Token USB

V1 - Guida rapida

Indice

1 Informazioni sul documento

1.1 Scopo del documento

Il presente documento intende essere una guida rapida per il titolare dell' Token USB nello svolgimento delle seguenti operazioni:

1. Apposizione di Firme Digitali in formato .P7M
2. Apposizione di Firme Digitali in formato .PDF
3. Apposizione di Marche Temporali
4. Verifica di Firme Digitali in formato .P7M e .PDF
5. Verifica di Marche Temporali
6. Gestione Pin e Puk della smart card contenuta all'interno del Token USB

2 Caratteristiche del dispositivo

Token USB è il dispositivo USB evoluto che permette di avere sempre a portata di mano la propria Firma Digitale.
Il token USB non necessita di installazione Hardware o Software, ed è sempre pronta per sottoscrivere digitalmente e/o marcare temporalmente documenti informatici.
Il dispositivo, inoltre, può essere anche utilizzato per l'autenticazione sicura nei siti di web.

2.1 Prerequisiti

Di seguito sono descritti i prerequisiti Hardware e Software che deve possedere la postazione a cui viene collegata il Token.

2.1.1 Software

Le versioni minime di OS supportate sono:

- Windows: Vista 32bit. Una JRE viene distribuita ed installata assieme al pacchetto di installazione per Windows: 1.8.0_73
- MacOS X 10.7.5 64 bit o successive. Browser Safari 4.0 o successive. Una JRE viene distribuita ed installata assieme al pacchetto di installazione per OSX: 1.8.0_144
- Linux: Distribuzione Ubuntu 16.04 32bit o successive. Una JRE viene distribuita ed installata assieme al pacchetto di installazione per Linux: 1.8.0_144

2.1.2 Rete

Di seguito sono riportati i parametri di rete che devono possedere le postazioni alle quali viene collegato il Token:

1. Disponibilità di connessione Internet senza presenza di Proxy.
2. Possibilità di poter instaurare connessioni HTTP, HTTPS e LDAP.

3 Installazione della smart card

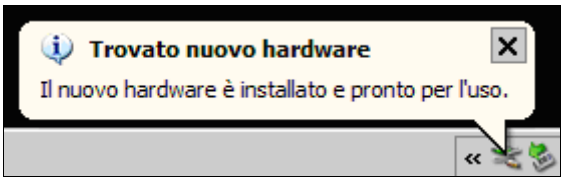
Rimuovere lo sportellino di protezione, sul lato posteriore del dispositivo, e farlo scorrere verso l'esterno.
Una volta aperto il vano del lettore smart card, inserire la SIM di Firma Digitale, come illustrato di seguito.

Passo1:
Inserire la SIM card con il chip rivolto verso il basso come indicato nella figura accanto.

Passo 2:
Una volta inserita la SIM card, reinserire lo sportellino.

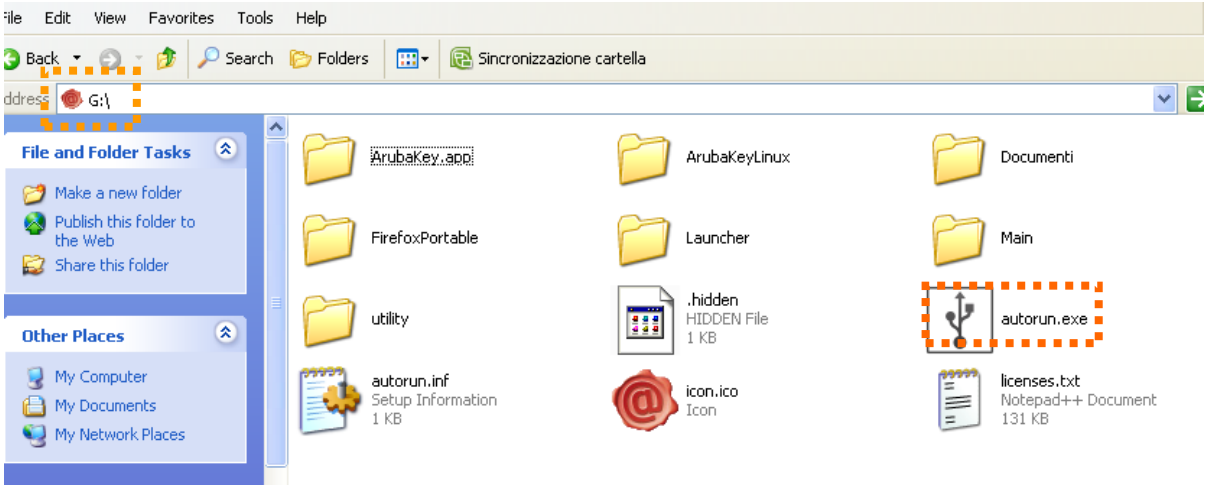
4 Avvio del Token USB

Collegare il Token USB ad una presa USB del PC ed attendere che compaia il messaggio indicato nella figura a fianco.
Il Token viene visto dal PC come una periferica HID (Human Interface Device), pertanto i driver per il corretto riconoscimento sono presenti all'interno del dispositivo stesso.



Se nella postazione è attiva la funzione di esecuzione automatica (Autorun) al momento del collegamento del Token verrà avviata automaticamente la Barra degli strumenti come quella riportata nella figura seguente.

Se, invece, al momento dell'inserimento del dispositivo, non viene avviata la Barra degli strumenti del Token USB, è probabile allora che la funzione di esecuzione automatica sia disattivata.
In tal caso, visualizzare il contenuto del Token ed avviare il file *autorun.exe*, come indicato nella figura seguente.



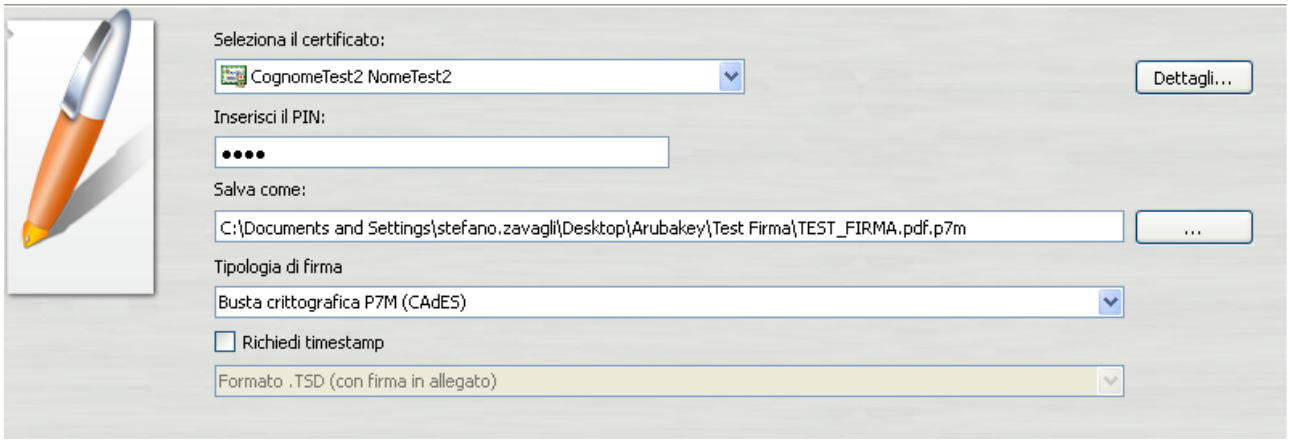
5 Firmare digitalmente un file in formato P7M

Passo 1
Trascinare il file sopra l'icona **"Firma".**

Passo 2
Attendere che il Token USB recuperi le informazioni relative ai certificati contenuti nella smart card.

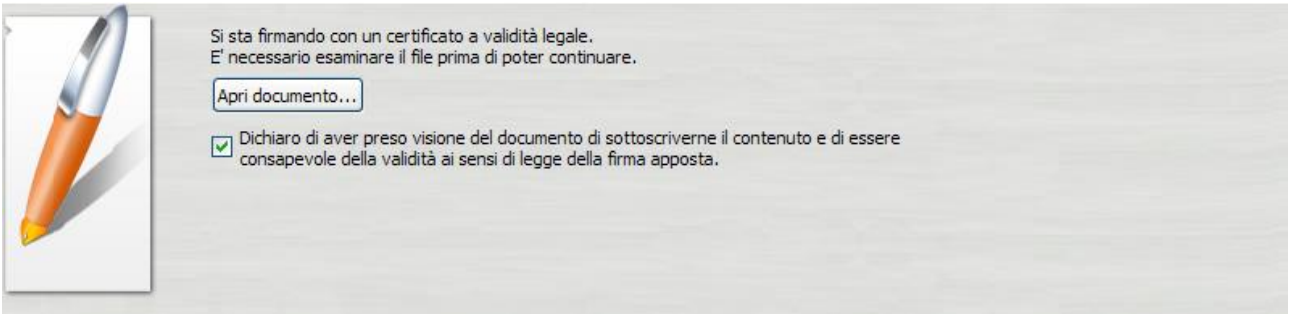
Passo 3

a. Assicurarsi che sia selezionato il certificato per la firma digitale (Cognome Nome);
b. Inserire il PIN di protezione della smart card;
c. Selezionare l'opzione *"Firma come busta crittografica P7M";*
d. Verificare che il percorso utilizzato per salvare il file firmato sia quello desiderato.
e. Cliccare sul pulsante **Next >**



Passo 4

a. Visualizzare eventualmente il contenuto del documento attraverso il pulsante **“Apri documento”**;
b. Selezionare l’opzione relativa alla presa visione del documento;
c. Cliccare sul pulsante **Next >**



Passo 5

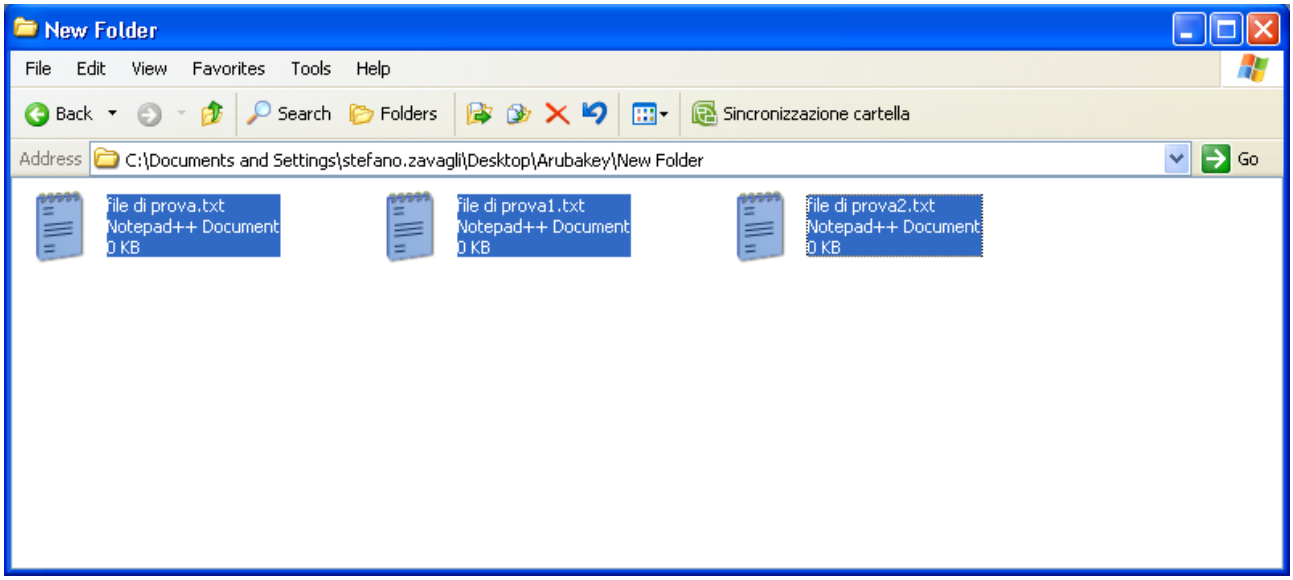
Attendere il completamento dell’operazione di firma.

Passo 6

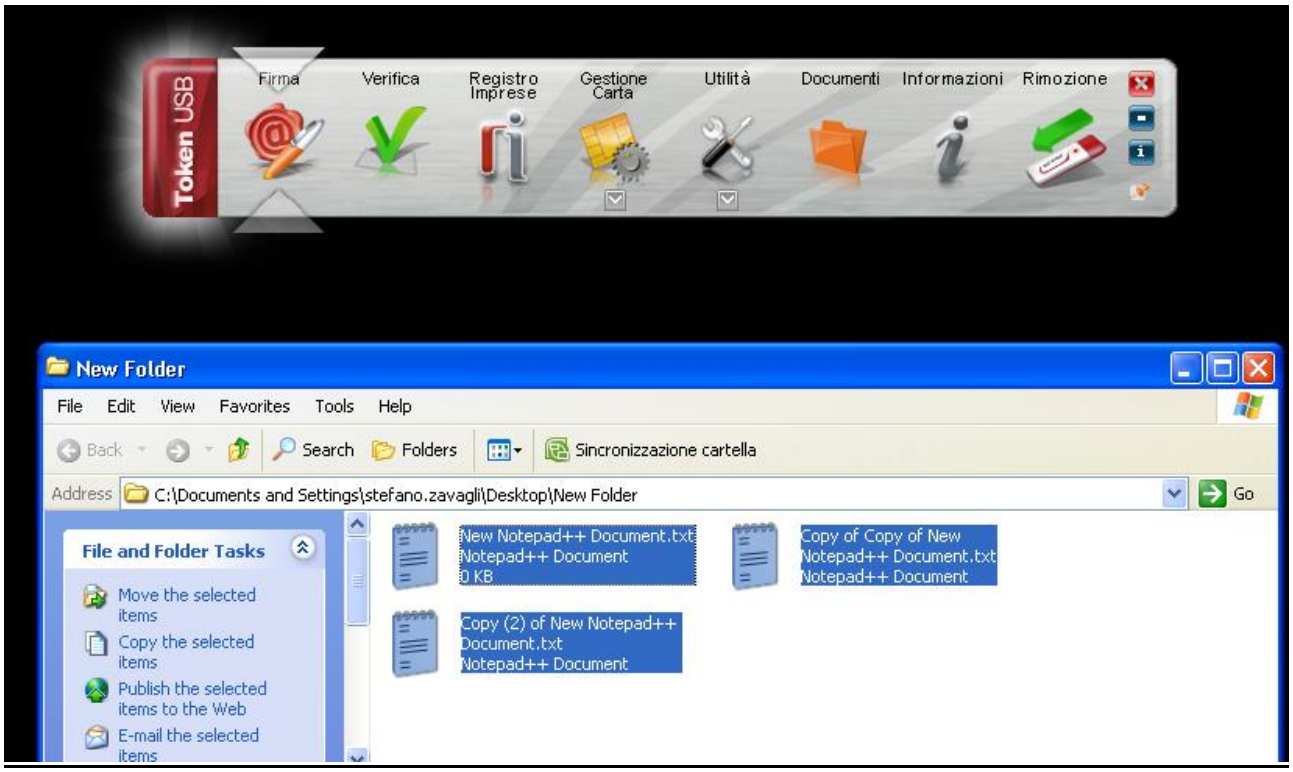
Verificare che al termine dell’operazione, venga riportata una schermata che notifica la corretta firma del file.

5.1 Firmare digitalmente più file in formato P7M

Passo 1
Selezionare tutti i documenti da firmare.



Passo 2
Trascinare i documenti selezionati sopra l'icona **"firma"**.

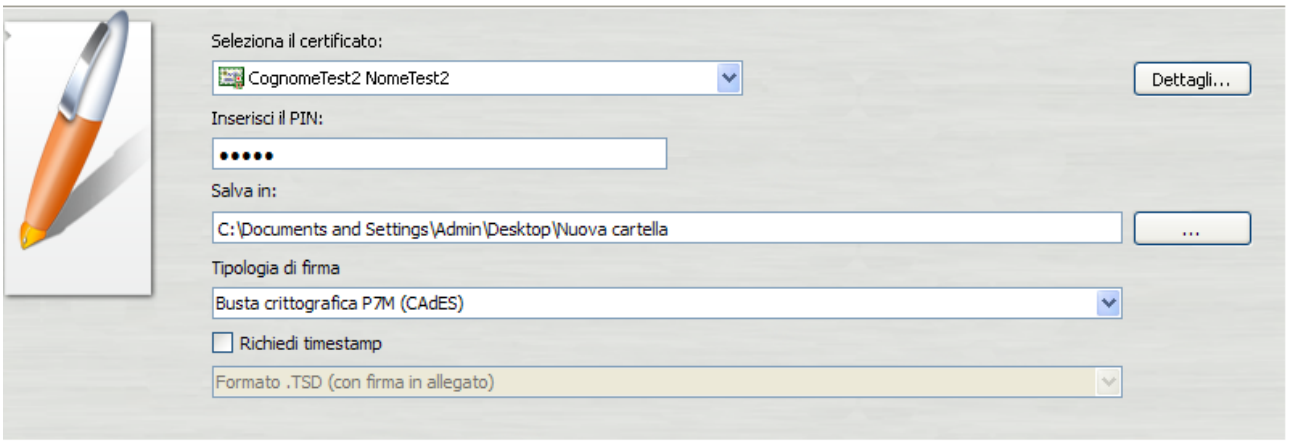


Passo3

Attendere che il Token USB recuperi le informazioni relative ai certificati contenuti nella smart card.

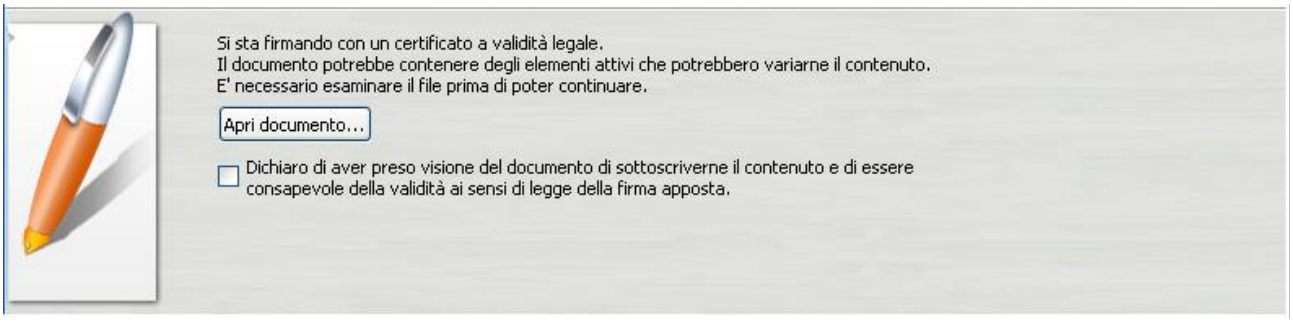
Passo4

a. Assicurarsi che sia selezionato il certificato per la firma digitale (Cognome Nome);
b. Inserire il PIN di protezione della smart card;
c. Selezionare l'opzione *"Firma come busta crittografica P7M";*
d. Verificare che il percorso utilizzato per salvare il file firmato sia quello desiderato.
e. Cliccare sul pulsante **Next >**



Passo 5

a. Visualizzare eventualmente il contenuto del documento attraverso il pulsante **"Apri documento"**;
b. Selezionare l'opzione relativa alla presa visione del documento;
c. Cliccare sul pulsante **Next >**

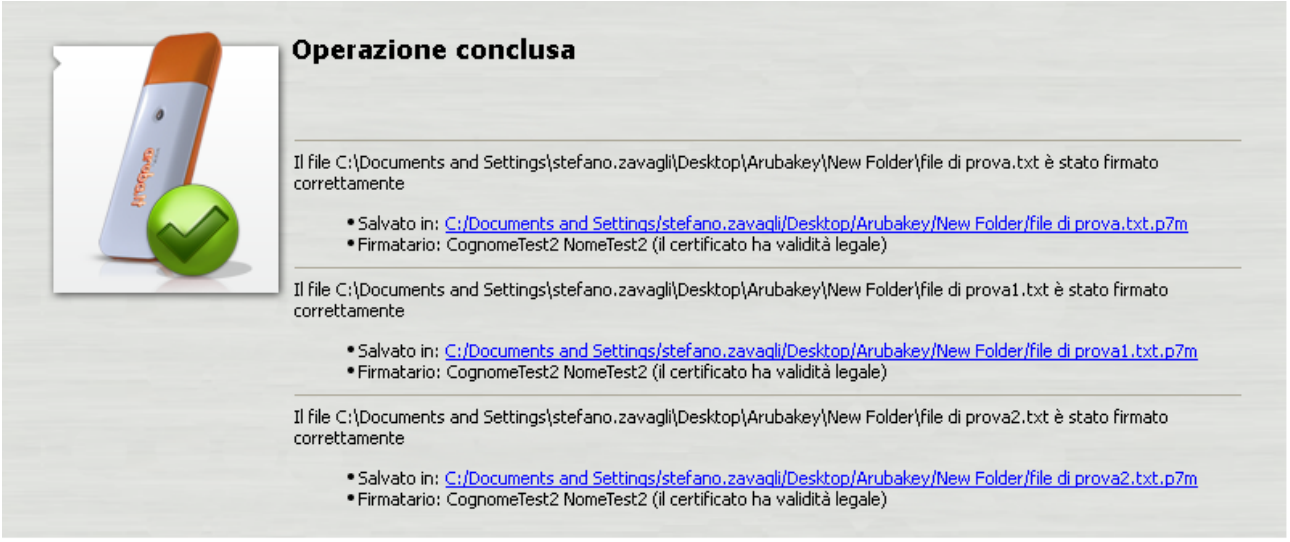


Passo 6

Attendere il completamento dell'operazione di firma.

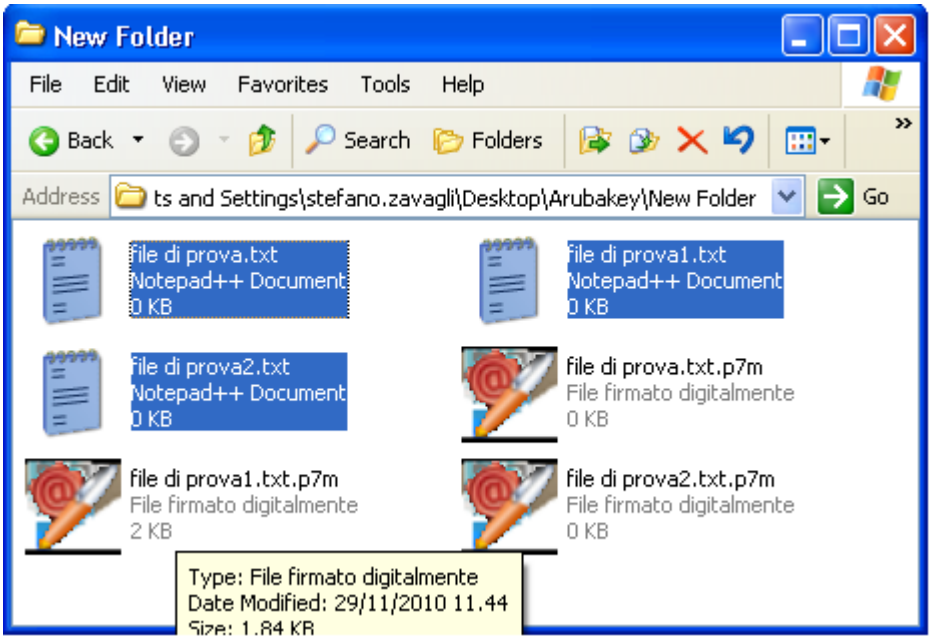
Passo7

Verificare che al termine della operazione, venga riportata una schermata che notifica la correttezza delle firma su ogni singolo documento.



Passo 8

I documenti firmati verranno salvati nella stessa cartella dove risiedono i documenti originali aggiungendo al nome l'estensione .7m.



6 Firmare digitalmente un file in formato PDF

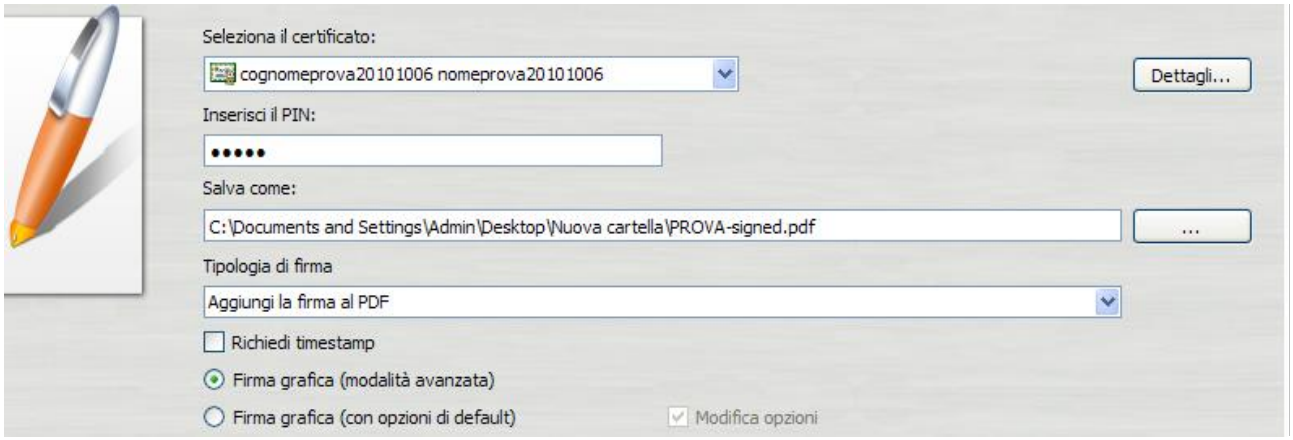
La procedura di firma in formato PDF è applicabile ai soli file .PDF.
Non è quindi possibile, attraverso il Token USB, firmare in PDF un file che non sia già stato convertito in questo formato.

Passo 1
Trascinare il file PDF sopra il pulsante **"Firma".**

Passo 2
Attendere che il TOken USB recuperi le informazioni relative ai certificati contenuti nella smart card.

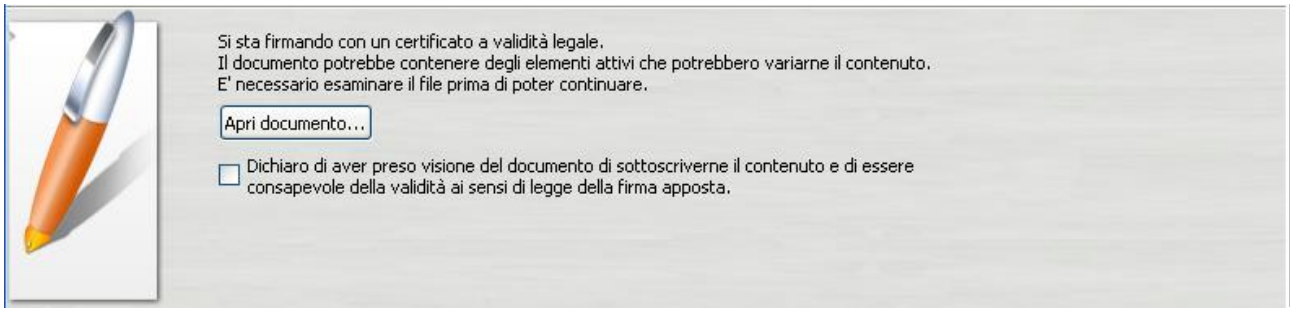
Passo 3

a. Assicurarsi che sia selezionato il certificato per la firma digitale (Cognome Nome);
b. Inserire il PIN di protezione della smart card;
c. Selezionare *"Aggiungi la firma al PDF" e attivare l'opzione "Firma grafica (modalità avanzata);*
d. Cliccare sul pulsante **Next >**



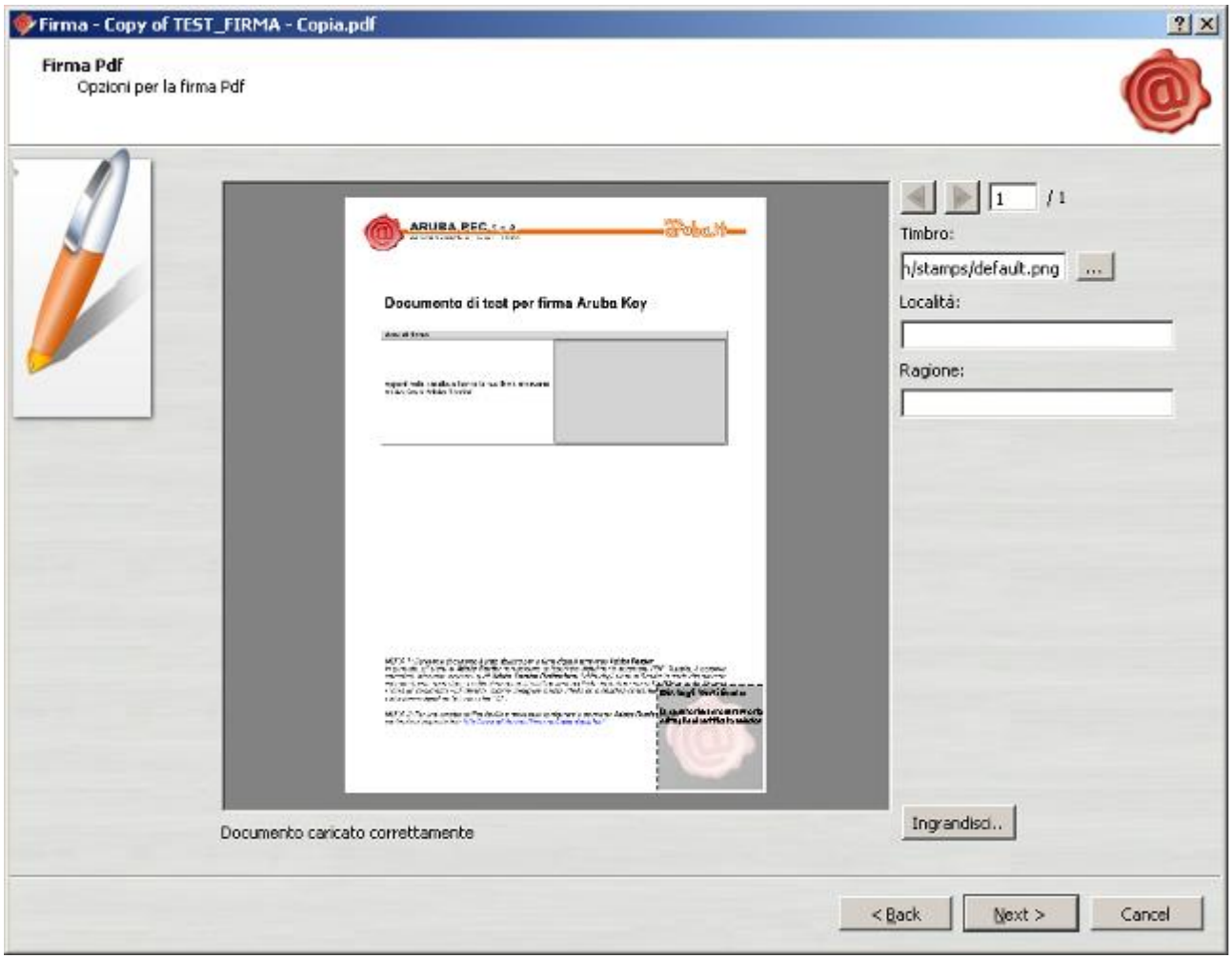
Passo 4

a. Visualizzare eventualmente il contenuto del documento attraverso il pulsante **Apri documento**;
b. Selezionare l'opzione relativa alla presa visione del documento;
c. Cliccare sul pulsante **Next >**



Passo 5

a. Definire, attraverso la finestra di anteprima, la posizione, la dimensione e il logo del campo che ospiterà la firma digitale;
b. Cliccare sul pulsante **Next >**

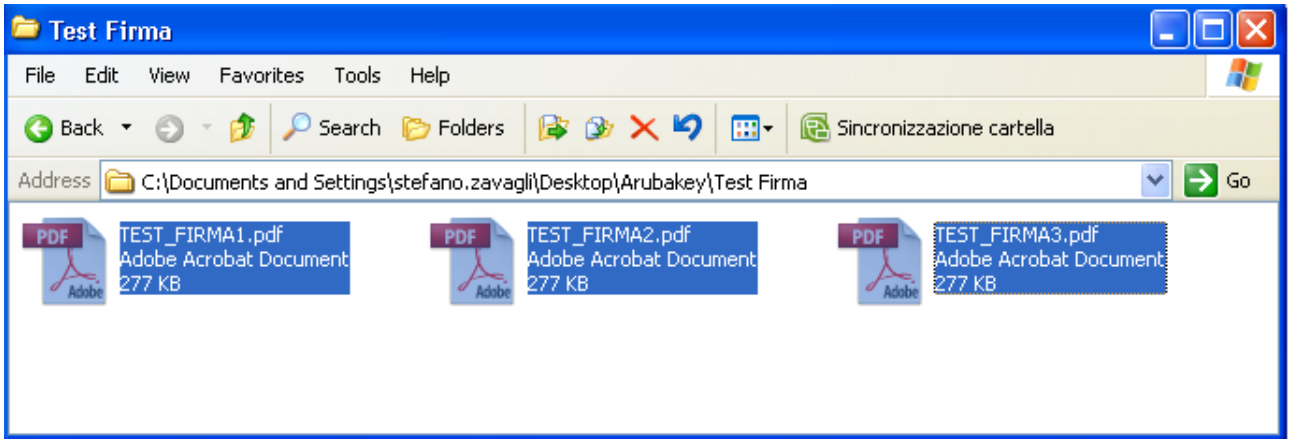


Passo 6
Attendere il completamento dell'operazione di firma.

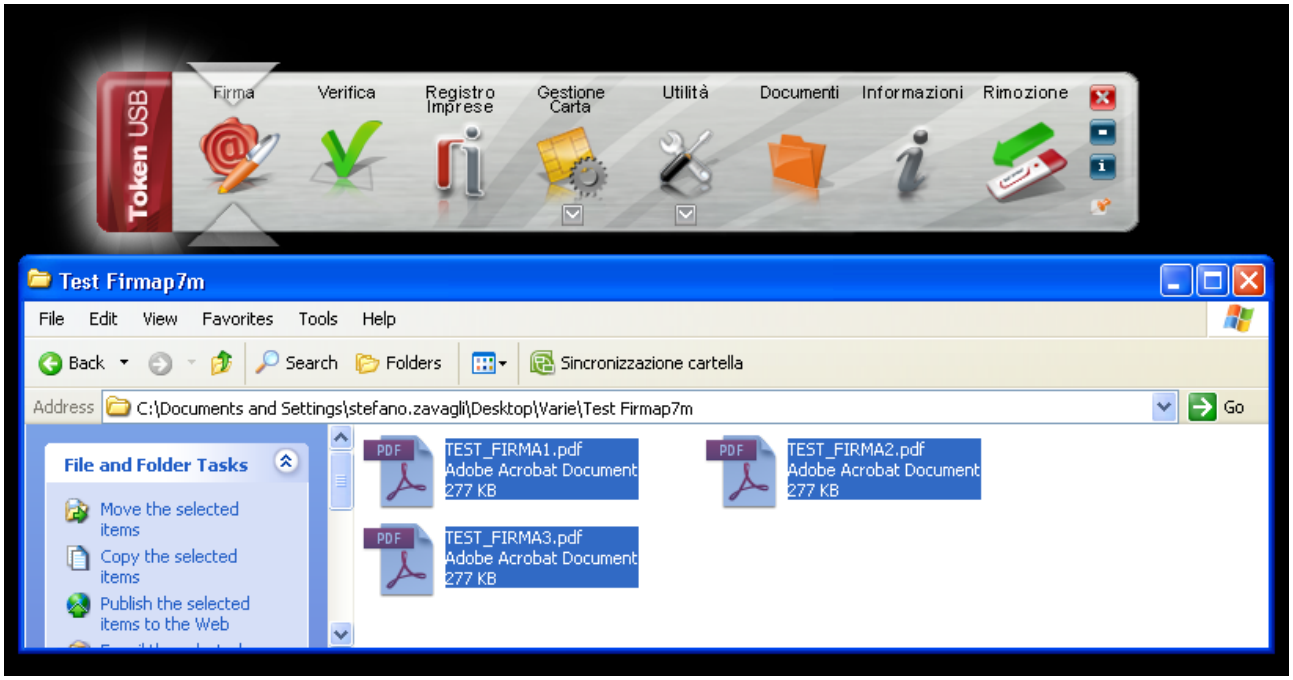
Passo 7
Verificare che al termine dell'operazione venga riportata una schermata che notifica la corretta firma del file.

6.1 Firmare digitalmente più file in formato PDF

Passo1
Selezionare tutti i documenti .PDF da firmare.



Passo 2
Trascinare i file selezionati sopra l'icona **"firma"**, e rilasciare il mouse.

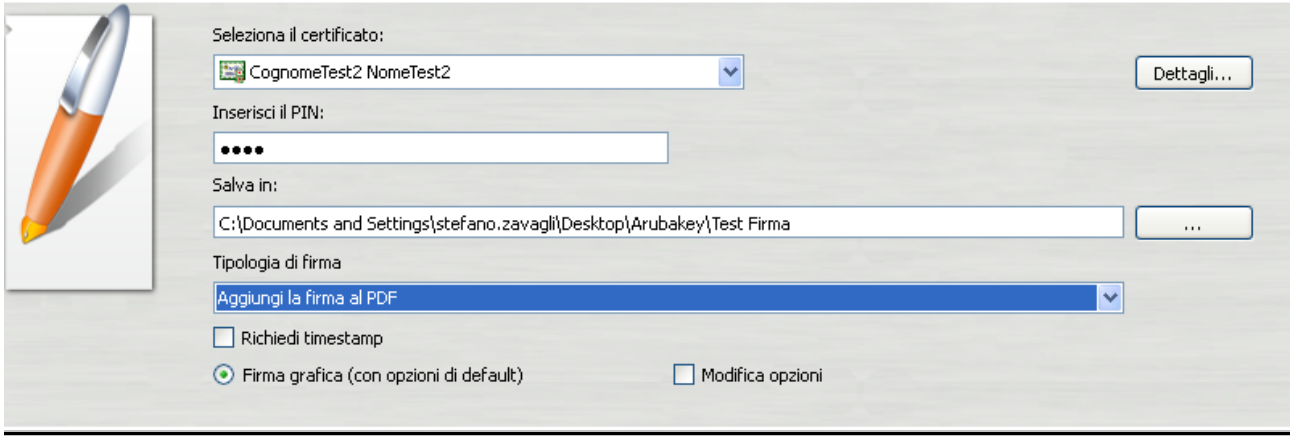


Passo 3

Attendere che il Token USB recuperi le informazioni relative ai certificati contenuti nella smart card.

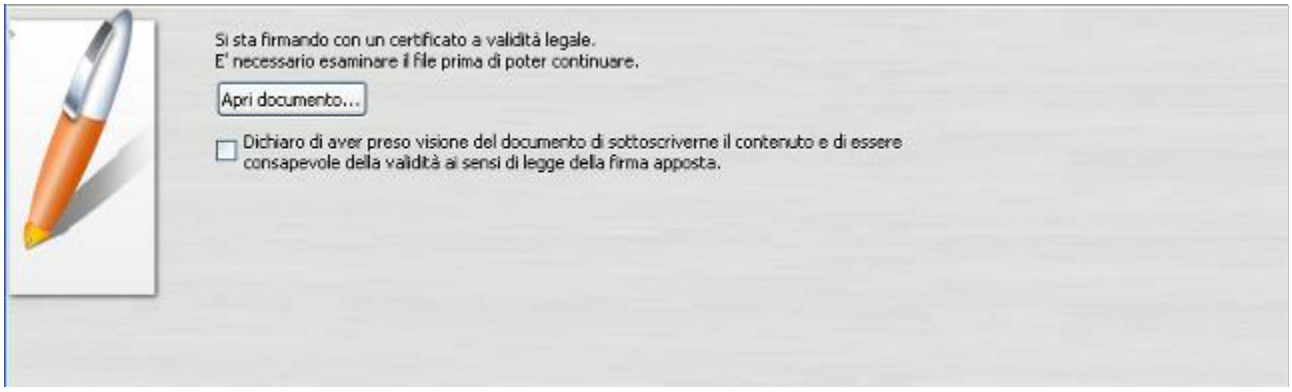
Passo 4

a. Assicurarsi che sia selezionato il certificato per la firma digitale (Cognome Nome);
b. Inserire il PIN di protezione della smart card;
c. Selezionare l'opzione *"Aggiungi la firma al PDF";*
d. Cliccare sul pulsante **Next >**

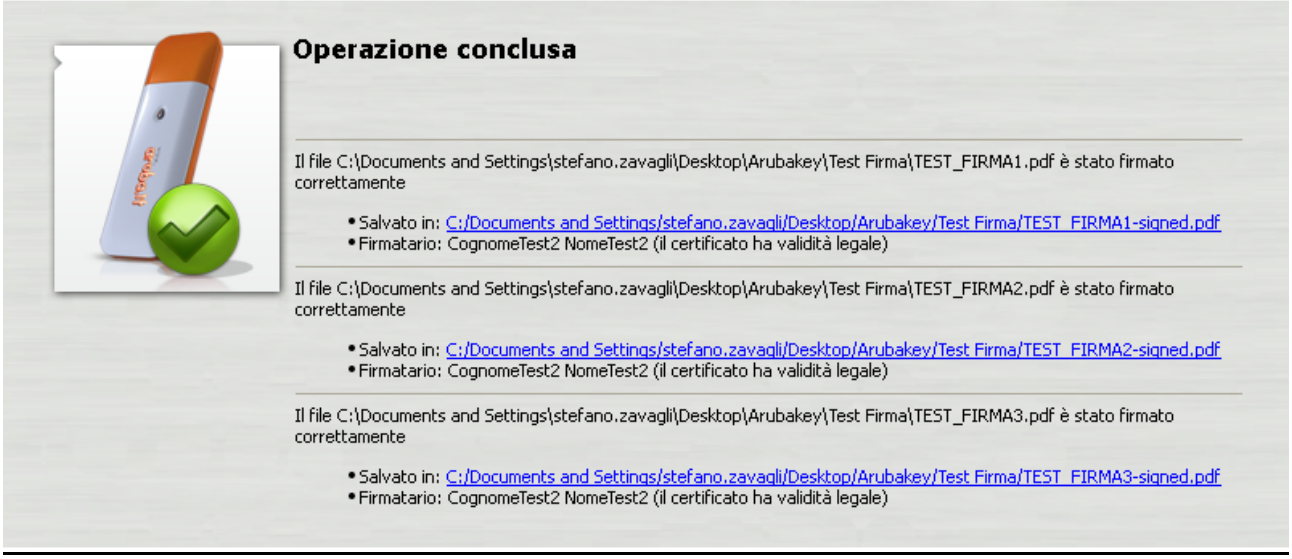


Passo 5

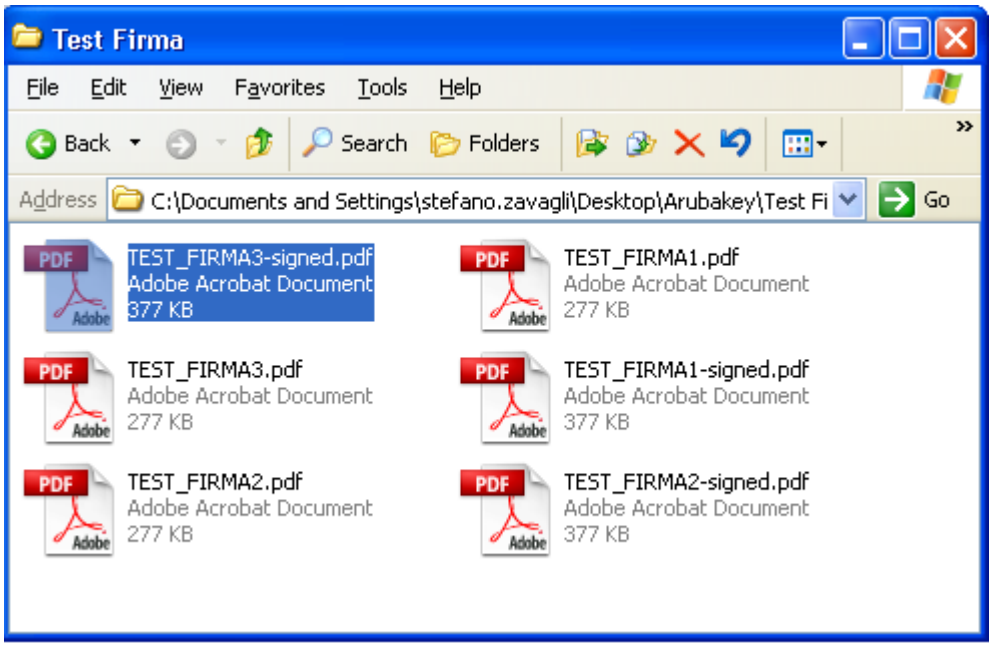
a. Visualizzare eventualmente il contenuto del documento attraverso il pulsante **Apri documento**;
b. Selezionare l'opzione relativa alla presa visione del documento;
c. Cliccare sul pulsante **Next >**



Passo 6
Verificare che al termine dell'operazione, venga visualizzata una finestra che notifica la corretta firma di ogni singolo documento.



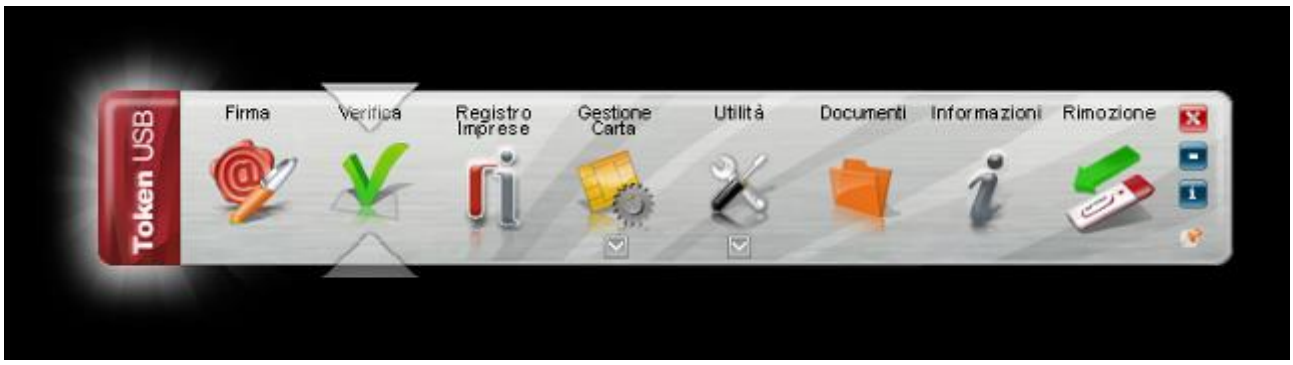
Passo 7
I documenti firmati verranno salvati nella stessa cartella dove risiedono i documenti originali aggiungendo al nome il suffisso "signed".



7 Verifica di file firmati in P7M

Passo 1
Trascinare il file da verificare sopra il pulsante **"Verifica".**

ATTENZIONE: Le indicazioni riportate di seguito sono applicabili ai soli file recanti estensione .P7M



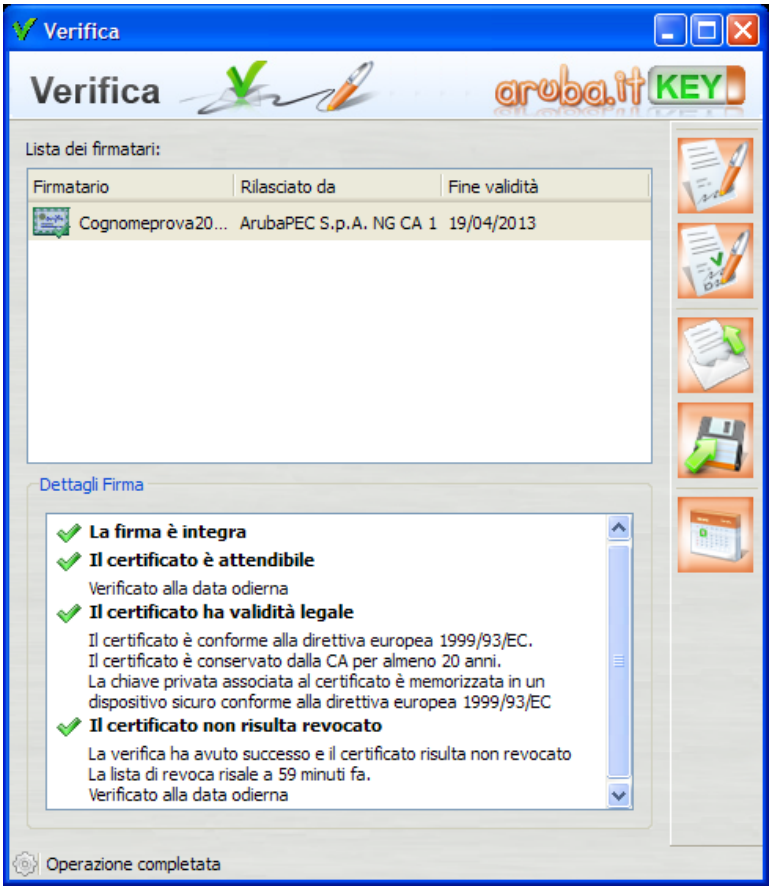
Passo 2
Completate le verifiche sul Token USB restituirà una finestra di riepilogo simile alla seguente:

La firma è integra.
Il messaggio indica che il documento non è stato alterato dopo essere stato firmato.

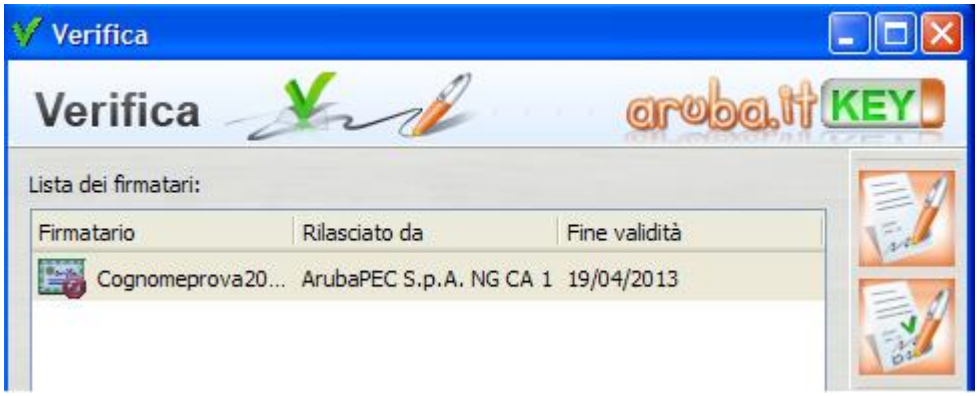
Il certificato è attendibile.
Il messaggio indica che il certificato del sottoscrittore è garantito da una Autorità di Certificazione inclusa nell'Elenco Pubblico dei Certificatori e che non risulta scaduto alla data della verifica.

Il certificato ha validità legale.
Questo messaggio sta ad indicare che il certificato del sottoscrittore è un certificato di Firma Digitale qualificato.

Il certificato non risulta revocato.
Questo messaggio sta ad indicare che il certificato del sottoscrittore non risulta nè revocato nè sospeso.

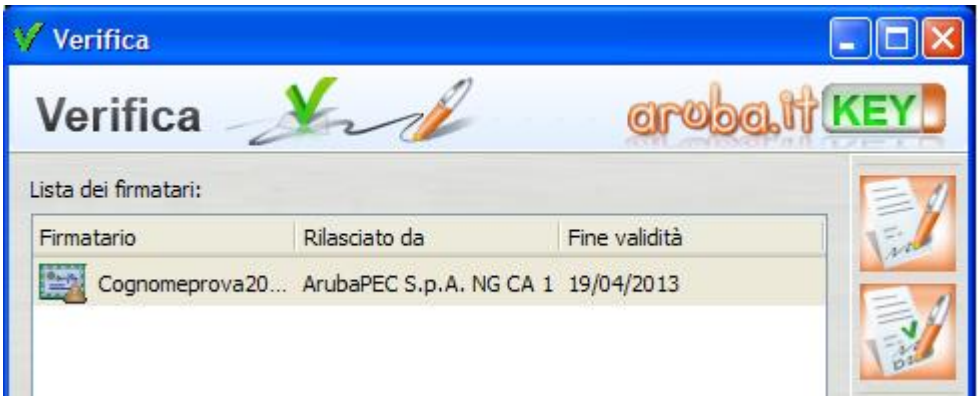


Qualora la finestra di riepilogo dovesse mostrare un esito simile al seguente:



Allora ciò sta ad indicare che sono stati portati a termine tutti i controlli previsti per la verifica della validità della firma, ma qualcuno di questi non è andato a buon fine. Per analizzare meglio il tipo di errore riscontrato è sufficiente visualizzare i messaggi restituiti dall'applicativo all'interno della sezione "Dettagli Firma".

Qualora invece la finestra di riepilogo dovesse mostrare un messaggio simile al seguente:



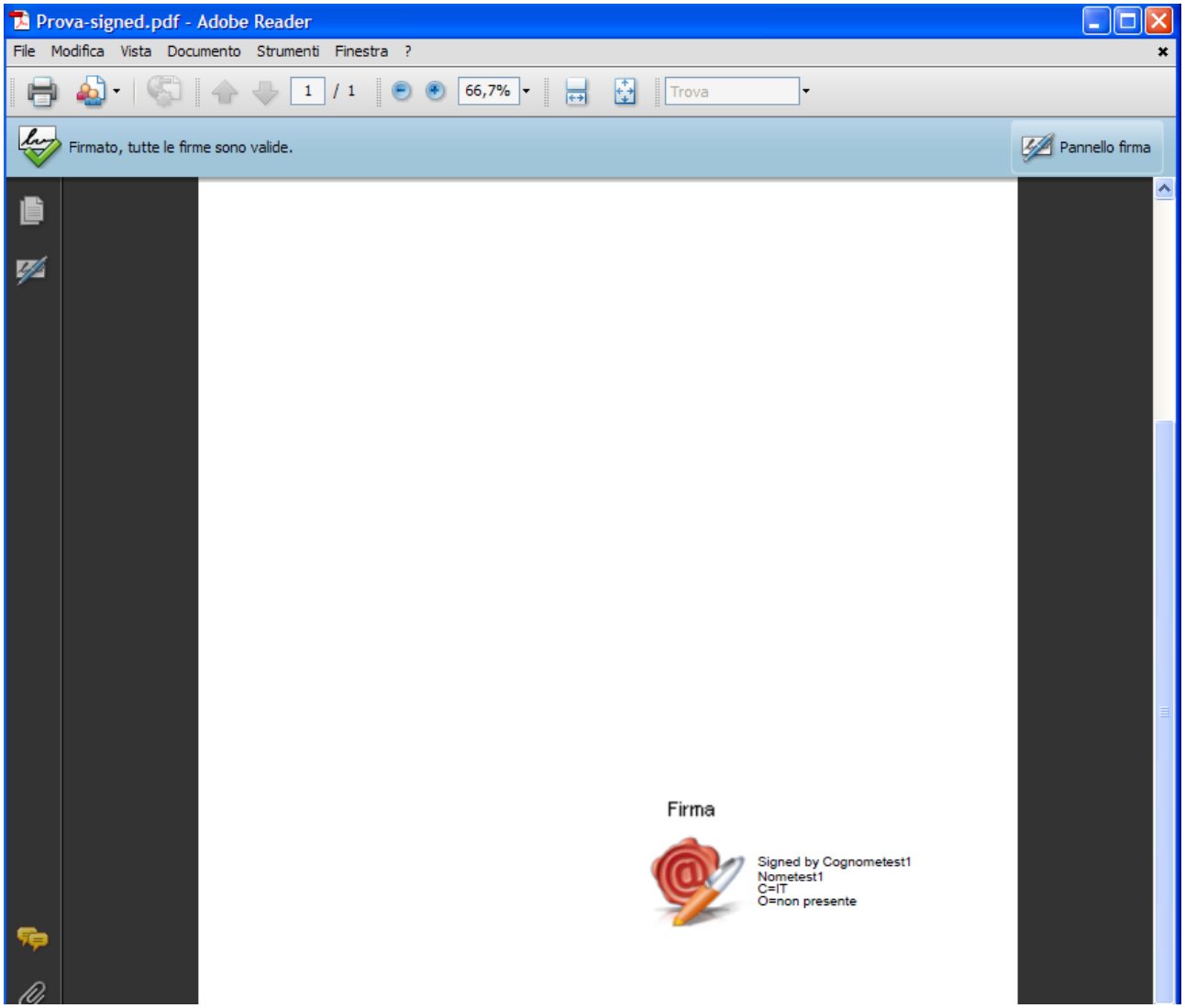
Allora ciò sta ad indicare che non è stato possibile portare a termine tutti i controlli previsti per verificare la validità della firma ed è necessario analizzare meglio il tipo di errore riscontrato visualizzando i messaggi restituiti dall'applicativo all'interno della sezione "Dettagli Firma".

8 Verifica di file firmati in PDF

Per la verifica di file firmati in formato .pdf è necessario utilizzare prodotti Adobe (Es.Adobe Reader), dopo averli configurati come da indicazioni presenti sul sito: http://www.adobe.com/it/security/italiandigsig.html

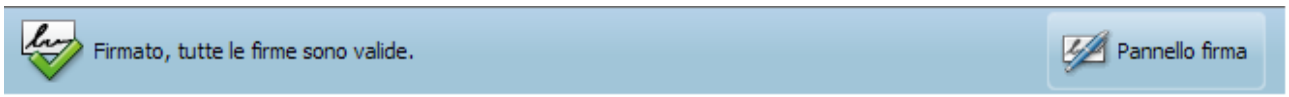
Passo 1

Aprire il file PDF firmato attraverso Adobe Reader (preferibilmente versione 9 o successive):



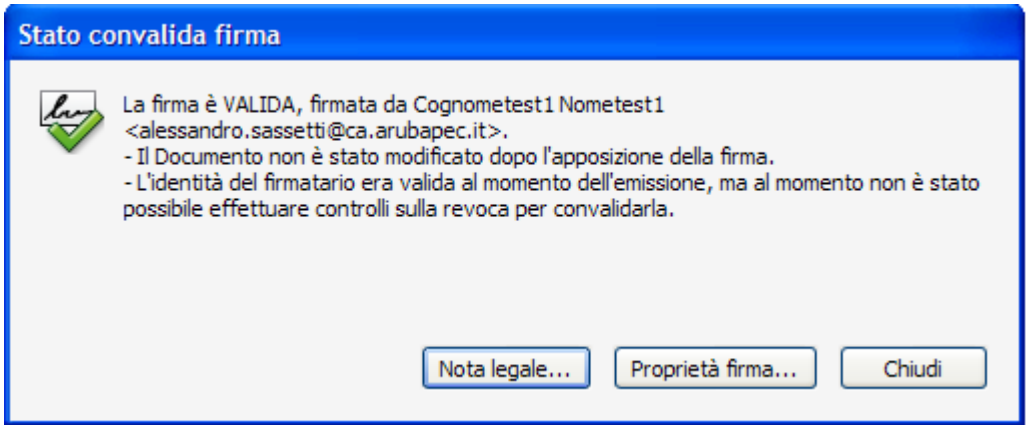
Passo 2

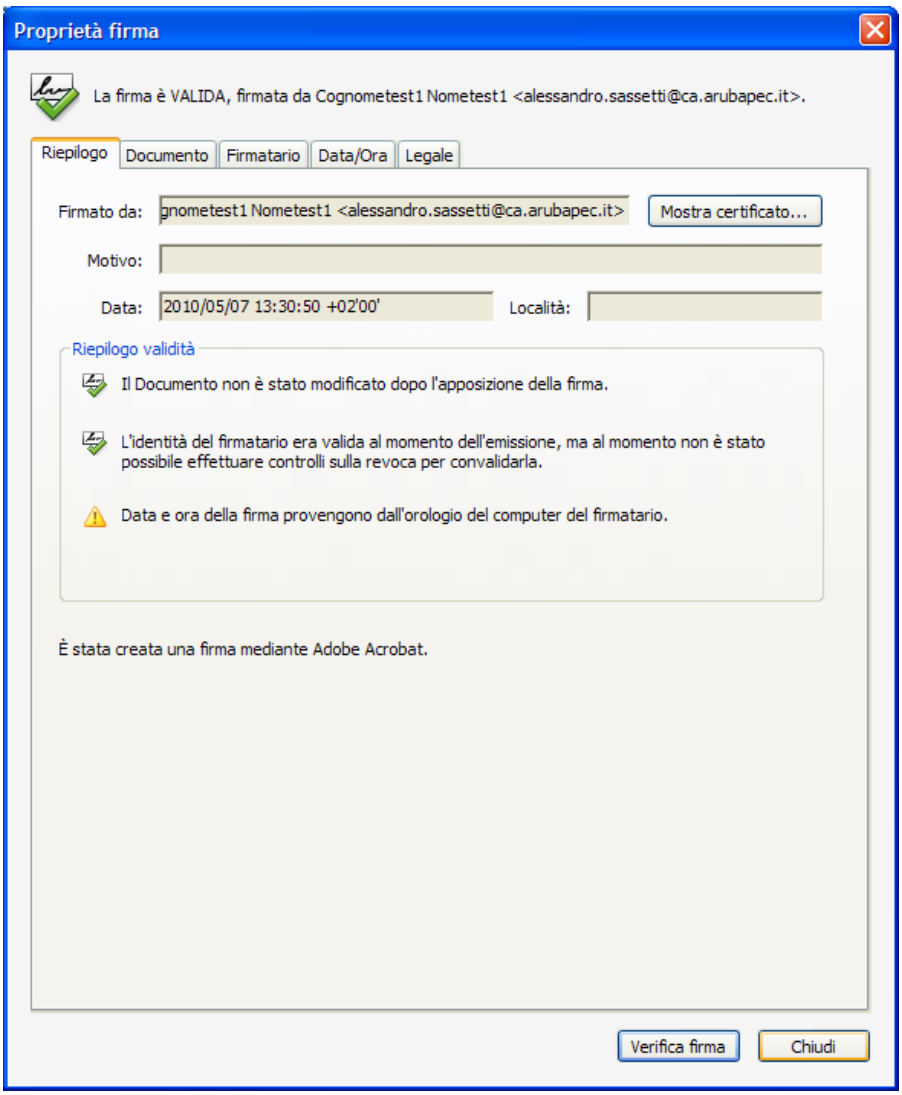
Verificare che il messaggio riportato sotto la barra degli strumenti Adobe riporti che tutte le firme apposte al documento sono valide.



Passo 3

Cliccare sopra la firma e quindi sopra il pulsante **"Proprietà firma"** per ottenere maggiori informazioni



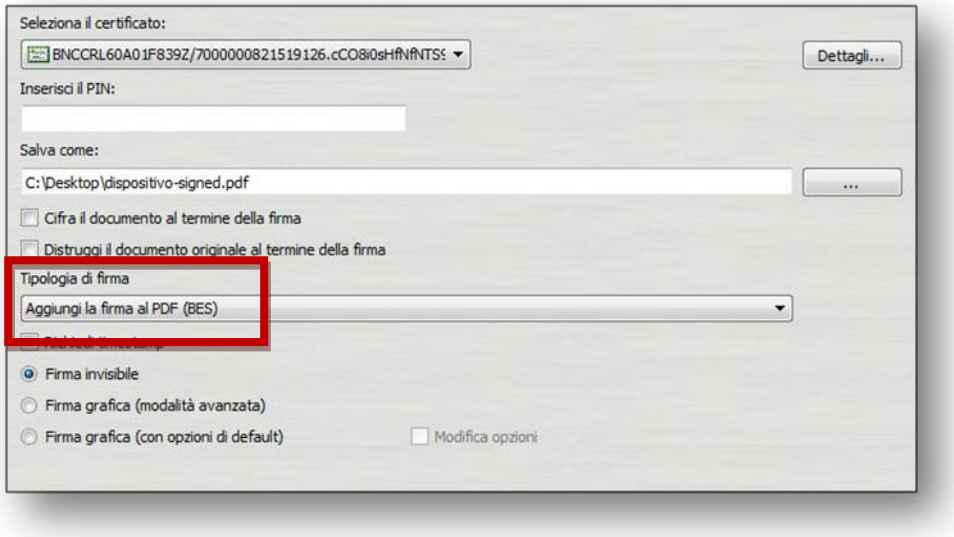


Qualora il messaggio riportato sotto la barra degli strumenti Adobe riporti un esito simile al seguente:

Allora è probabilmente necessario procedere con la configurazione dell'Adobe Reader seguendo le indicazioni contenute al seguente link: http://www.adobe.com/it/security/italiandigsig.html.

9 Ulteriori tipologie di firma (BES e Xades)

Il sofware a bordo del Token USB consente anche l'apposizione di firme di tipo BES e Xades-BES.
Trascinando il file da firmare nell'area apposita, il software consente la scelta del formato nel quale si desidera apporre la firma:



A seconda della tipologia di file trascinato nell'area di firma saranno disponibili, oltre ai formati descritti nei capitoli precedenti (PDF-Basic e .p7m), una o più delle seguenti opzioni:

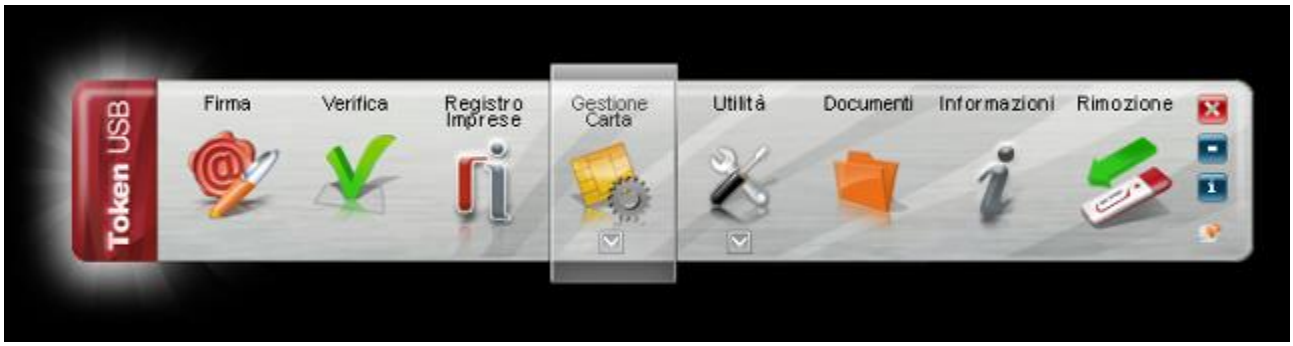
- Aggiungi la firma al PDF (BES);
- XADES-BES;

Selzionando il primo formato si sceglierà di apporre una firma PDF di tipo BES: l'estesione del file firmato sarà sempre di tipo ".signed.pdf", ma la firma verrà riconosciuta – per quanto riguarda Acrobat - solamente dalle versioni più recenti (dalla ver.10 in poi).
Selezionando invece XADES-BES si otterrà una firma nell'omonimo formato ed un file con estensione ".xml".
La verfica dei file firmati nelle modalità sopra descritte si esegue nelle stesse modalità descritte nei precedenti capitoli.

10 Cambio PIN

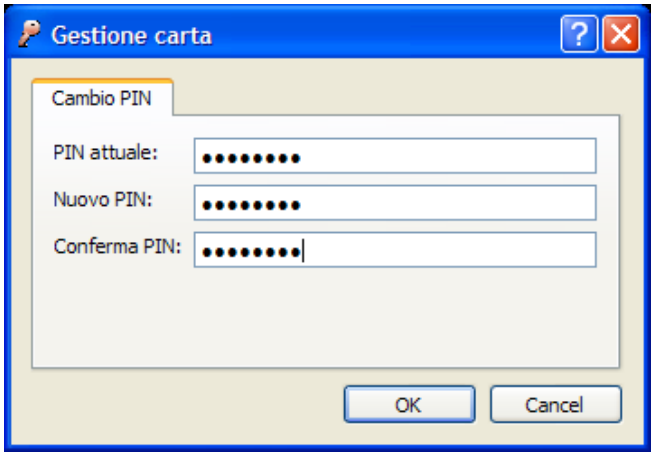
Passo 1
Per cambiare il codice PIN della carta inserita a bordo del Token USB cliccare sopra il pulsante "**Gestione Carta".**

Passo 2
Cliccare sul **"Cambio PIN".**



Passo 3
All'interno della finestra "Cambio Pin" inserire il precedente PIN, impostare il nuovo valore e cliccare sul pulsante OK.

ATTENZIONE:
Per il codice PIN non sono ammessi caratteri alfabetici (a,b,A,B, etc..) ma solo numerici (0,1,2,3,4,5,6,7,8 e 9). Ai fini della sicurezza si consiglia l'utilizzo di codici PIN composti almeno da 8 numeri.



Durante l'operazione di cambio del PIN Token USB può restituire i seguenti messaggi d'errore:

Errore: Il Pin attuale è errato. Attenzione: troppi tentativi errati possono bloccare il PIN.	Questo messaggio indica che il campo "Vecchio Pin" della finestra "Cambio Pin", non è corretto. In questo caso l'utente deve tener ben presente il fatto che l'inserimento ripetuto di PIN non validi può causare il blocco del PIN e quindi della carta.
Errore: Il PIN è bloccato.	Questo messaggio indica che il PIN della carta è bloccato. E' necessario procedere con lo sblocco del PIN seguendo le indicazioni contenute nel paragrafo "Sblocco PIN".

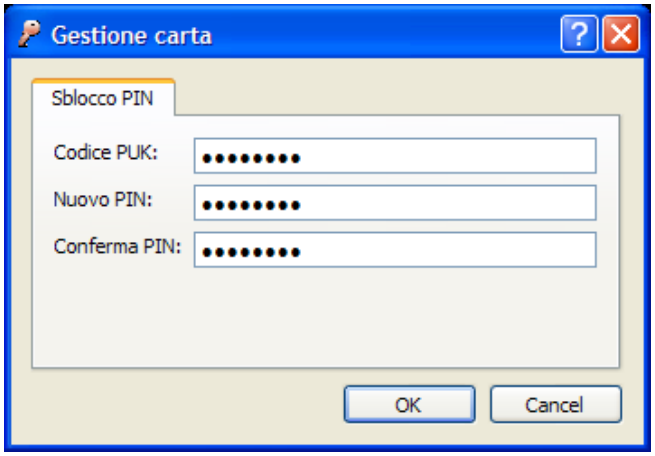
11 Sblocco PIN

Passo 1
Per sbloccare il codice PIN della carta inserita a bordo del Token USB cliccare sopra il pulsante **"Gestione Carta".**

Passo 2
Cliccare sul pulsante **"Sblocco PIN".**

Passo 3
All'interno della finestra "Sblocco Pin" inserire il PUK, impostare il nuovo valore del PIN e cliccare sul pulsante OK.

ATTENZIONE:
Per il codice PIN non sono ammessi caratteri alfabetici (a,b,A,B, etc..) ma solo numerici (0,1,2,3,4,5,6,7,8 e 9). Ai fini della sicurezza si consiglia l'utilizzo di codici PIN composti almeno da 8 numeri.



Durante l'operazione di sblocco del PIN il Token USB può restituire i seguenti messaggi d'errore:

Errore: Il Codice PUK è errato. ***Attenzione: troppi tentativi errati potrebbero bloccare il PUK!***	Questo messaggio indica che il campo "Puk" della finestra "Sblocco Pin", non è corretto. In questo caso l'utente deve tener ben presente il fatto che l'inserimento ripetuto di PUK non validi può causare il blocco definitivo della carta.
Errore: Il PUK è bloccato.	Questo messaggio indica che il PUK della carta è bloccato. E' necessario contattare l'Ente Certificatore che ha fornito la smart card procedendo alla revoca dei certificati attuali e con l'acquisto di una nuova carta.

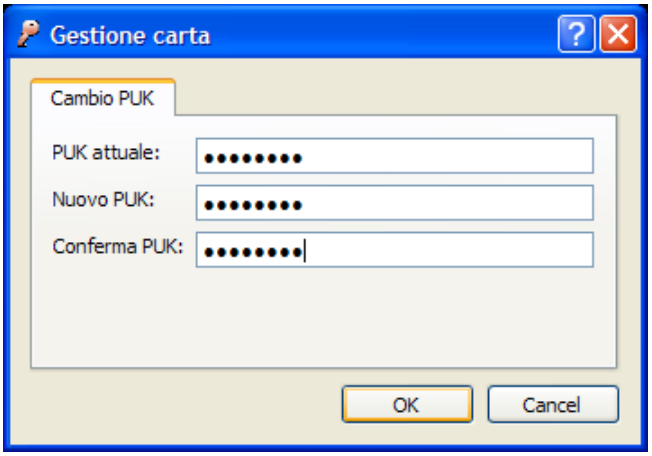
12 Cambio PUK

Passo 1
Per cambiare il codice PUK della carta inserita a bordo dell'Token USB cliccare sopra il pulsante "**Gestione Carta".**

Passo 2
Cliccare su **"Cambio PUK"**.

Passo 3
All'interno della finestra "Cambio PUK" inserire il precedente PUK, impostare il nuovo valore e cliccare sul pulsante OK.

ATTENZIONE:
Per il codice PUK non sono ammessi caratteri alfabetici (a,b,A,B, etc..) ma solo numerici (0,1,2,3,4,5,6,7,8 e 9). Ai fini della sicurezza si consiglia l'utilizzo di codici PUK composti almeno da 8 numeri.

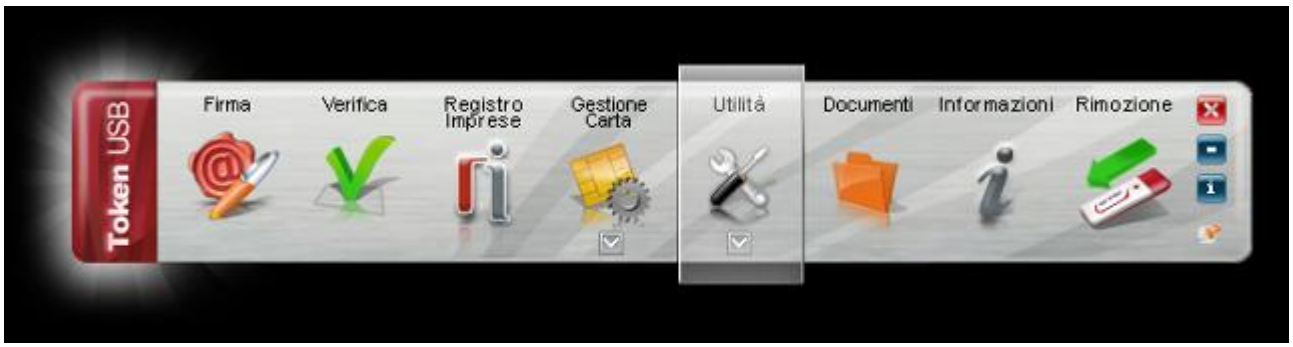


Durante l'operazione di Cambio del PUK il Token USB può restituire i seguenti messaggi d'errore:

Errore: Il PUK attuale è errato. ***Attenzione: troppi tentativi errati potrebbero bloccare il PUK!***	Questo messaggio indica che il campo "Puk" della finestra "Cambio Puk", non è corretto. In questo caso l'utente deve tener ben presente il fatto che l'inserimento ripetuto di PUK non validi può causare il blocco definitivo della carta.
Errore: Il PUK è bloccato.	Questo messaggio indica che il PUK della carta è bloccato. E' necessario contattare l'Ente Certificatore che ha fornito la smart card procedendo alla revoca dei certificati attuali e con l'acquisto di una nuova carta.

13 Autodiagnosi del dispositivo Token Usb

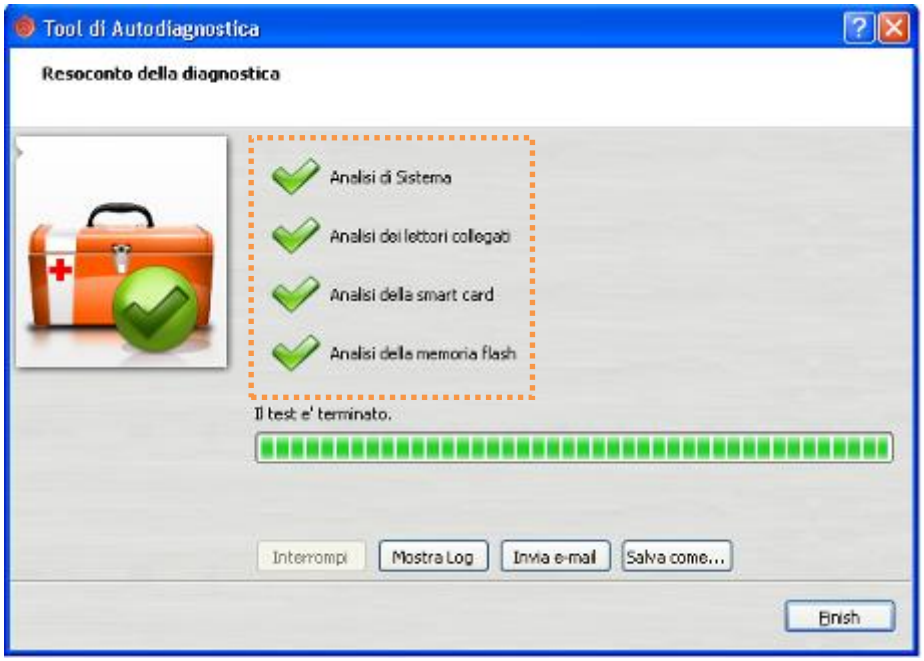
Passo 1
Per accedere all'applicazione di auto-diagnosi presente a bordo del Token USB cliccare sopra il pulsante "**Utilities".**



Passo 2
Cliccare su "**Auto-diagnostica**".

Passo 3
Cliccare su “**Next**”.

Passo 4
Completata l’analisi, se non vengono riscontrate anomalie, comparirà all’utente una pagina analoga alla seguente.



All’utente verrà lasciata l’opportunità di inviare via e-mail l’esito dell’’analisi del dispositivo o salvarlo in un file .txt.

Nota: *Per utilizzare questa funzione presente a bordo del Token USB l’utente deve avere i privilegi di amministratore.*

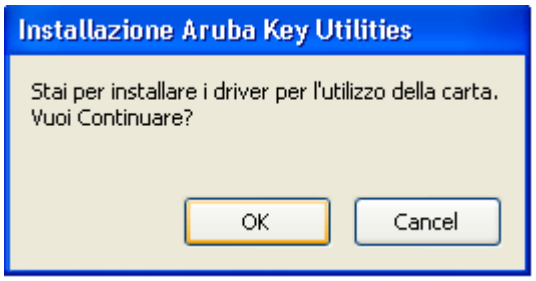
14 “Import” del certificato di firma

L’applicativo “Import” del certificato consente l’importazione dei certificati del’Token USB all’interno dello Store di Microsoft.
Questa operazione ,viene fatta una tantum, e permette di utilizzare il Token USB anche con quei software che, per le funzionalità di crittografia fanno uso dei CSP di Microsoft come ad esempio Internet Explorer.

Passo 1
Per accedere alla applicazione di “import” del certificato, cliccare sopra il pulsante “**Utilities”.**

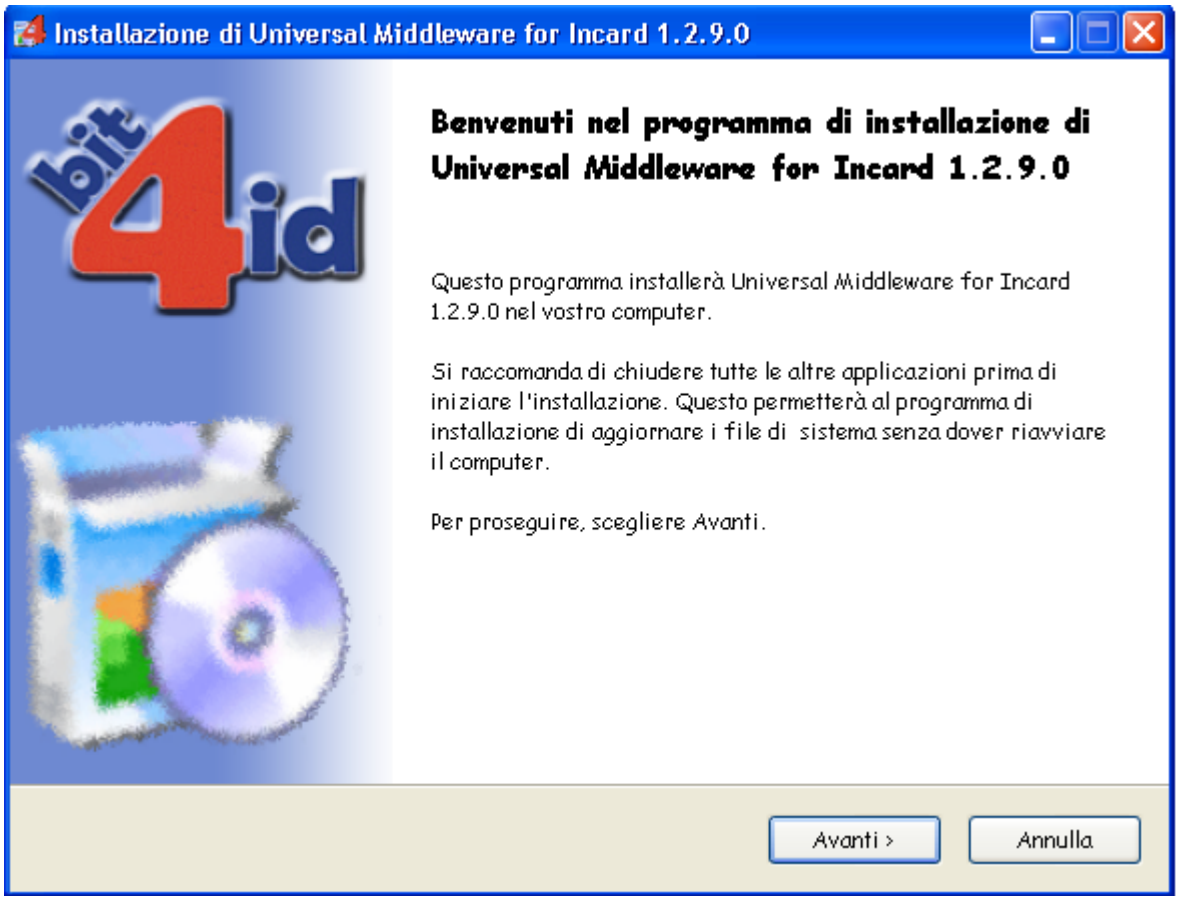
Passo2
Cliccare su “**import” certificato**.

Passo 3
Cliccare su Ok per installare i driver presenti a bordo del Token USB.

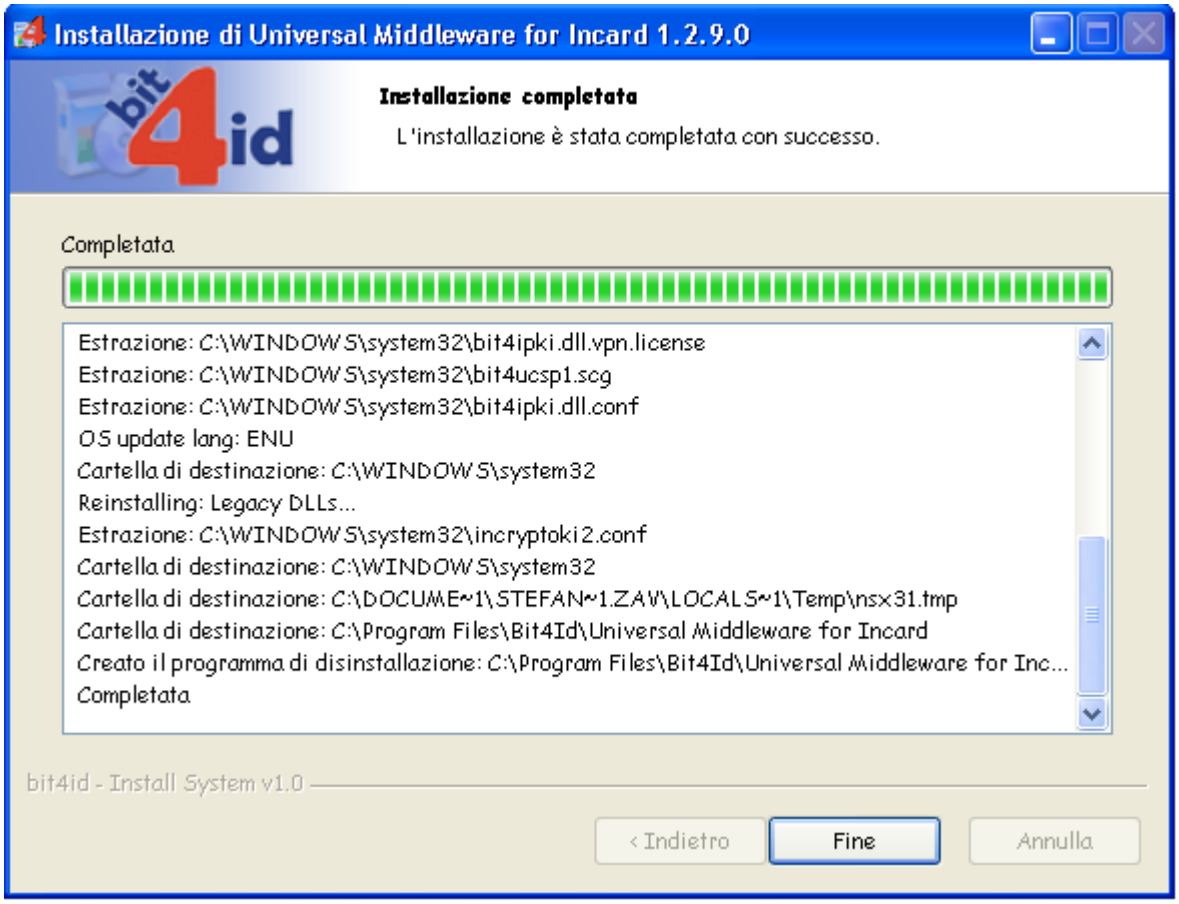


Nota: *Per utilizzare questa funzione presente a bordo del Token USB l'utente deve avere i privilegi si amministratore del PC.*

Passo 4
Cliccare su Avanti.



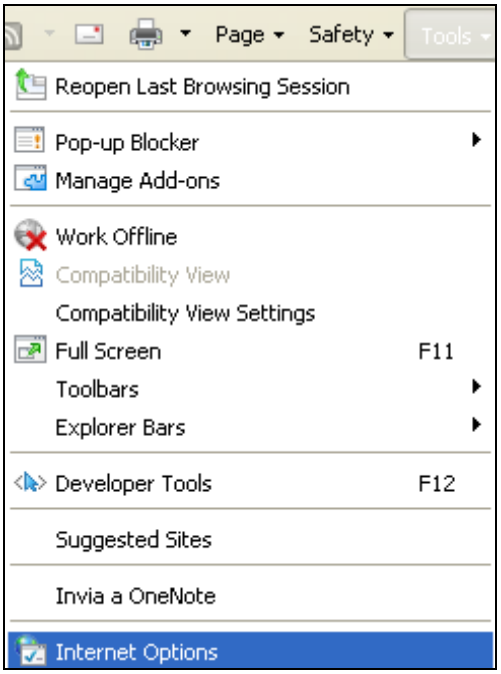
Passo 5
Accettare le condizioni per l'utilizzo della licenza e cliccare su Installa.



Passo 6
Attendere il completamento della installazione dei driver nella vostra postazione e cliccare su **"Fine"**.

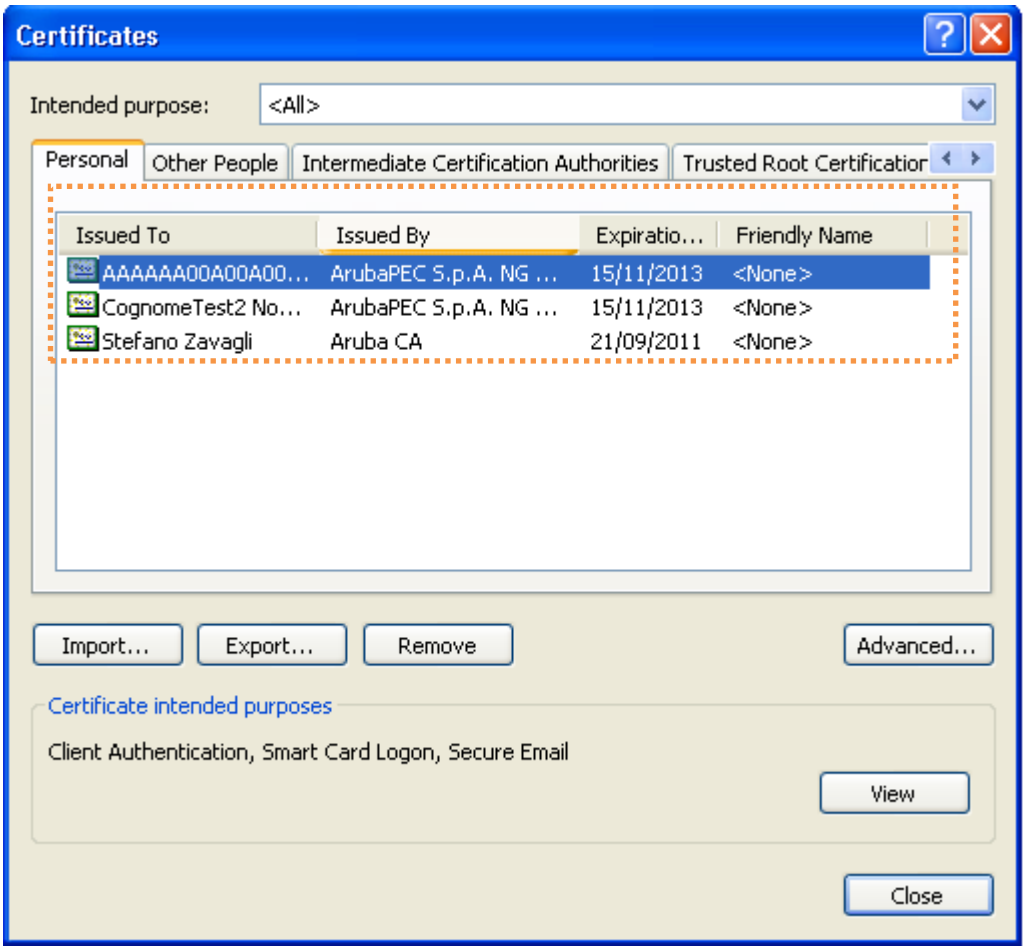
Passo 7
Verificare l'installazione del certificato.

1. Avviare Microsoft Internet Explorer;
2. Selezionare Strumenti → Opzioni Internet;
3. Selezionare la scheda Contenuto e quindi il pulsante Certificati



Passo 8

Verificare che all'interno della cartella "Certificati" siano presenti i propri certificati. E cliccare su "**Chiudi**".

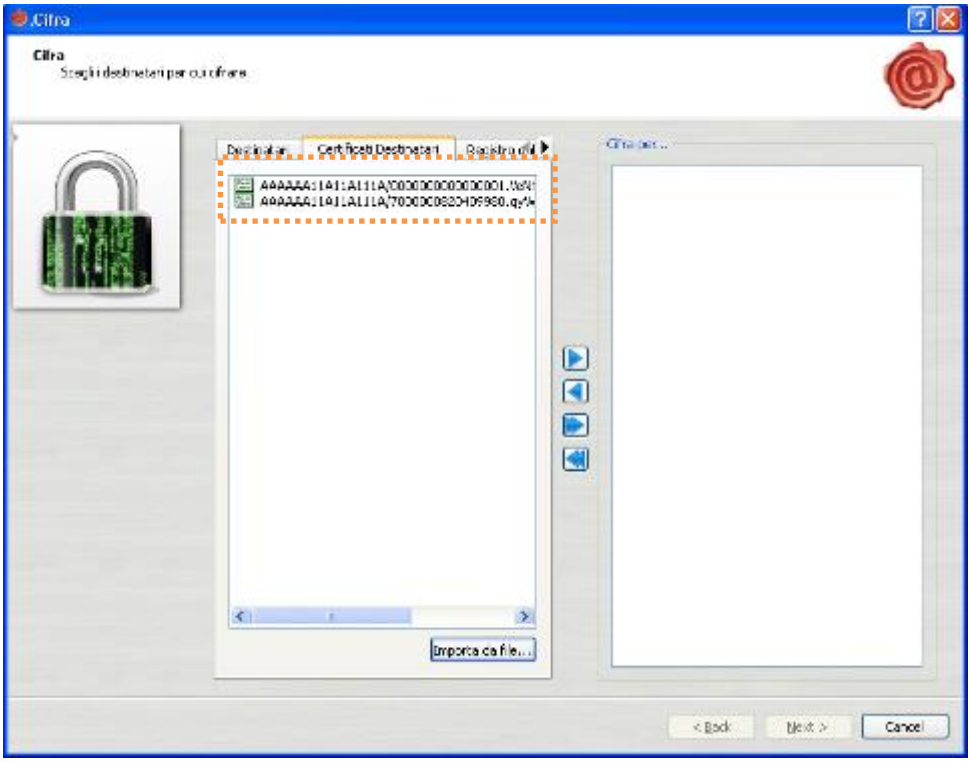


15 Cifratura File

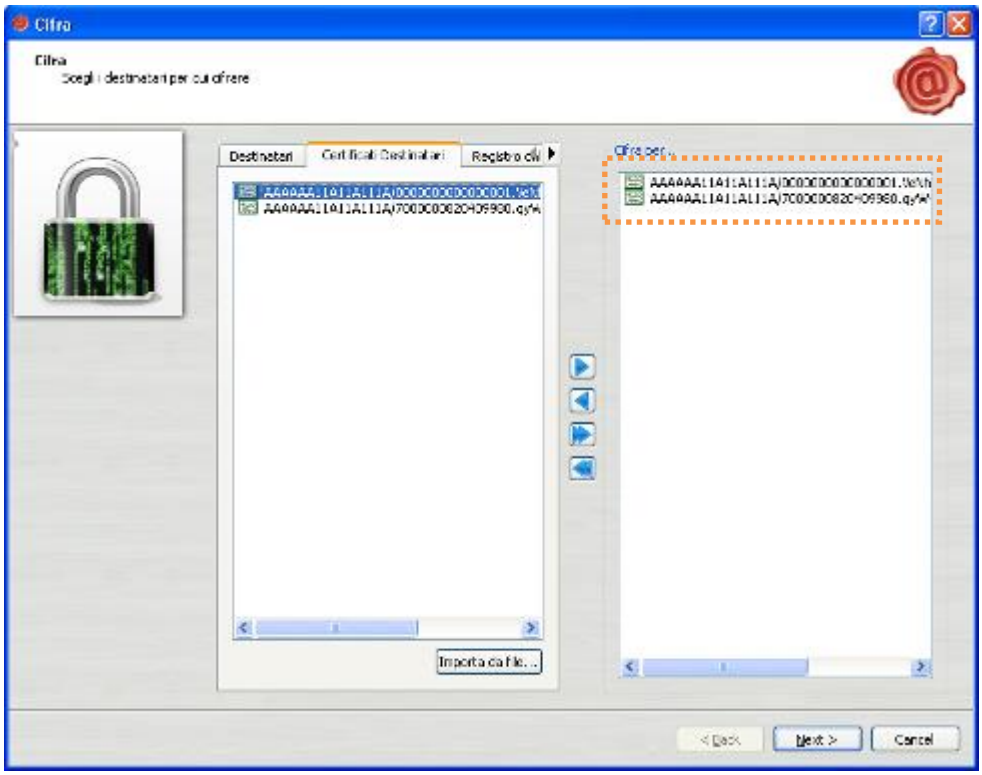
Passo 1
Per cifrare un file selezionare **“Utilities”.**

Passo 2
Trascinare il file da cifrare sopra il pulsante **“Cifra”**.
.

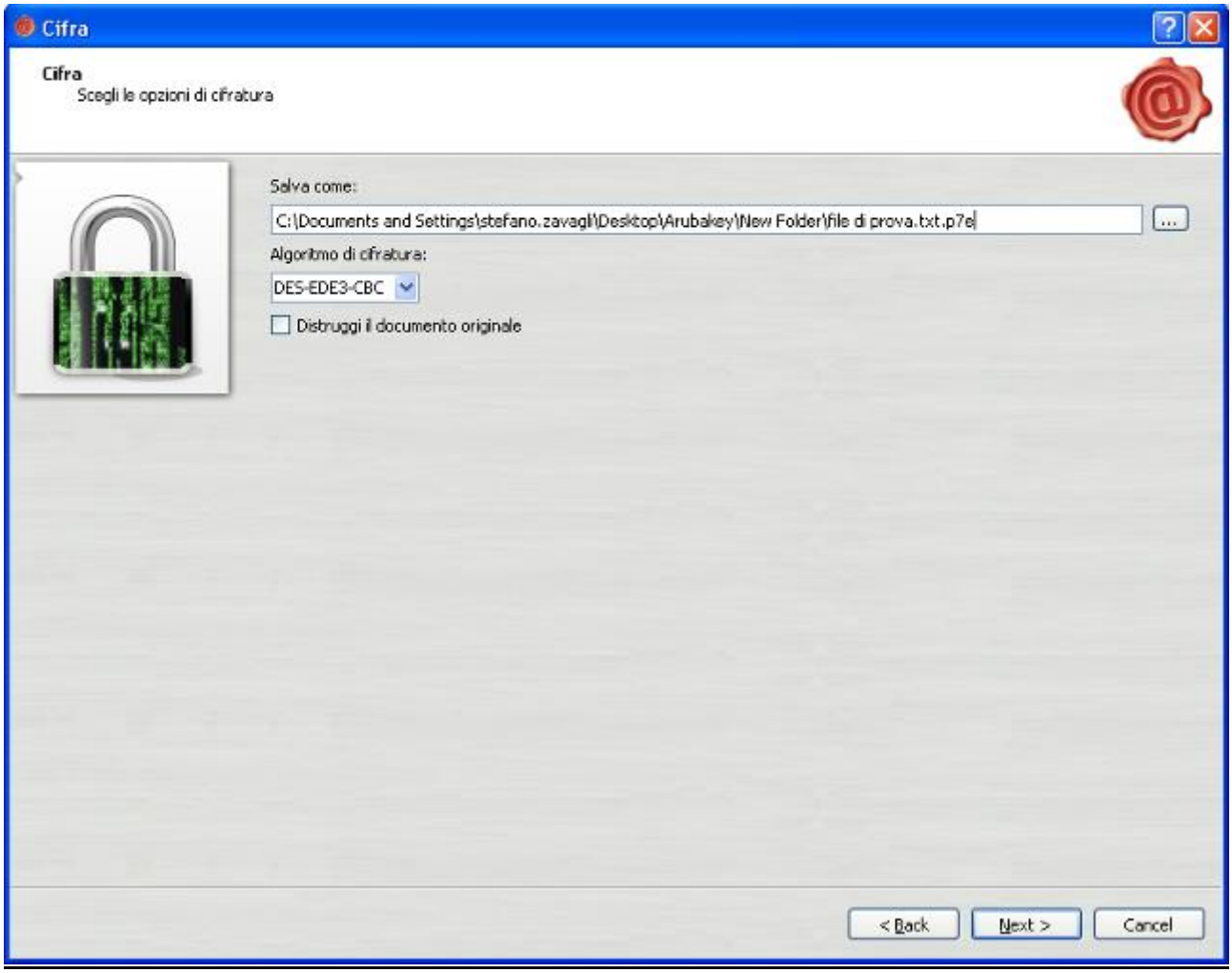
Passo 3
All'interno della finestra di cifratura selezionare, dalla sezione di sinistra, l'elenco dei destinatari del file cifrato e cliccare su "**Aggiungi**".



Passo 4
Cliccare su "**Next**".



Passo 5
Selezionare la cartella all'interno della quale s'intende salvare il file cifrato e cliccare su "**Next**".



Nota: *Se si selezionano più certificati per la cifratura del file, il risultato sarà un unico file decifrabile da ogni singolo titolare dei certificati selezionati.*

Nota: *In fase di cifratura del file il Token USB propone automaticamente, nell'area "destinatari", il proprio certificato di autenticazione, quello presente cioè nella SIM inserita nel Token USB.*

Passo 6
Se la procedura è andata a buon fine verrà mostrata la seguente schermata, cliccare su **"Finish"**.

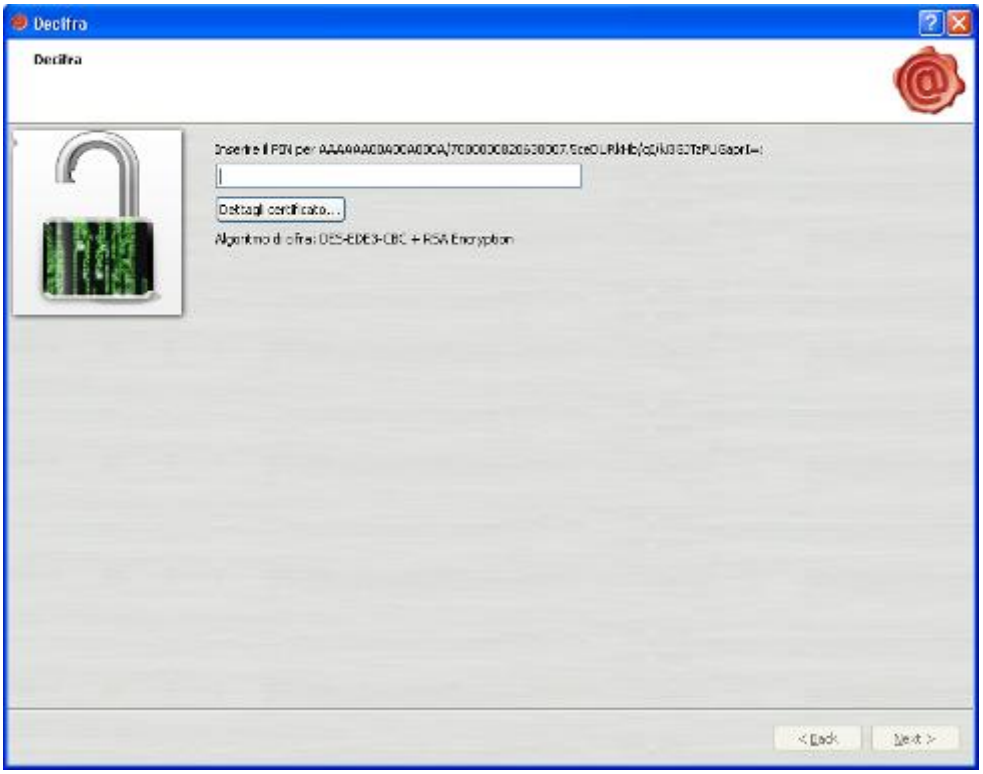
Nota: *Il programma di Cifratura crea un file con estensione ".p7e" che include il file originale.*

16 Decifratura File

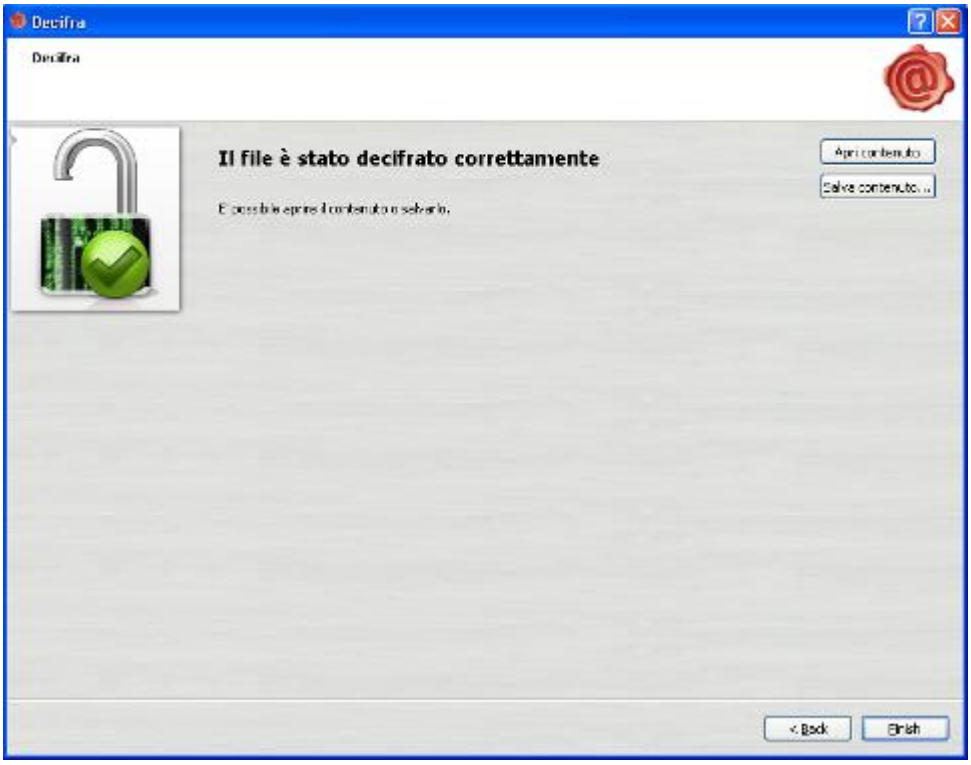
Passo 1
Per cifrare un file selezionare "**Utilities"**.

Passo 2
Trascinare il file **".p7e"** sull'icona **"Decifra"**.

Passo 3
Il Token Usb verifica che nella SIM sia presente almeno uno dei certificati indicati nella fase di cifratura.
Il programma in questa fase chiede il PIN della SIM inserita nel Token USB.



Passo 4
Il Token USB, dopo aver completato il processo di decifratura del file, propone all'utente l'apertura o il salvataggio dello stesso.



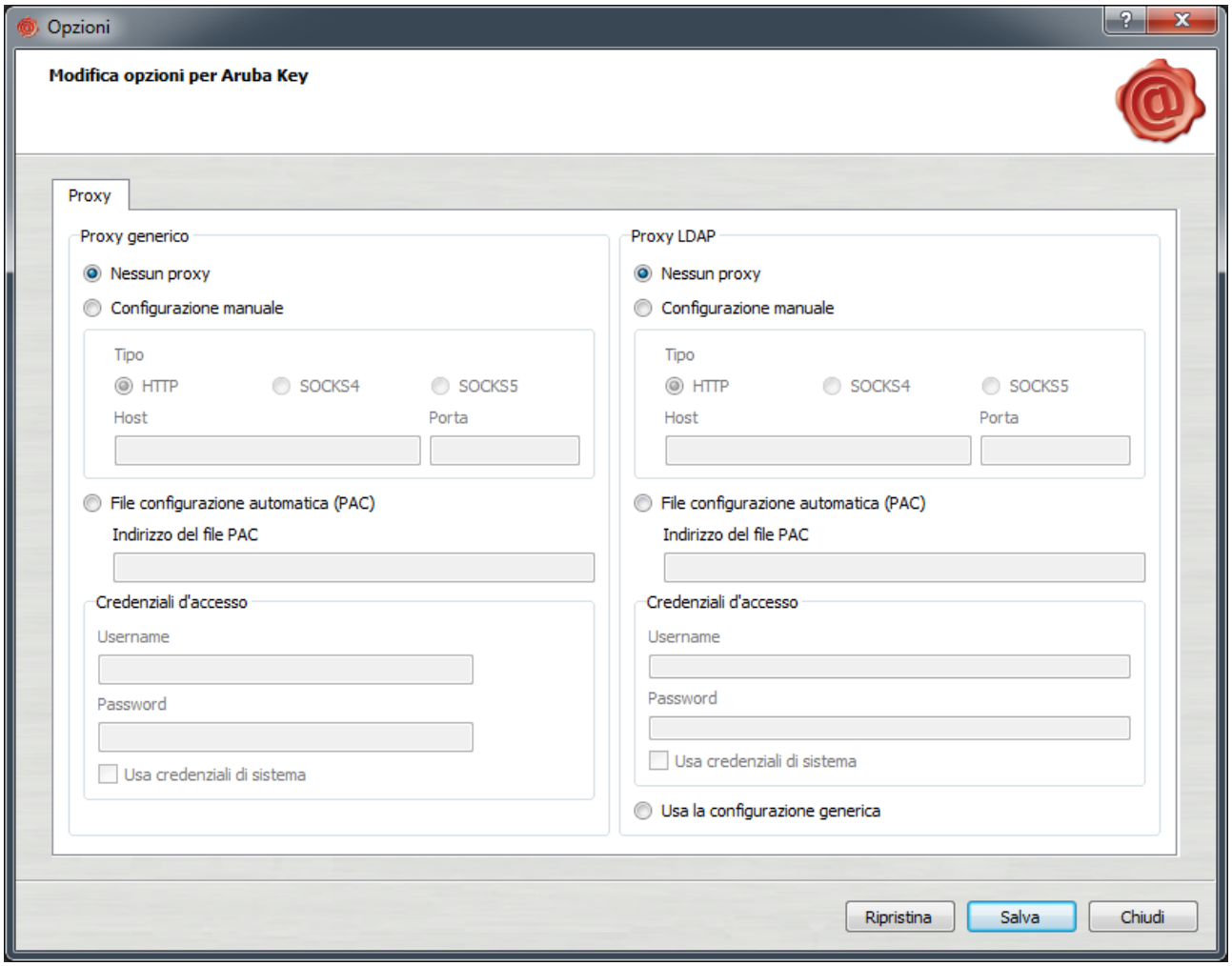
17 Impostazione Proxy

Per utilizzare il Token USB in una rete protetta da Proxy, far riferimento alle seguenti istruzioni:

Passo 1
Selezionare il pulsante "**Utilities".**

Passo2
Cliccare su "**Proxy"**.

Passo 3
Procedere alla configurazione della relative sezione del Proxy (HTTP/LDAP)



Per ciascuna delle due configurazioni (Proxy generico e Proxy LDAP) è possibile selezionare le seguenti opzioni:

- **Nessun proxy**: se selezionato non viene utilizzato nessun proxy;
- **Configurazione manuale**: se selezionato viene utilizzato il proxy specificato da 'Tipo', 'Host' e 'Porta';
- **File configurazione automatica (PAC)**: se selezionato è necessario specificare un indirizzo valido per il file di configurazione automatica del proxy (PAC) nel campo 'Indirizzo del file PAC'.
  L'indirizzo può essere nella forma *http://address/to/file* o *file://path/to/file*. Tale file viene utilizzato per determinare l'indirizzo del proxy da utilizzare (o eventualmente se non utilizzare proxy) per un particolare indirizzo di destinazione.
  NOTA 1: Tale opzione non è attualmente disponibile nelle versioni per Macosx e Linux.

Le credenziali di accesso specificano nome utente e password da utilizzare per l'autenticazione proxy.
Se non specificate su sistemi operativi Windows, verranno utilizzate, se possibile, le credenziali dell'utente attualmente autenticato sul sistema. Se le credenziali non dovessero essere valide per il proxy in uso, ciascun applicativo provvederà alla richiesta delle credenziali quando necessario.

Per la configurazione 'Proxy LDAP' è possibile inoltre selezionare anche l'opzione **Usa la configurazione generica** in modo tale che per indirizzi LDAP venga utilizzata la stessa configurazione specificata in 'Proxy generico'.

Nota: *Se non sono disponibili i dati relativi ad una delle due sezioni HTTP o LDAP (perché ad esempio la rete non supporta entrambe le configurazioni), procedere solo con la sezione relativa alla tipologia di Proxy supportata.*

Passo 4

Se le configurazione è stata salvata correttamente comparirà la seguente finestra.