Firma Digitale

Manuale di installazione

Contenuto

PREMESSA 3
REQUISITI DI SISTEMA 3
SMART CARD E CREDENZIALI 3
DISINSTALLARE PROGRAMMI OBSOLETI 5
SISTEMA OPERATIVO A 32 O 64 BIT 5
CONTROLLARE LA VERSIONE JAVA 7
SCARICO DEL SOFTWARE 8
INSTALLAZIONE DEI DRIVER (SMART CARD) 9
SCARICO E INSTALLAZIONE DI JAVA 12
SCARICO E INSTALLAZIONE DI FILE PROTECTOR 16
CONFIGURAZIONE DI FILE PROTECTOR (APPLICATIVO DI FIRMA) 21
RICHIESTA (SCARICO) DEL CERTIFICATO DI FIRMA 23
DISINSTALLAZIONE 28
RINNOVO DEL CERTIFICATO TRAMITE PORTALE WEB 29
RINNOVO TRAMITE FILE PROTECTOR 32
APPENDICE 1 – CONFIGURAZIONE DELLA SMART CARD SU MOZILLA 34
APPENDICE 2 – DRIVER PER SMART CARD FINO A HC19 COMPRESE 36
APPENDICE 3 – FIRMA PDF CON FILE PROTECTOR 40
APPENDICE 4 – IMPORTARE IL CERTIFICATO NEL DATABASE PERSONALE 44

PREMESSA

Questo manuale ha lo scopo di illustrare i passaggi necessari per installare e abilitare al funzionamento la firma digitale fornita da Banca MPS.
Per usare la firma digitale occorre installare preventivamente il software sulla postazione da cui si vorrà utilizzarla.
Poi bisogna scaricare il certificato di firma sulla tessera (smart card) consegnata dalla Banca.
Infine occorre possedere le credenziali necessarie per accedere alle applicazioni e firmare i documenti.
Il manuale descrive i passaggi sopra accennati per facilitare tali operazioni. Esso è strutturato per risalire velocemente all'attività da svolgere, senza dover ricorrere all'assistenza (numero verde) indicato sul sito della banca.

REQUISITI DI SISTEMA

- Essere amministratore della postazione → se si usa una rete aziendale può essere necessario chiedere all'amministratore di sistema di effettuare l'accesso per consentire lo scarico del software di firma digitale. Ogni installazione deve essere eseguita come utente amministratore.
- Utilizzare un Sistema Operativo Windows (oppure ambiente virtuale Windows per gli utenti IOS, come per es. Parallels).
- Sbloccare temporaneamente eventuali antivirus o firewall che non permettano l'installazione di nuove applicazioni.
- Ulizzare il browser consigliato (di solito Explorer) per le operazioni di attivazione del certificato, come di seguito indicato.

SMART CARD E CREDENZIALI

Le credenziali e gli strumenti che si devono possedere per poter utilizzare la firma digitale sono:

- **Codice CRP (codice riservato personale)** → cfr. fig. 1; è il codice che consente di scaricare il certificato di firma digitale. Viene consegnato in filiale ed è formato da 2 lettere + 10 numeri.

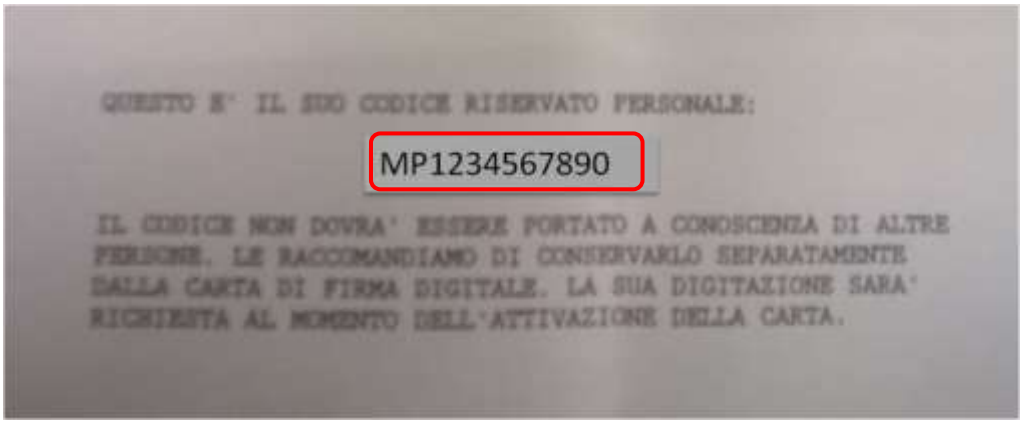


Figura 1

- **PIN** → cfr. fig. 2; è il codice che consente di firmare un documento o un file. Viene consegnato in filiale, assieme alla smart card e al codice PUK (da utilizzare solo per reimpostare il PIN, qualora questo fosse stato bloccato). Il PIN è formato da 8 cifre.

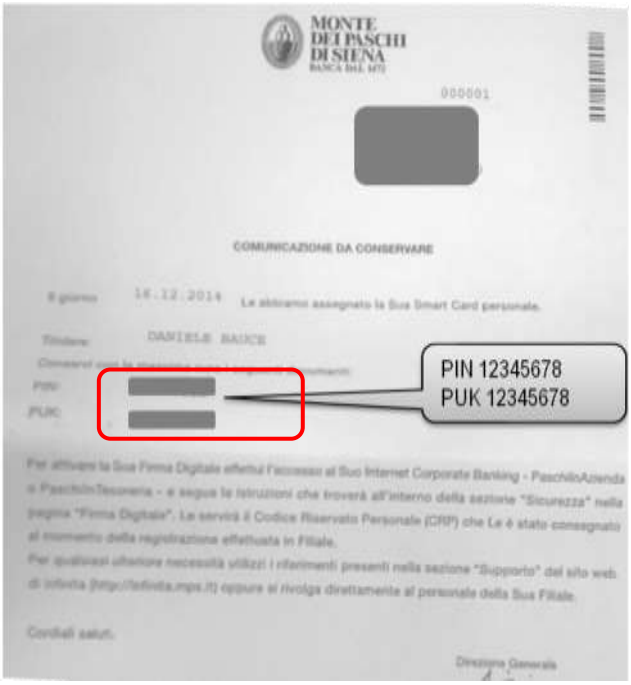


Figura 2

- **Smart Card** → cfr. fig. 3; è la tessera con microchip che viene consegnata in filiale. È personalizzata con i dati dell'assegnatario ed è destinata a contenere il certificato di firma digitale. È importante stabilire il tipo di tessera: verificare il codice della carta (cfr. riquadro rosso): ad es. serie MP20XXXX oppure HC19XXXX (di solito si tratta delle carte più vecchie), dove i primi 4 caratteri indicano appunto il tipo di tessera. Servirà per l'installazione del software corretto[1].

Figura 3

- **Lettore** → è un lettore di smart card, da collegare alla postazione del cliente per scaricare il certificato di firma e per firmare i documenti. Può essere richiesto alla Banca (cfr. fig. 4) oppure si può utilizzare un proprio lettore. È importante che durante la configurazione iniziale e tutte le volte che si vuole firmare un documento il lettore sia collegato alla postazione e la smart card correttamente inserita. La rilevazione corretta della smart card è segnalata dal led luminoso con luce fissa (mentre il led che pulsa indica che non è stata riconosciuta la smart card).

[1] I possessori di carte HC14XXXX devono procedere alla sostituzione della smart card con una di ultima generazione alla prima occasione utile, e comunque prima di un eventuale rinnovo.

Figura 4

DISINSTALLARE PROGRAMMI OBSOLETI

Il caso tipico è quello di installazione di smart card di tipo MP20. Se in passato sulla stessa postazione è stata installata una carta di tipo diverso, i driver della vecchia carta possono rendere incompatibile l'installazione dei nuovi. È buona regola disinstallare eventuali vecchi programmi in questi casi. Occorre naturalmente essere amministratori della propria postazione (in caso contrario contattare l'amministratore di sistema) e procedere alla disinstallazione, se presenti, dei seguenti 2 programmi:

- Actalis Kit (versione precedente a quella raccomandata);
- SSC API (sono i driver delle carte HC19, da disinstallare se la propria smart è di tipo MP20).

Importante: prima di confermare la disinstallazione, rimuovere il lettore dalla postazione (scollegare il lettore).

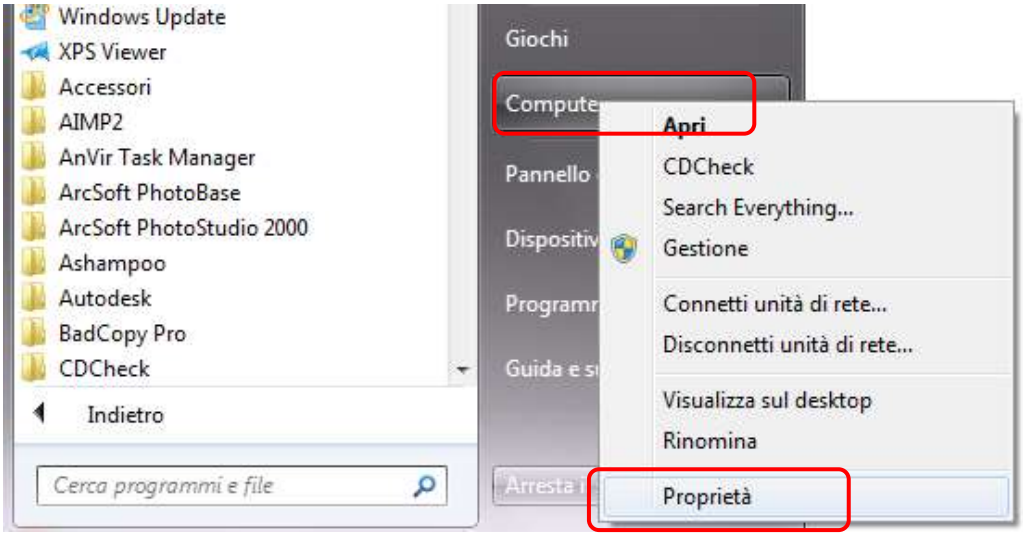
Figura 5

SISTEMA OPERATIVO A 32 O 64 BIT

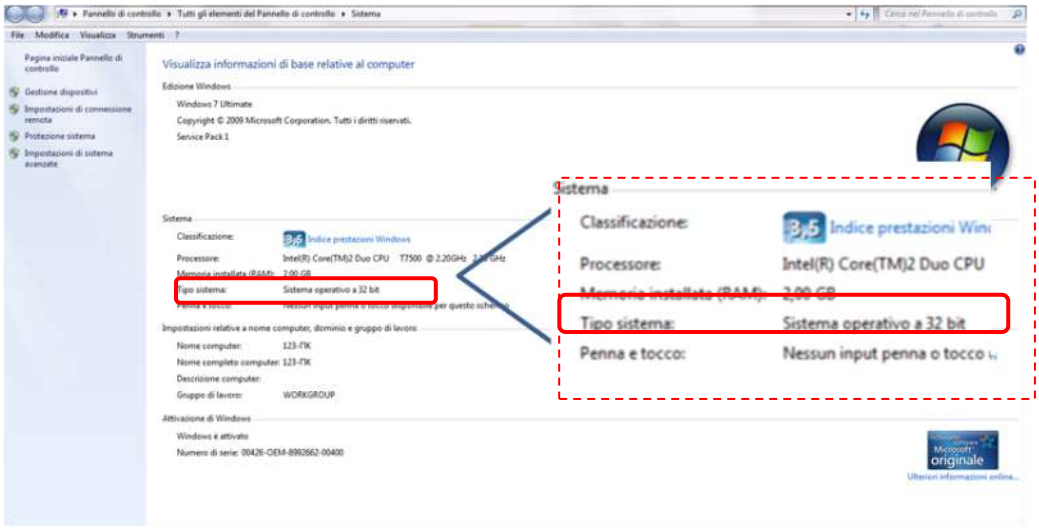
È necessario sapere se la postazione sulla quale deve essere usata la firma digitale funzioni con un sistema operativo a 32 o a 64 bit. Ciò serve per la successiva fase dell'installazione. Si può procedere in modi diversi.

- PROPRIETÀ DELL'UNITÀ C:

Accedere a START > COMPUTER (questo PC) e cliccare sul disco C: con il tasto destro del mouse. Si apre quindi il menù a scomparsa sotto riportato. Selezionare PROPRIETÀ.

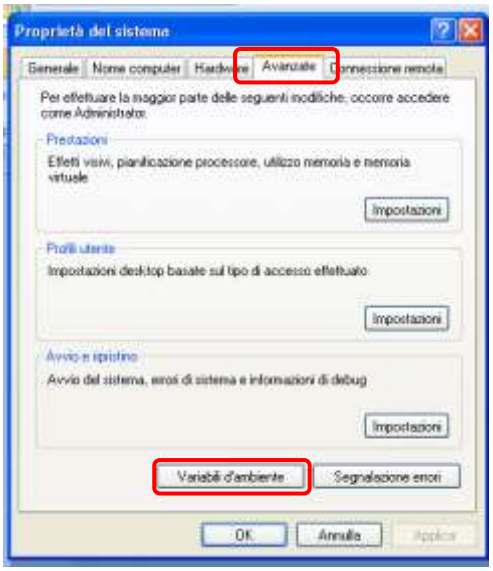


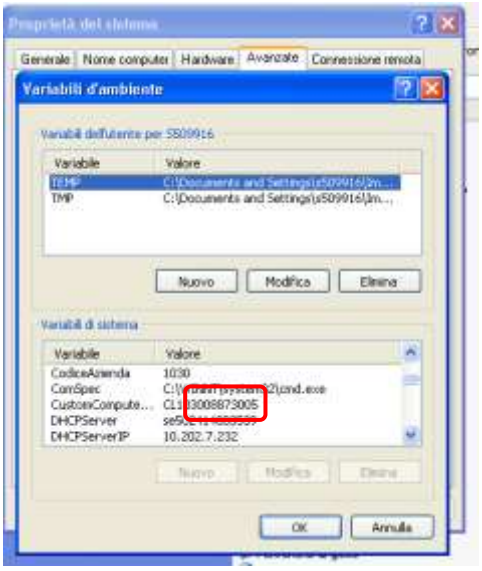
A seconda della versione del Sistema Operativo, le videate possono essere differenti, ma la logica è la medesima.
Controllando alla voce **"TIPO SISTEMA"** si può verificare se a 32 o 64 bit. Nella figura sotto riportata il SO è a 32 bit, ma generalmente tutti i computer più recenti sono a 64 bit.



- PANNELLO DI CONTROLLO

Un altro modo di verificare se il SO è a 32 o 64 bit è quello di accedere al PANNELLO OPERATORE: procedere da START > PANNELLO OPERATORE > SISTEMA > PROPRIETÀ DEL SISTEMA > AVANZATE > VARIABILI D'AMBIENTE. Nelle variabili presentate nella figura sottostante il SO è a 32 bit in quanto si trova System32.

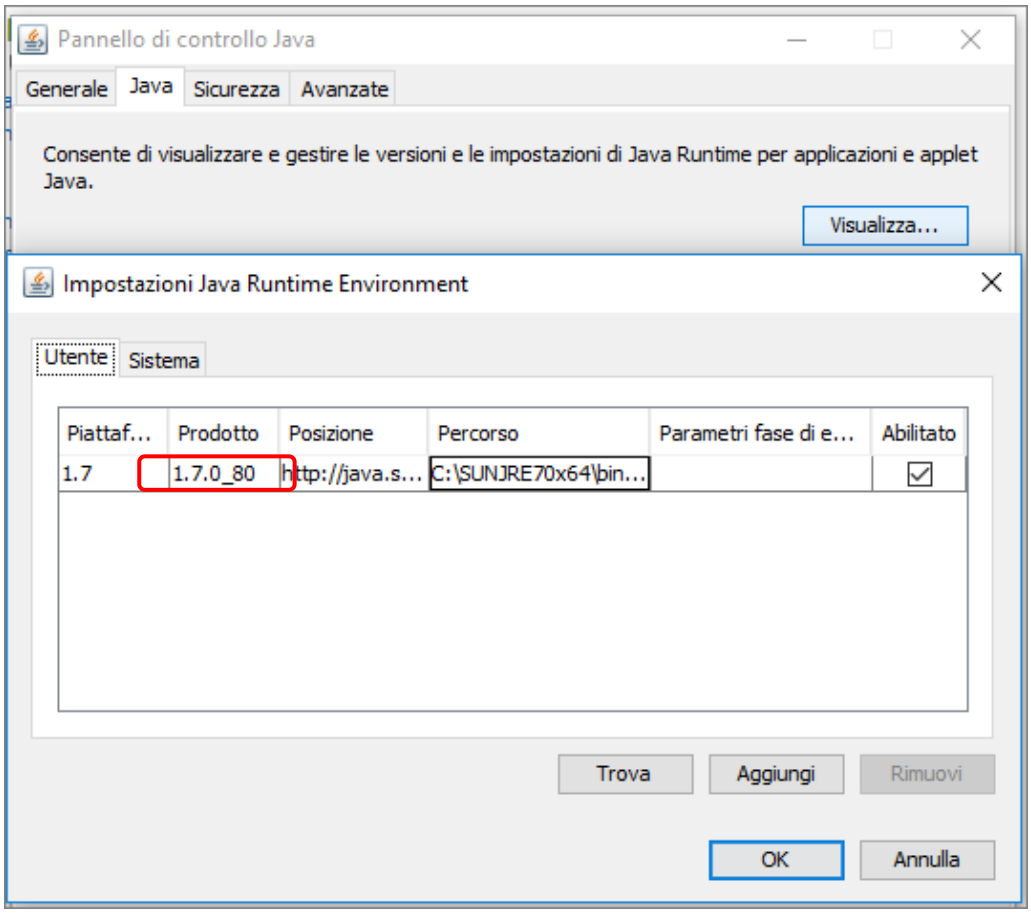




Su Windows 10 è invece necessario accedere a Pannello di Controllo > Sistema … > Sistema per ottenere la medesima informazione.
In caso di necessità, per capire se il SO è a 32/64 bit, è anche possibile consultare la pagina di assistenza di Microsoft per avere supporto (https://support.microsoft.com/it-it/kb/827218).

CONTROLLARE LA VERSIONE JAVA

Nel caso fosse necessario verificare la versione java disponibile sulla propria postazione, occorre seguire questi passaggi: Pannello di Controllo > Programmi > Java > Visualizza.



Nel caso di cui alla figura precedente la versione di java è la 1.7.

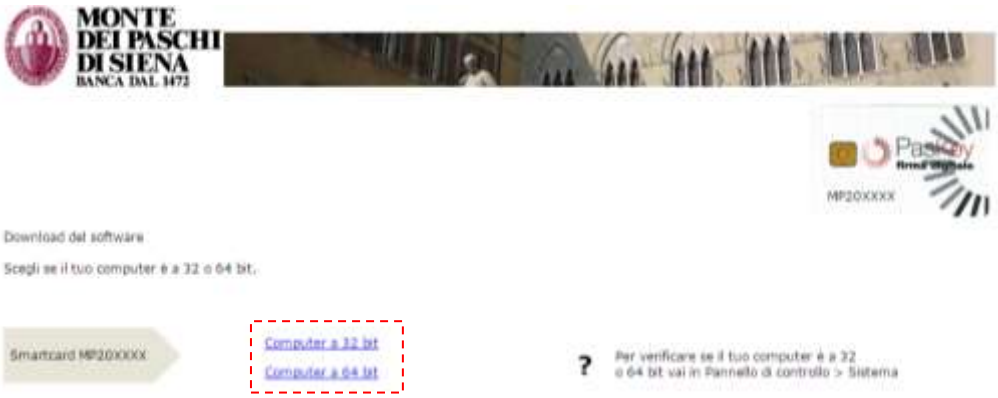
SCARICO DEL SOFTWARE

Come già evidenziato, occorre essere amministratori della propria postazione, altrimenti questa fase non si può portare a terminale.
Lo scarico del software avviene da una pagina pubblica: http://firmadigitale.mps.it.

Nella pagina sopra riportata è possibile:

- scegliere il software da scaricare (in base al tipo di carta e al sistema operativo utilizzato);
- consultare informazioni utili sul manuale di File Protector.

A seconda del tipo di smart card posseduta (MP20, HC19 o altro) si deve cliccare sull'immagine corrispondente. In questo modo si passa alle istruzioni specificamente predisposte per quel tipo di carta. A questo punto occorre cliccare sul link corrispondente al Sistema Operativo da utilizzare (32 o 64 bit).

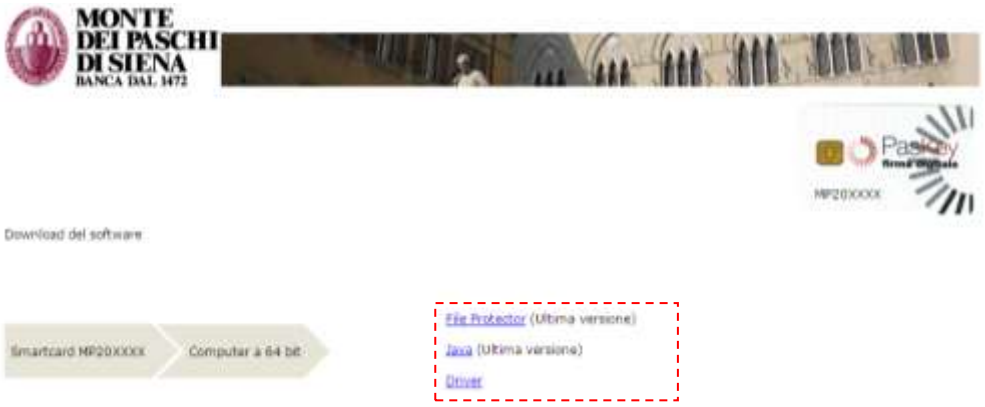


Generalmente per installare il software necessario all'uso della firma digitale occorre scaricare ed eseguire in questo ordine:

- i driver della smart card
- java

- l'applicazione di firma (file protector)

Le versioni consigliate di questi programmi sono diverse a seconda del tipo di smart card e del SO.



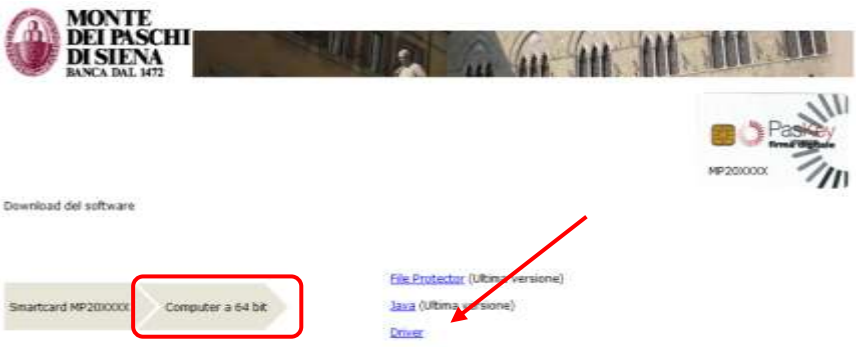
Nelle prossime pagine viene descritta l'installazione largamente più diffusa, ossia di **carte MP20 su sistemi operativi a 64 bit**. Per dubbi sul proprio sistema operativo e sulla tipologia di carta posseduta, rivedere i paragrafi specifici di questo manuale.

N.B.: con l'installazione di File Protector dalla serie 6 i driver e il java sono embedded: questo significa che **è possibile limitare l'installazione di File Protector (senza driver e senza java)** purchè ci si limiti a usare la firma digitale sempre e **solo con il programma File Protector.** Se invece si vuole utilizzare la firma anche per altri scopi (es. utilizzo su un sito web), allora è necessaria l'installazione completa.

INSTALLAZIONE DEI DRIVER (SMART CARD)

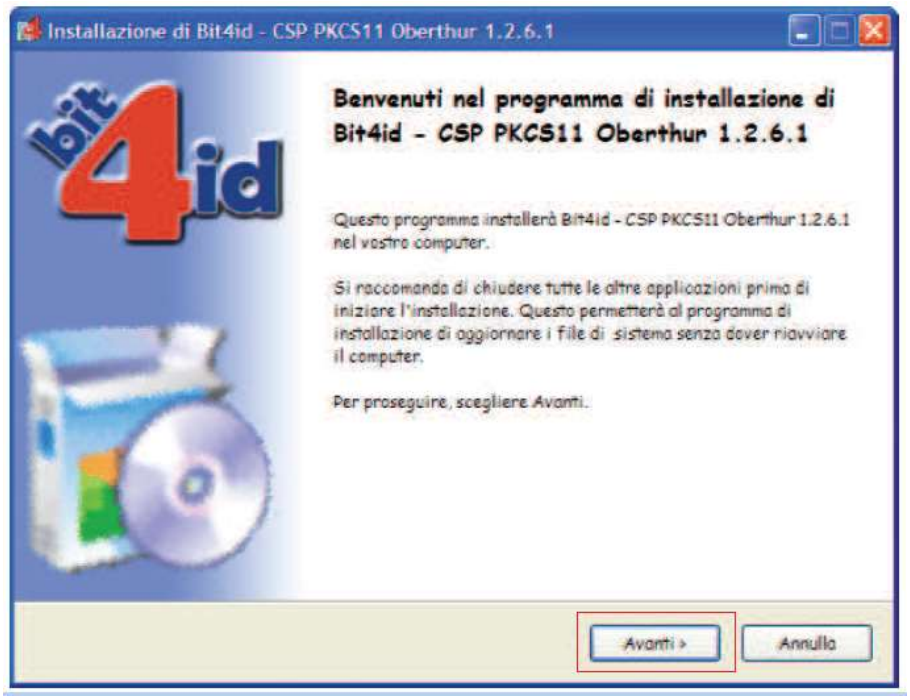
Importante: prima di avviare l'installazione dei driver, rimuovere il lettore dalla postazione (scollegare il lettore). È importante non confondere i driver delle smart card MP20 (bit4ID) con quelli delle carte HC19 (SSC API). In caso di dubbio, consultare il paragrafo specifico di questo manuale o contattare l'assistenza.

Avviare lo scarico dei DRIVER della smart card cliccando sul corrispondente link nella pagina http://firmadigitale.mps.it. L'installazione è differenziata a seconda del tipo di smart card.
N.B.: di seguito vengono descritti i passaggi necessari per **le smart card MP20xxxx**. Per l'installazione dei vecchi driver fino a HC19xxxx consultare il paragrafo apposito in appendice.
Preferibilmente utilizzare browser come Explorer o Chrome.
Fare clic sul percorso di scarico del software (http://firmadigitale.mps.it), facendo attenzione a selezionare quello coerente con il Sistema Operativo usato (32 o 64 bit):

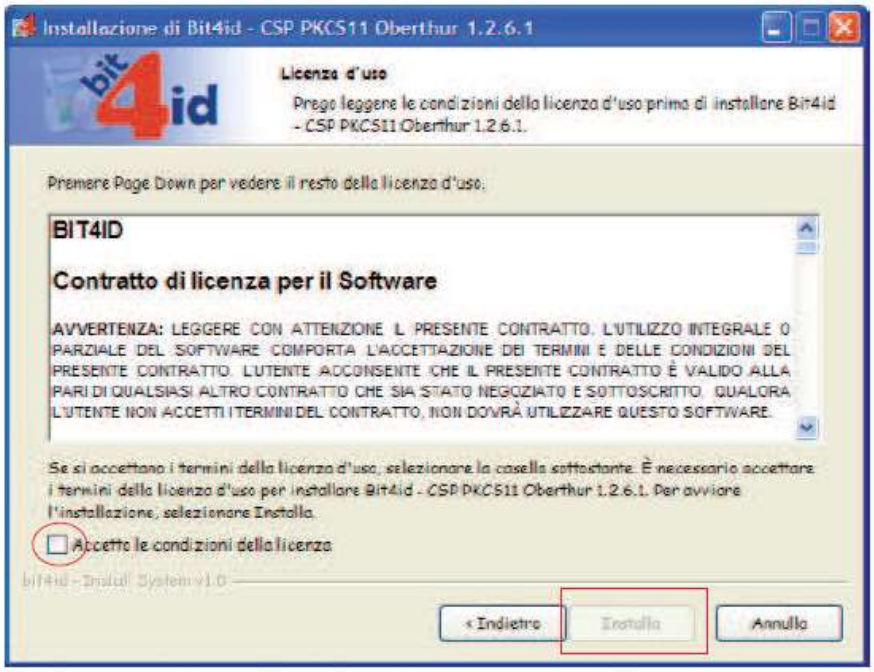


Il programma scaricato è compresso (cartella .zip). Estrarre il file da installare ("estrai tutto" con un programma di decompressione, es. Unzip) Avviare l'esecuzione con doppio click sul programma e proseguire seguendo le indicazioni dell'installazione consigliata.

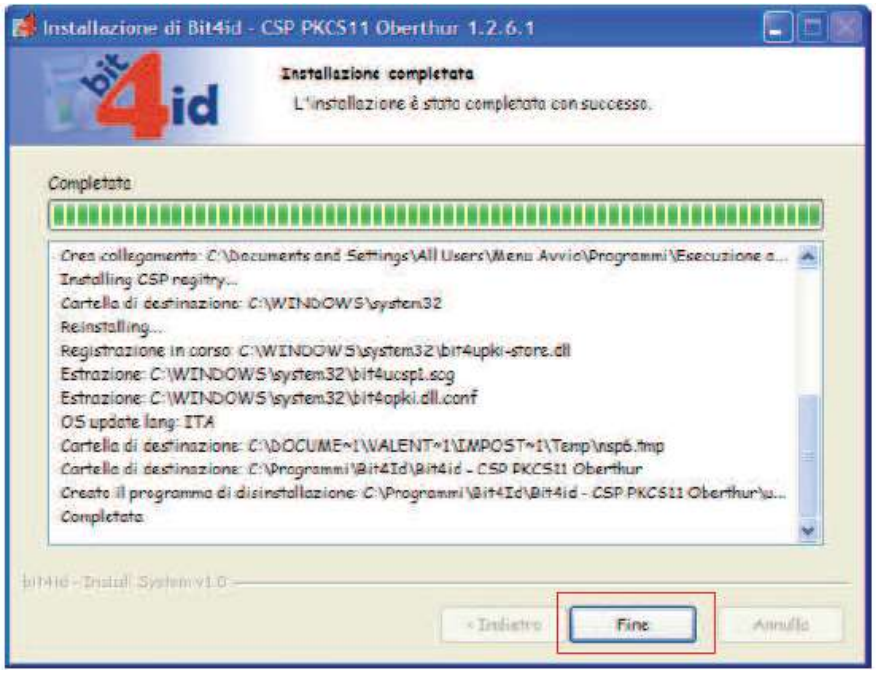
Se già collegato il lettore smart-card al computer disconnetterlo e poi fare click su AVANTI.



Fare click sul pulsante INSTALLA; in questo modo partirà la procedura di installazione dei driver.



Fare click su FINE. Se richiesto dal sistema operativo, riavviare il computer (tipicamente sui sistemi meno recenti).



L'installazione prosegue in automatico: confermare il percorso consigliato fino a che non sarà installato l'ultimo driver[2].
Se l'installazione è andata a buon fine, nell'area di notifica del sistema operativo si avrà l'icona del software di gestione della carta: (bit4id).

[2] Quando viene richiesto se spuntare la casella TIPO LETTORE: BIT4IDMINILECTOR, attivare la spunta se si sta usando un computer con SO pari o precedente a Windows XP (driver per la retro-compatibilità).

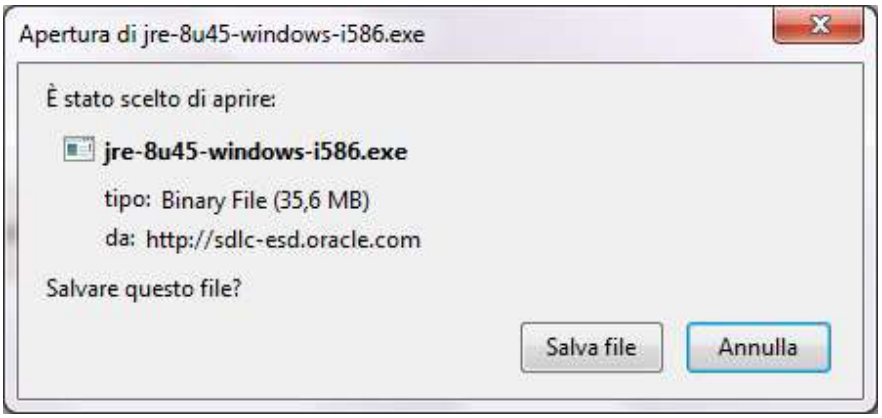
A questo punto è possibile ricollegare il lettore e la smart card. Cliccando sull'icona si apre il relativo programma: controllare che la carta sia correttamente visibile. In caso contrario contattare l'assistenza per ripetere l'installazione.

Per poter utilizzare la tessera con Mozilla Firefox è necessario effettuare un'abilitazione specifica (cfr. appendice).

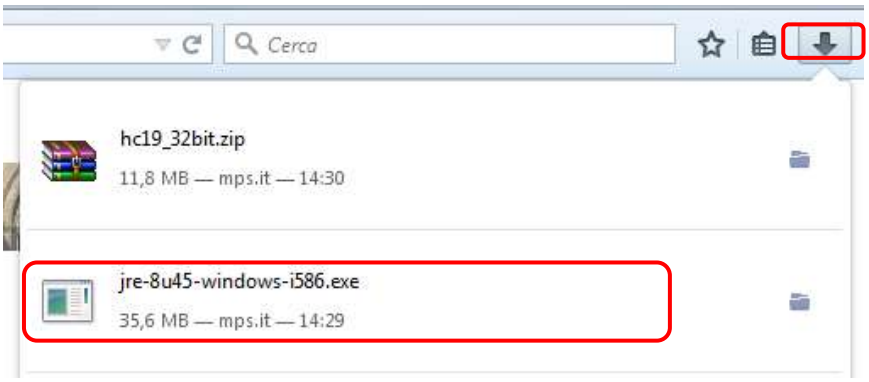
SCARICO E INSTALLAZIONE DI JAVA

NOTA BENE: Se sul computer è già presente la versione indicata a video di JAVA, allora questa installazione non è necessaria. Nel caso invece non fosse presente la versione richiesta di JAVA e si provasse a procedere con l'installazione di File Protector ugualmente, un avviso bloccante durante l'installazione di quest'ultimo ricorderebbe la necessità di installare JAVA nella versione consigliata.

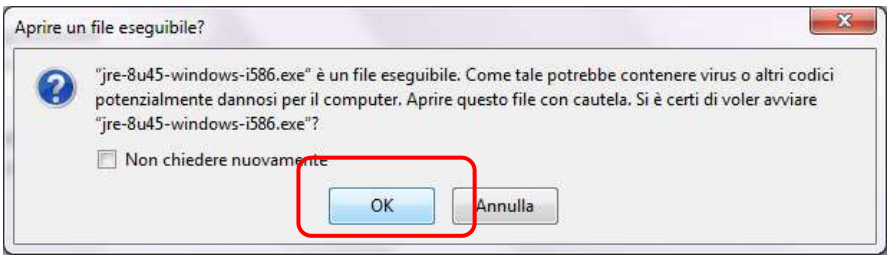
Avviare lo scarico di JAVA cliccando sul link nella pagina http://firmadigitale.mps.it.



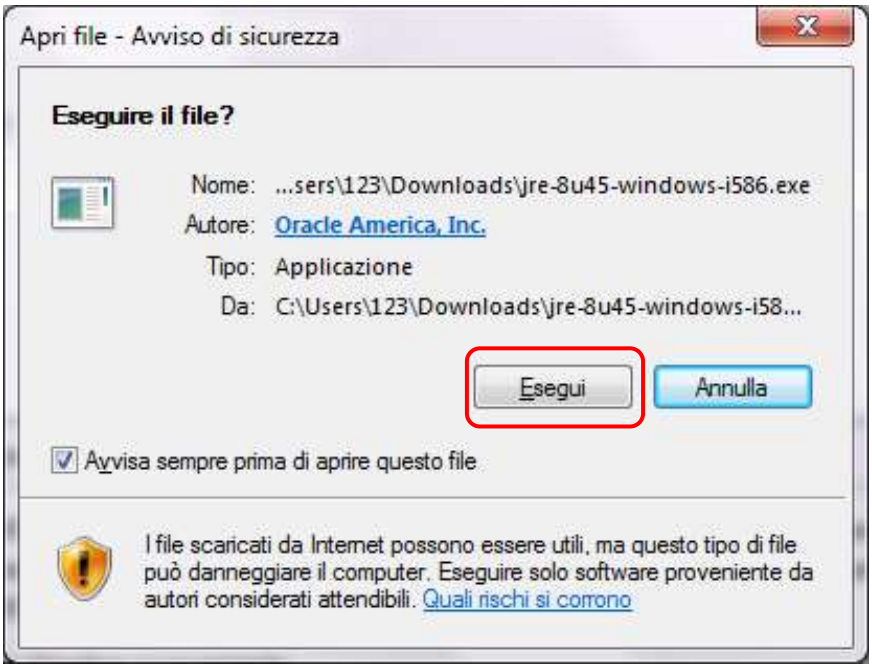
Salvare il file. Quindi identificare il file salvato ed eseguirlo (doppio click).



Un apposito avviso informa che si sta eseguendo un programma. Confermare con OK.



Confermare con ESEGUI.



A questo punto occorre verificare in quale cartella installare JAVA. La cartella proposta in default dalla procedura è C:\Program Files\ oppure C:\Program Files (x86) a seconda che il SO sia a 32 o 64 bit (x86 compare solo per quelli a 64 bit). Mantenere la cartella impostata dal SO a meno che siano verificate entrambe le seguenti condizioni:

- si sta operando su una postazione a 64 bit
- e la smart card da utilizzare **ha una serie HC19 o precedente**

Se entrambe queste condizioni sono verificate, allora modificare il percorso di installazione eliminando **(x86)**:

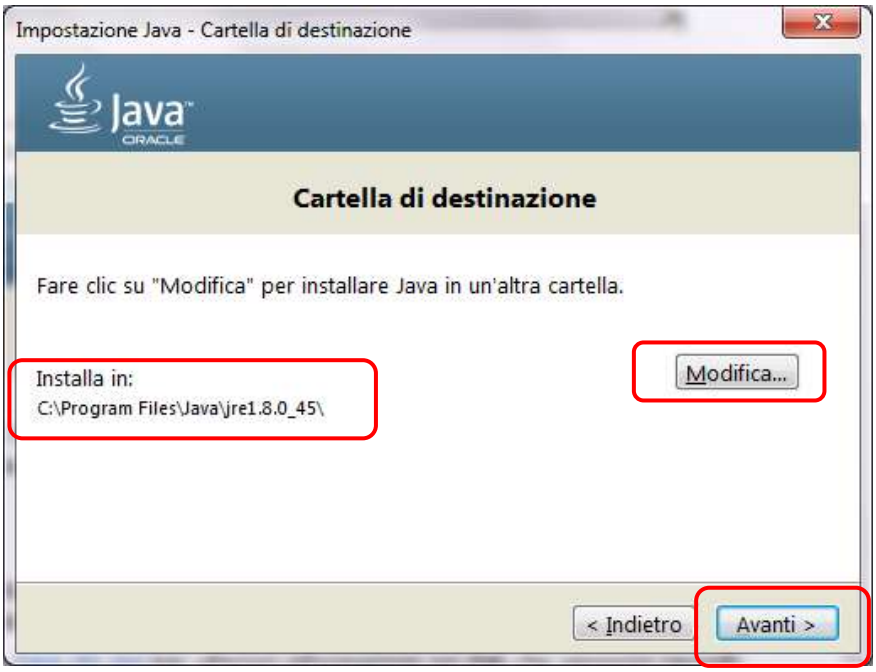
- C:\Program Files (x86)\ … diventa C:\Program Files\...

Per fare questo è necessario intervenire sul tasto MODIFICA CARTELLA DI DESTINAZIONE e selezionare il percorso di installazione desiderato tramite il tasto MODIFICA. Infine cliccare su AVANTI.

Riepilogando le istruzioni sono le seguenti:

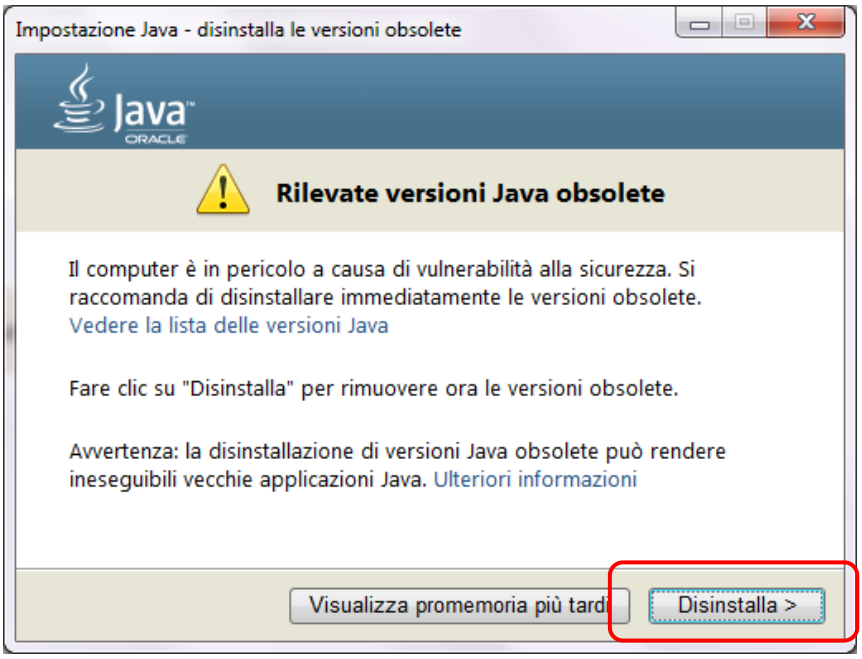
- il SO è a 64 bit **E** - la smart card è di serie HC19 o inferiore	Modificare il percorso di installazione eliminando (x86)
- in tutti gli altri casi	Mantenere il percorso di installazione impostato automaticamente

Cliccare su AVANTI per terminare l'installazione.

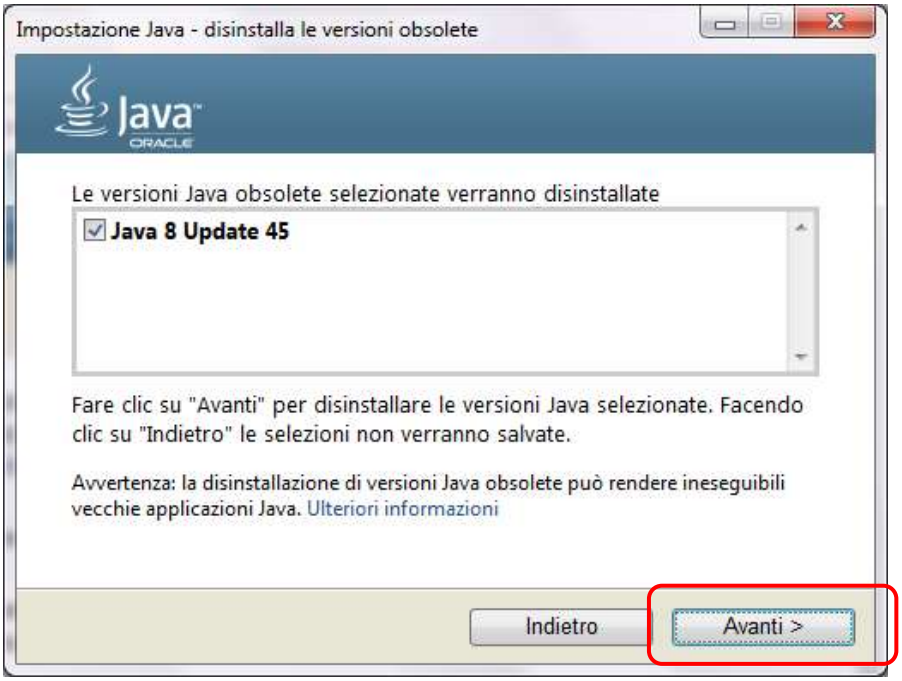


L'installazione dura pochi minuti e una progress bar indica il tempo d'attesa rimanente.

Se sulla postazione sono presenti versioni JAVA superate il programma avvisa con il messaggio sotto riportato ed è possibile provvedere immediatamente alla disinstallazione.



N.B.: è consigliabile verificare, soprattutto in caso di postazione di lavoro aziendale, se la disinstallazione di precedenti versioni di java possano interferire con altri programmi che invece ne abbiano bisogno. Dopo questa verifica, se l'esito è negativo, cliccare su AVANTI per disinstallare versioni preesistenti.

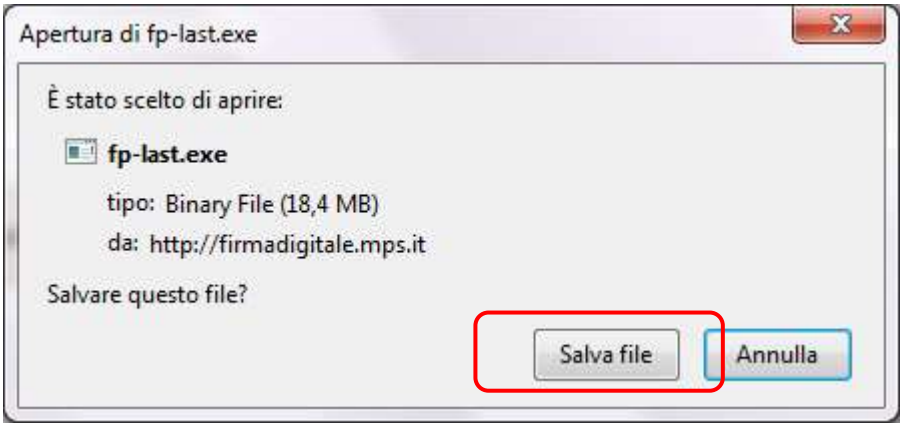


A questo punto un messaggio informa l'utente che l'installazione è stata completata.

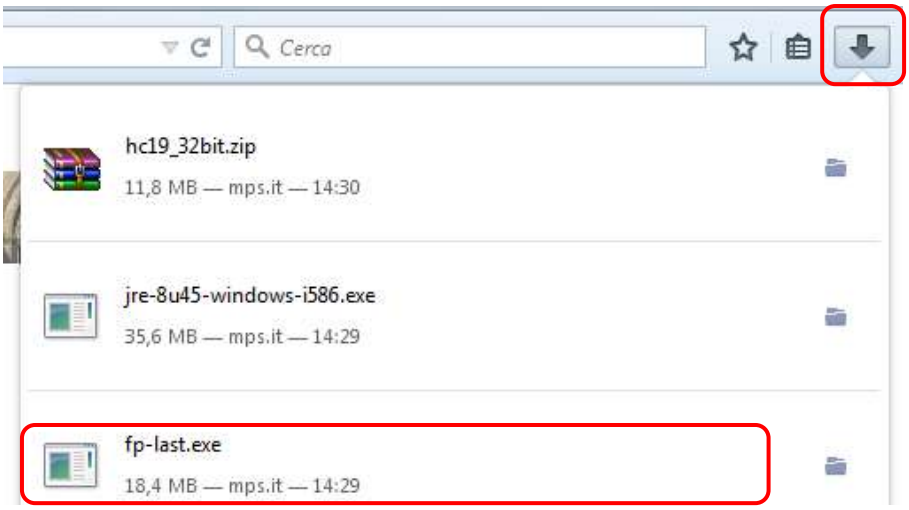
Si può passare all'installazione dell'elemento successivo.

SCARICO E INSTALLAZIONE DI FILE PROTECTOR

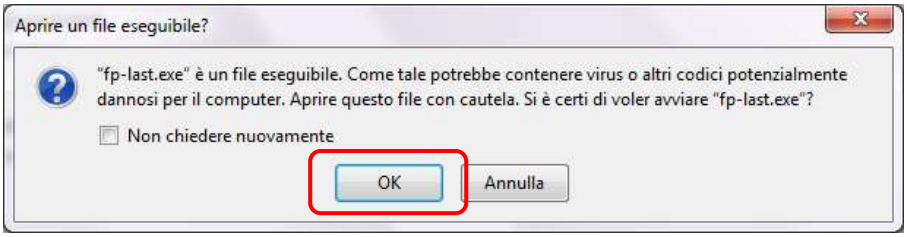
Avviare lo scarico di FILE PROTECTOR cliccando sul link nella pagina http://firmadigitale.mps.it.



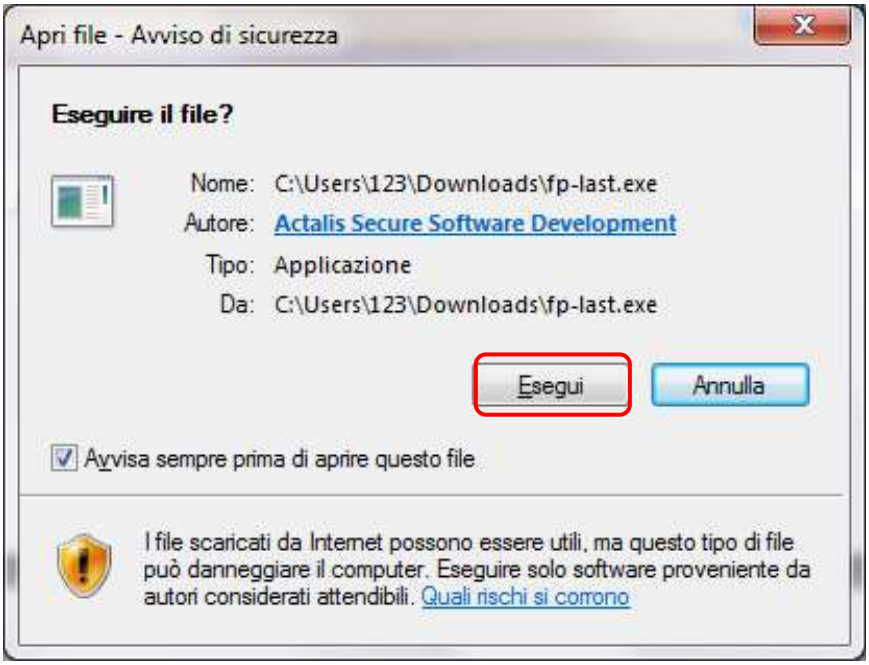
Salvare ed eseguire il file.



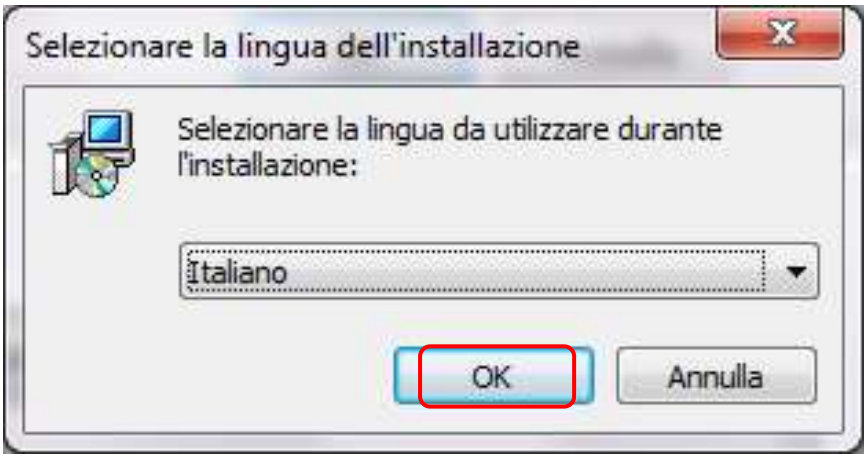
Premere OK al messaggio che si sta eseguendo un programma.



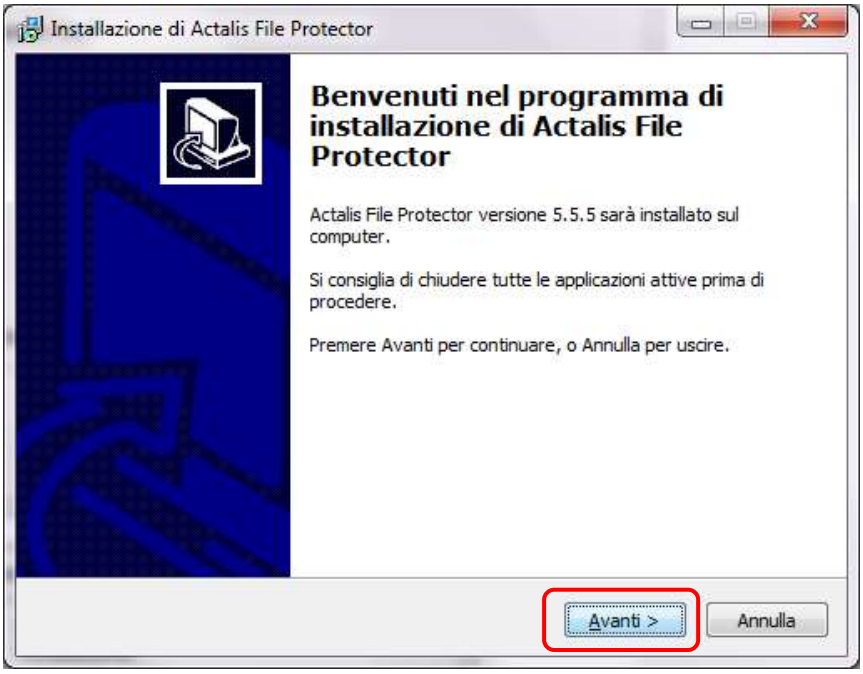
Cliccare su ESEGUI.



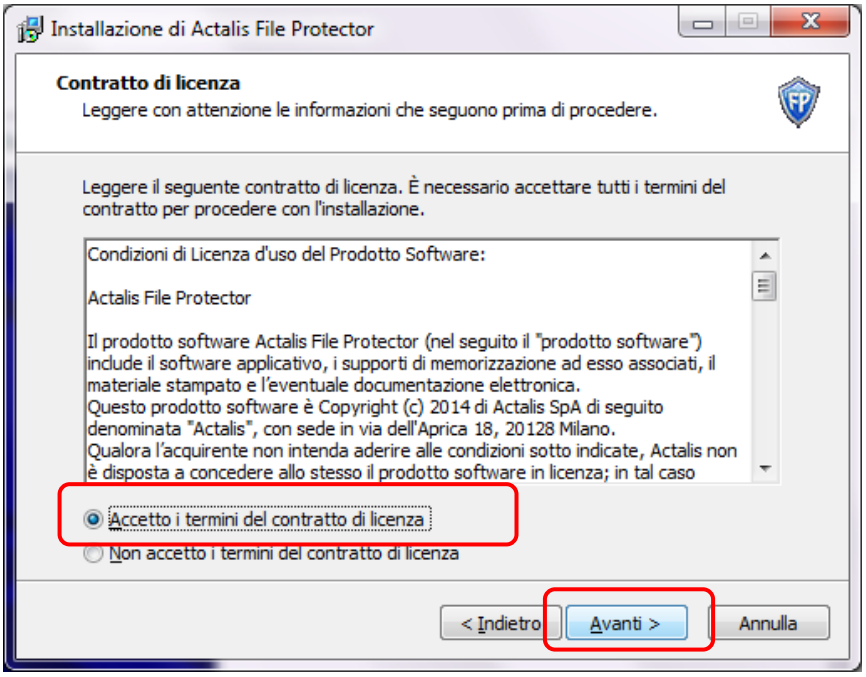
Selezionare la lingua preferita per l'applicazione.



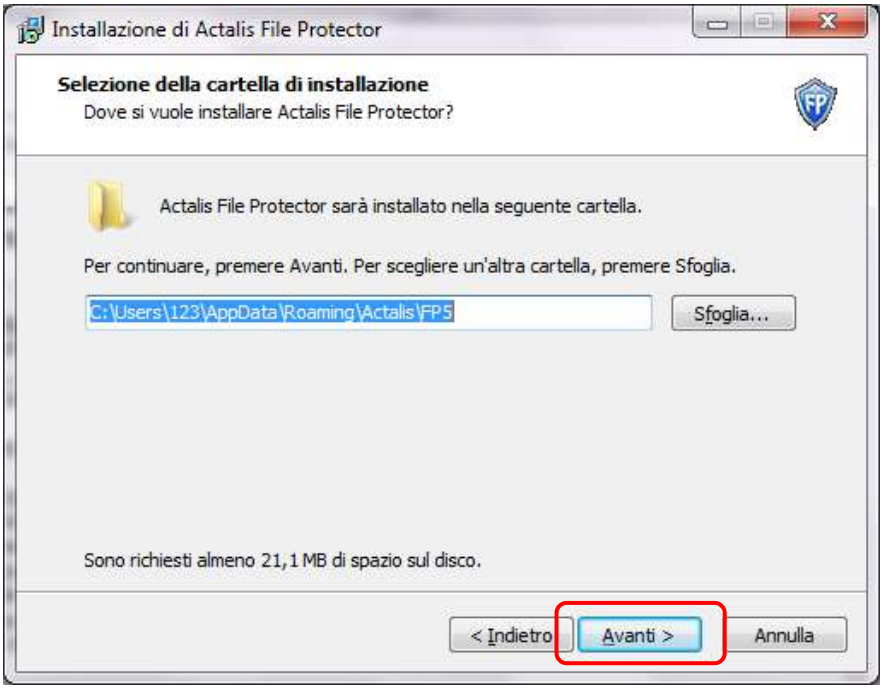
Cliccare su AVANTI per iniziare l'installazione vera e propria.



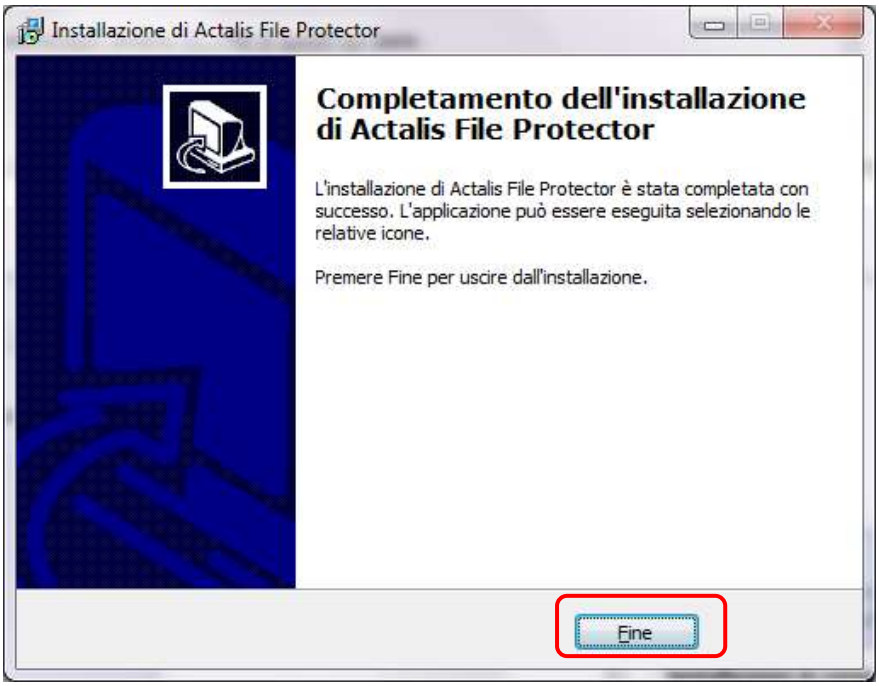
Accettare i termini del contratto di licenza



Verificare il percorso proposto per l'installazione e poi cliccare su AVANTI.



L'installazione dura alcuni minuti e anche in questo caso una progress bar indicherà il tempo residuo d'attesa (l'installazione dell'ultima versione avrà una numerazione che differisce da quella indicata nella figura soprastante, in quanto il software viene continuamente arricchito e perfezionato). Al termine dell'installazione cliccare su FINE.

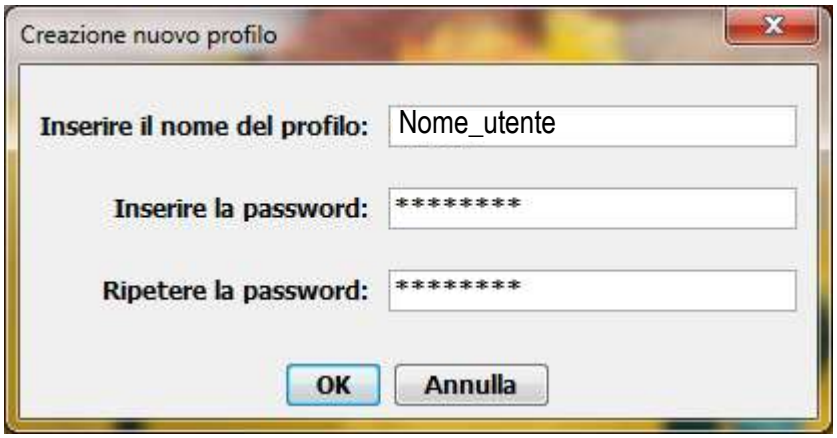


Sul desktop si deve trovare la seguente icona, da utilizzare per lanciare l'applicazione FILE PROTECTOR quando si inizierà ad usare la firma digitale.

CONFIGURAZIONE DI FILE PROTECTOR (APPLICATIVO DI FIRMA)

Per iniziare a usare la firma digitale è necessario (sola al primo accesso) effettuare la configurazione. Aprire **File Protector** con doppio click sull'icona creata sul desktop o richiamando il programma dalle applicazioni. In automatico il programma riconosce che non è presente alcun profilo utente e ne richiede la creazione.

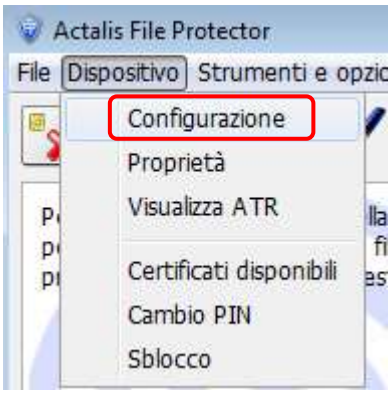
È possibile inserire il nome desiderato (non ci sono limitazioni particolari) e la password di propria scelta.



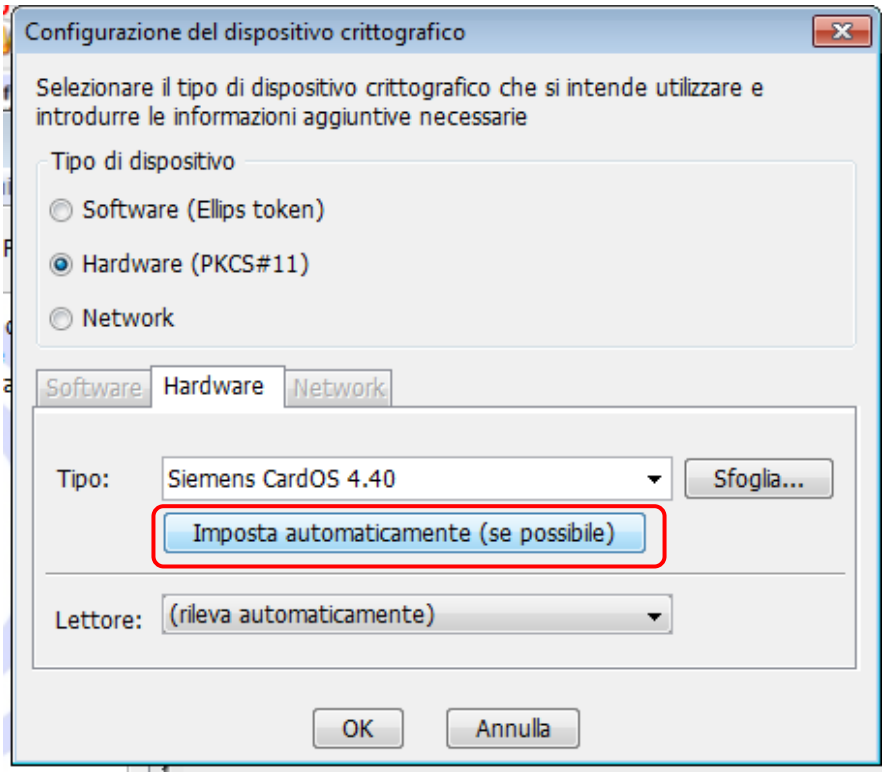
Dopo aver creato il profilo di accesso si apre l'applicazione di firma File Protector.

Dopo l'accesso è necessario eseguire la configurazione della smart card (solo la prima volta).

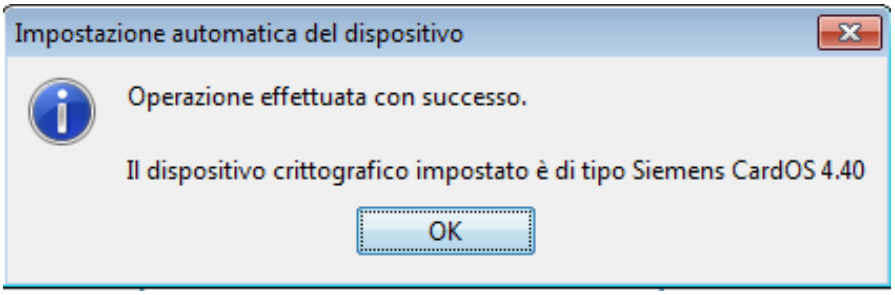
Dal menù DISPOSITIVO cliccare su CONFIGURAZIONE.



Cliccare su IMPOSTA AUTOMATICAMENTE.



Per le smart card fino a HC19 il tipo viene impostato con "Siemens CardOS 4.40". **Per le smart MP20 invece si deve impostare "Incard CNS"**. Confermare con OK 2 volte.



Dopo la configurazione è possibile fare il login e scaricare i certificati di firma.

RICHIESTA (SCARICO) DEL CERTIFICATO DI FIRMA

In questa sezione è descritta la procedura per richiedere un certificato di Firma Digitale. É possibile utilizzare due diverse modalità:

- accedendo a File Protector;
- accedendo al Portale web dei Servizi Actalis.

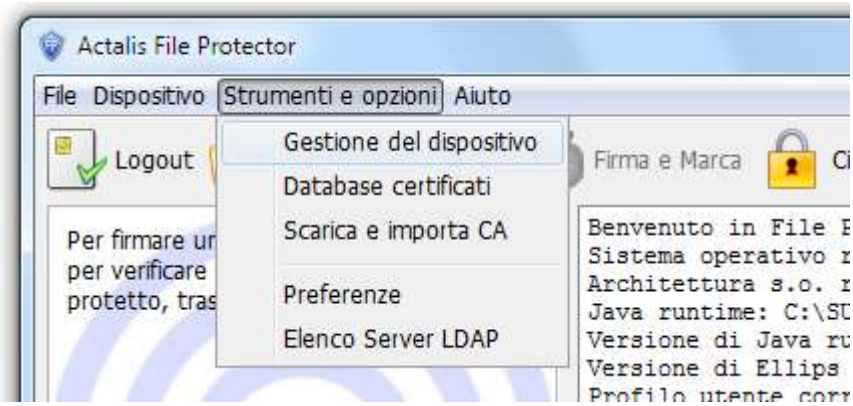
Le 2 modalità sono alternative. Illustriamo entrambe di seguito.

RICHIESTA DI CERTIFICATO DA FILE PROTECTOR

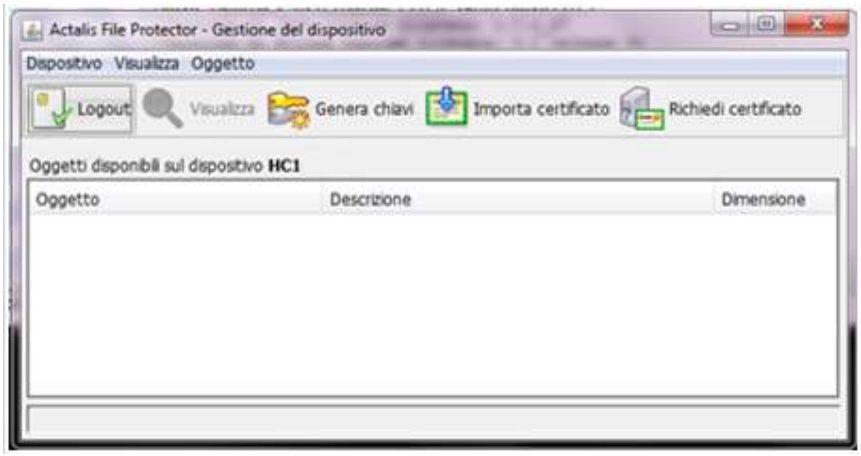
Inserire la smartcard nel relativo lettore e collegarlo al proprio PC. Avviare il programma File Protector

Effettuare il login inserendo il PIN della smart card.

Da **Strumenti e opzioni** cliccare su **Gestione del dispositivo**.



Si apre una nuova finestra.



Cliccare su **Richiedi certificato** e poi su **Avanti**.

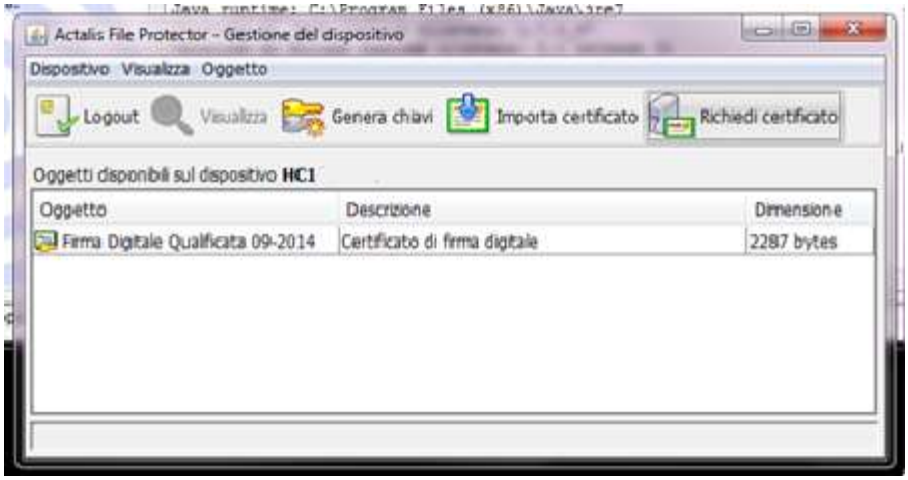
Nella nuova finestra di Identificazione dell'utente digitare il proprio CODICE FISCALE e il CODICE RISERVATO PERSONALE (C.R.P.) ricevuto in fase di identificazione da parte della Banca.

Cliccare su **Prosegui** e poi su **OK**. L'applicazione procede automaticamente con tutti i passi necessari per la creazione della credenziale di firma digitale. Durante la procedura l'utente non deve compiere alcuna azione.

Una volta terminata la procedura di cui alla figura precedente, l'applicazione mostra all'utente una finestra di dialogo recante il codice di revoca. Il codice può essere necessario all'utente nel caso desideri richiedere alla CA (tramite telefono o web) la revoca del proprio certificato.

Salvare in un file di testo o annotare il codice di revoca e cliccare su **Prosegui**. La procedura si conclude cliccando sul pulsante **OK** presente nella finestra di dialogo mostrata nella figura seguente.

Nel dispositivo ora è presente il Certificato di firma digitale.



Una volta scaricato il certificato la propria firma digitale può essere utilizzata tramite il software File Protector.

PORTALE DEI SERVIZI ACTALIS: RICHIESTA DEL CERTIFICATO

In alternativa alla richiesta da File Protector è possibile attivare la richiesta di certificato direttamente dal sito del certificatore. Se si utilizza questo metodo accedere con il browser Internet Explorer (non raccomandato Edge o altro browser). Inserire la smartcard nel relativo lettore e collegarlo al proprio PC. Accedere al Portale dei Servizi Actalis al seguente indirizzo web: https://portal.actalis.it.

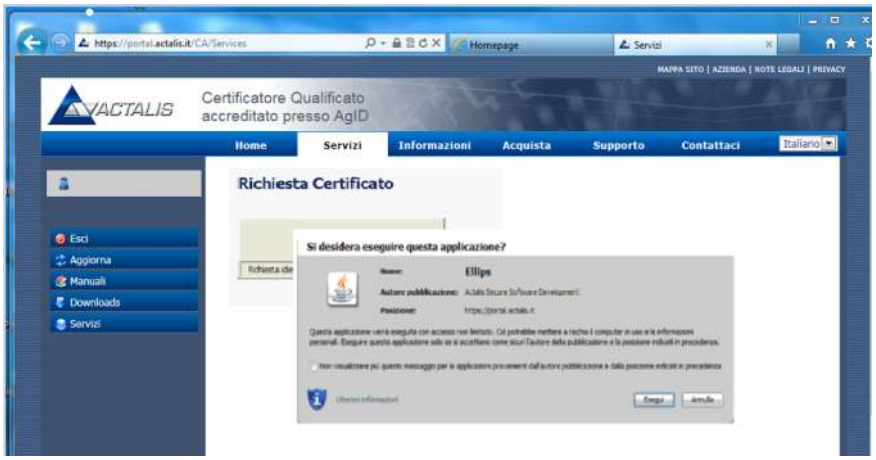
Una volta collegati al Portale dei Servizi Actalis, è necessario autenticarsi tramite le credenziali CODICE FISCALE e CODICE RISERVATO PERSONALE (C.R.P.) che l'utente ha ricevuto in fase di identificazione da parte della Banca.

Una volta inseriti i valori richiesti nell'area ACCESSO CLIENTI, cliccando sul bottone LOGIN, apparirà la pagina descritta nella figura seguente:

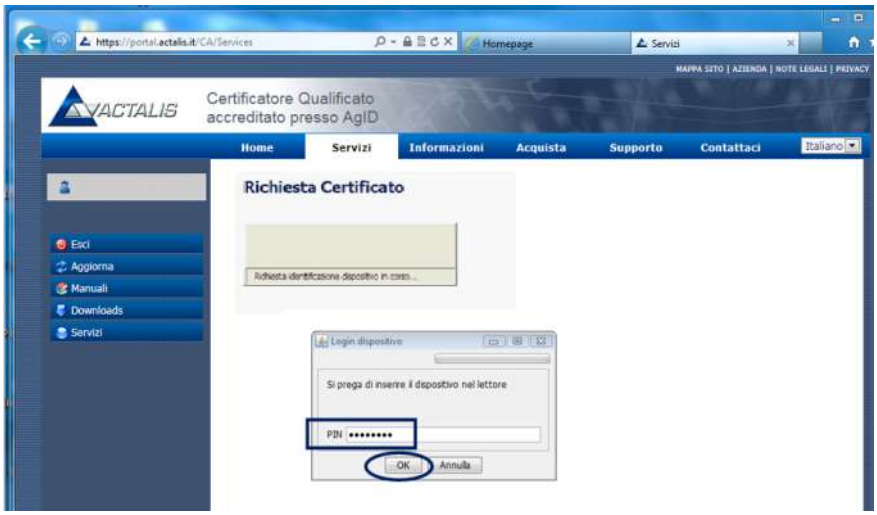
Se fossero disponibili più certificati autorizzati, l'utente deve semplicemente procedere con la richiesta per il certificato di **FIRMA DIGITALE QUALIFICATA**. Premere quindi sull'icona **Richiesta Certificato.**

N.B.: non tenere in considerazione il contenuto del messaggio presente nella pagina che invita ad effettuare la "pulizia del token" (non è un caso che riguarda le smart card di firma digitale).

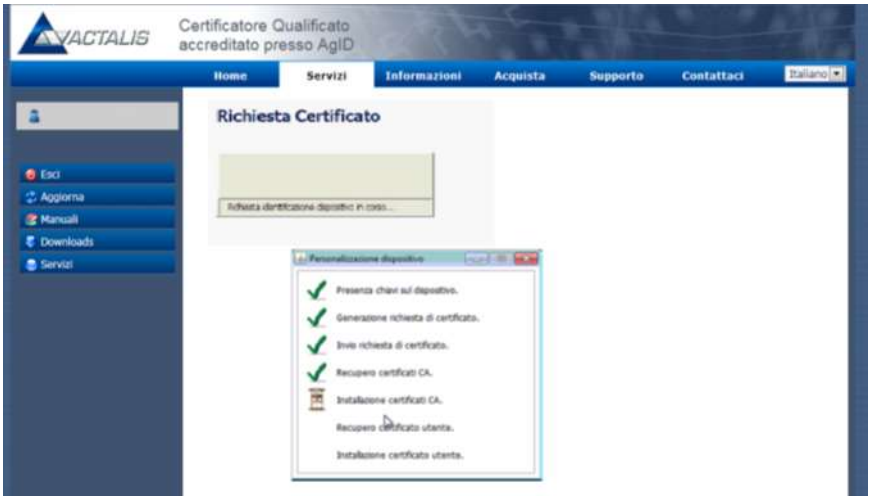
Inizia la fase di caricamento dell'applicazione incaricata di effettuare tutti i passi necessari per la creazione della credenziale di Firma Digitale Qualificata.



Una volta completato il caricamento dell'applicazione, questa richiede all'utente il PIN d'acceso al dispositivo. Per procedere, quindi, inserire il PIN della smart card e premere su **OK**.



A questo punto, verificata la correttezza del pin appena inserito, l'applicazione procede con la creazione della credenziale di firma digitale qualificata. Durante la transizione tra ciascuna di queste operazioni, l'utente non deve compiere alcuna azione.

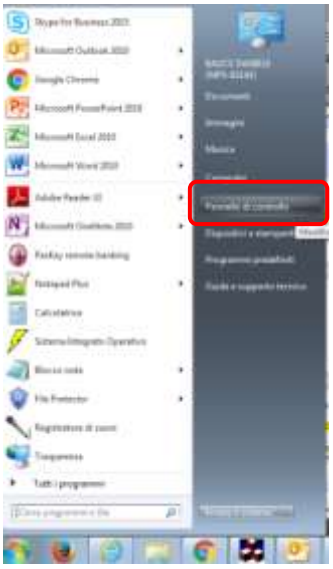


Una volta terminata la procedura di cui alla figura precedente, l'applicazione mostra all'utente una finestra di dialogo recante il codice di revoca. Tale codice può essere necessario all'utente nel caso desideri richiedere alla Certification Authority (tramite telefono o web) la revoca del proprio certificato. L'utente può annotare tale codice o salvarlo in un file di testo.

A questo punto è possibile concludere la procedura, arrivando alla finestra mostrata nella figura seguente.

DISINSTALLAZIONE

Nel caso in cui sia necessario rimuovere le applicazioni di firma o a queste collegate (es. java) è consigliabile partire dal PANNELLO DI CONTROLLO.

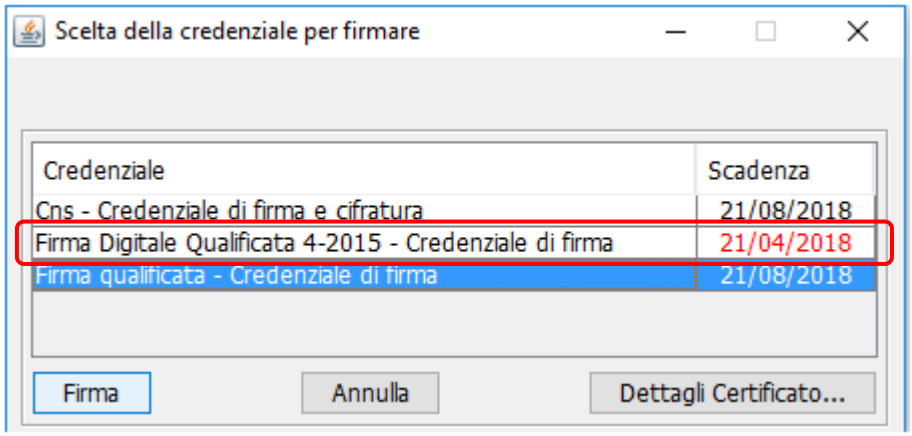


Individuare l'applicazione da rimuovere nell'elenco e cliccarci sopra con il tasto destro del mouse. Compare il tasto DISINSTALLA, utile a rimuovere l'applicazione. Si può procedere analogamente per le varie componenti del pacchetto di firma digitale.

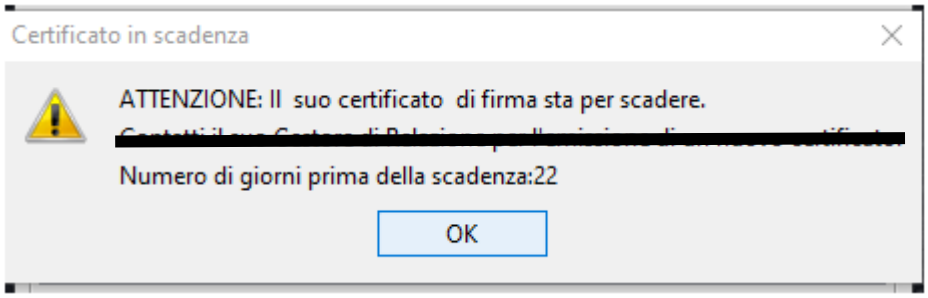
RINNOVO DEL CERTIFICATO TRAMITE PORTALE WEB

In questa sezione è descritta la procedura per rinnovare un certificato di Firma Digitale. Il rinnovo di un certificato può essere effettuato **autonomamente dall'utente nei 30 giorni antecedenti la data di scadenza**. Fare attenzione a non fare scadere il termine senza rinnovare il certificato perché in questo caso è necessario recarsi nuovamente allo sportello per una nuova registrazione.

Per evidenziare che il certificato è prossimo alla scadenza, la scadenza è riportata con colore rosso quando si deve utilizzare la firma digitale.

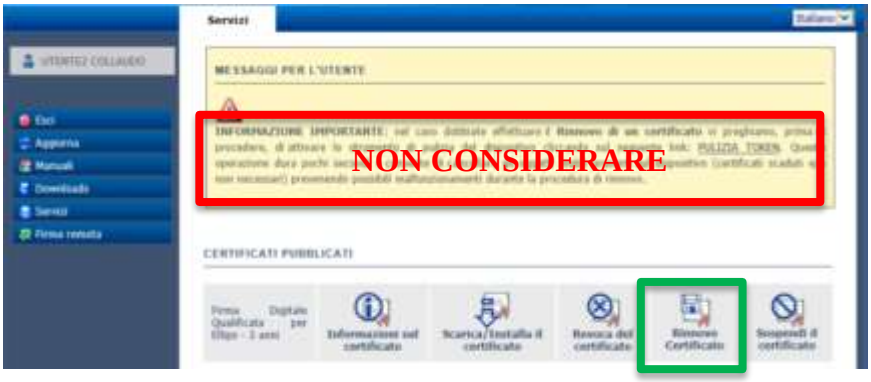


Un apposito messaggio avverte quanti giorni restano per effettuare l'operazione di rinnovo in autonomia. Solo dopo che il termine è scaduto diventa necessario invece contattare il gestore per l'emissione di un nuovo certificato.



Per rinnovare il certificato entro la scadenza inserire la smart card nel relativo lettore e collegarlo al proprio PC. Accedere al Portale dei Servizi Actalis al seguente indirizzo web: https://portal.actalis.it. Utilizzare il browser Internet Explorer preferibilmente (se si possiede Firefox, non utilizzare oltre la versione 41, che non supporta i plugin NPAPI).
Una volta collegati al Portale dei Servizi Actalis, è necessario autenticarsi tramite le credenziali CODICE FISCALE e CODICE RISERVATO PERSONALE (C.R.P.) che l'utente ha ricevuto in fase di identificazione da parte della Banca.

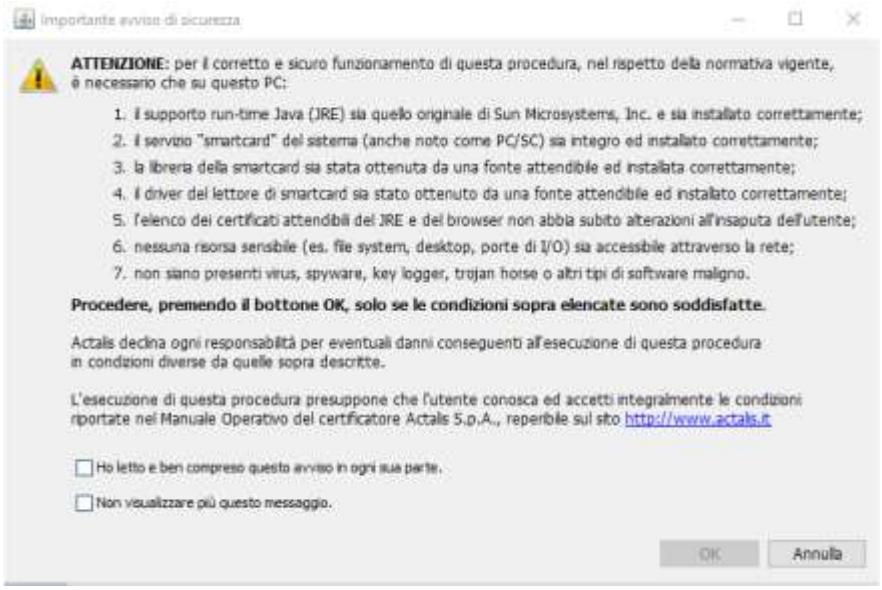
Dopo aver inserito le credenziali ACCESSO CLIENTI, cliccando sul bottone LOGIN, apparirà la pagina descritta nella figura seguente:



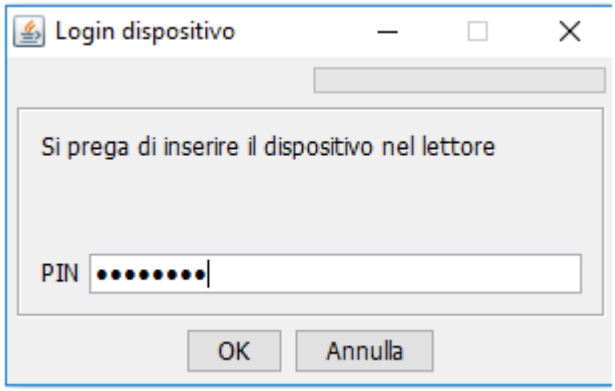
Non prendere in considerazione invece l'avviso su sfondo giallo di effettuare la "pulizia token": questo intervento NON va assolutamente eseguito.

N.B. Se fossero disponibili più certificati rinnovabili, l'utente dovrà procedere con la richiesta per quello di firma digitale qualificata.

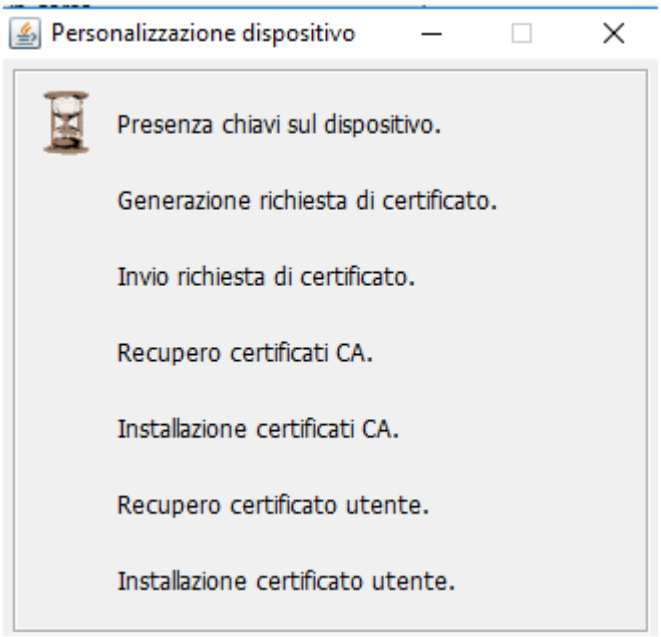
Prendere in esame i messaggi di sicurezza che vengono automaticamente visualizzati e procedere quindi alla spunta dei 2 check box in basso per proseguire:



Inserire il PIN:



Viene avviato il processo di rinnovo del certificato:



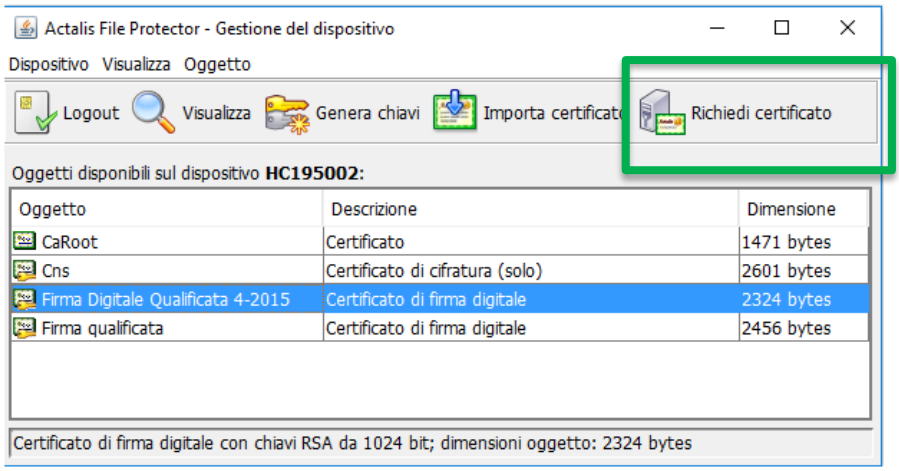
In automatico viene proposto di memorizzare (o di salvare in formato txt) il codice di revoca, utile appunto per revocare in caso di necessità la propria firma digitale in modo autonomo. Al termine un messaggio indica l'esito dell'operazione.

Una volta scaricato il certificato la propria firma digitale può essere utilizzata tramite il software File Protector, accedendo con il PIN consegnato nella busta della smart card.

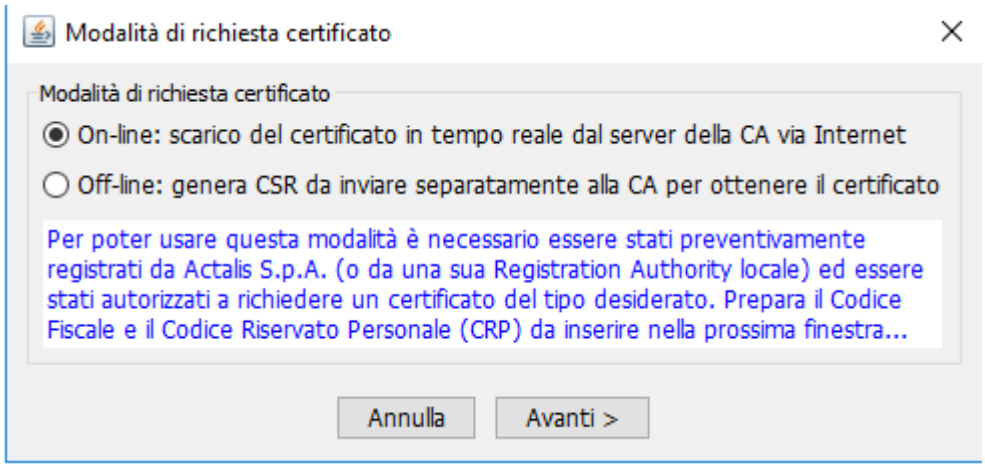
RINNOVO TRAMITE FILE PROTECTOR

Il rinnovo del certificato può essere eseguito **in alternativa** al portale web dal programma File Protector. Si accede dal menù Strumenti e opzioni > Gestione del Dispositivo.

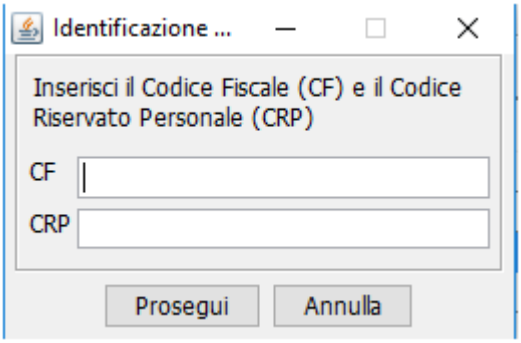
Si seleziona il certificato da rinnovare e poi si clicca su Richiedi certificato



Si conferma la modalità di scarico online.



Si inserisce il Codice Fiscale e il CRP per autenticare l'operazione.

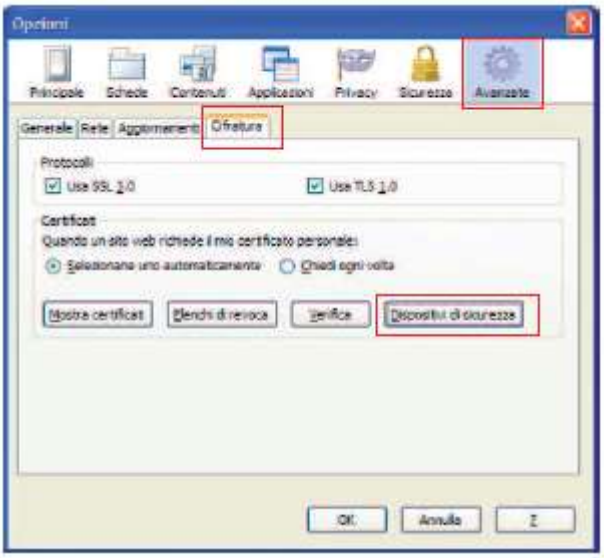


A questo punto i passaggi di creazione del rinnovo sono automatici ed analoghi a quelli della procedura via portale web.

APPENDICE 1 – CONFIGURAZIONE DELLA SMART CARD SU MOZILLA

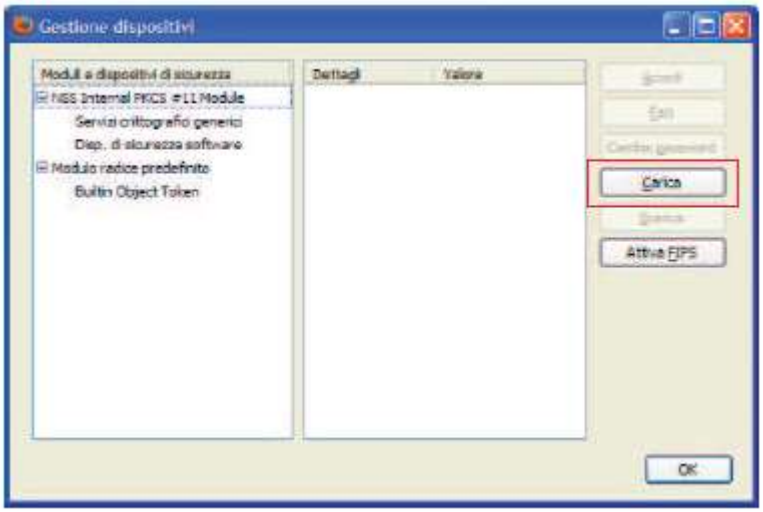
Per utilizzare la smart card sul browser Mozilla è necessario effettuare questi passaggi preliminari.

Passo 1: dal menu **Strumenti** selezionare la voce **Opzioni**. Nella finestra che si aprirà selezionare la sezione **Avanzate** e il tab **Cifratura** corrispondente. Fare click sul pulsante **Dispositivi di sicurezza**.



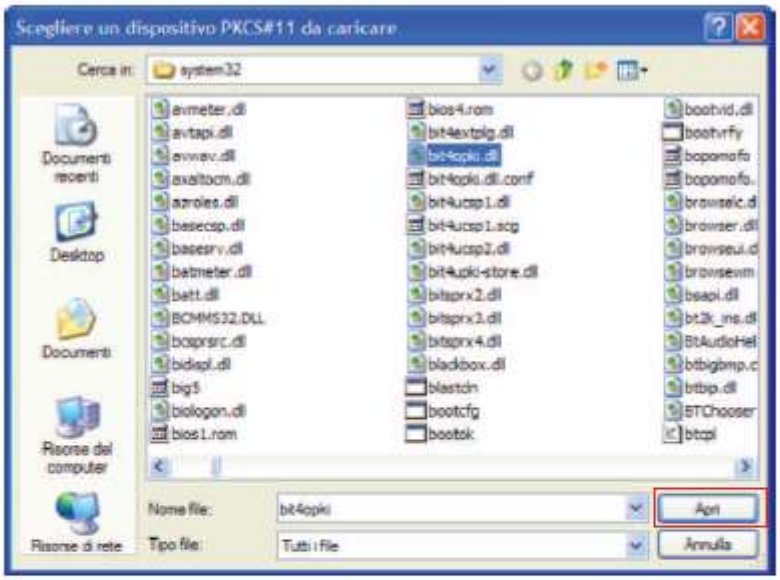
Si apre la finestra di **Gestione dispositivi** in cui bisogna caricare un nuovo dipositivo.

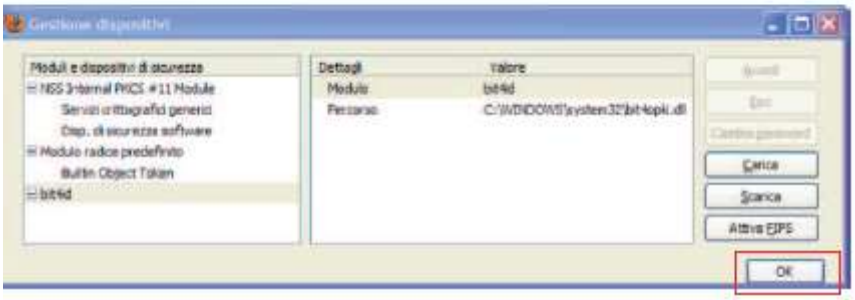
Passo 2: dal menu di destra fare click su pulsante **Carica:**



Si apre la finestra di **Caricamento di un nuovo dispositivo**.
Passo 3: inserire nel campo **Nome modulo** un nome identificativo del dispositivo. Nel campo **Nome file modulo** bisogna caricare il file bit4opki.dll che si trova nella directory C:\WINDOWS\system32 (o system a seconda del SO; in caso di bisogno rintracciare il percoso con "esplora risorse" e "cerca"). Fare click sul pulsante **Sfoglia**, andare alla directory sopra indicata, selezionare il file menzionato e fare click sul pulsante **Apri**.

Confermare facendo click sul pulsante OK della finestra **Carica** dispositivo e della finestra **Gestione dispositivo**.





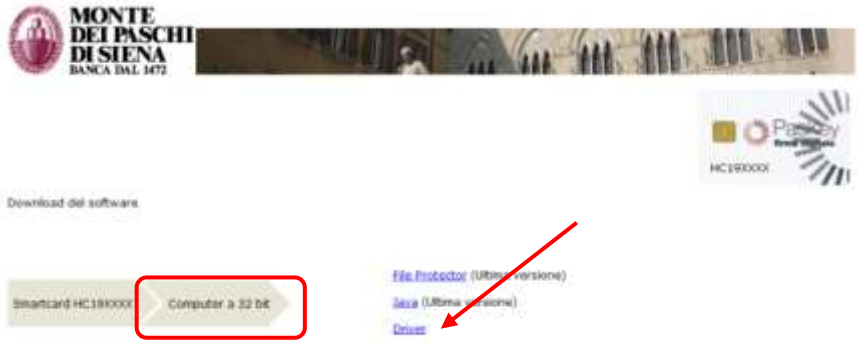
La procedura di installazione del nuovo dispositivo è completata.

APPENDICE 2 – DRIVER PER SMART CARD FINO A HC19 COMPRESE

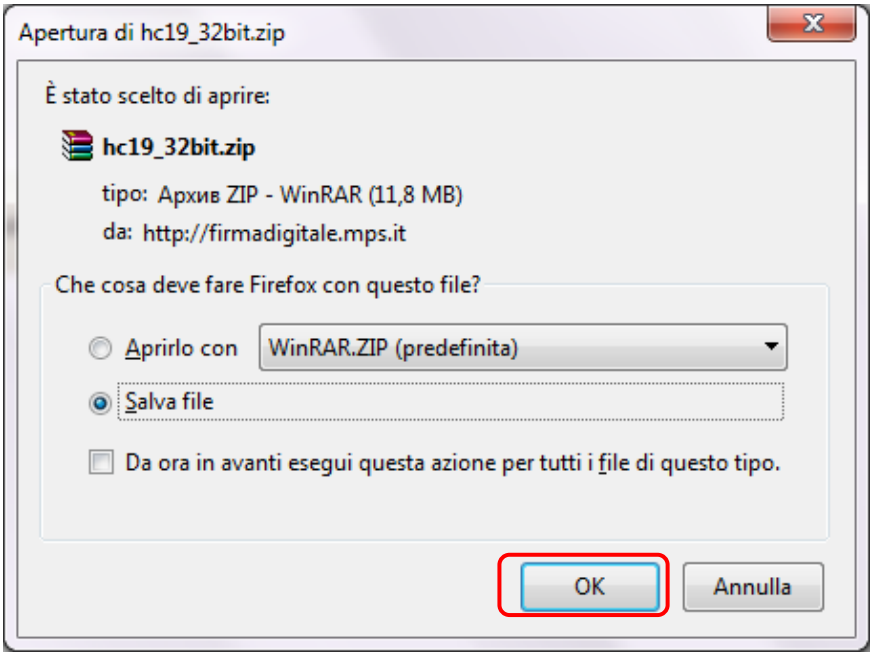
Utilizzare questa procedura per installare i driver delle vecchie smart card fino a HC19 comprese (di solito necessario quando si cambia computer). N.B.: i possessori di carte HC14XXXX devono preferibilmente procedere alla sostituzione della smart card con una di ultima generazione alla prima occasione utile, e comunque prima di un eventuale rinnovo.

Scollegare il lettore con la smart card prima di procedere con l'installazione effettiva.

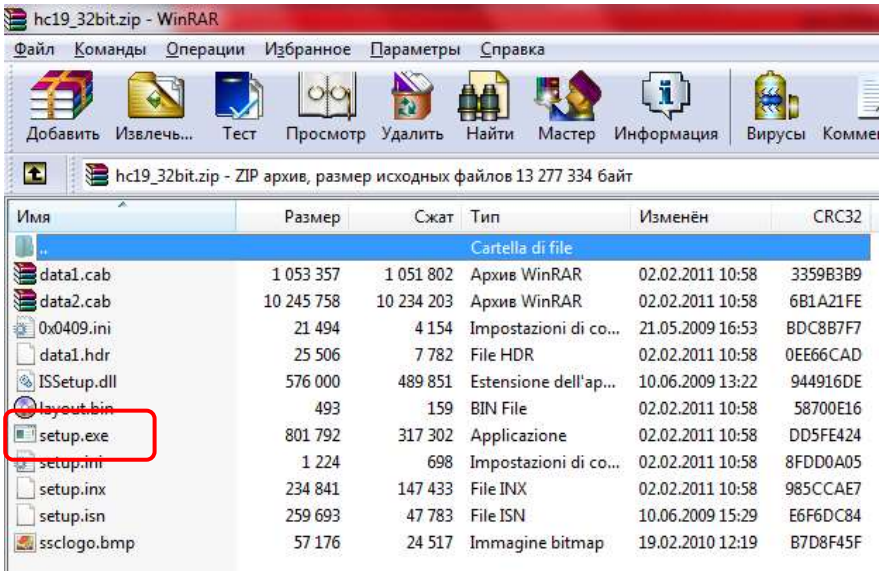
Fare clic sul percorso di scarico del software (http://firmadigitale.mps.it), facendo attenzione a selezionare quello coerente con il SO usato (32 o 64 bit):



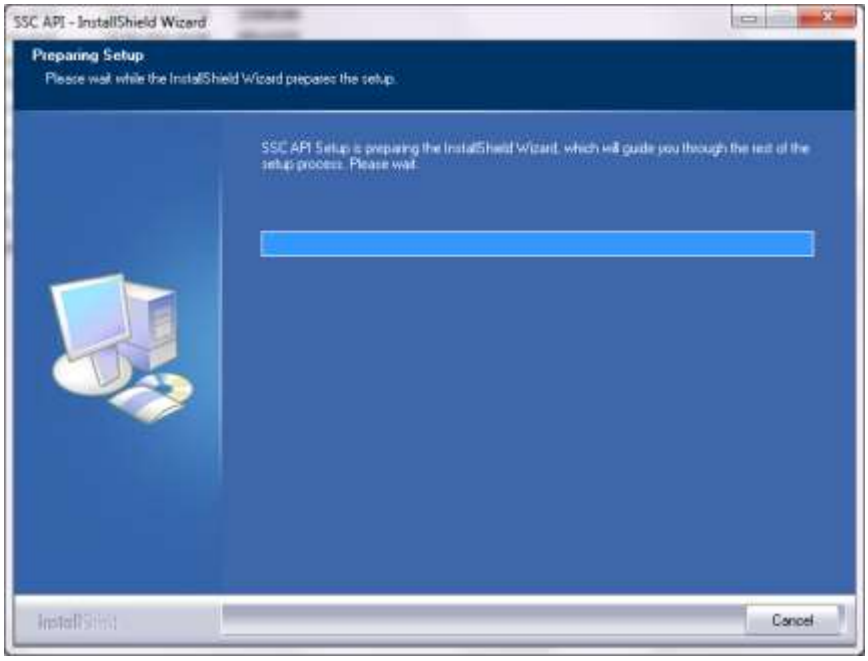
Aprire la cartella compressa per eseguire l'applicazione.



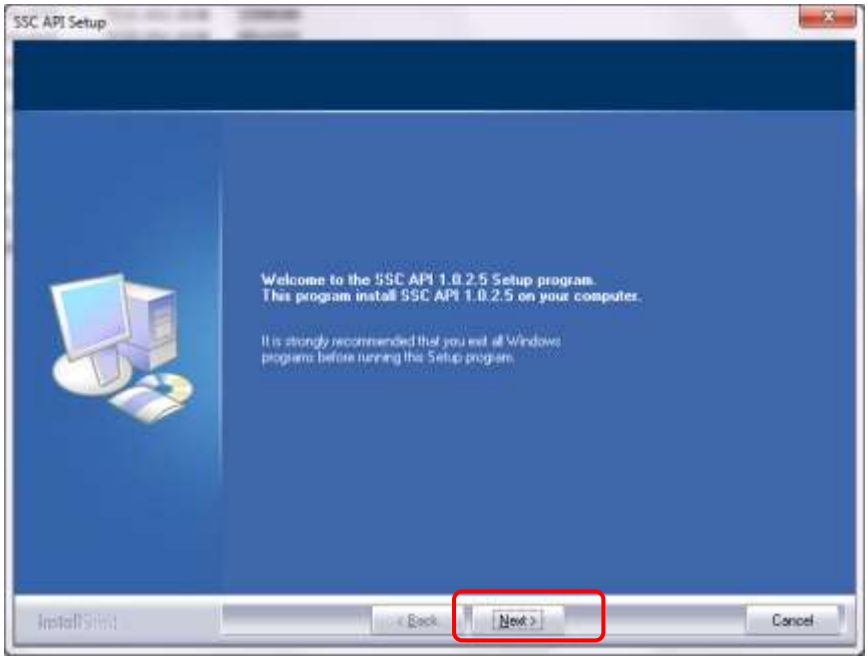
Salvare i driver ed estrarre i file in una cartella. Aprire la cartella e identificare il file SETUP.EXE, eseguendolo (doppio click).



Una progress bar indicherà che l'installazione è in corso.



Chiudere le applicazioni di Windows prima di procedere cliccando su NEXT.



A questo punto occorre verificare in quale cartella installare i driver di firma. La cartella proposta in default dalla procedura è C:\Program Files\ oppure C:\Program Files (x86) a seconda che il SO sia a 32 o 64 bit. Mantenere la cartella impostata dal SO a meno che siano verificate entrambe le seguenti condizioni:

- si sta operando su una postazione a 64 bit
- e la smart card da utilizzare ha una serie HC19 o precedente

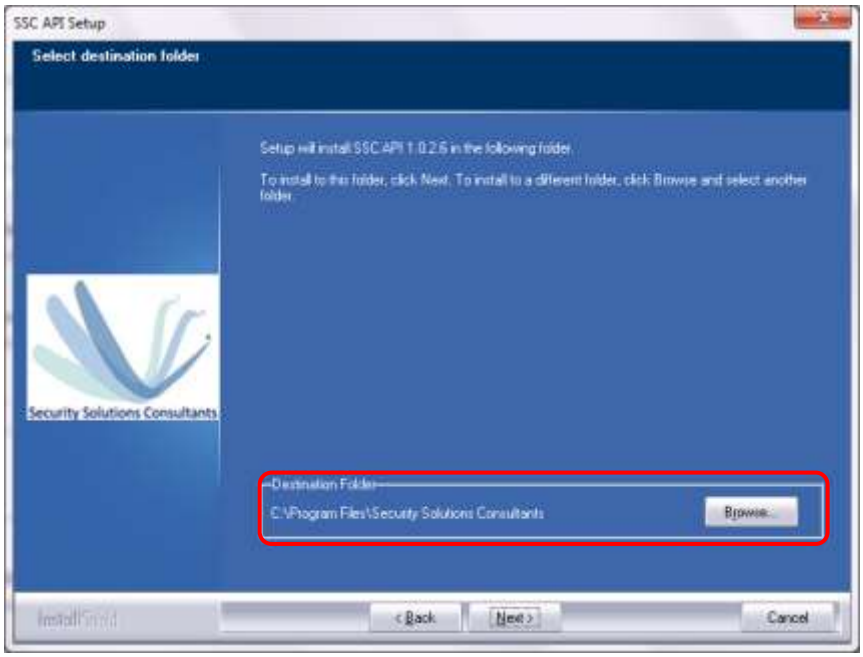
Se entrambe queste condizioni sono verificate, allora modificare il percorso di installazione eliminando **(x86)**:

- C:\Program Files (x86)\ … diventa C:\Program Files\...

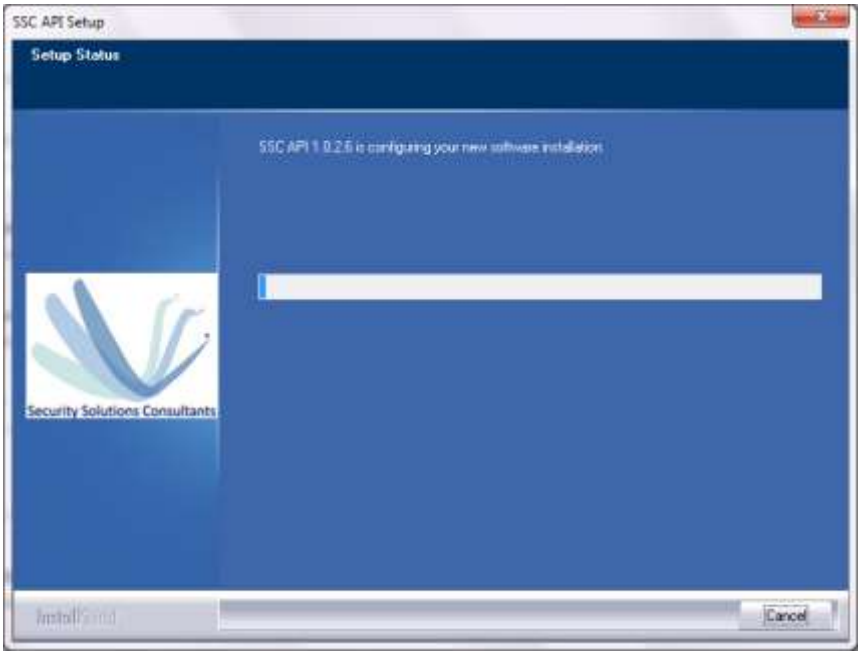
Per fare questo è necessario intervenire sul tasto BROWSE (sfoglia) e selezionare il percorso di installazione desiderato.

Riepilogando le istruzioni sono le seguenti:

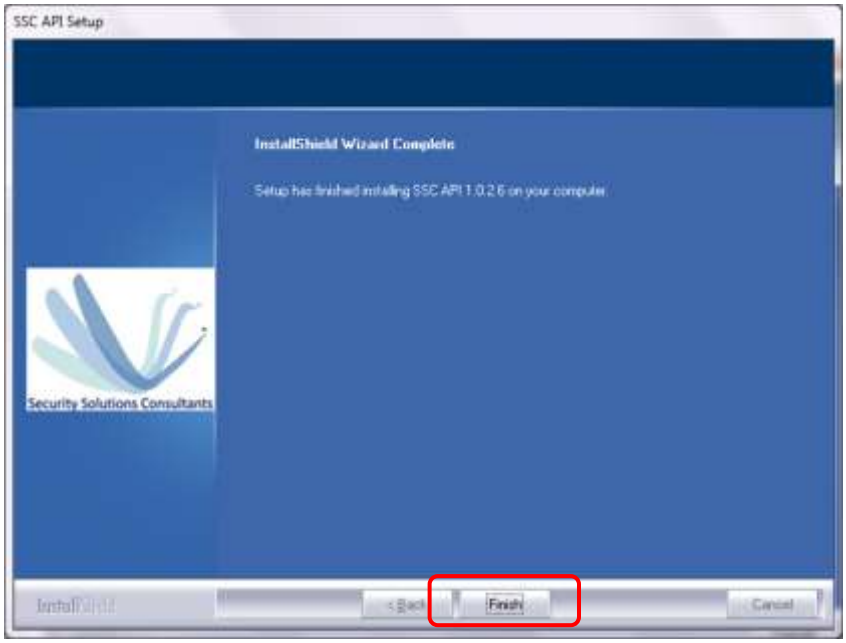
- il SO è a 64 bit **E** - la smart card è di serie HC19 o inferiore	Modificare il percorso di installazione eliminando (x86)
- in tutti gli altri casi	Mantenere il percorso di installazione impostato automaticamente



Dopo aver cliccato NEXT l'installazione passa alla fase finale.



Un avviso indica che l'installazione è completata.

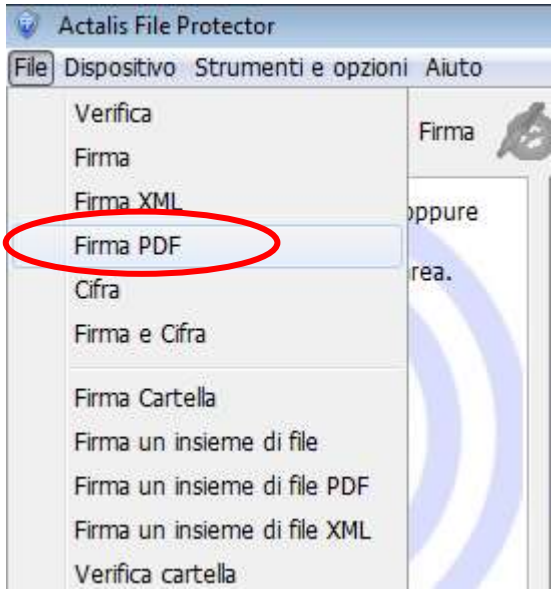


Cliccare su FINISH per chiudere l'installazione. Chiudere anche l'applicazione WINRAR utilizzata per leggere i file compressi (o altra dello stesso tipo).
A questo punto sul computer compaiono i driver di firma (SCardPinMngr – applicazione per gestire il PIN della smart card).

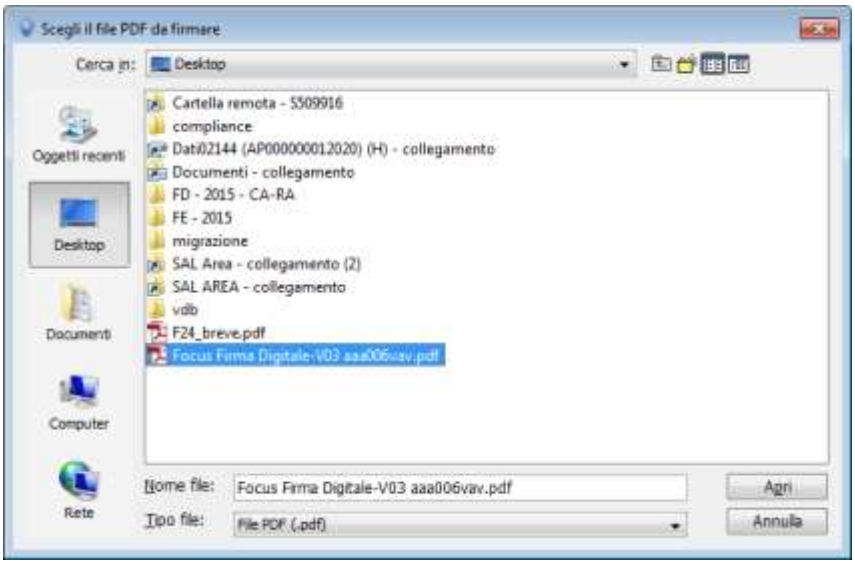
Aprendo tale applicazione, dopo aver ricollegato il lettore e la smart card, si può controllare se la carta viene riconosciuta correttamente. In caso negativo, contattare l'assistenza tecnica.

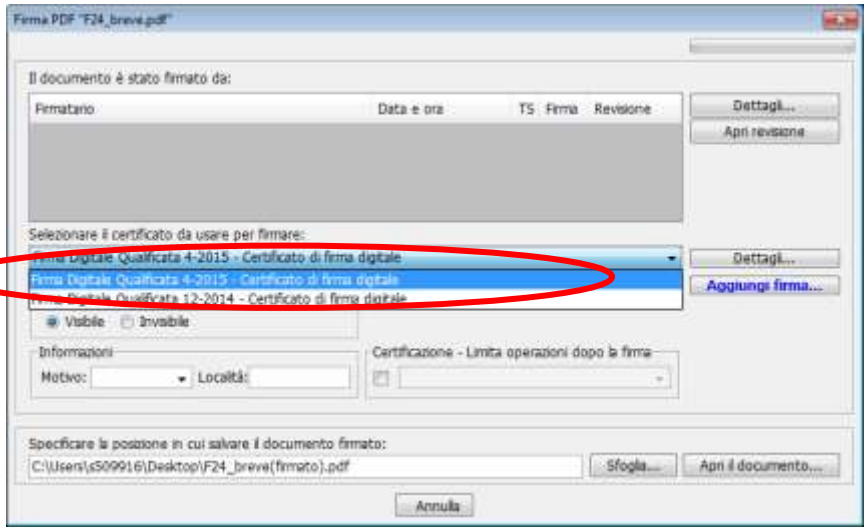
APPENDICE 3 – FIRMA PDF CON FILE PROTECTOR

Aprire File Protector > File > Firma PDF

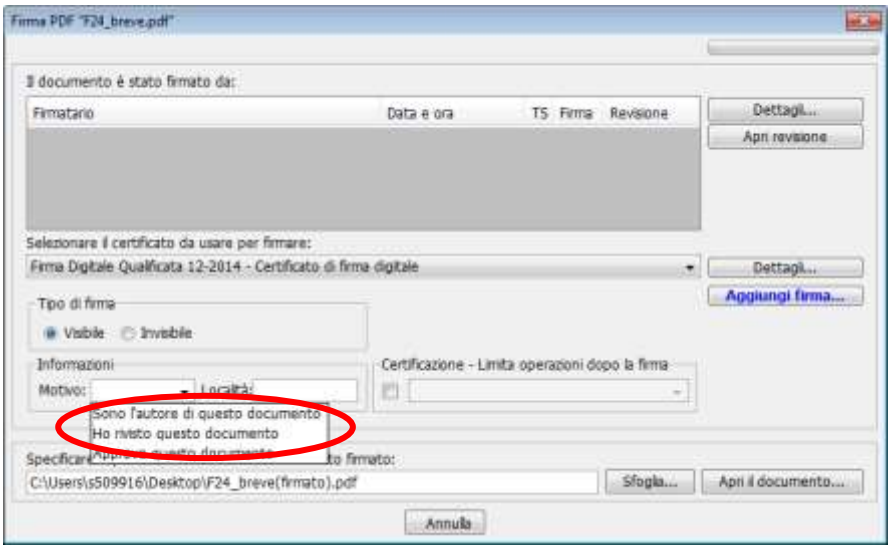


Selezionare il file da firmare.

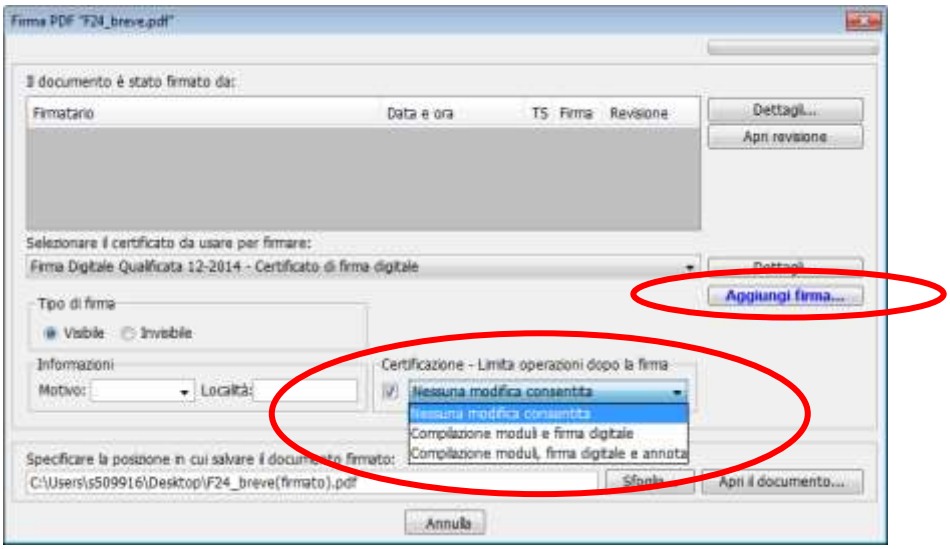




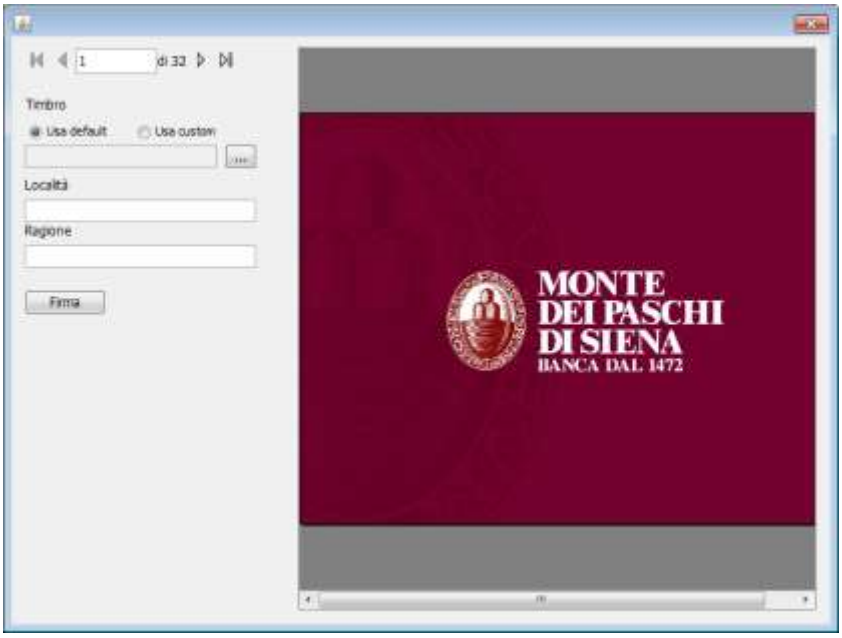
Se il firmatario ha più certificati di firma, selezionare quello desiderato. Impostare anche il motivo di firma ritenuto meglio rispondente al proprio caso (approvazione, revisione, ecc.).



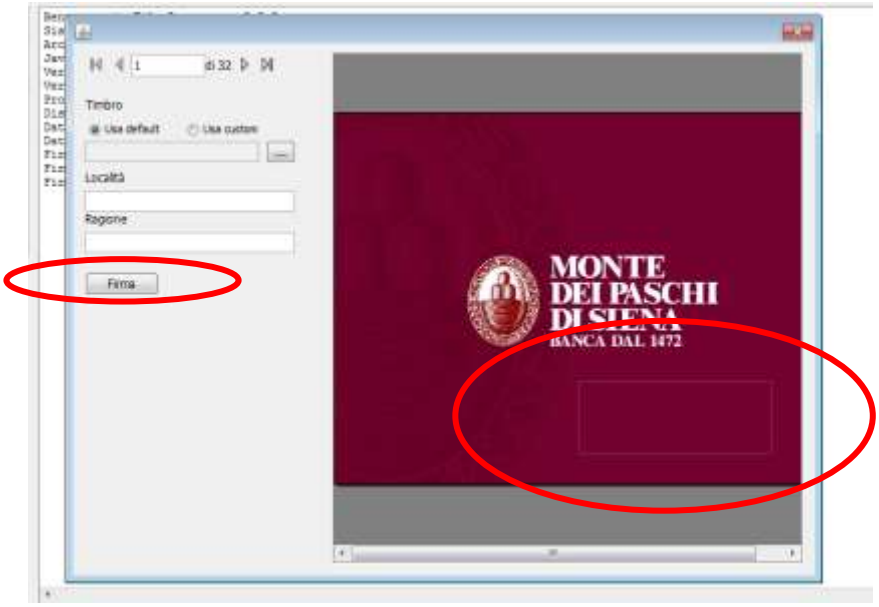
Al termine cliccare su AGGIUNGI FIRMA per firmare il documento.

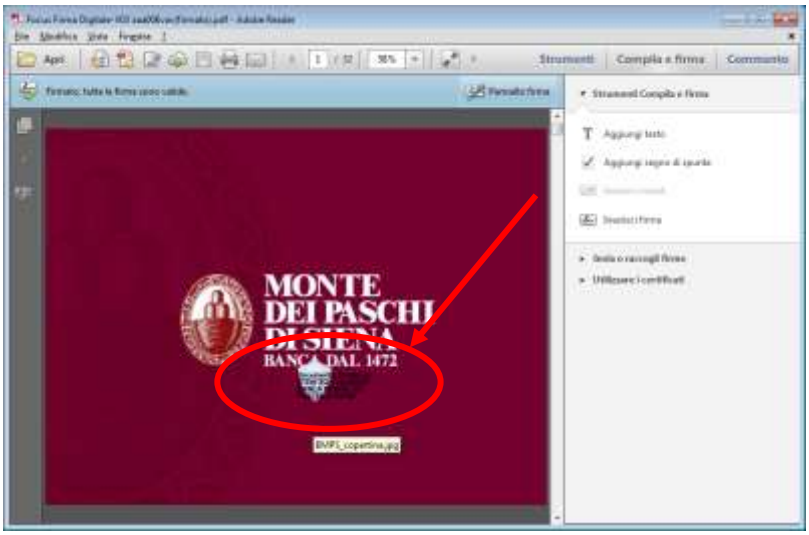


Nella pagina che si apre compare il documento sul quale andrà apposta la firma, come nella figura che segue.



Cliccare su firma e disegnare con il mouse un rettangolo che sarà lo spazio destinato ad accogliere la firma digitale.



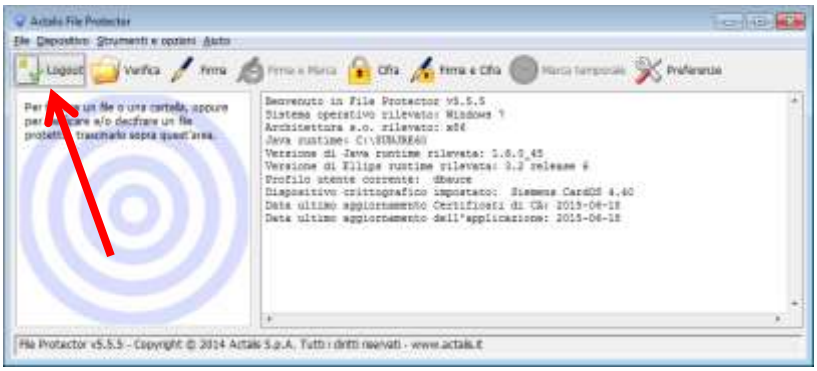


APPENDICE 4 – IMPORTARE IL CERTIFICATO NEL DATABASE PERSONALE

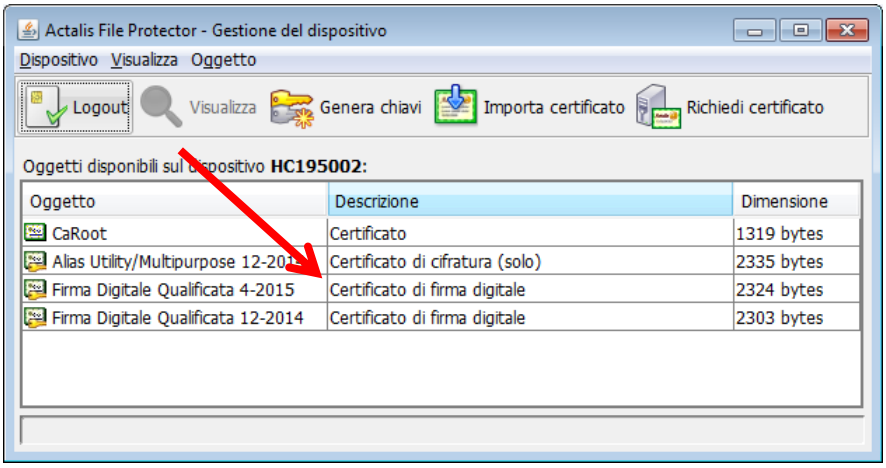
Scopo: far sì che il sistema, quando verifica un documento firmato da quel certificato, lo riconosca come certificato attendibile.

Accedere a File Protector e inserire il PIN

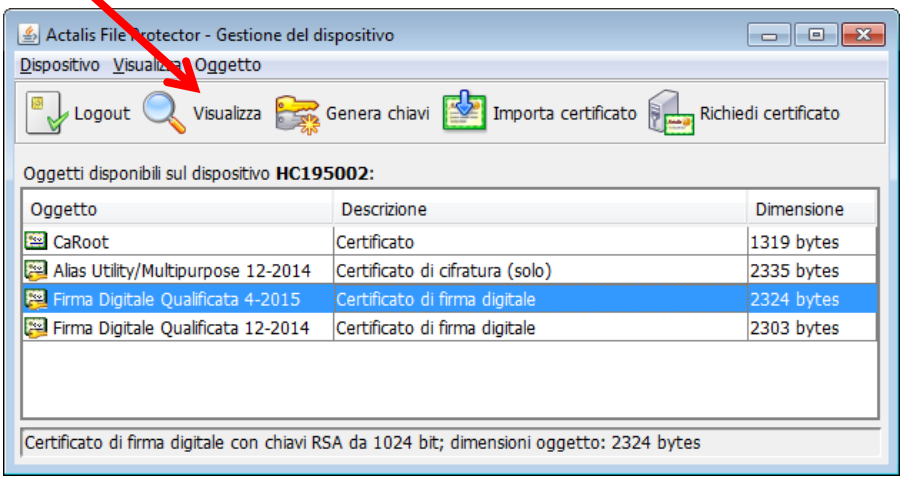
Se il PIN è corretto la prima icona LOGOUT presenta una spunta di colore verde.



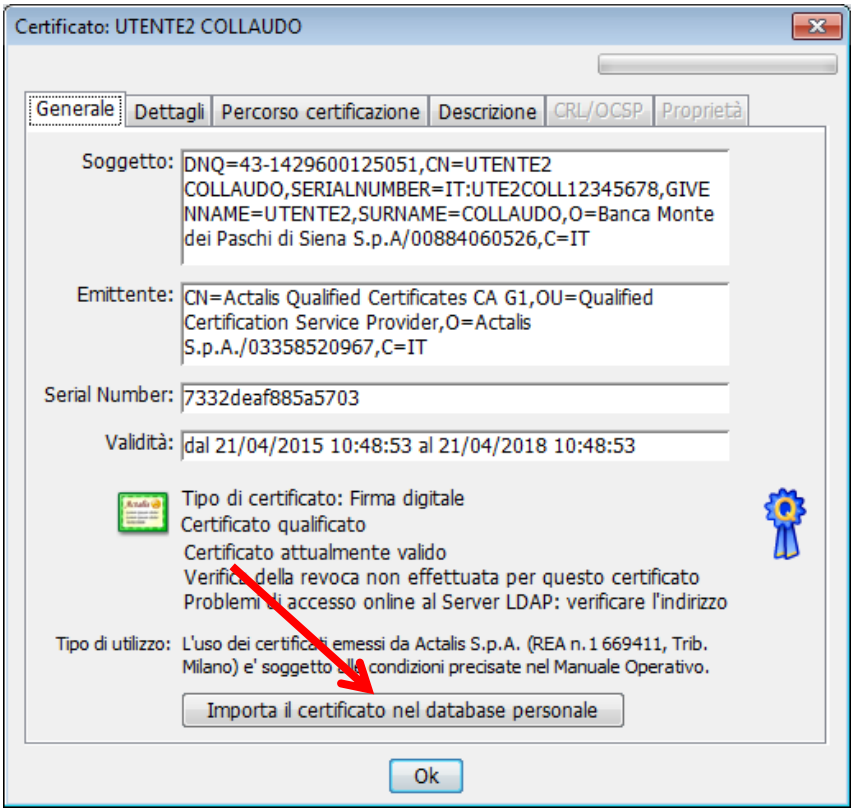
Accedere quindi a STRUMENTI E OPZIONI > GESTIONE DEL DISPOSITIVO. Si arriva a questa finestra:

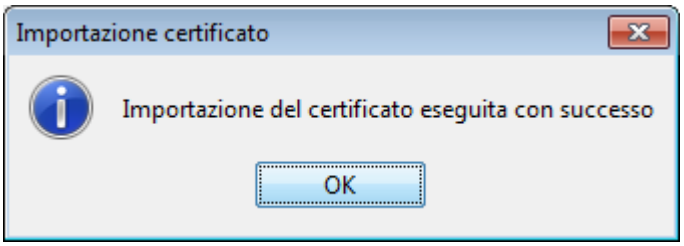


Selezionare il certificato di FIRMA QUALIFICATA di interesse (normalmente è presente un solo certificato di FIRMA QUALIFICATA).



Cliccare su VISUALIZZA per arrivare a questa videata:


Certificato: UTENTE2 COLLAUDO
Generale
Dettagli
Percorso certificazione
Descrizione
CRL/OCSP
Proprietà
Soggetto:
DNQ=43-1429600125051,CN=UTENTE2 COLLAUDO,SERIALNUMBER=IT:UTE2COLL12345678,GIVENNAME=UTENTE2,SURNAME=COLLAUDO,O=Banca Monte dei Paschi di Siena S.p.A/00884060526,C=IT
Emittente:
CN=Actalis Qualified Certificates CA G1,OU=Qualified Certification Service Provider,O=Actalis S.p.A./03358520967,C=IT
Serial Number:
7332deaf885a5703
Validità:
dal 21/04/2015 10:48:53 al 21/04/2018 10:48:53
Tipo di certificato: Firma digitale
Certificato qualificato
Certificato attualmente valido
Verifica della revoca non effettuata per questo certificato
Problemi di accesso online al Server LDAP: verificare l'indirizzo
Tipo di utilizzo:
L'uso dei certificati emessi da Actalis S.p.A. (REA n.1 669411, Trib. Milano) e' soggetto alle condizioni precisate nel Manuale Operativo.
Importa il certificato nel database personale
Ok


Importazione certificato
Importazione del certificato eseguita con successo
OK