o più firmatari.

VERIFICA DELLA VALIDITÀ DI UN DOCUMENTO

La verifica di un documento firmato digitalmente e/o marcato è importante tanto quanto lo è l'attività di firma e di marcatura temporale.

La validità dei documenti firmati

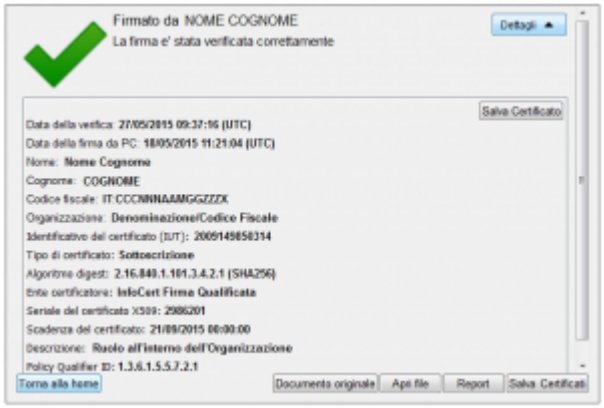
Passando il mouse sul riquadro *Verifica* lo faccio ruotare e accedo all'elenco delle funzioni di verifica.



Poiché sto utilizzando Dike 6, ho a disposizione l'opzione *Verifica* che mi permette di selezionare il documento da verifica e di richiamarlo all'interno del software.
L'opzione *Verifica multipla*, di colore grigio, è disponibile nella versione PRO.

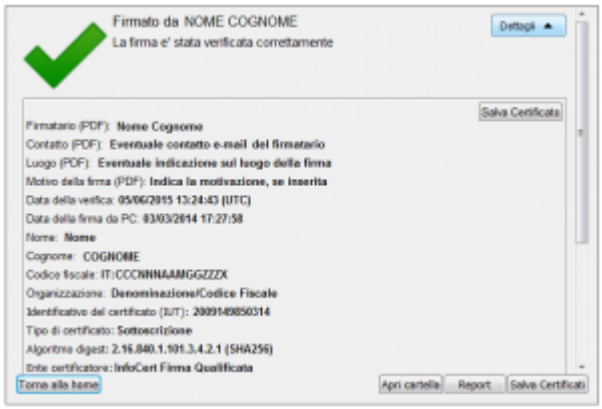
La risposta di Dike 6 è diretta e consiste in una sintesi dell'esito di verifica.

Un clic sul pulsante *Dettagli* mi permette di ottenere maggiori informazioni sulla firma (standard CAdES), sul firmatario e sul certificato utilizzato per firmare.
Tra le informazioni di dettaglio è presente anche la data di aggiornamento della *lista CRL*, ovvero la lista che fornisce informazioni sui certificati revocati, sospesi o scaduti.



Se ho selezionato un documento firmato in modalità PDF (standard PAdES), l'esito della verifica produrrà una sintesi identica alla precedente.

Un clic sul pulsante *Dettagli* mi permette di ottenere maggiori informazioni sulla firma, sul firmatario e sul certificato utilizzato per firmare nonché sui particolari della firma PDF: motivo, luogo della firma, eventuale contatto del firmatario.



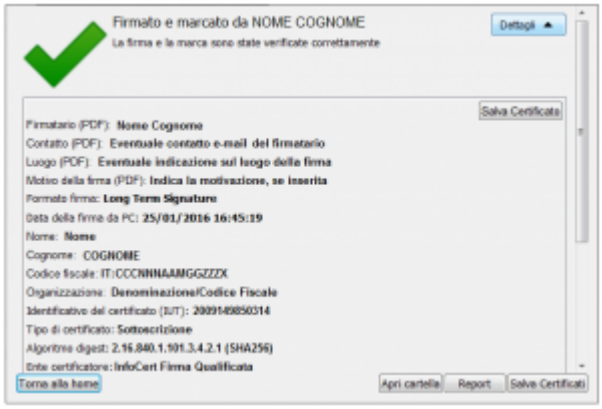
La validità dei documenti firmati e marcati

Un clic sull'opzione *Verifica* mi permette di selezionare il documento, scegliendolo tra quelli disponibili sul mio computer, su un server o un hard disk, ecc.
La risposta di Dike 6 è diretta e consiste in una sintesi dell'esito di verifica.

Un clic sul pulsante *Dettagli* mi permette di ottenere maggiori informazioni sulla firma, sul firmatario e sul certificato utilizzato per firmare (standard CAdES). Subito dopo, troverò le informazioni di dettaglio sulla marca temporale apposta.
Se ho selezionato un documento firmato in modalità PDF (standard PAdES), l'esito della verifica produrrà una sintesi identica alla precedente.

Anche in questo caso, un clic sul pulsante *Dettagli* mi permette di ottenere maggiori informazioni sulla firma, sul firmatario e sul certificato utilizzato per firmare nonché sui particolari della firma PDF: motivo, luogo della firma, eventuale contatto del firmatario. Di seguito le informazioni di dettaglio sulla marca temporale apposta.
Dike 6 permette di verificare la **validità** dei documenti con **firma LTV**, indipendentemente dallo standard della firma apposta ai documenti (CAdES o PAdES).
Dopo aver selezionato il documento ricevo una risposta che è diretta e consiste in una sintesi dell'esito di verifica.

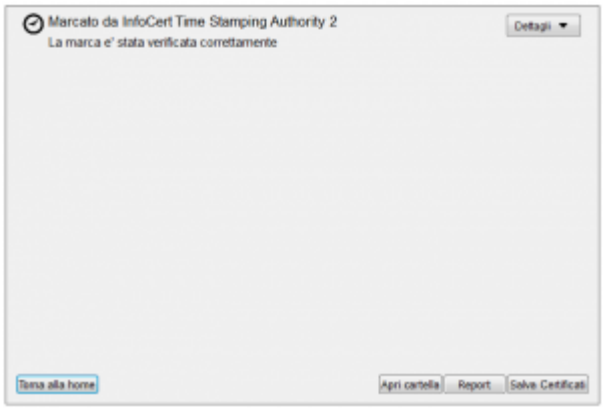
Un clic sul pulsante *Dettagli* mi permette di ottenere maggiori informazioni sulla firma, sul firmatario e sul certificato utilizzato per firmare nonché sul *Formato firma* che risulterà essere **Long Term Signature** indipendentemente dallo standard della firma apposta ai documenti (CAdES o PAdES).



Dike 6 PRO consente la verifica dei documenti ai quali la marca temporale è stata apposta successivamente alla firma digitale (documento con estensione .tsd).
Un caso particolare è rappresentato dai documenti marcati in formato *MIME*(documento con estensione .m7m). Si tratta di documenti che riuniscono al loro interno il documento elettronico firmato e la relativa marca temporale che in effetti ha estensione .tsr.
E' per questo motivo che, in fase di verifica, non è necessario selezionare il file da associare alla marca temporale.

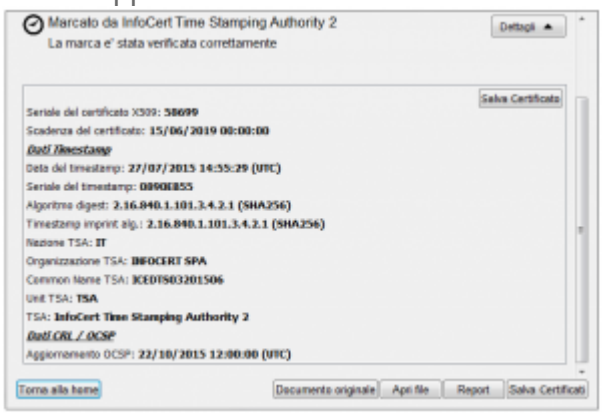
La validità dei documenti marcati temporalmente (attualmente in azienda non si utilizzano le marcature temporali ma può capitare di ricevere documenti firmati digitalmente e con marcatura temporale)

Un clic sull'opzione *Verifica* mi permette di selezionare il documento, scegliendolo tra quelli disponibili sul mio computer, su un server o un hard disk, ecc.
La risposta di Dike 6 è diretta e consiste in una sintesi dell'esito di verifica.
La marca temporale apposta ad un documento non firmato presenta questo esito di verifica:



La marca temporale apposta ad un documento precedentemente firmato presenta questo esito di verifica:

Un clic sul pulsante *Dettagli* posto a fianco delle informazioni sulla Time Stamping Authority che ha apposto la marcatura temporale mi permette di ottenere maggiori informazioni sulla marca apposta.



Dike 6 mi permette di verificare anche i documenti caratterizzati da una marca temporale apposta in modalità *detached* (documento con estensione .tsr), permettendomi di eseguire la verifica della sola marca temporale o di associarla al documento informatico cui era stata apposta e passare successivamente alla verifica.
Un caso particolare è rappresentato dai documenti marcati in formato *MIME*(documento con estensione .m7m). Si tratta di documenti che riuniscono al loro interno il documento elettronico e la relativa marca temporale che in effetti ha estensione .tsr.

E’ per questo motivo che, in fase di verifica, non è necessario selezionare il file da associare alla marca temporale.