

FIRMA DIGITALE RETAIL

Guida per l'installazione

Giugno 2013



Banca Monte dei Paschi di Siena S.p.A.

Sommario

Avvertenza:	3
1. FIRMA DIGITALE RETAIL – INSTALLAZIONE.....	4
Passo 1 – installazione del programma per la firma digitale (clienti privati)	4
Passo 2 – scaricamento dei certificati di firma	7
Passo 3 – configurazione del dispositivo di firma e avvio operatività.....	9
2. ESEMPIO DI FIRMA DI UN DOCUMENTO	13

Avvertenza:

Per completare l'installazione ed avviare l'operatività con Firma Digitale occorrono:

- La chiave elettronica USB (contiene il software per l'installazione e su di essa verrà memorizzato il certificato di firma)
- Il codice CRP ritirato presso la Banca
- Il codice PIN ricevuto per posta (insieme alla Chiave USB), necessario per l'autenticazione e l'utilizzo del programma di firma digitale.

Si rimanda alla legenda in fondo a questo paragrafo per maggiori informazioni sui codici.

Il primo passaggio da effettuare è collegare la Chiave elettronica in una porta USB. Se il sistema operativo è compatibile con il software auto-installante, la procedura è automatica. Sono sufficienti pochi passaggi (e la conferma delle impostazioni di default) per iniziare a operare.

Se invece l'auto-installazione non parte, allora è possibile avviarla manualmente, seguendo le istruzioni contenute in questa Guida (passo 1).

Le indicazioni contenute negli altri passi (2-3) sono valide anche quando l'installazione automatica è stata condotta regolarmente.

Per l'utilizzo del programma di firma digitale si rinvia invece al manuale completo scaricabile direttamente dall'applicativo (cfr. infra fig. 14 – guida).

NOTA BENE: per l'uso del servizio è necessario essere dotati del sistema operativo Windows.

Legenda:

- Chiave elettronica USB – è il dispositivo che genera password numeriche monouso necessarie per accedere ai canali telematici; viene assegnato dalla Banca con il servizio Multicanalità Integrata e supporta la firma digitale in quanto è destinato a memorizzare i certificati di firma. Viene recapitata al domicilio con corriere.
- Codice CRP – è il Codice Riservato Personale che viene consegnato (preimbustato) insieme al contratto direttamente allo sportello. Serve a scaricare i certificati di firma sulla chiave elettronica.
- Codice PIN – è il codice personale (Personal Identification Number), fornito dalla Banca insieme alla chiave elettronica USB. Serve ad attivare la firma digitale (quindi serve tutte le volte che occorre apporre una firma).

1. FIRMA DIGITALE RETAIL – INSTALLAZIONE

Passo 1 – installazione del programma per la firma digitale (clienti privati)

Inserire la chiave USB nel computer. Se CEEDO non parte automaticamente, cliccare su START CEEDO all'interno del contenuto della chiave.

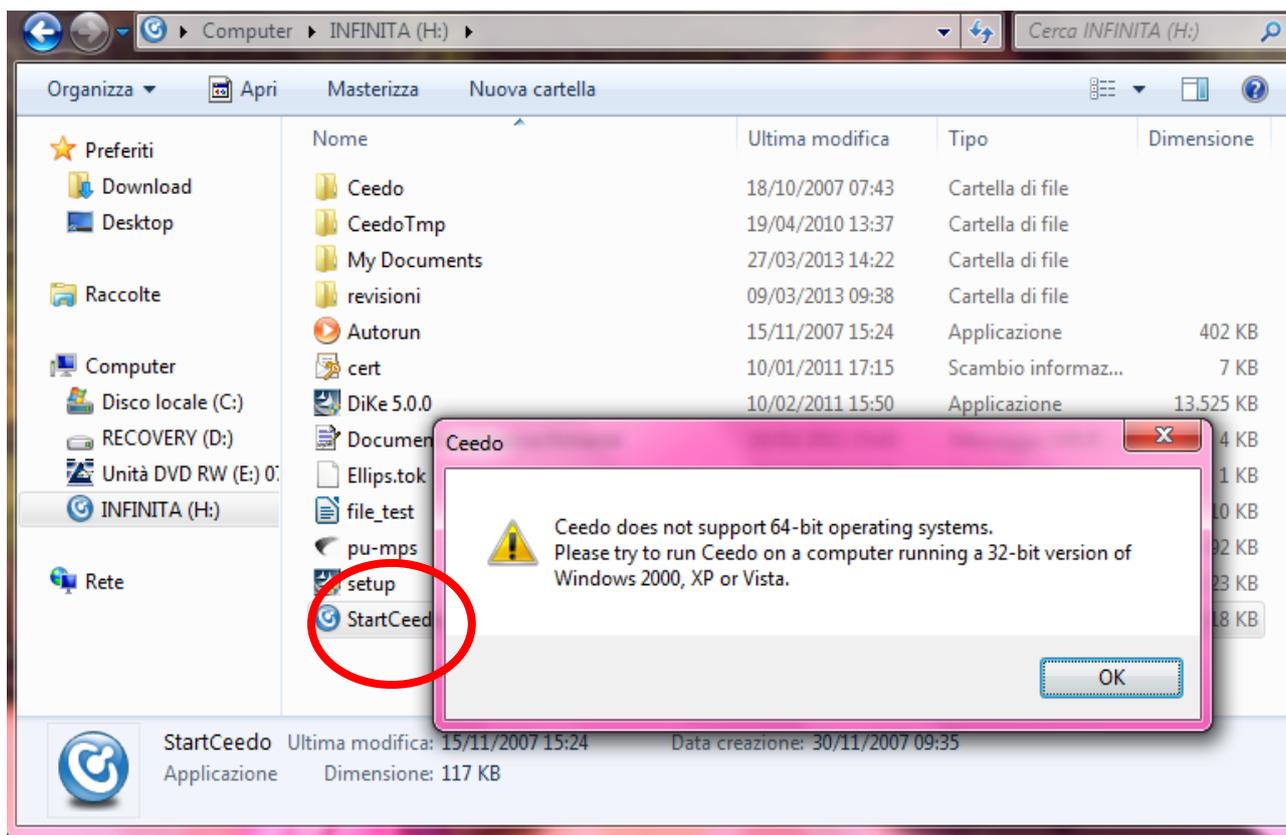


Figura 1

Sui sistemi a 64 bit il programma non risponde automaticamente. Occorre pertanto collegarsi via internet all'indirizzo:

firmadigitale.mps.it/.

e seguire le istruzioni per le chiavi USB: vedi fig. seguente.

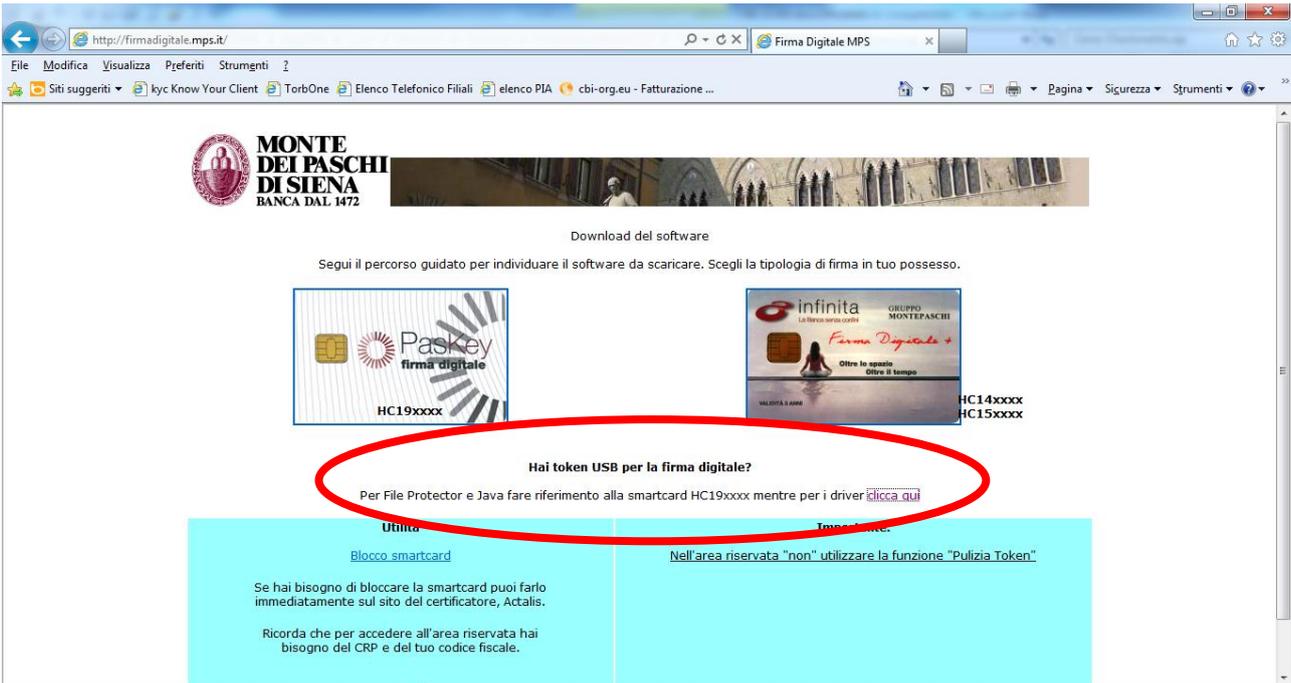


Figura 2

In questo modo si scarica in locale una cartella (denominata Charismatics) e un file eseguibile: cfr. fig. successiva. Occorre lanciare il file eseguibile **Actalis_KIT_5.1.2_Light.exe**.

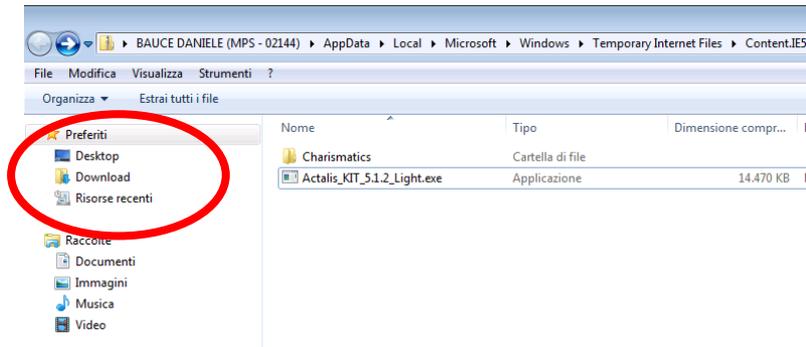


Figura 3

Quindi aprire la cartella Charismatics e lanciare:

- Instmsiw.exe
- Setup.exe

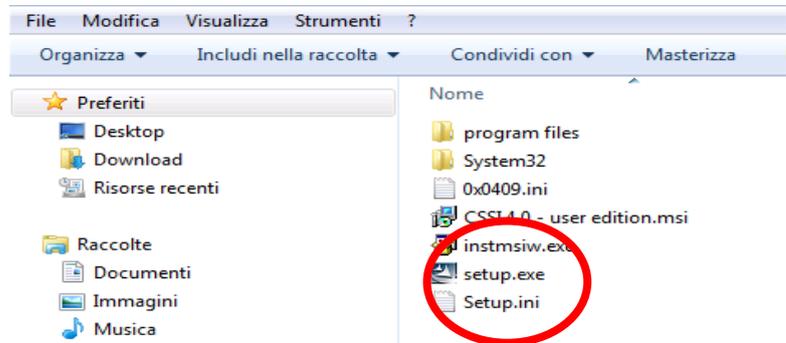


Figura 4

Alla fine dell'installazione sulla postazione sono presenti 2 programmi:

- File protector (questo è il programma da usare per firmare digitalmente)
- Smart security interface utility



Figura 5

Passo 2 – scaricamento dei certificati di firma

Dopo aver installato il programma, occorre scaricare i certificati di firma digitale. È necessario collegarsi al sito <http://portal.actalis.it>. Nella pagina iniziale (in alto a sinistra) bisogna inserire il codice fiscale e il Codice Riservato Personale (CRP). Questo codice è consegnato in filiale al momento della sottoscrizione del contratto per il servizio di firma digitale.

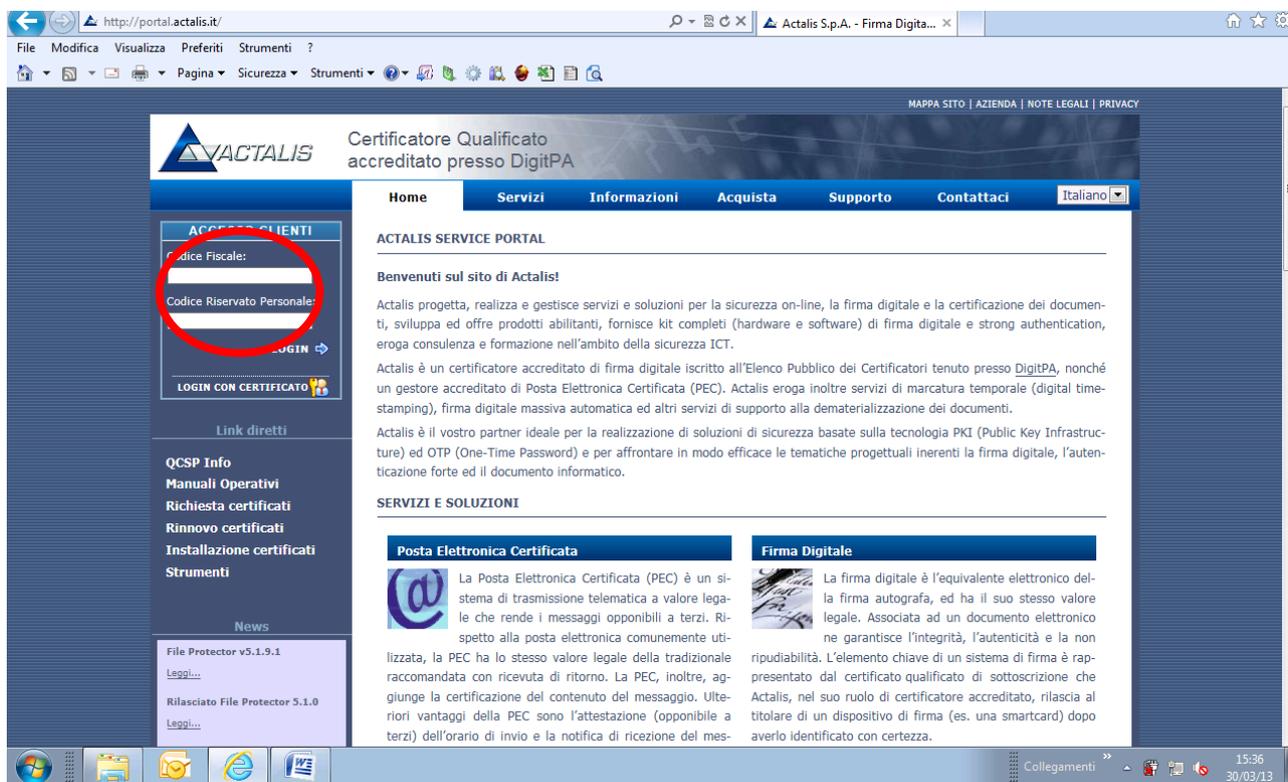


Figura 6

Dopo aver inserito i codici e cliccato su login si accede alla pagina da cui si possono scaricare i certificati di firma digitale (cfr. figura successiva). In questa mappa l'utente deve cliccare su **SCARICA/INSTALLA** il certificato; l'azione va ripetuta per entrambi i certificati presenti. **PRIMA DI INIZIARE lo scaricamento** l'utente deve inserire nella porta USB la chiave elettronica fornita dalla Banca (ricevuta per posta).

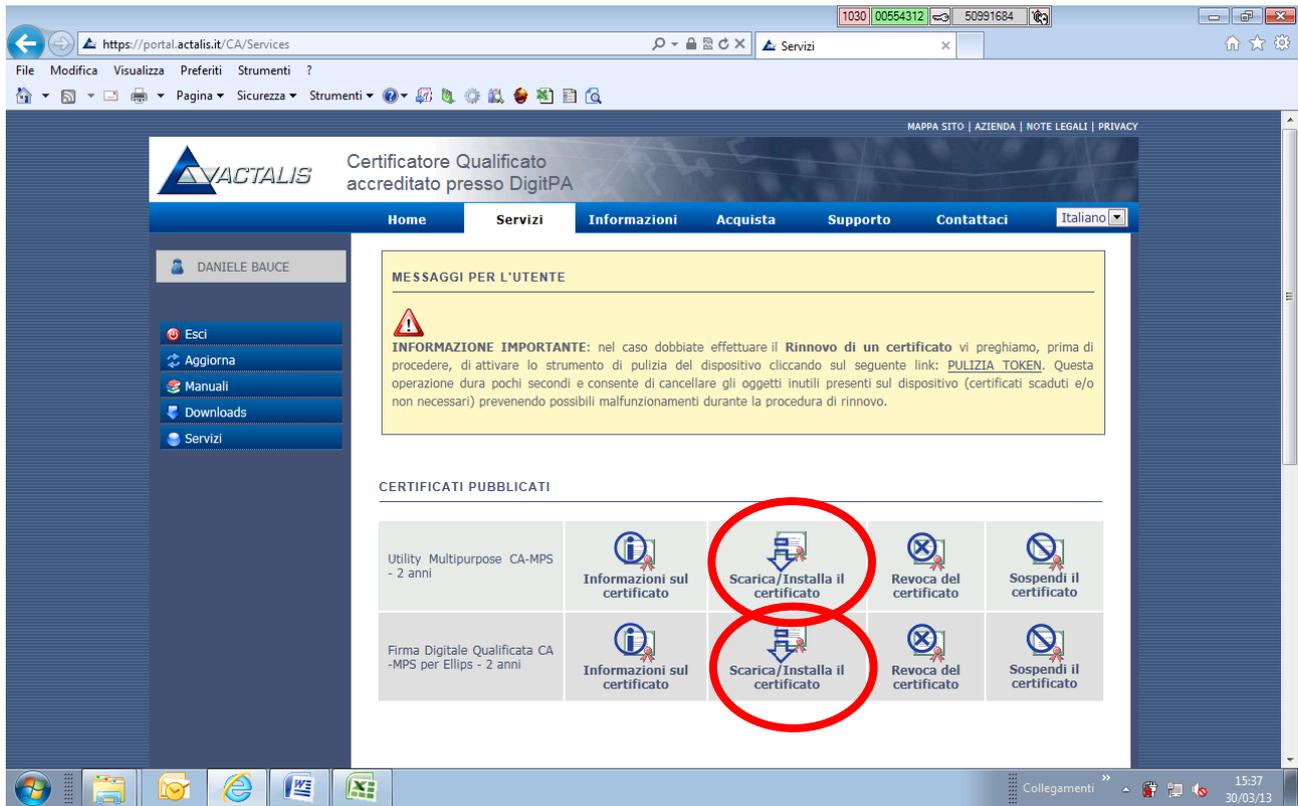


Figura 7

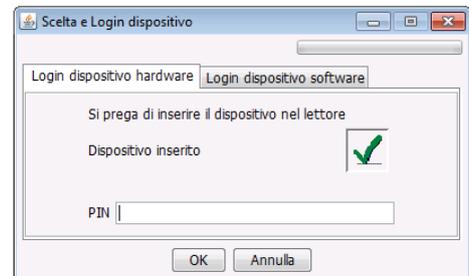
Se ci si dimentica di inserire la chiave USB, un pop-up informativo richiede questa azione. A questo punto è sufficiente inserire il codice PIN (ricevuto dalla Banca per posta).



Figura 8

INSTALLAZIONE CERTIFICATO

Accesso al dispositivo in corso...



Passo 3 – configurazione del dispositivo di firma e avvio operatività

Occorre lanciare il programma installato al punto 1, ossia FILE PROTECTOR e INSERIRE LA CHIAVE USB (se non già fatto). Se è la prima volta che il programma viene eseguito, occorre creare un profilo.

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**. L'applicazione guida automaticamente e intuitivamente l'utente alla creazione di un profilo nel caso di primo accesso.

Se il PC è usato in modo esclusivo, può essere utile selezionare l'opzione "Memorizza la password" e l'opzione "Autologin"; questa seconda opzione fa in modo che File Protector non mostri più questa finestra, così da velocizzare la partenza dell'applicazione.

Dopo aver lanciato il FILE PROTECTOR e aver creato/selezionato il profilo utente, l'aspetto è quello riportato nella figura successiva. L'ultimo passo dell'installazione è costituito dalla configurazione del dispositivo di firma, attivabile dal menù **DISPOSITIVO – CONFIGURAZIONE**.

L'aspetto della finestra che compare è simile a quella a fianco riportata.

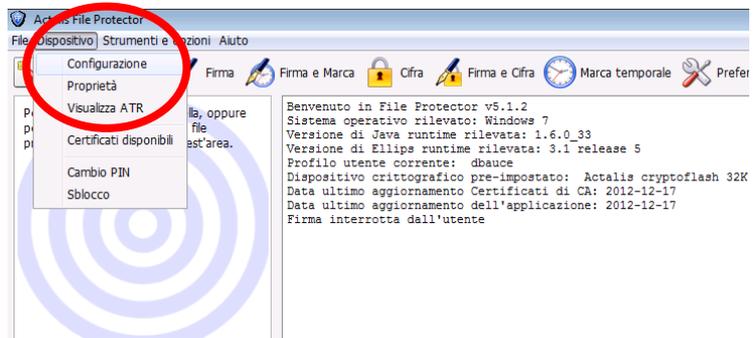


Figura 9

L'aspetto della finestra che compare è simile a quella a fianco riportata.

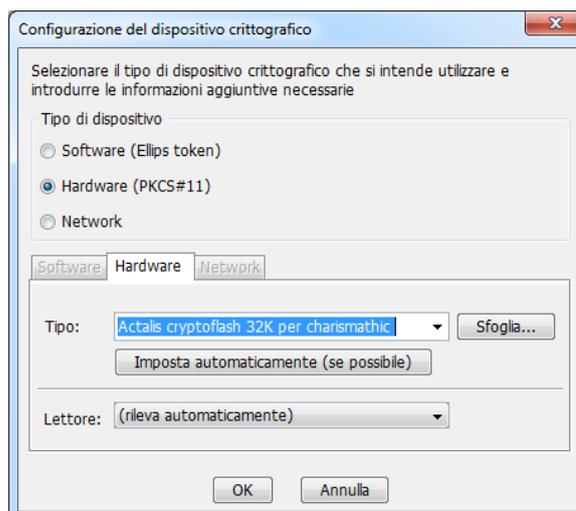


Figura 10

L'impostazione del tipo di dispositivo (se non già automaticamente opzionata) è HARDWARE (PKCS#11). Nella parte sottostante della finestra c'è lo spazio che riporta l'indicazione del tipo di dispositivo hardware. È necessario cliccare sul tasto "IMPOSTA AUTOMATICAMENTE (SE POSSIBILE)". Se l'installazione è stata portata a termine correttamente, questo campo si completa automaticamente.

Se la configurazione automatica non dovesse funzionare, verificare se il tipo corretto di dispositivo ("Actalis cryptoflash 32K per charismatic") sia presente nel menu a discesa e, in caso positivo, selezionarlo. Se non è presente, contattare l'assistenza ([indirizzo email](#)).

Verificare dunque che i parametri di seguito indicati siano corrispondenti a quelli indicati nella finestra della figura successiva, ovvero:

- Tipo di dispositivo → hardware
- Dispositivo hardware / Tipo → Actalis cryptoflash 32K per charismatic

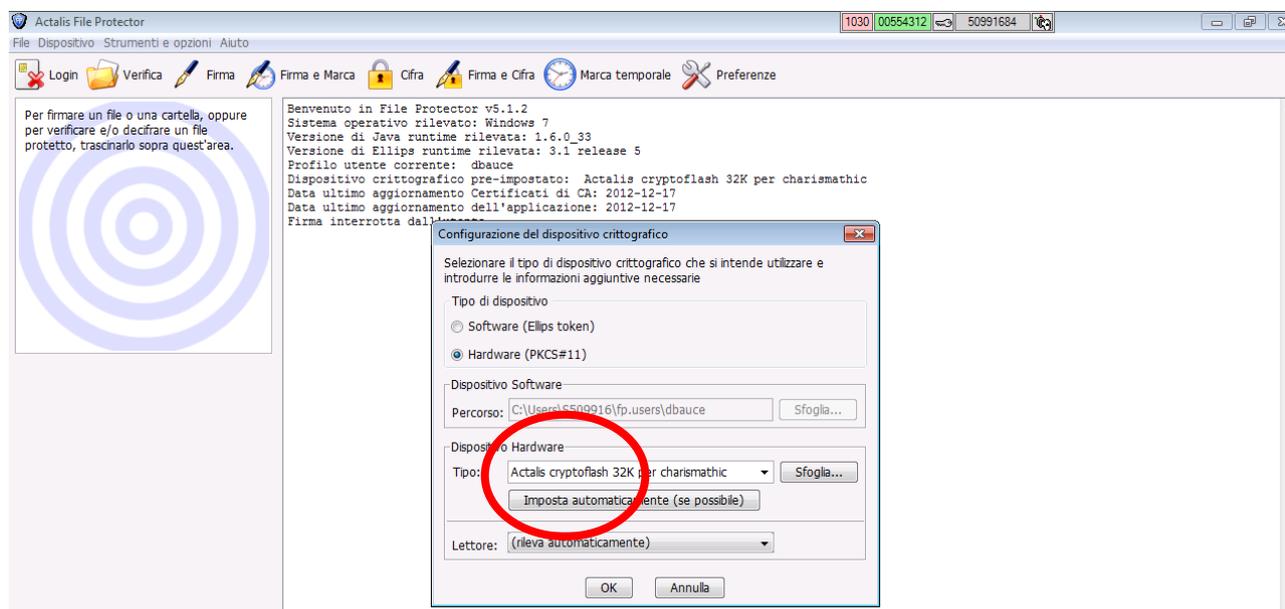


Figura 11

Cliccare infine sul bottone "OK" per concludere. L'impostazione viene memorizzata, quindi in seguito non sarà più necessario svolgere questa operazione.



Figura 12

Il programma a questo punto è completamente installato.

Tuttavia, ogni volta che si accede al programma (file protector) la firma è inizialmente disabilitata per motivi di sicurezza, ma questa opzione può essere modificata (cfr. figura successiva, la prima icona a sinistra in alto). Cliccando su LOGIN compare il pop-up nel quale inserire il PIN.

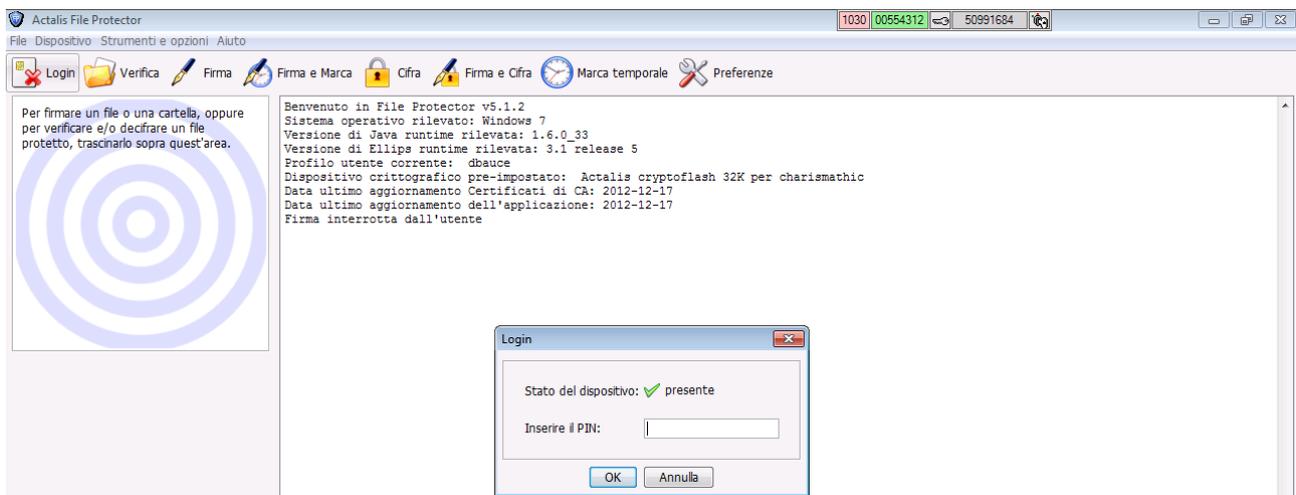


Figura 13

A questo punto la firma è abilitata e si può iniziare a firmare propri documenti.

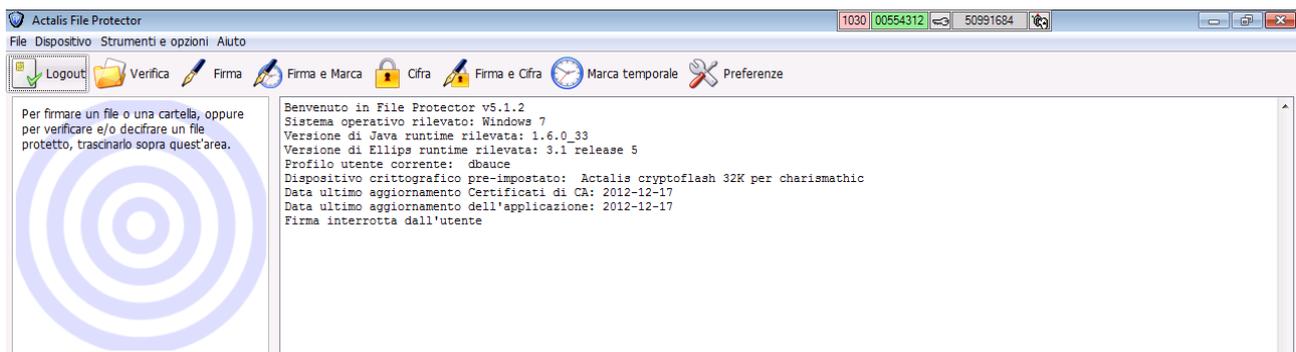


Figura 14

Per consultare una guida rapida sull'utilizzo della firma digitale è molto utile accedere all'aiuto nel menu omonimo (cfr. fig. seguente).

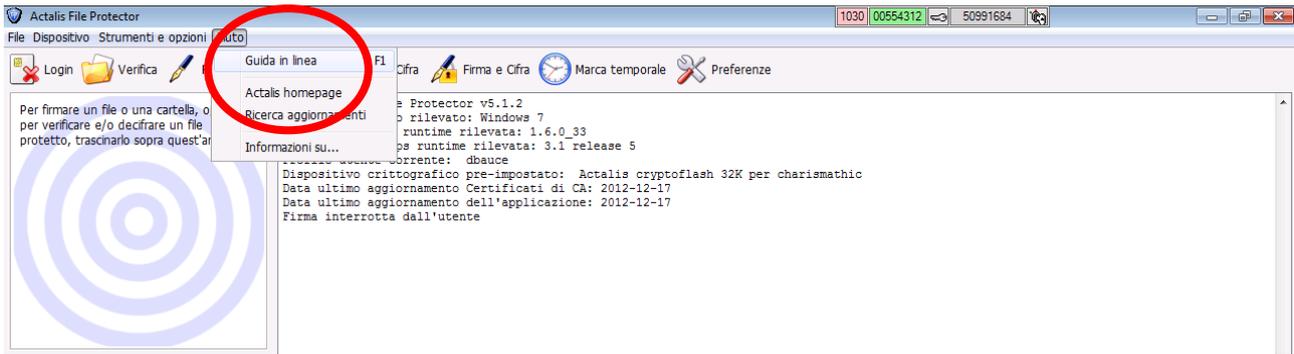


Figura 15

2. ESEMPIO DI FIRMA DI UN DOCUMENTO

Lanciare il programma File Protector e inserire le proprie credenziali.

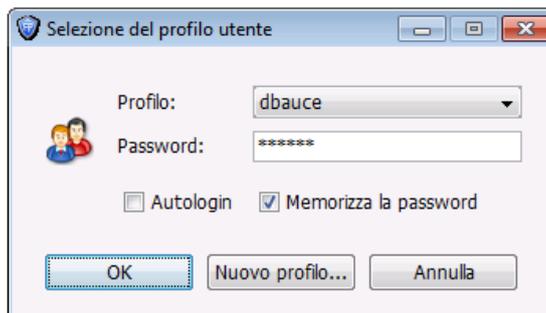


Figura 16

Quindi cliccare su login e inserire il PIN:

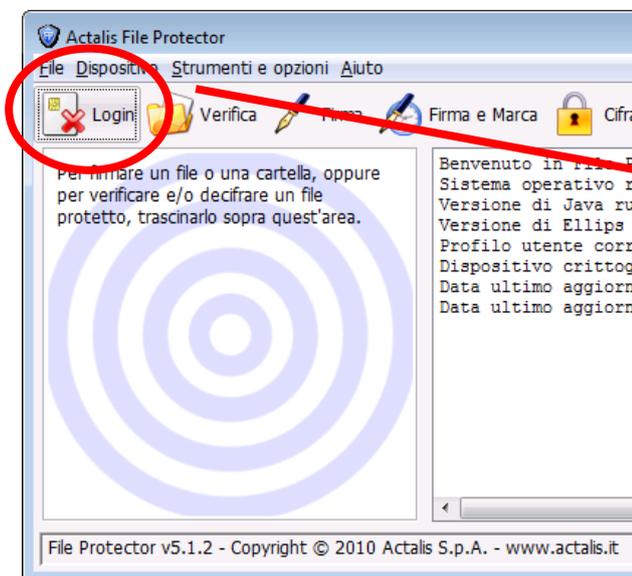
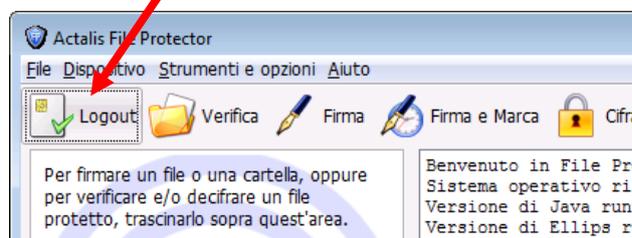


Figura 17



Figura 18



Esistono 3 modi diversi per firmare un documento. Per una piena conoscenza delle funzionalità si rimanda al manuale di utilizzo. Di seguito si porta un semplice esempio con la modalità più intuitiva, ossia il *drag-and-drop*.

Tenere aperto il file protector in cui è visibile il riquadro con un "bersaglio".

Aprire la cartella da cui "prelevare" il documento da firmare. È sufficiente cliccare sul file da firmare e trascinarlo (click+trascinamento) nel bersaglio.

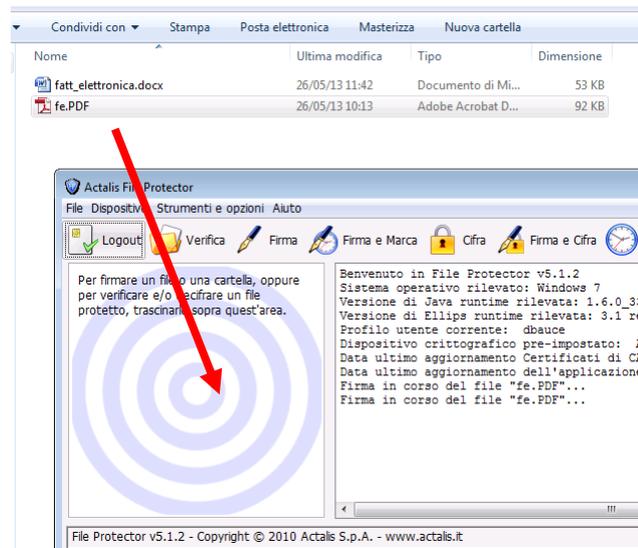


Figura 19

Se il file da firmare è di tipo PDF, allora compare una finestra come in fig. 19. Le impostazioni di default permettono già di firmare il file, ma è comunque possibile selezionare un altro certificato di firma (se esiste) o una diversa directory dove salvare il documento firmato. Alla fine è sufficiente fare click su "aggiungi firma..." per creare il documento firmato nella cartella indicata.

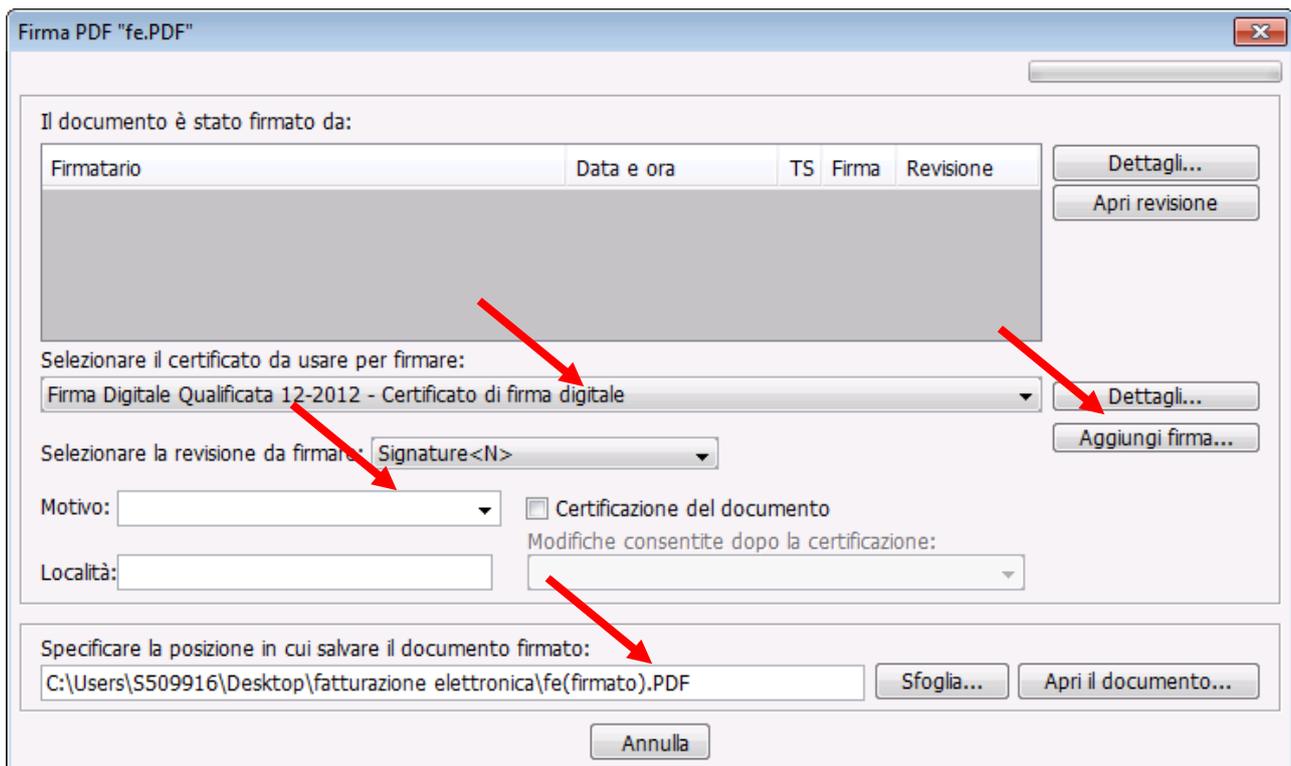


Figura 20

Apposito messaggio informa dell'esito della firma apposta al documento.

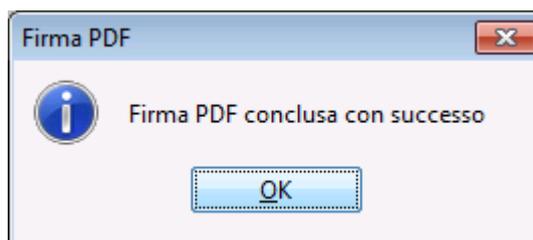


Figura 21

<<FINE>>