BANCA D'ITALIA

EUROSISTEMA

MANUALE DI UTILIZZO DEL SOFTWARE DI FIRMA E CIFRA "FILE PROTECTOR"

Novembre 2011

Sommario

Introduzione

Il **File Protector** è un software che consente di utilizzare i certificati elettronici per:

- Firmare un documento;
- Cifrare un documento;
- Firmare e cifrare un documento;
- Verificare la validità della firma con cui è stato sottoscritto un documento;
- Decifrare un documento cifrato;
- Decifrare un documento firmato e cifrato e verificare la validità della firma con cui esso è stato sottoscritto;
- Apporre marche temporali;
- Firmare , cifrare e decifrare una intera cartella di files.

Alcune operazioni, quali la firma di un documento o la decifratura di un documento crittografato, richiedono che l'utente disponga di un certificato elettronico residente su smart card oppure su file in formato PKCS#11. Per svolgere altre operazioni, quali la cifratura di un documento, occorre invece disporre dei certificati elettronici con la chiave pubblica dei destinatari.
Tali certificati possono risiedere su un archivio locale del PC su cui è installato il File Protector ppure essere disponibili su un server LDAP raggiungibile attraverso la rete.

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**, oppure su un **token USB** (in entrambi i casi si tratta di microchip con funzionalità crittografiche):

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. Banca d'Italia)
- 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.

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 decifrare 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:

Firmare un file

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:

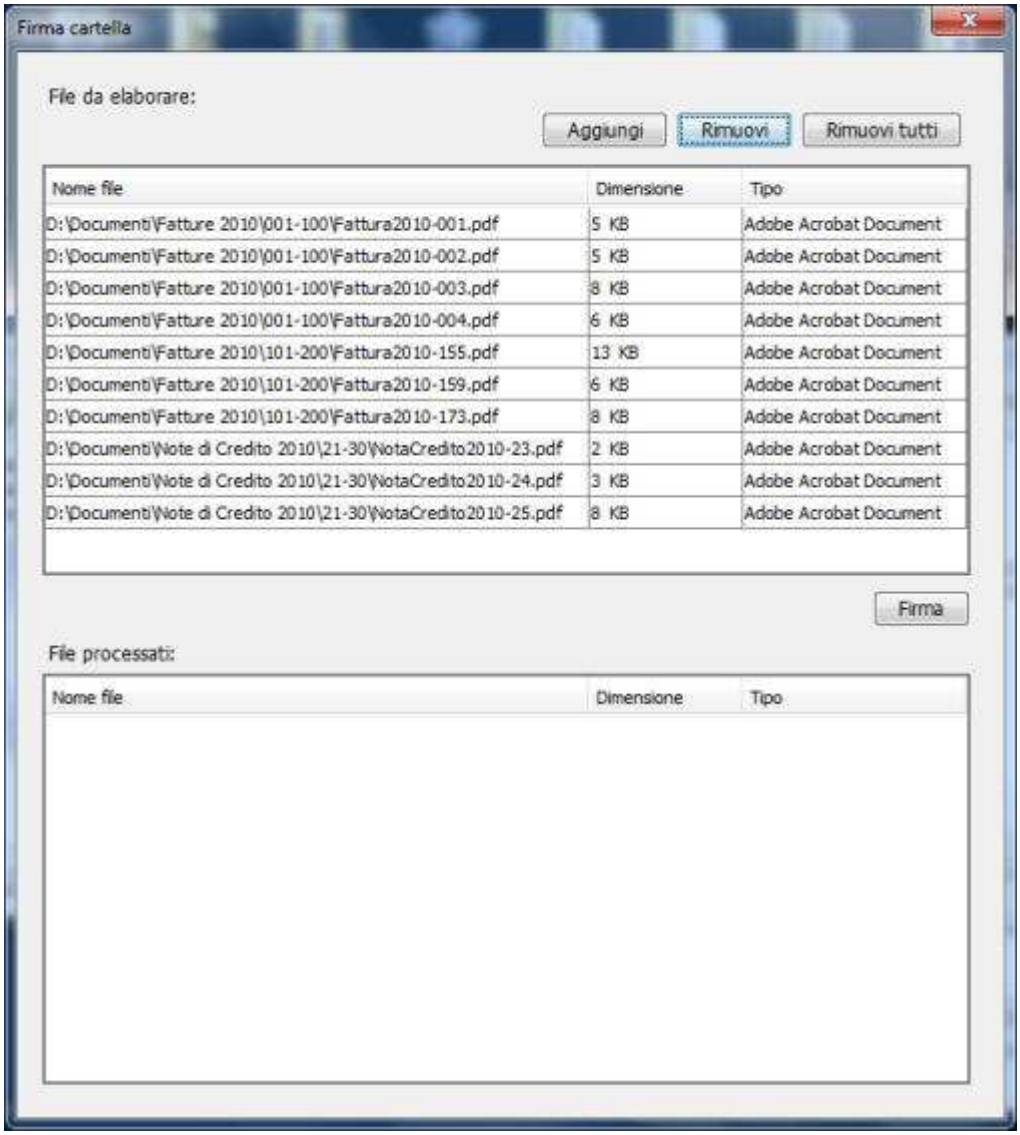
- selezionare la voce "**Firma**" dal menu "**File**"
- oppure cliccare sul bottone "**Firma**" della toolbar

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

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

Firma in unica soluzione

Selezionando la voce di menu "**Firma in unica soluzione**" (oppure cliccando sul bottone corrispondente) appare una finestra di dialogo che permette di firmare "in un'unica soluzione" un insieme qualsiasi di file, anche residenti in cartelle diverse:

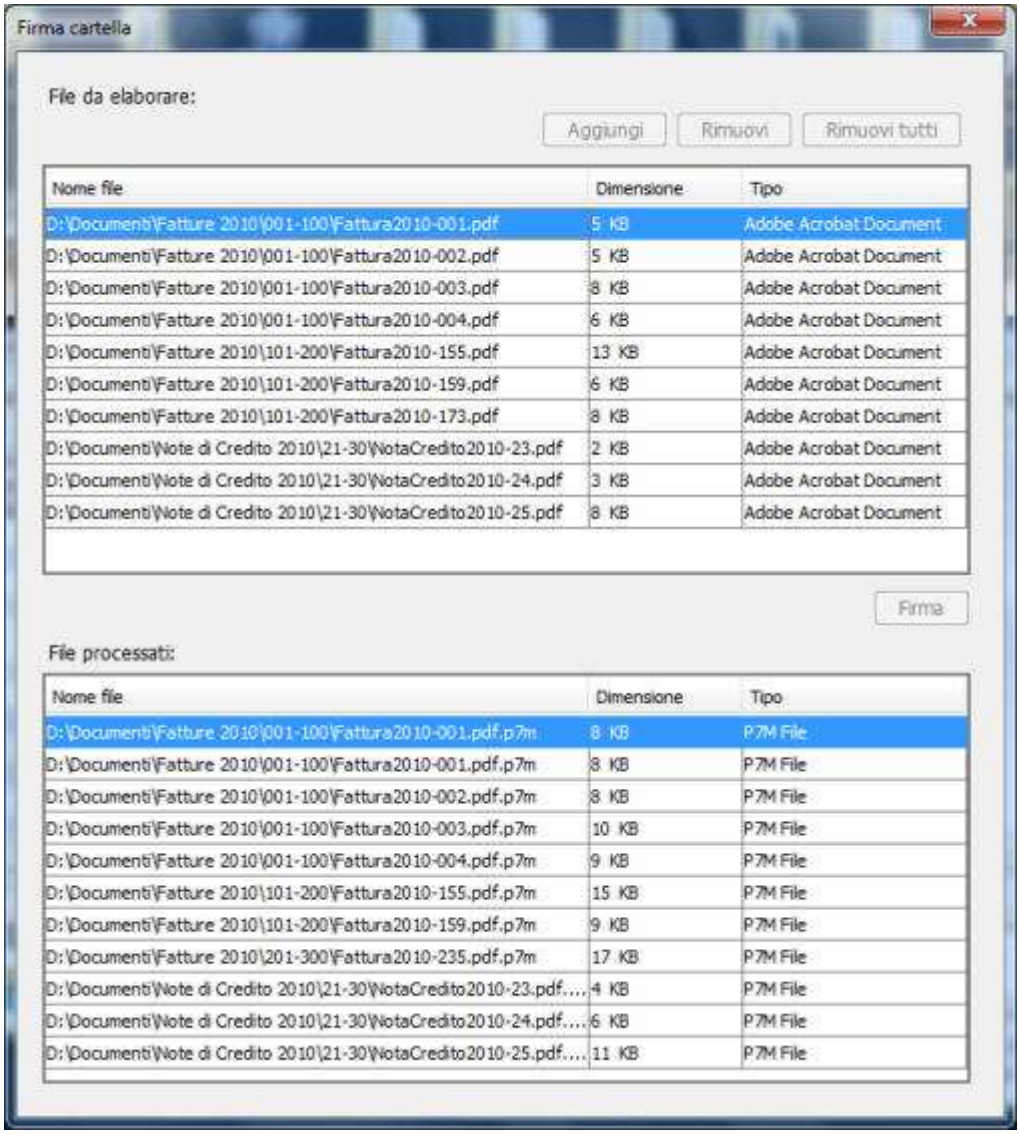


La parte superiore della finestra ("basket") elenca i file che verranno firmati. L'elenco può essere compilato sia cliccando sul bottone "**Aggiungi**" e selezionando un file, sia *trascinando* l'icona del file desiderato sull'elenco stesso (drag and drop). Possono essere aggiunti al basket anche file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

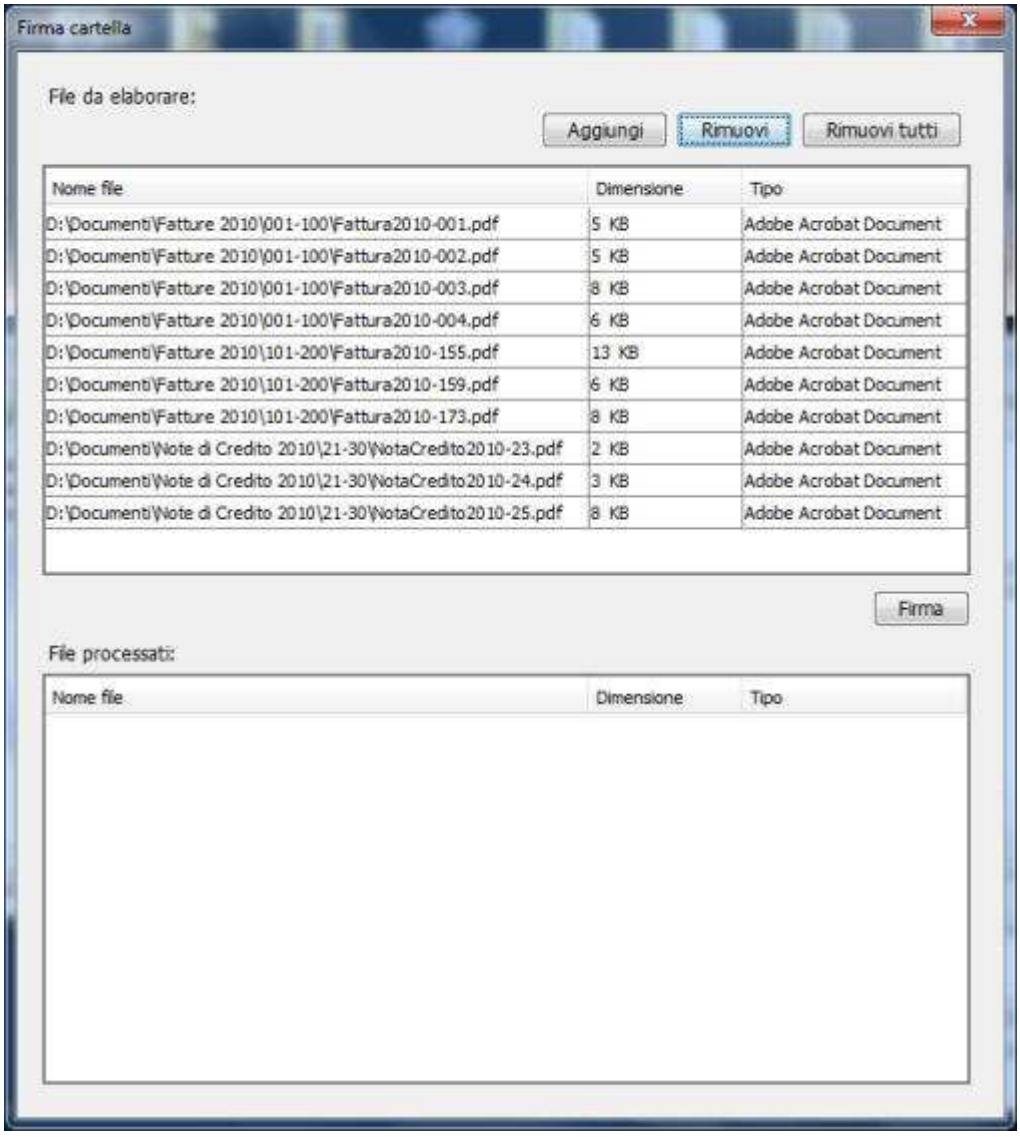
Cliccando infine sul bottone "**Firma**", verrà avviato il processo di firma digitale (in formato P7M) di tutti i file dell'elenco. Le buste P7M risultanti, elencate nella parte inferiore della finestra, vengono salvate nella stessa cartella del documento di origine:



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

Firma in unica soluzione XML

Selezionando la voce di menu "**Firma in unica soluzione XML**" (oppure cliccando sul bottone corrispondente) appare una finestra di dialogo che permette di firmare "in un'unica soluzione" un insieme qualsiasi di file, anche residenti in cartelle diverse:

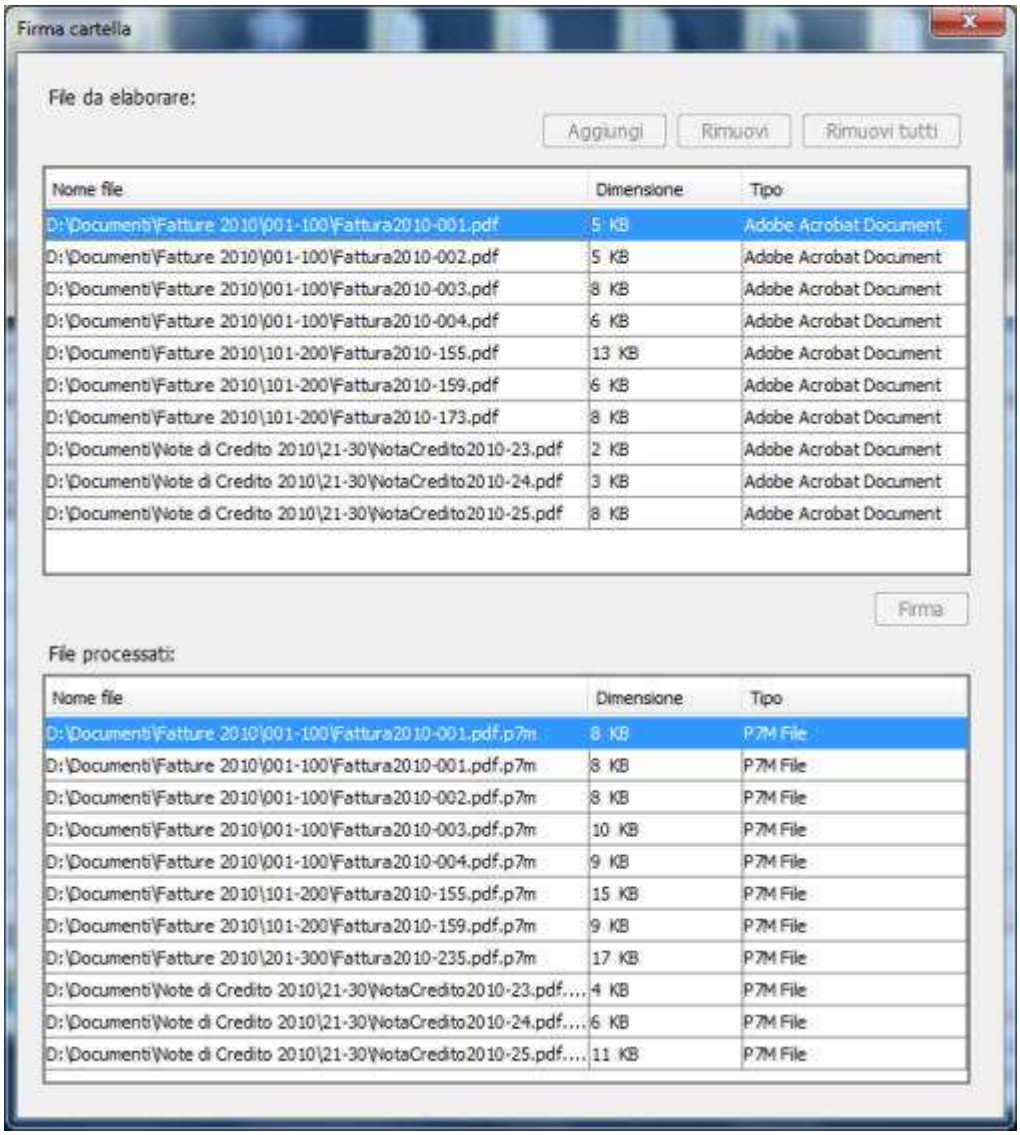


La parte superiore della finestra ("basket") elenca i file che verranno firmati. L'elenco può essere compilato sia cliccando sul bottone "**Aggiungi**" e selezionando un file, sia *trascinando* l'icona del file desiderato sull'elenco stesso (drag and drop). Possono essere aggiunti al basket anche file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

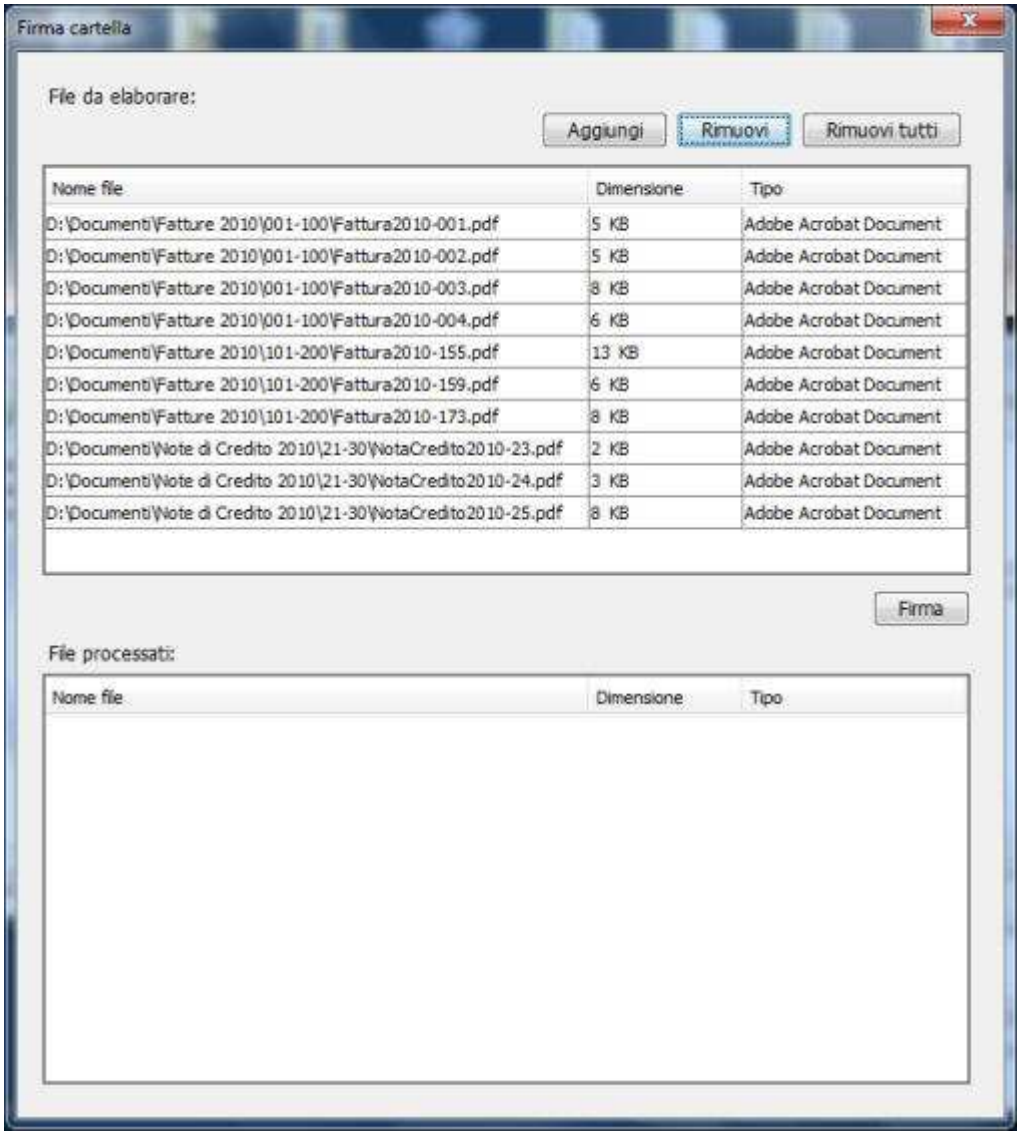
Cliccando infine sul bottone "**Firma**", verrà avviato il processo di firma digitale (in formato P7M) di tutti i file dell'elenco. Le buste P7M risultanti, elencate nella parte inferiore della finestra, vengono salvate nella stessa cartella del documento di origine:



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

Firma in unica soluzione PDF

Selezionando la voce di menu "**Firma in unica soluzione PDF**" (oppure cliccando sul bottone corrispondente) appare una finestra di dialogo che permette di firmare "in un'unica soluzione" un insieme qualsiasi di file con estensione PDF, anche residenti in cartelle diverse:

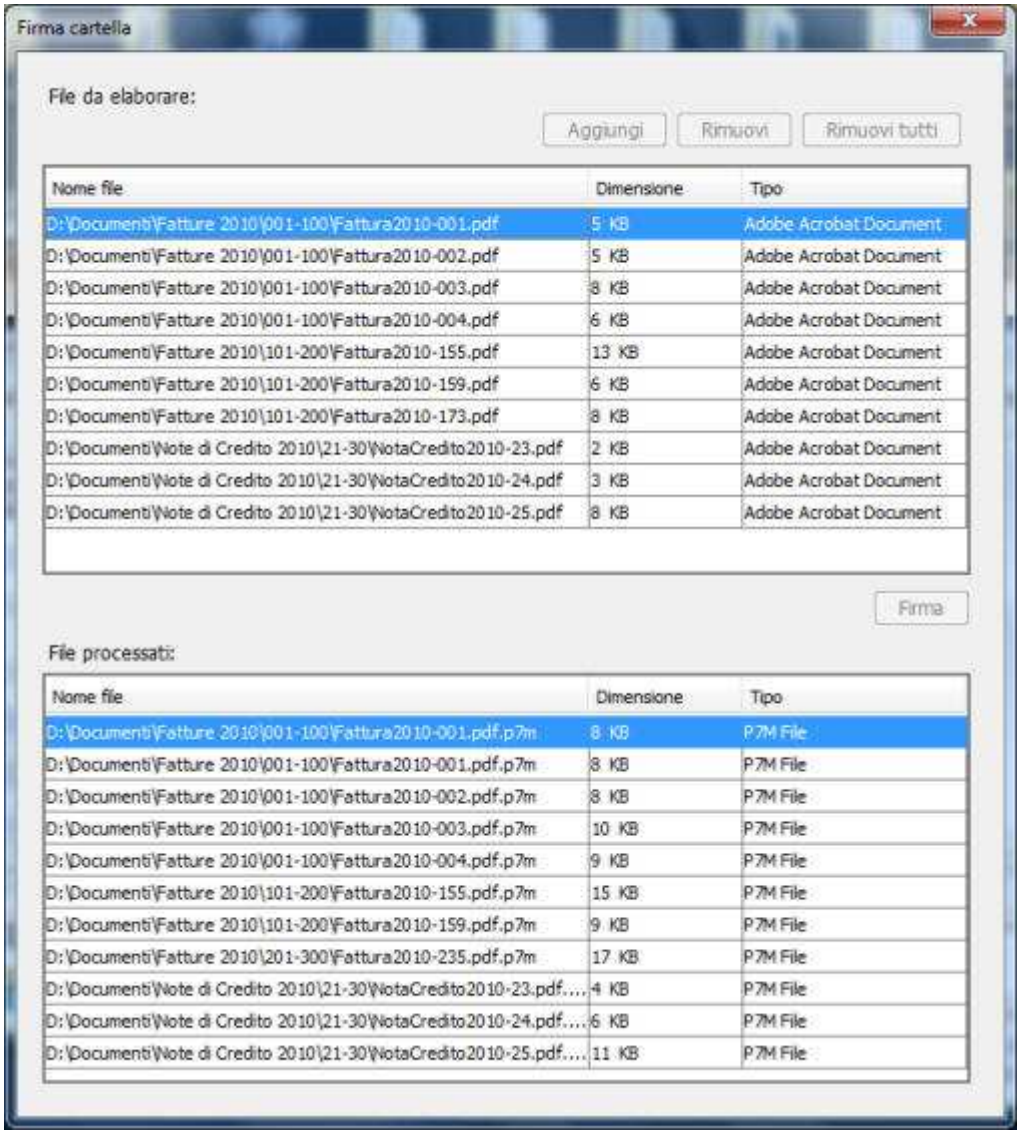


La parte superiore della finestra ("basket") elenca i file che verranno firmati. L'elenco può essere compilato sia cliccando sul bottone "**Aggiungi**" e selezionando un file, sia *trascinando* l'icona del file desiderato sull'elenco stesso (drag and drop). Possono essere aggiunti al basket anche file 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 ESC oppure cliccare sull'icona di chiusura.

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:

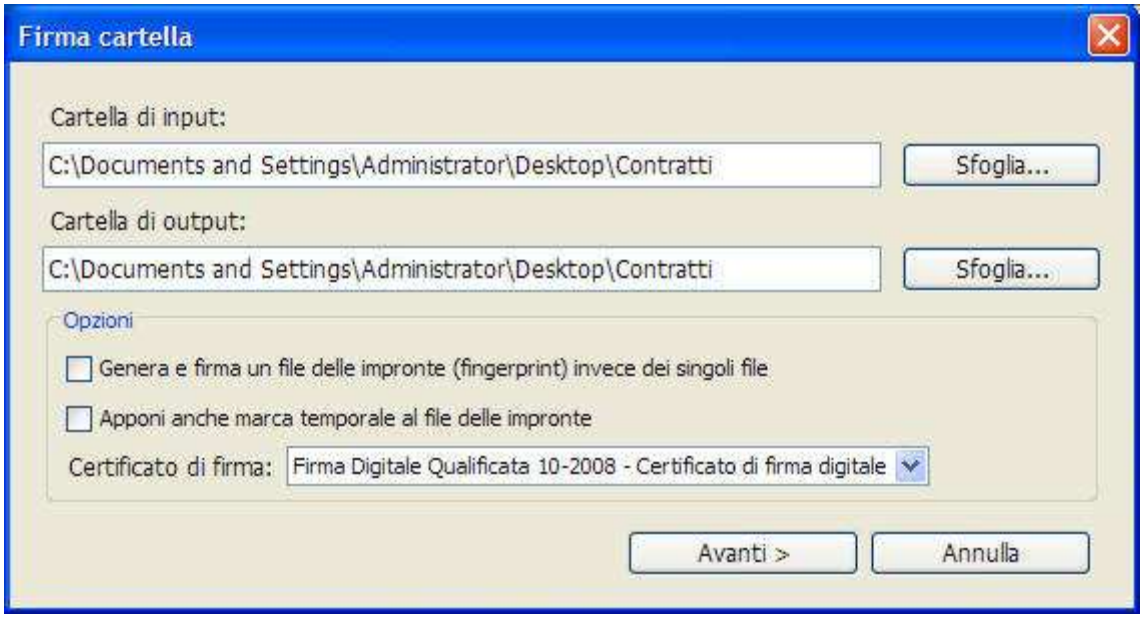
- dall'esterno dell'applicazione, attraverso il menu contestuale di Windows Explorer
- dall'esterno dell'applicazione, mediante "drag-and-drop"
- dall'interno di File Protector

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.

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)

File Protector è sempre in grado di produrre una firma PDF "invisibile", mentre per produrre una firma visibile è necessario che il documento PDF contenga un **campo firma** approsimatamente predisposto. Ad ogni firma apposta al documento corrisponde una "revisione" del documento stesso.

Le firme PDF si differenziano poi in:

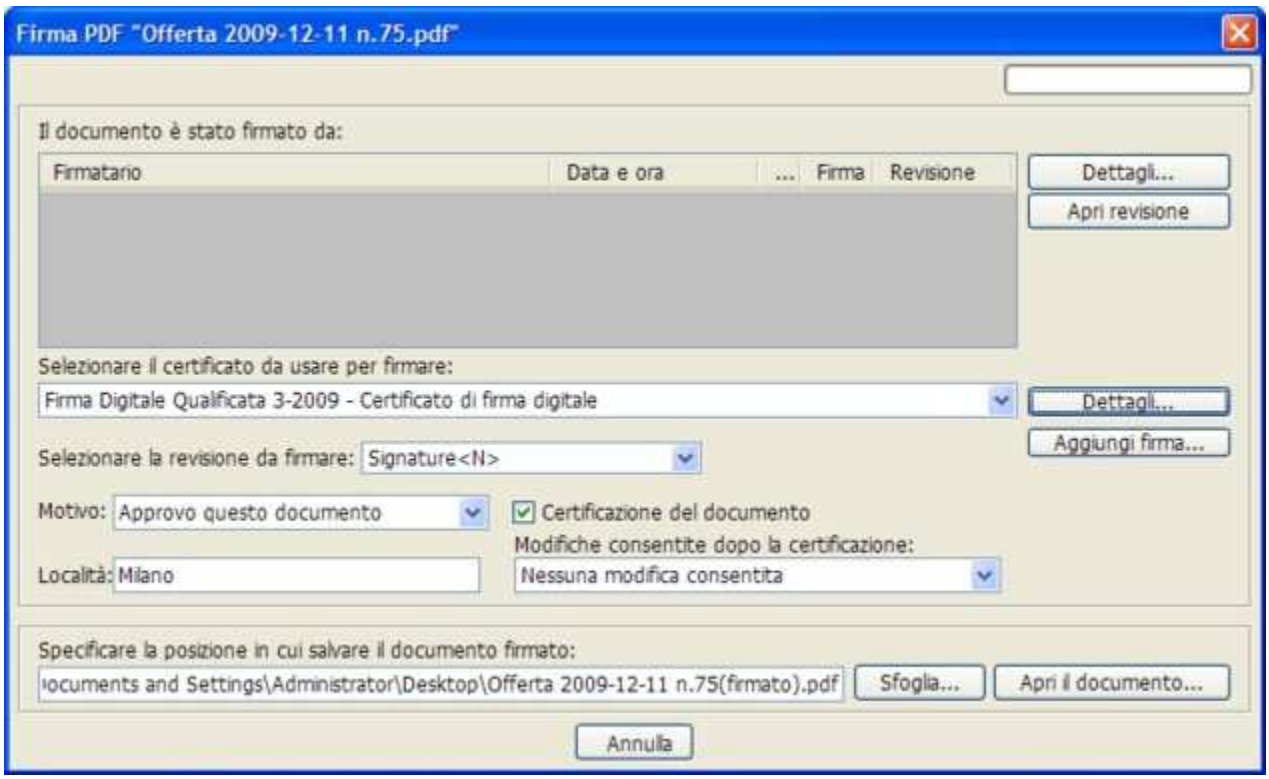
- firma di *certificazione*
- firme di *approvazione*

La "firma di approvazione" è quella che generalmente si appone su un documento prodotto da altri e non ha altri effetti se non quello di attestare l'identità del firmatario e l'integrità del documento.

La "firma di certificazione", invece, consente anche di impostare permessi sul documento che limitano le successive modifiche. Solitamente, chi appone una firma di certificazione è l'autore o responsabile del documento. Inoltre, una firma di certificazione viene *sempre evidenziata* dalle applicazioni Adobe, anche se non apposta in un campo firma.

Entrambi i tipi di firma sono supportati da File Protector.

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:



Volendo apporre una firma di certificazione, selezionare la casella corrispondente e scegliere dal menu a discesa i permessi desiderati.

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

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

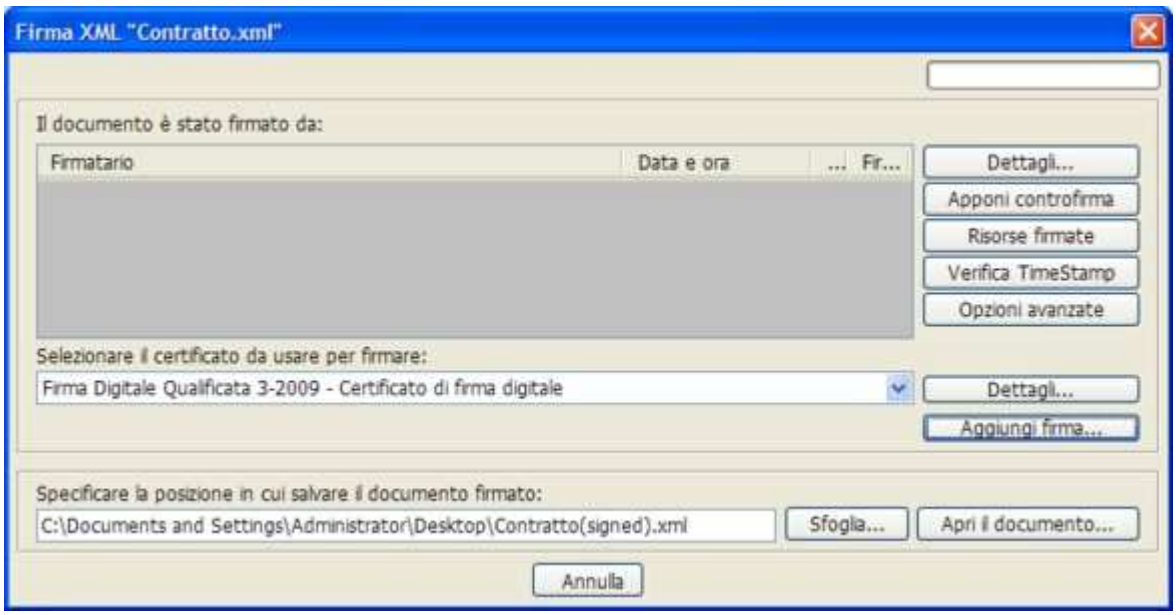
Firmare in modalità XML

In alternativa ai formati P7M e PDF, la firma digitale può anche avere una codifica di tipo XML (eXtended Markup Language). La firma in modalità XML è particolarmente adatta ai documenti che sono essi stessi in formato XML, ma può essere applicata a documenti di qualsiasi tipo.

La firma in standard XML non è ancora molto diffusa, essendo usata prevalentemente nell'ambito sanitario e bancario; tuttavia, la firma XML ha lo stesso valore tecnico e legale degli altri formati (P7M e PDF).

Rispetto alla firma P7M, la firma in modalità XML è più flessibile ma anche più "tecnica": può infatti assumere tre diverse forme (*enveloped*, *enveloping*, *detached*) e prevede numerose opzioni che in questa guida, per brevità, non approfondiamo. Per ulteriori dettagli si rimanda al Manuale Utente. Lo standard tecnico di riferimento è scaricabile dal seguente link.

Per firmare un documento in modalità XML, selezionare la voce "**Firma XML**" dal menu "**File**"; dopo aver selezionato il documento desiderato, apparirà la seguente finestra di dialogo:



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).

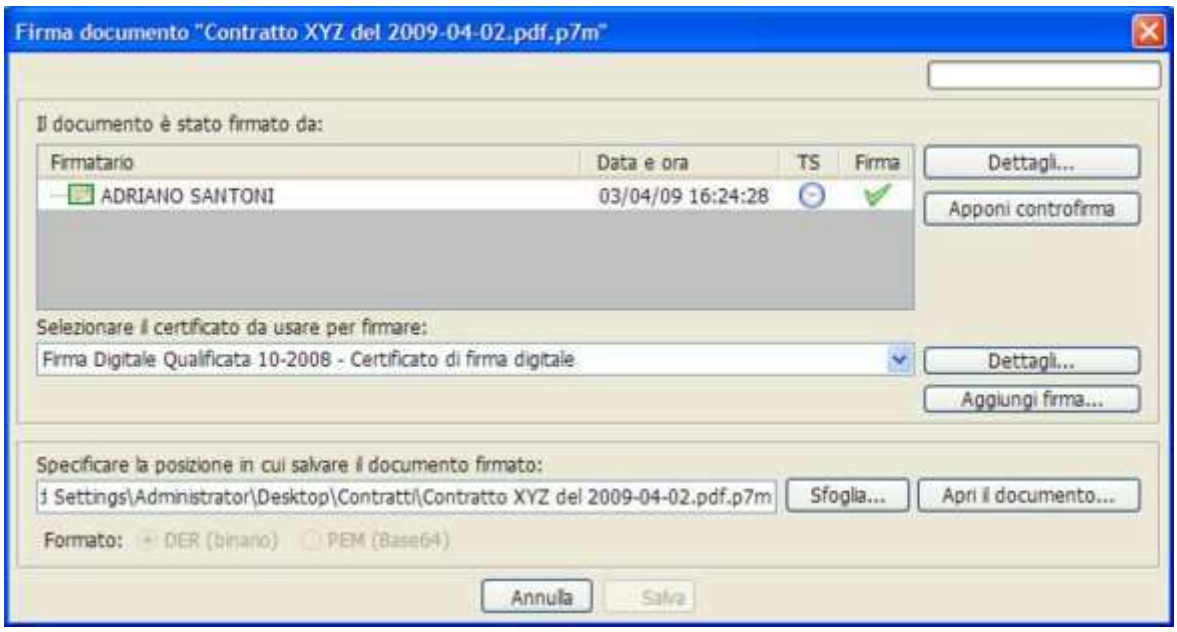
Esistono tre tipologie di firme multiple:

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

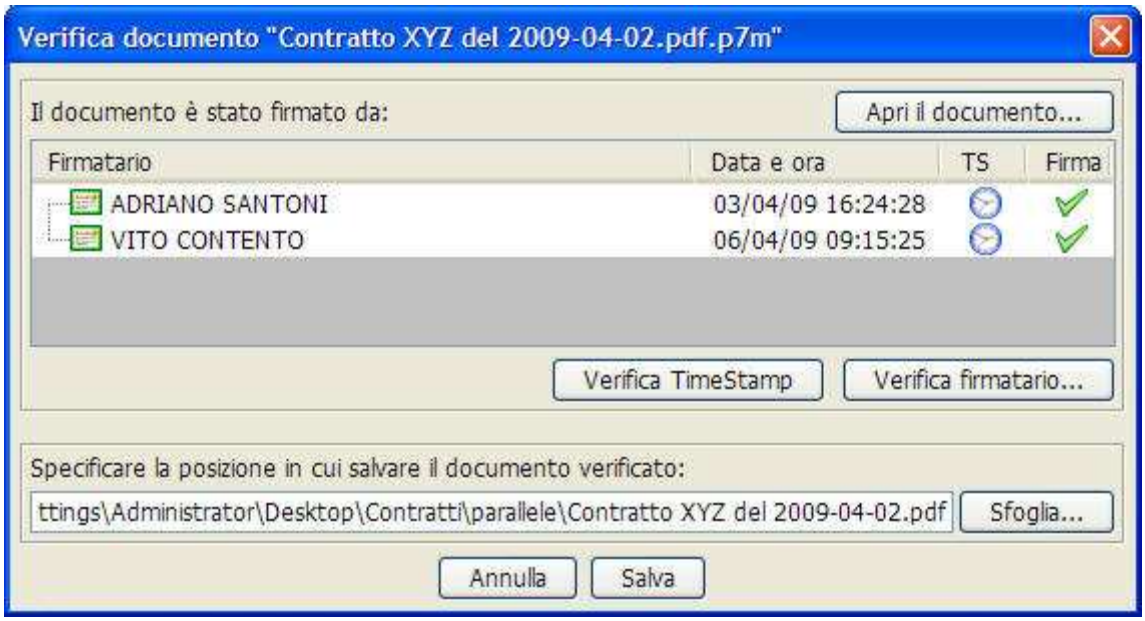
Il primo tipo si ottiene semplicemente firmando una busta crittografica P7M (che contiene un documento già firmato). Questa operazione digitale equivale, nel mondo della carta, a firmare una busta che contiene un documento firmato, ciò che in effetti a volte viene fatto (si pensi alle buste che contengono 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**".

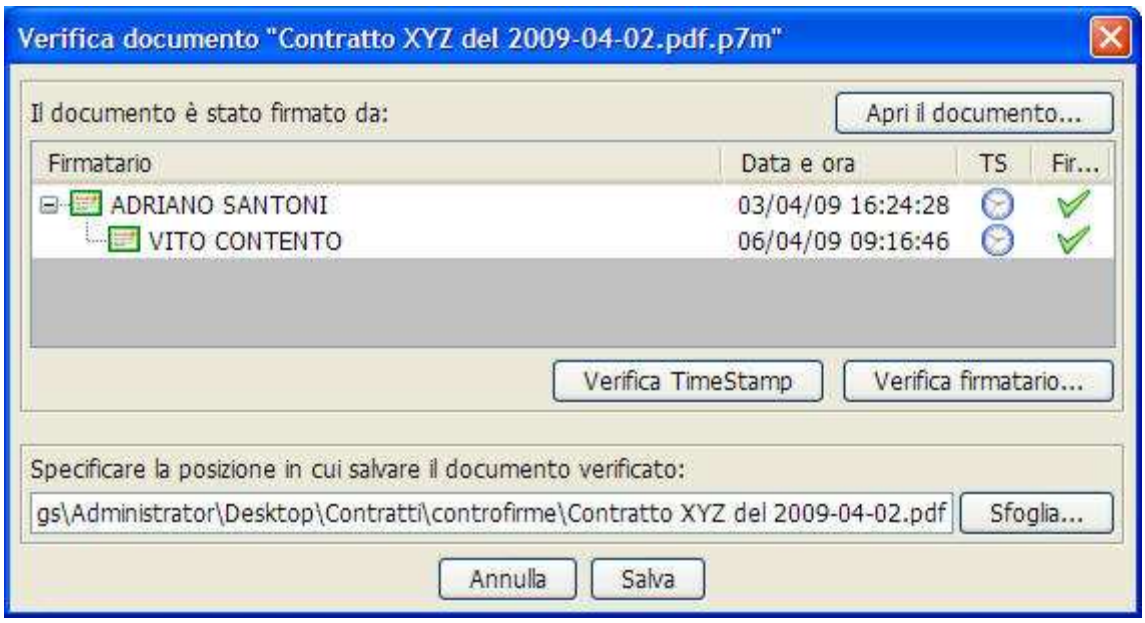
Selezionando invece la voce "**Firma interna**", sarà possibile eseguire firme multiple del secondo e del terzo tipo; apparirà a questo punto la seguente finestra di dialogo:



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):


Verifica documento "Contratto XYZ del 2009-04-02.pdf.p7m"
Il documento è stato firmato da:
Apri il documento...
Firmatario
Data e ora
TS
Fir...
ADRIANO SANTONI
03/04/09 16:24:28
VITO CONTENTO
06/04/09 09:16:46
Verifica TimeStamp
Verifica firmatario...
Specificare la posizione in cui salvare il documento verificato:
gs\Administrator\Desktop\Contratti\controfirme\Contratto XYZ del 2009-04-02.pdf
Sfoglia...
Annulla
Salva

Cifrare (crittografare) un file

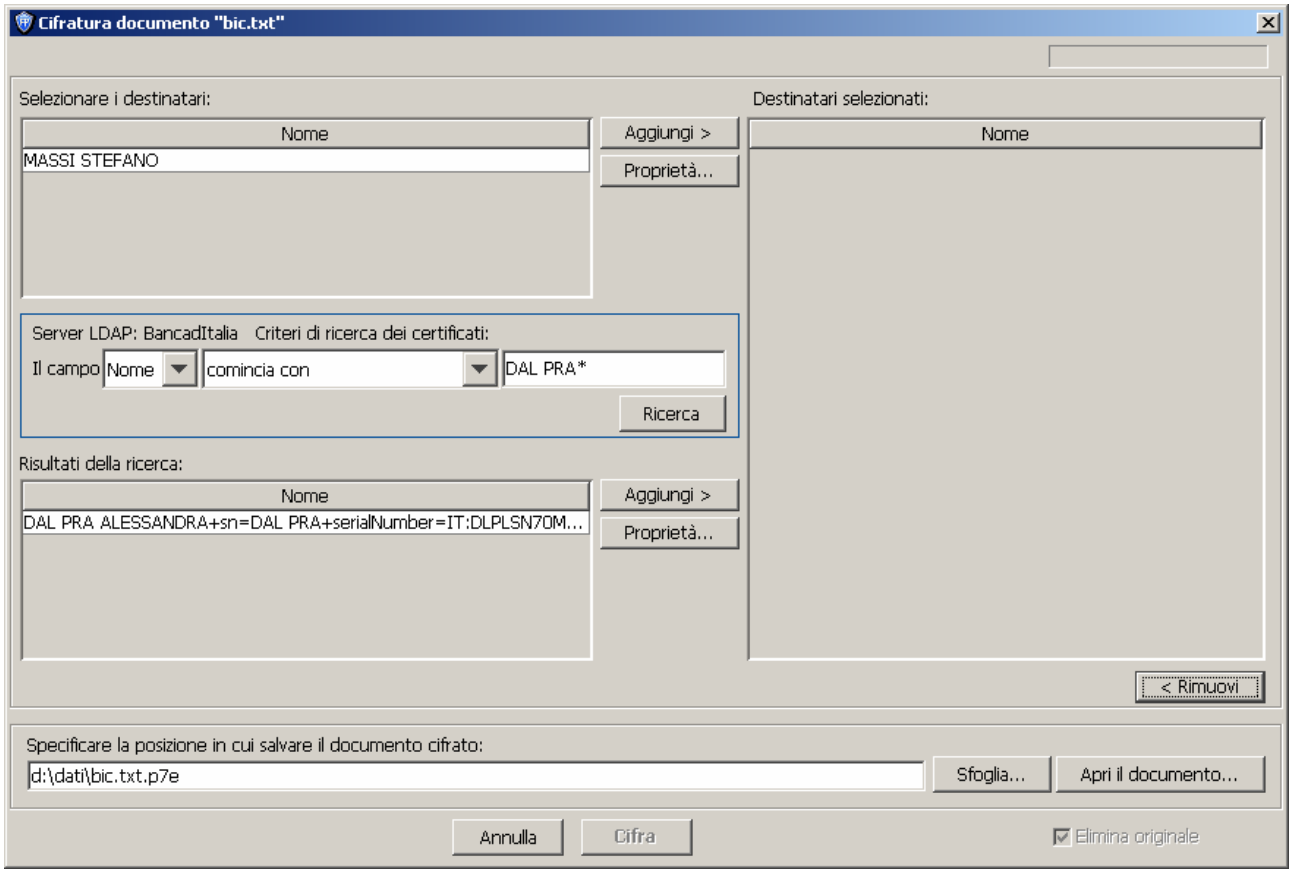
Ricordiamo anzitutto che per cifrare un documento è necessario possedere il certificato di cifratura del destinatario (ossia dell'utente che vogliamo sia l'unico a poter decifrare il documento).

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. Altrimenti, si può richiedere il certificato al destinatario e poi importarlo manualmente nel proprio database di certificati. In tal modo, quel certificato sarà sempre a disposizione nelle successive operazioni di cifratura anche in temporanea assenza di connettività LDAP.

In ogni caso, i certificati pubblicati su directory server possono essere reperiti ed utilizzati per la cifratura anche in modo dinamico (senza necessità di importarli nel proprio database), come descritto di seguito.

È possibile cifrare un documento per più utenti contemporaneamente, 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:



È possibile aggiungere alla busta cifrata:

- sia i destinatari presenti nel proprio **database personale** (parte superiore sinistra della finestra),

- sia quelli **reperibili sul server LDAP** prescelto (parte intermedia sinistra della finestra); il server LDAP di default è quello della Banca d'Italia.

Selezionando la casella "**Elimina originale**", il file di partenza (in chiaro) sarà automaticamente eliminato. In tal caso, il certificato dell'utente corrente sarò automaticamente incluso nell'elenco dei destinatari per evitare di perder la possibilità di accedere al documento originale (è dunque indispensabile che l'utente corrente disponga di un certificato di cifratura sul proprio dispositivo).

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

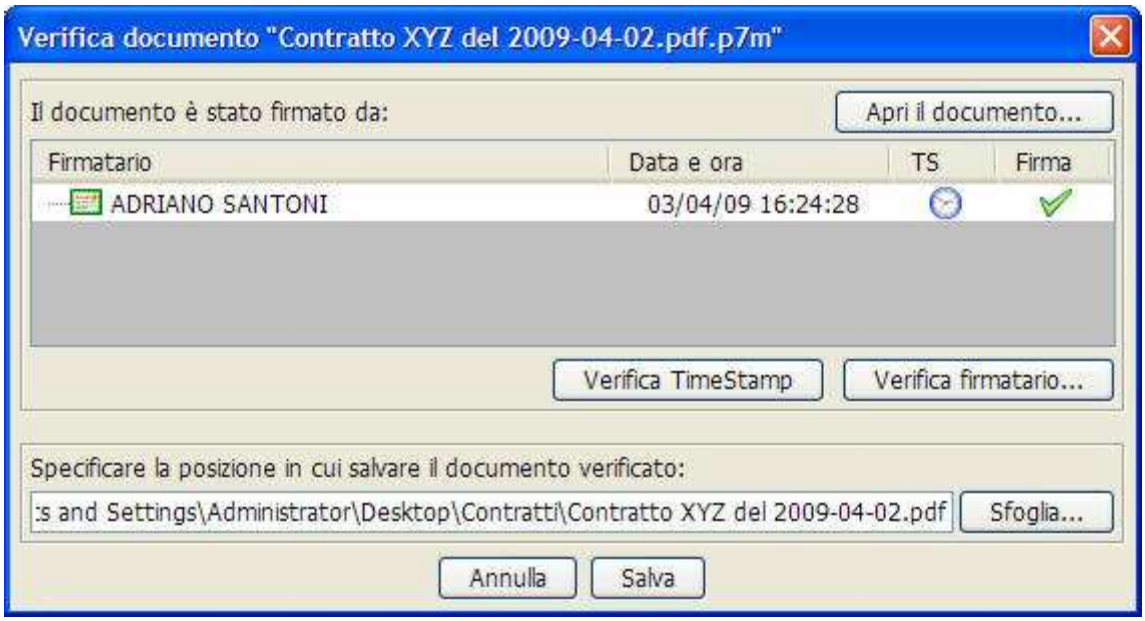
La firma digitale e la cifratura possono essere applicate in modo combinato ad un medesimo documento, in modo da assicurarne sia l'origine (ed integrità) sia la segretezza. Per fare questo, cliccare sul bottone "**Firma e Cifra**" nella finestra principale di File Protector, oppure selezionare la voce corrispondente dal menu "File".

Verificare e/o decifrare

La verifica di un documento firmato in standard P7M si può avviare in cinque 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:



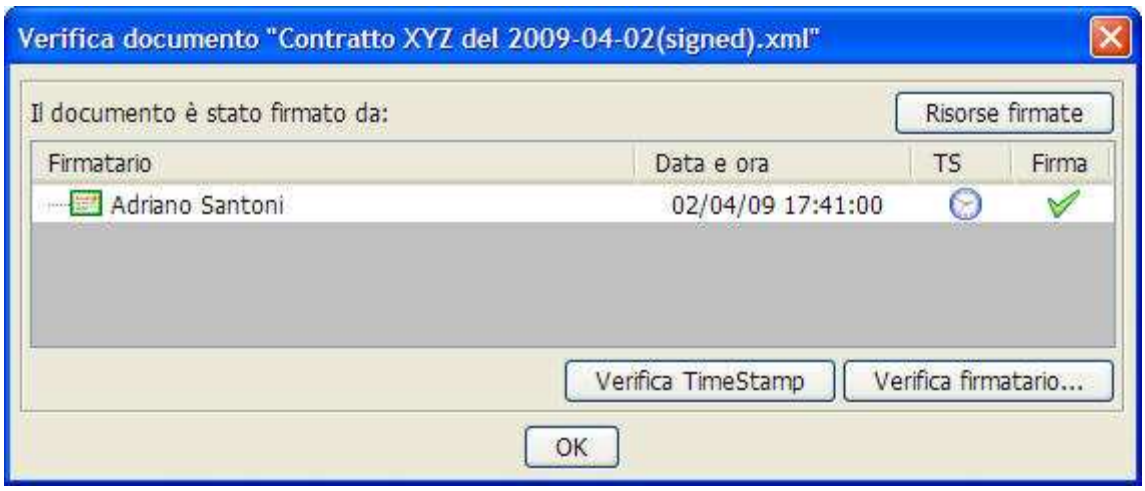
Da questa finestra è possibile:

- verificare la validità della firma
- verificare la validità del certificato di ogni firmatario
- visualizzare il documento fimato, estrarlo e salvarlo su file
- visualizzare e verificare la marca temporale (se presente) associata alla firma

La verifica di un documento firmato in standard XML si può avviare in due modi diversi:

- dall'esterno dell'applicazione, attraverso il menu contestuale di Windows Explorer (come sopra)
- dall'interno di File Protector (come sopra)

Al termine della verifica, apparirà la seguente finestra:



Da questa finestra è possibile:

- verificare la validità della firma
- verificare la validità del certificato di ogni firmatario
- visualizzare l'elenco delle risorse fimate ed eventualmente salvarle su file
- visualizzare e verificare la marca temporale (se presente) associata alla firma

Nel caso di un documento firmato in standard PDF, si procede esattamente allo stesso modo.

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":

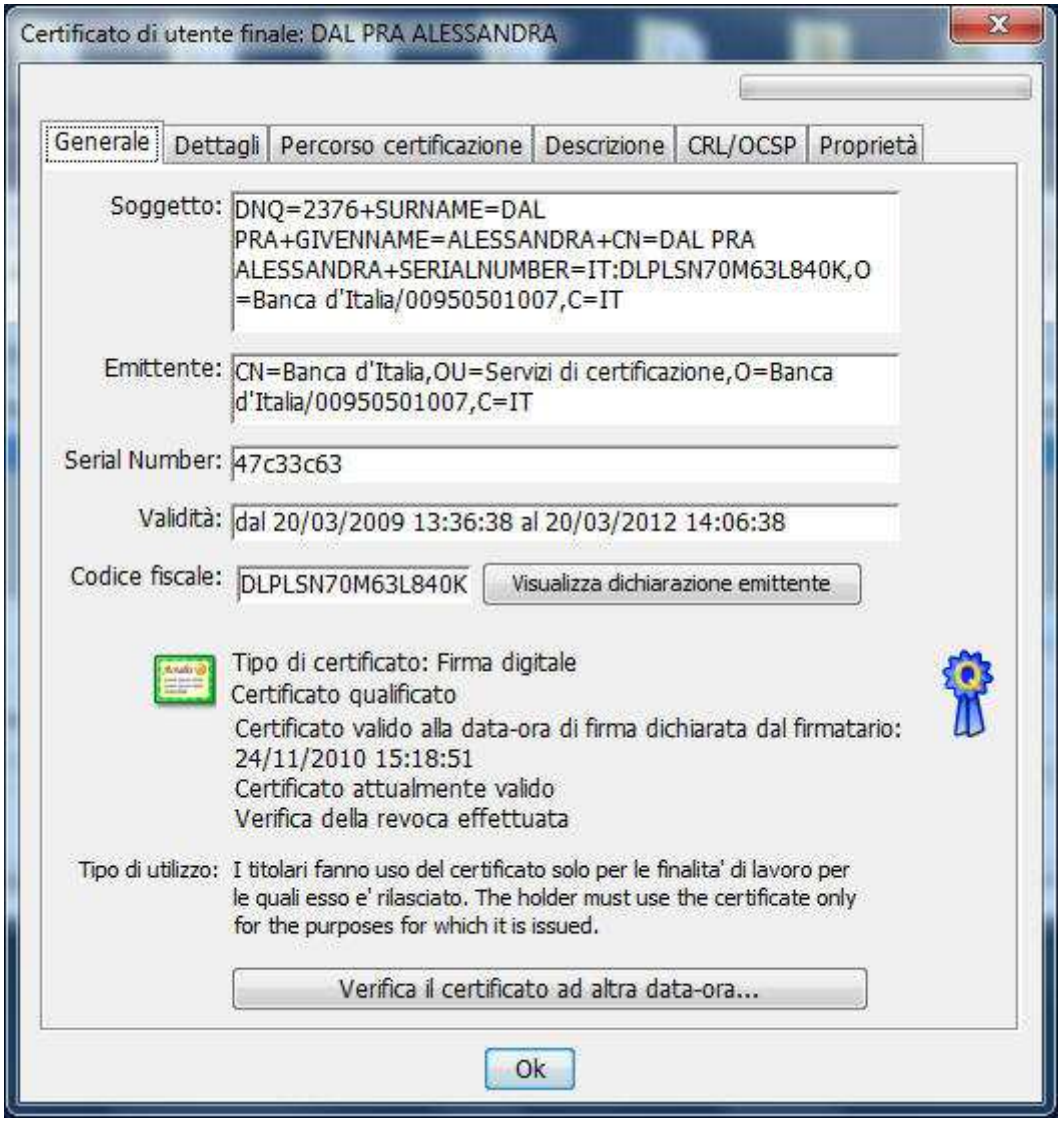

Verifica documento "Contratto XYZ del 2009-04-02....
Decifratura del documento effettuata con successo.
Apri il documento...
Specificare la posizione in cui salvare il documento verificato:
:tings\Administrator\Desktop\Contratto XYZ del 2009-04-02.pdf
Sfoglia...
Annulla
Salva

Verifica del firmatario

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

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

Nella sezione precedente abbiamo descritto come effettuare il primo passo. Per effettuare il secondo passo, di fondamentale importanza, si deve cliccare sul bottone "**Verifica firmatario**" presente nella finestra riepilogativa delle firme. Dopo qualche istante, apparirà una finestra del tipo seguente che mostra il risultato delle verifiche svolte:



È importante notare che la verifica del certificato viene sempre svolta alla data-ora di firma, 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 "**Verifica il certificato ad altra data-ora**"; apparirà la seguente finestra di dialogo:

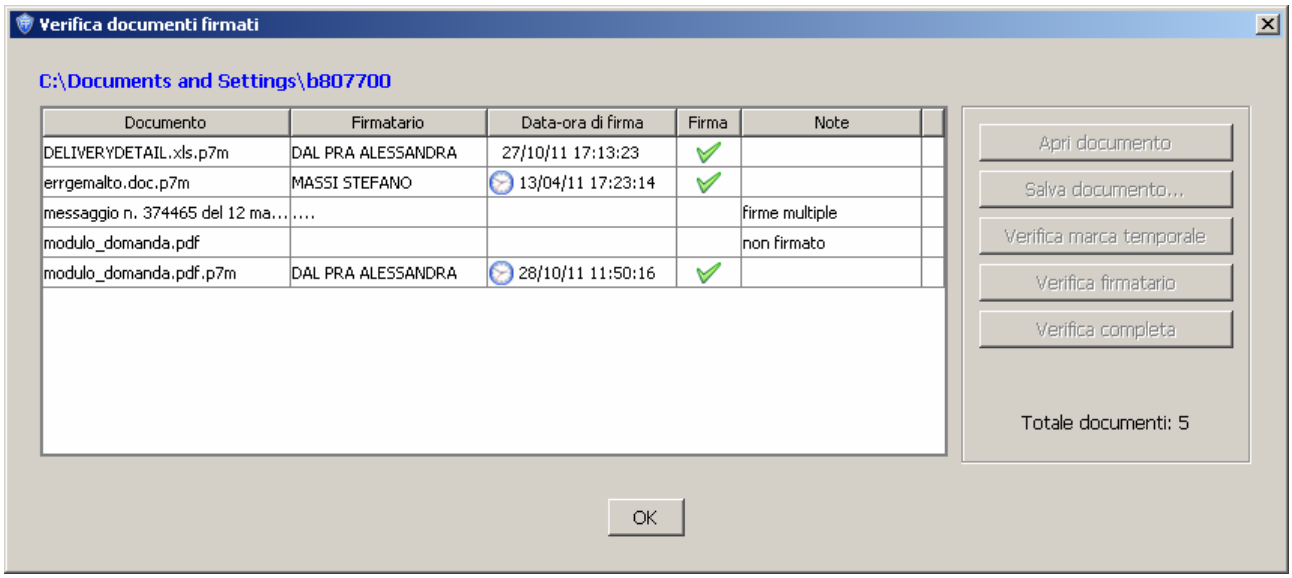
Da qui, usando gli appositi selettori, è possibile impostare la data e ora desiderate per la verifica del certificato. Cliccando sul bottone "**Oggi**" la data-ora viene reimpostata alla data-ora corrente del sistema operativo.

Tornando alla finestra 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.

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. Per completare la verifica, cliccare sul bottone "**Verifica firmatario**" e sul bottone "**Verifica marca temporale**" (se presente).

Nel caso in cui, invece, il file selezionato presenti più firme, si dovrà cliccare sul bottone "**Verifica completa**".

Se il documento è contenuto nel file firmato, è possibile visualizzarlo ed eventualmente salvarlo cliccando sul bottone "**Apri documento**".

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

Marcatura temporale

File Protector permette di apporre la marca temporale (time-stamp) in due modi:

- marca temporale di una singola firma digitale
- marca temporale di un intero documento

Marcatura della singola firma digitale

Le marche temporali associate alle singole firme sono visualizzabili e verificabili in fase di verifica di un documento firmato.

Marcatura di un intero documento

Si può anche ottenere una marca temporale che attesta la data/ora di esistenza di un intero documento, indipendentemente da quante firme digitali contiene (ma può anche trattarsi di un documento non firmato). Questa operazione si attiva cliccando sul bottone "**Marca temporale**" nella finestra principale, oppure selezionando la voce corrispondente nel menu "**File**".

La marca temporale ottenuta per un intero documento può essere salvata in due modi diversi:

1. come file separato (con estensione TSR)
2. insieme al documento di riferimento, all'interno di una "busta marcata" (con estensione TSD)

La "busta marcata" è una busta conforme alla specifica pubblica TimeStampedData che racchiude:

- un documento o file qualsiasi (non necessariamente firmato)
- opzionalmente, dei metadati riferiti al documento (per es. il nome)
- una o più marche temporali

Le marche temporali sono associate al documento nel modo seguente:

- la prima marca temporale (tempo T1) è calcolata sul documento di riferimento ed eventualmente sui metadati
- la seconda marca temporale (tempo T2) è calcolata sulla prima (e ne attesta l'esistenza al tempo T1)
- la terza marca temporale (tempo T3) è calcolata sulla seconda (e ne attesta l'esistenza al tempo T2)
- eccetera...

La busta marcata, dunque, oltre alla convenienza di contenere il documento di riferimento, consente di *estendere a piacere* l'attestazione di esistenza del documento al tempo T1, anche molto tempo dopo che la prima marca temporale è scaduta.

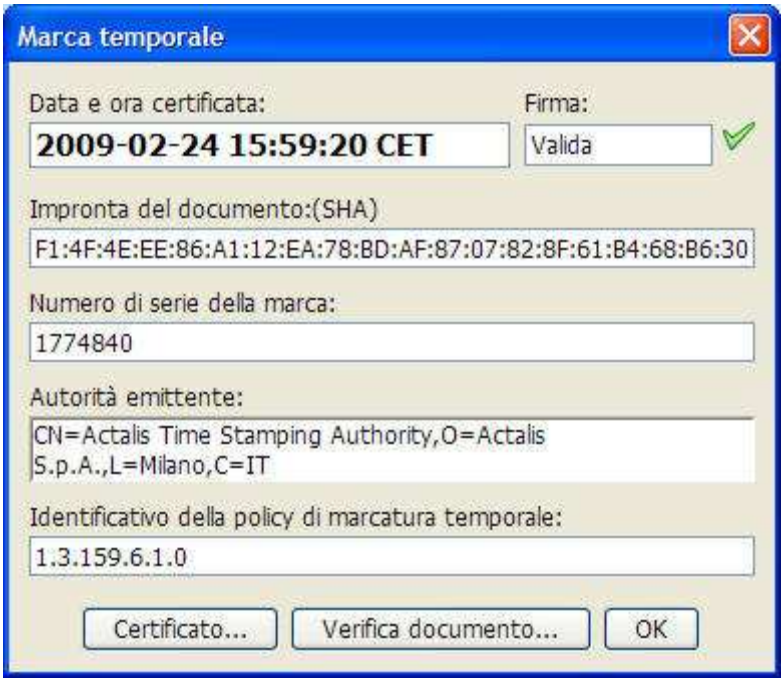
Per ottenere marche temporali, in entrambi i casi sopra descritti, è necessario avere accesso ad un servizio di marcatura temporale ed impostare l'indirizzo del servizio e le credenziali di accesso nella finestra delle **Preferenze** (cliccare sul corrispondente bottone nella finestra principale, quindi selezionare la scheda "**Timestamping**").

Verifica marca temporale

È possibile verificare sia marche temporali "sciolte" sia buste marcate; in entrambi i casi, la verifica può essere fatta in 4 modi diversi:

- facendo "doppio-clic" col mouse sul file desiderato (con estensione TSR o TSD)
- cliccando sul file desiderato col tasto destro del mouse e quindi selezionando la voce "**Verifica con File Protector**"
- trascinando il file desiderato sull'area-bersaglio di File Protector
- selezionando la voce di menu "**Verifica marca temporale**"

Verificando una marca temporale "sciolta" (file con estensione .TSR) compare una finestra di questo tipo:



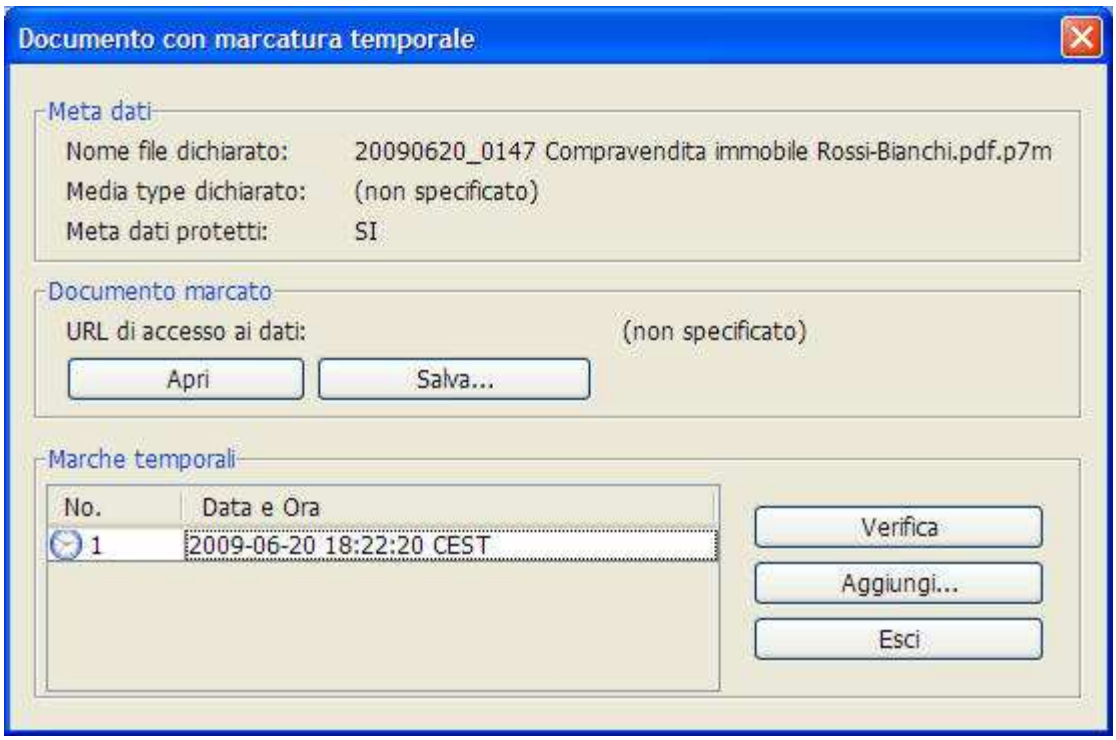
Questa finestra mostra una serie di importanti informazioni, tra cui:

- la data e ora in cui è stata emessa la marca temporale
- la validità della firma della TSA sulla marca temporale
- l'autorità (TSA) che ha emesso la marca temporale

Cliccando sul bottone "**Verifica documento**..." è possibile selezionare il documento di riferimento e controllare che corrisponda effettivamente alla marca temporale in esame (ossia che l'impronta ricalcolata del documento coincida con l'impronta contenuta nella marca).

Cliccando sul bottone "**Certificato**..." vengono visualizzati tutti i dettagli sul certificato della TSA.

Quando invece si verifica una "busta marcata", compare anzitutto una finestra di questo tipo:

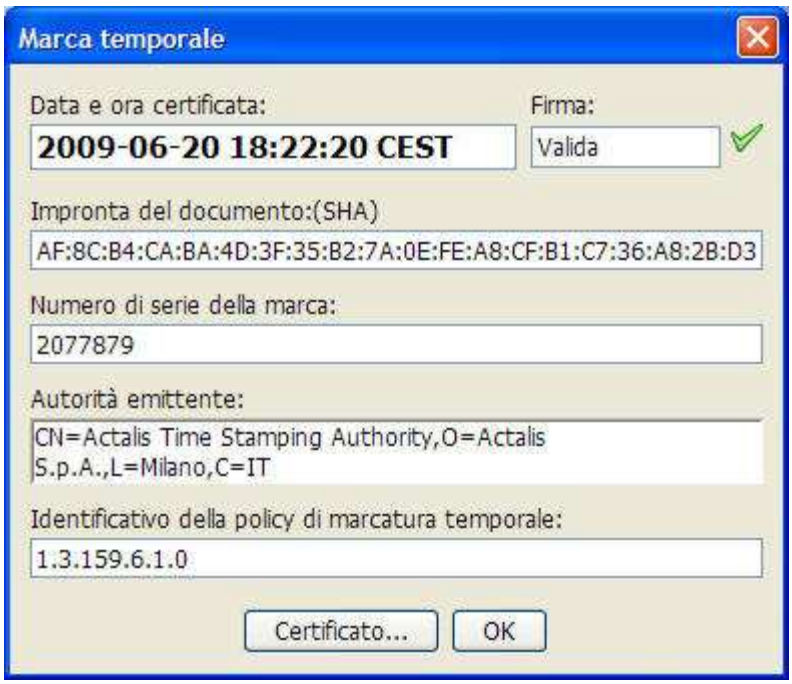


Questa finestra mostra le principali informazioni sulla busta in esame:

- metadati (tra cui, solitamente, il nome del documento contenuto nella busta)
- elenco delle marche temporali ottenute per il documento

Sono inoltre presenti due bottoni "**Apri**" e "**Salva**" che consentono rispettivamente di visualizze e salvare il documento contenuto nella busta.

Per verificare le singole marche temporali, selezionare dall'elenco quella desiderata e cliccare sul bottone "**Verifica**"; apparirà una finestra di questo tipo:



In questo caso non è presente il bottone "**Verifica documento**" in quanto la verifica viene fatta automaticamente rispetto al documento contenuto nella busta.

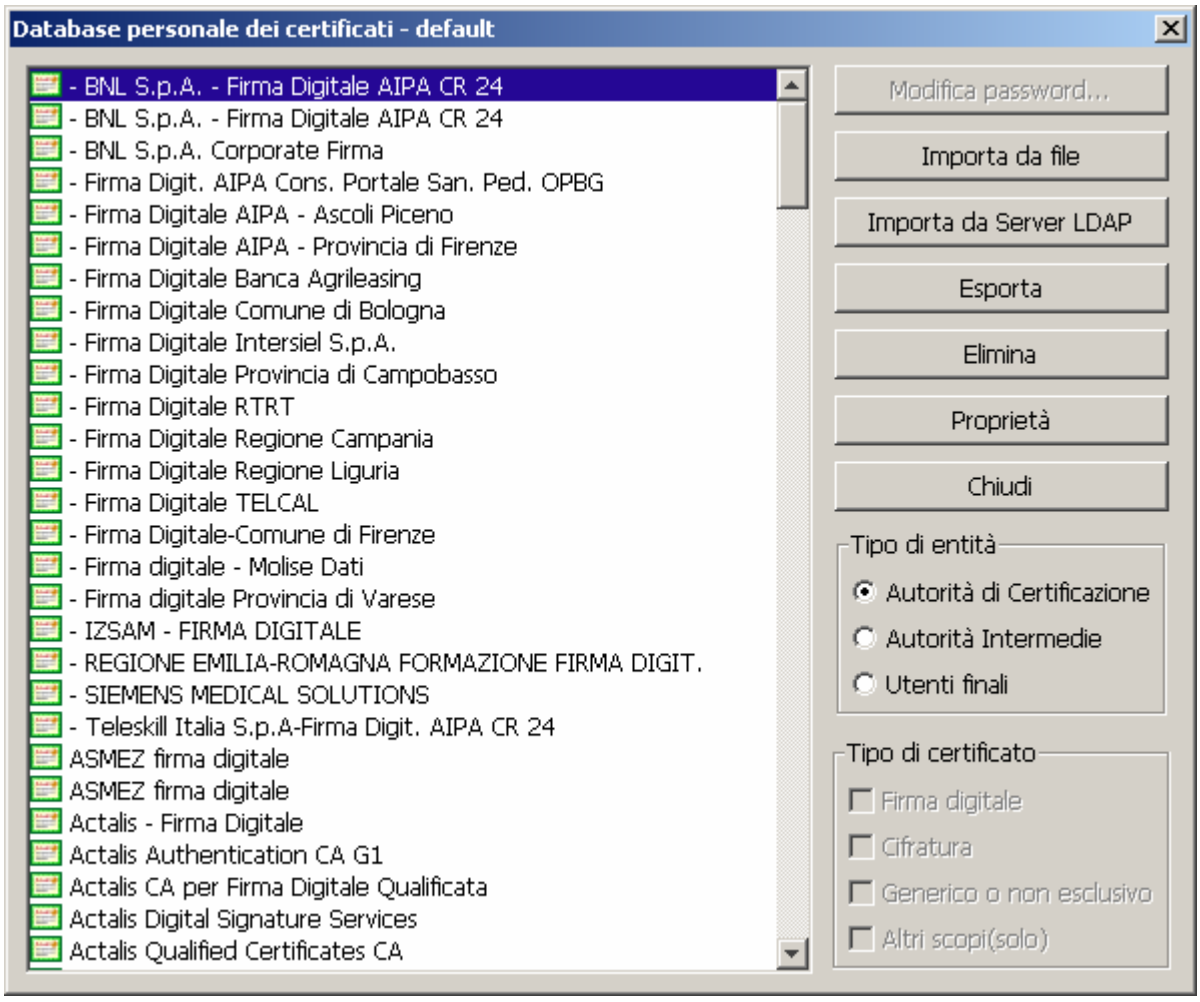
Cliccando sul bottone "**Aggiungi**..." nella finestra di verifica di una busta marcata, verrà aggiunta una marca temporale a quelle esistenti, secondo la logica descritta nella sezione precedente. Questa operazione è utile se il documento deve essere conservato per un lungo periodo di tempo, al di là della data di scadenza della marca temporale corrente.

Gestione dei certificati

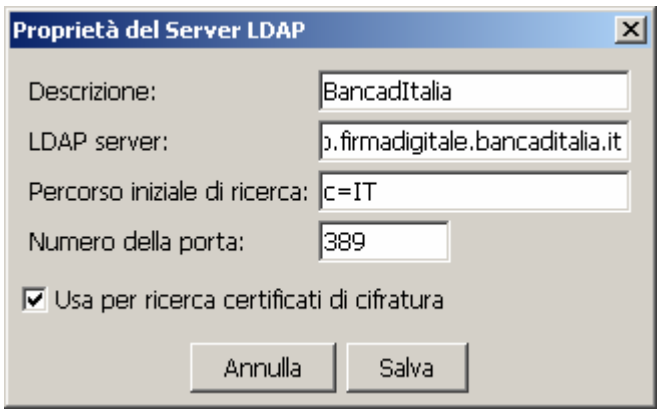
File Protector permette di gestire un database personale dei certificati delle CA e degli utenti;

- 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.

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**":



Per impostare il server LDAP da utilizzare nella ricerca dei certificati, selezionare la voce "**Elenco server LDAP**" dal menu "**Strumenti e opzioni**" nella finestra principale di File Protector, quindi aggiungereo modificare la voce desiderata in modo che la casella "**Usa per ricerca**..." sia abilitata (possono essere configurati diversi server LDAP, ma solo quello contrassegnato sarà poi utilizzabile nelle ricerche):


Proprietà del Server LDAP
Descrizione:
BancadItalia
LDAP server:
).firmadigitale.bancaditalia.it
Percorso iniziale di ricerca:
c=IT
Numero della porta:
389
Usa per ricerca certificati di cifratura
Annulla
Salva

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.

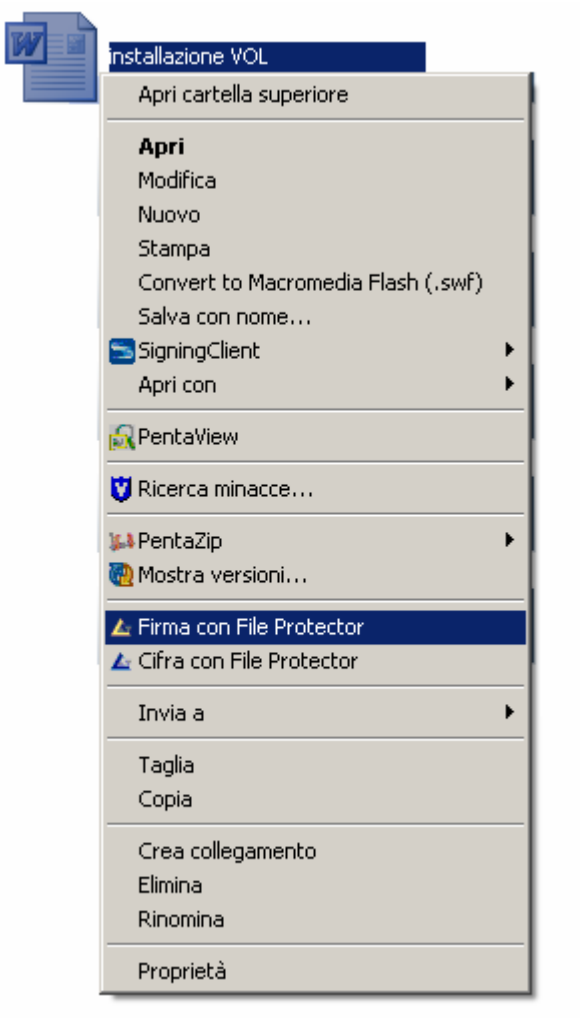
Si faccia attenzione a digitare correttamente il PUK, perché anche questo è soggetto al blocco in caso di errori ripetuti. In caso di blocco del PUK, non è più possibile ripristinare il normale funzionamento della smartcard.

Comandi da shell

Il File Protector si integra con l'interfaccia Windows. Se si seleziona un file, o una cartella all'interno di una finestra di Esplora Risorse, è possibile richiamare il "menu contestuale" del File Protector premendo il pulsante destro del mouse.

In particolare selezionando un singolo file da tasto destro del mouse è possibile:

- cifrare il file
- decifrare il file (solo file con estensione .p7e)
- firmare il file
- verificare il file (solo file con estensione .p7m).



Per le cartelle selezionare la cartella e cliccare sul tasto destro del mouse. E' possibile:

- cifrare la cartella (anche le sottocartelle);
- decifrare la cartella (solo i file con estensione .p7e contenuti nella cartella, comprese le sottocartelle);
- firmare la cartella (anche le sottocartelle);
- verificare la cartella (solo i file con estensione .p7m contenuti nella cartella).