Aruba Key

V2 - GUIDA RAPIDA

ARUBA PEC

ACTALIS

1 Indice

2 Informazioni sul documento

2.1 Scopo del documento

Il presente documento intende essere una guida rapida per il titolare dell'Aruba Key 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 presente all'interno dell'Aruba Key

3 Caratteristiche del dispositivo

Aruba Key è il dispositivo USB evoluto che permette di avere sempre a portata di mano la propria Firma Digitale e Marca Temporale. Aruba Key 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.

3.1 Prerequisiti

Di seguito sono descritti i prerequisiti Hardware e Software che deve possedere la postazione a cui viene collegata l'Aruba Key.

3.1.1 Software

Sistemi Operativi:

- MS Windows XP, Vista, Seven, Server 2003, Server 2008 (32 e 64 bit)
- Mac Os X Tiger (10.4 - Intel), Leopard (10.5 - Intel), Snow Leopard (10.6 - Intel), Lion (10.7 - Intel) (32 e 64 bit)
- Linux

3.1.2 Rete

Di seguito sono riportati i parametri di rete che devono possedere le postazioni alle quali viene collegata Aruba Key:

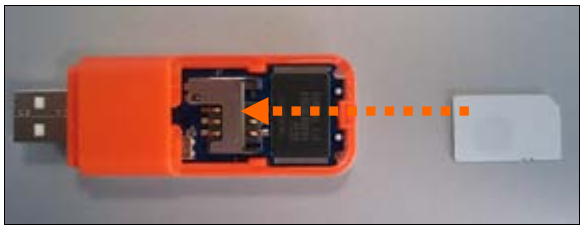
1. Disponibilità di connessione Internet.
2. Possibilità di poter instaurare connessioni HTTP, HTTPS e LDAP.

4 Installazione della smart card

Qualora la smart card non sia già inserita 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.

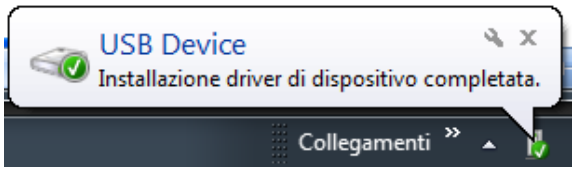


Passo 2:

Una volta inserita la SIM card, reinserire lo sportellino.

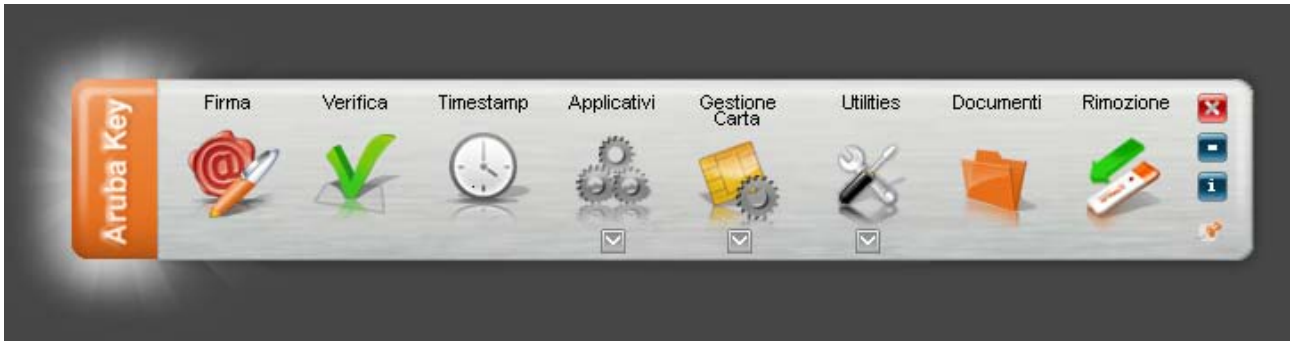
5 Avvio di Aruba Key

Collegare l'Aruba Key ad una presa USB del PC ed attendere che compaia il messaggio indicato nella figura a fianco.



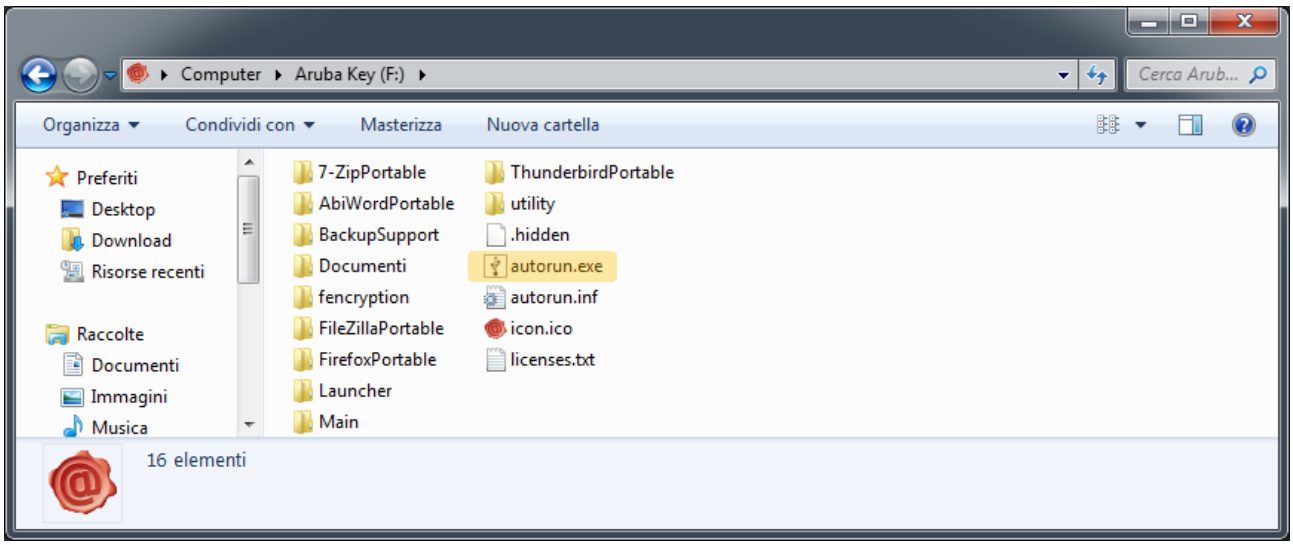
Aruba Key viene vista dal PC come una periferica HID (Human Interface Device), pertanto i driver per il corretto riconoscimento sono presenti all'interno del dispositivo stesso.

Se nella postazione è attiva la funzione di esecuzione automatica (Autorun) al momento del collegamento dell'Aruba Key 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 di Aruba Key, è probabile allora che la funzione di esecuzione automatica sia disattivata.

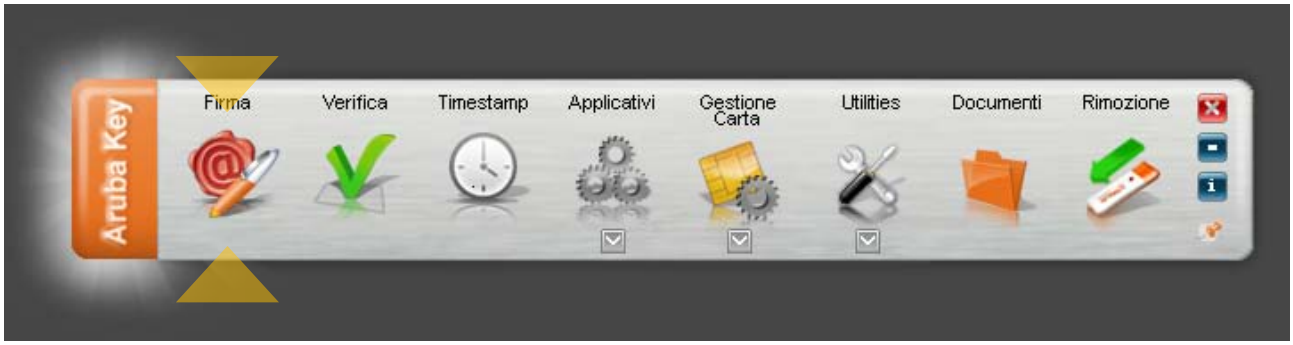
In tal caso, visualizzare il contenuto di Aruba Key ed avviare il file *autorun.exe*, come indicato nella figura seguente.



6 Firmare digitalmente un file in formato P7M

Passo 1

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

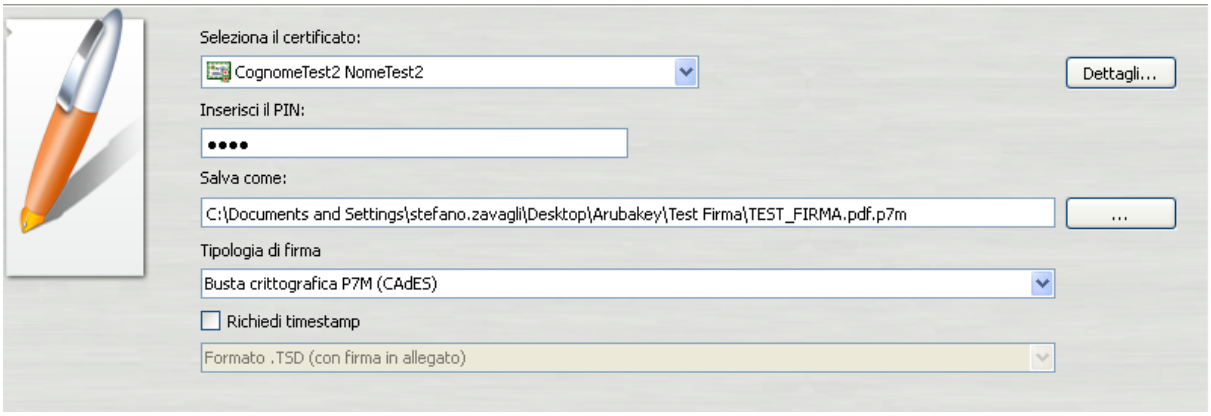


Passo 2

Attendere che Aruba Key recuperi le informazioni relative ai certificati contenuti nella smart card.

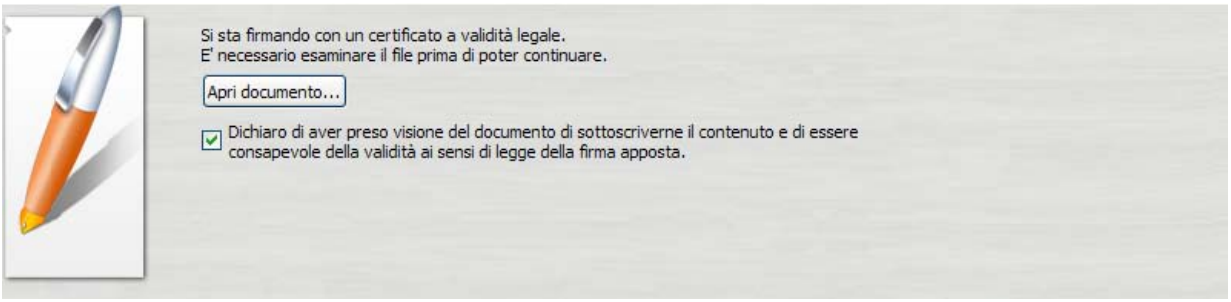
Passo 3

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.

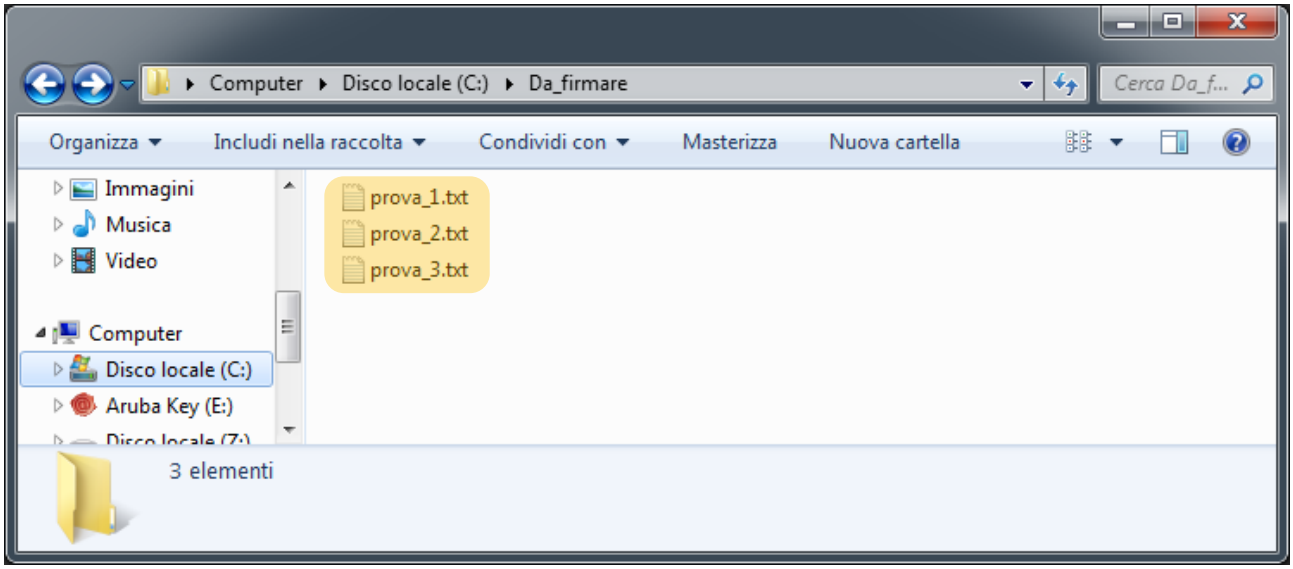
Passo 6

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

6.1 Firmare digitalmente più file in formato P7M

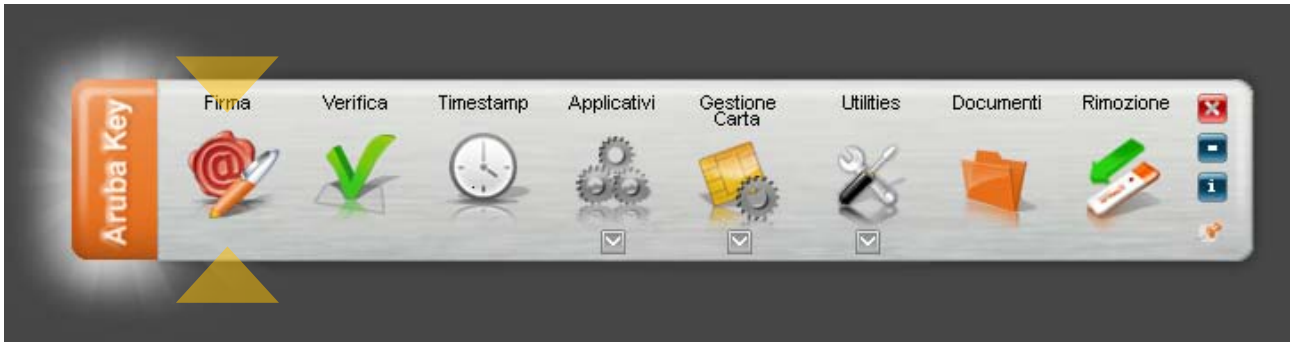
Passo 1

Selezionare tutti i documenti da firmare.



Passo 2

Trascinare i documenti selezionati sopra l'icona **"firma"** e rilasciare il mouse..

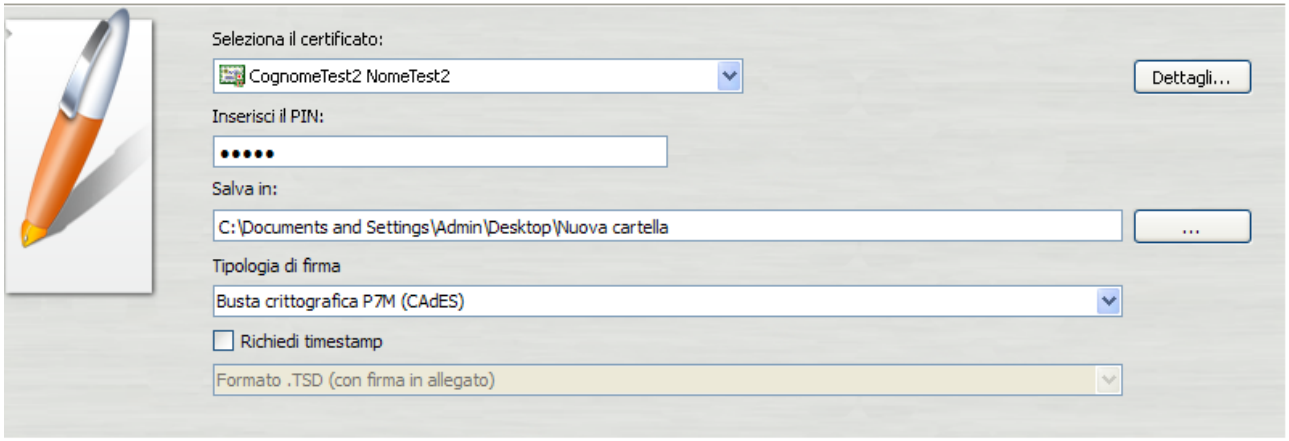


Passo3

Attendere che Aruba Key recuperi le informazioni relative ai certificati contenuti nella smart card.

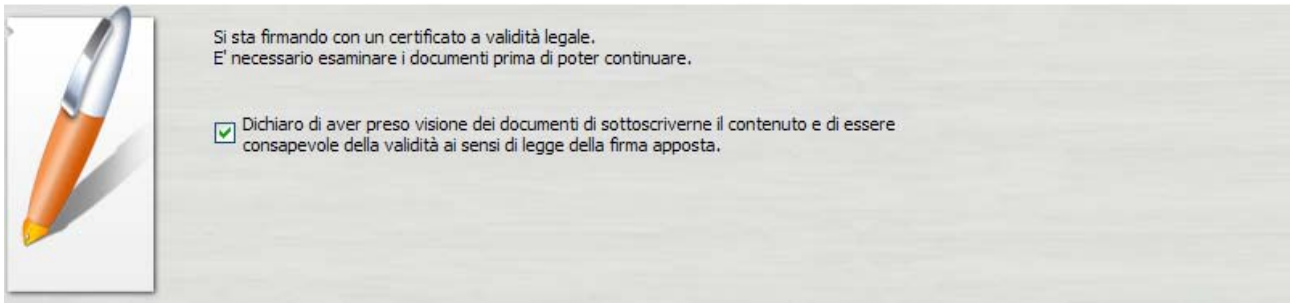
Passo 4

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 *"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. Selezionare l'opzione relativa alla presa visione dei documenti;
b. Cliccare sul pulsante **Next >**

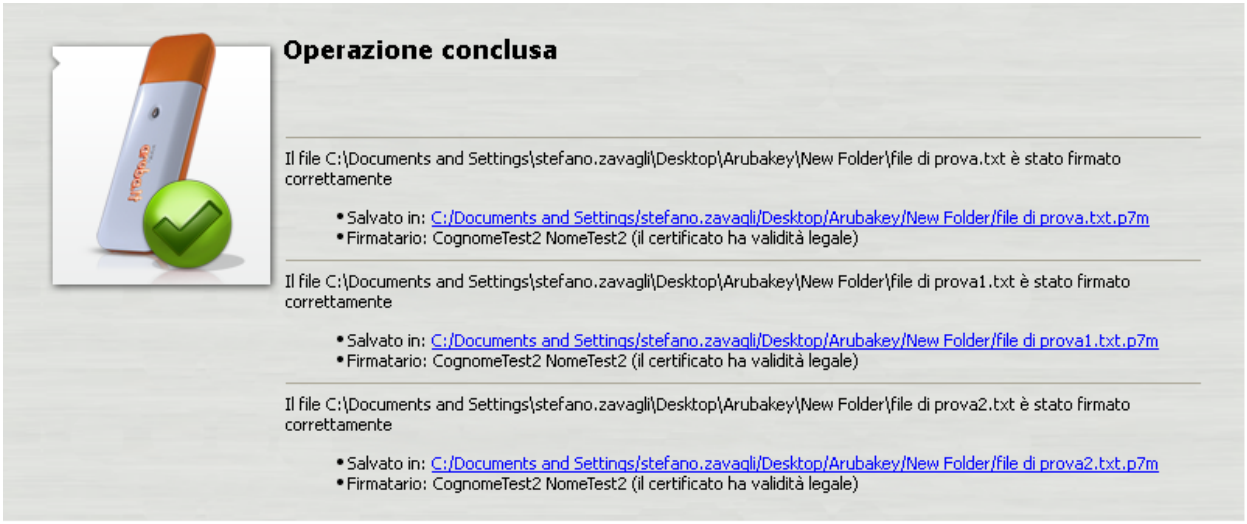


Passo 6

Attendere il completamento dell'operazione di firma.

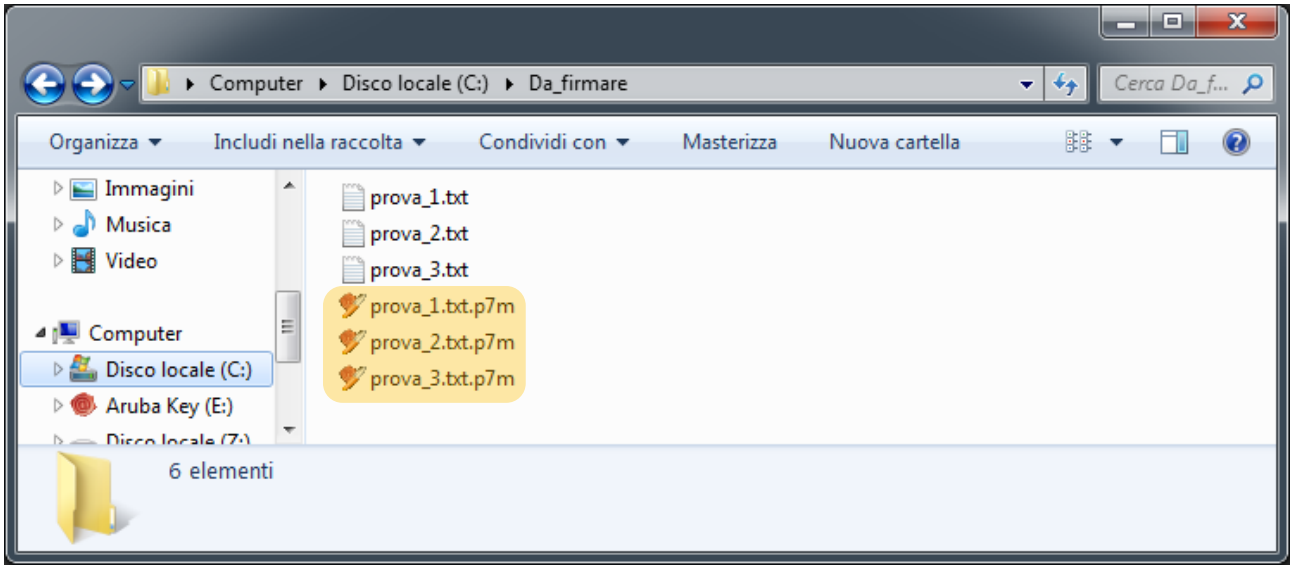
Passo 7

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



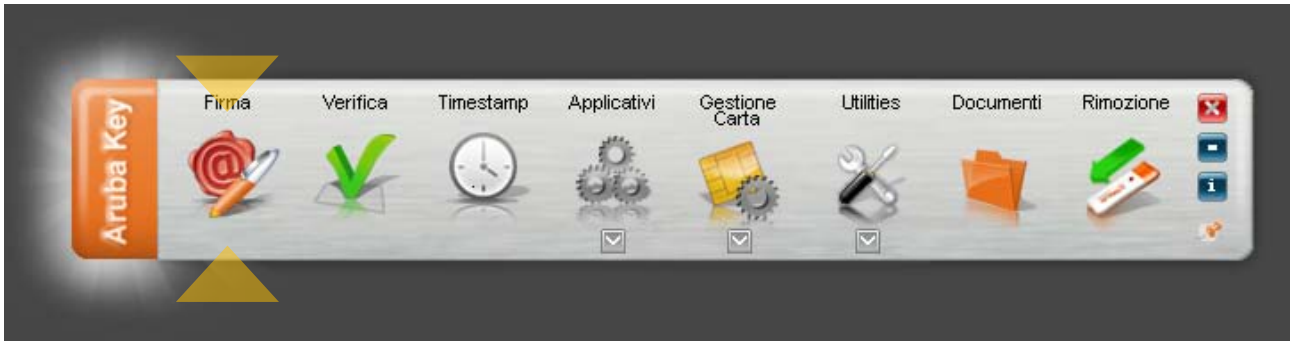
Passo 8

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



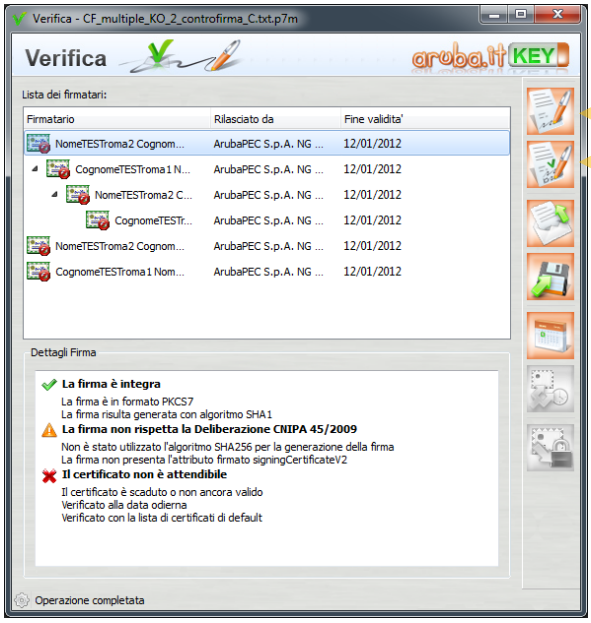
6.2 Funzione di Firma Eveloped e Firma Multipla

Trascinando sopra il pulsante di firma un file già firmato in formato p7m è possibile accedere alle funzioni di **Firma Multipla** o **Firma Enveloped**, vedi figure seguenti:



NOTA: Per attivare le funzioni appena citate è necessario che utilizzare un file firmato digitalmente che rechi in modo esplicito nel nome file l'estensione .p7m.

Selezionando **Firma Multipla** viene avviata la finestra di verifica del file firmato all'interno della quale è possibile poi selezionare la firma alla quale s'intende apporre una **Firma Parallela** (primo pulsante dall'alto nella colonna di destra) o **Controfirma** (secondo pulsante dall'alto).



Firma Parallela: E' un tipo di firma che viene aggiunta allo stesso livello di una firma già preesistente. Questa firma è apposta allo stesso contenuto della firma precedente e viene di norma utilizzata per aggiungere firme ad un documento già firmato in quei flussi documentali che ne prevedono l'utilizzo.

Controfirma: E' quel tipo di firma che viene inserita ad un livello sottostante ad una firma preesistente e di fatto sottoscrive quest'ultima. Questa firma è più annidata rispetto alla firma a cui si riferisce e di norma questo aspetto è messo in evidenza attraverso una rappresentazione ad albero delle firme.

Selezionando **Firma Enveloped** viene invece avviato il wizard per la firma dell'intero documento e le operazioni che l'utente deve svolgere sono le stesse indicate al paragrafo 6 (passo 2 in poi)

7 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 Aruba Key, firmare in PDF un file che non sia già stato convertito in questo formato.

Passo 1

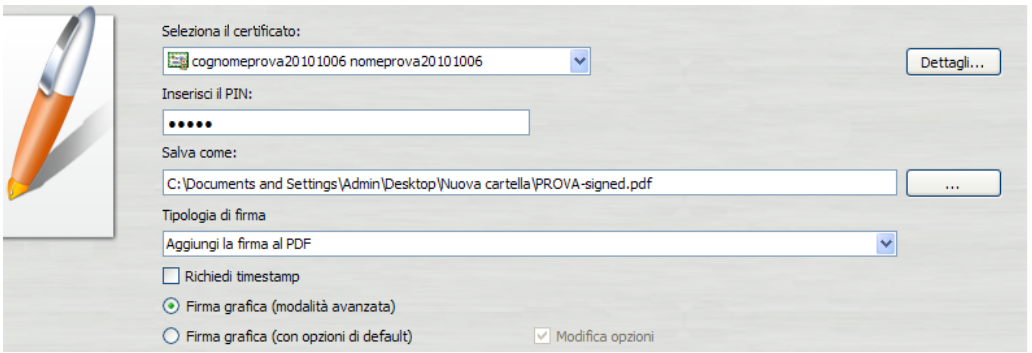
Trascinare il file PDF sopra il pulsante **"Firma".**

Passo 2

Attendere che Aruba Key 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 >**

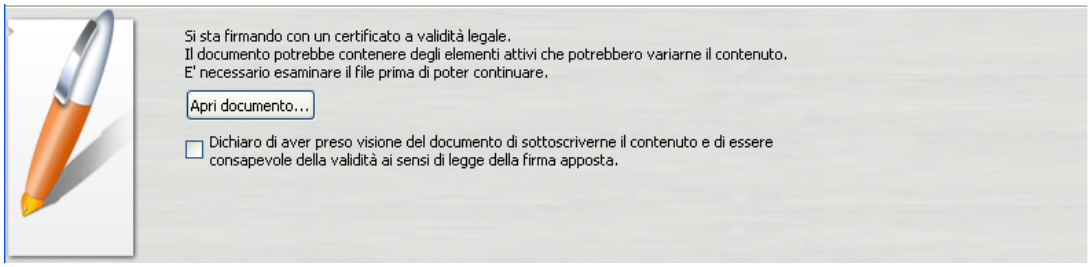


Passo 4

a. Visualizzare eventualmente il contenuto del documento attraverso il pulsante **Apri documento**;

b. Selezionare l'opzione relativa alla presa visione del documento;

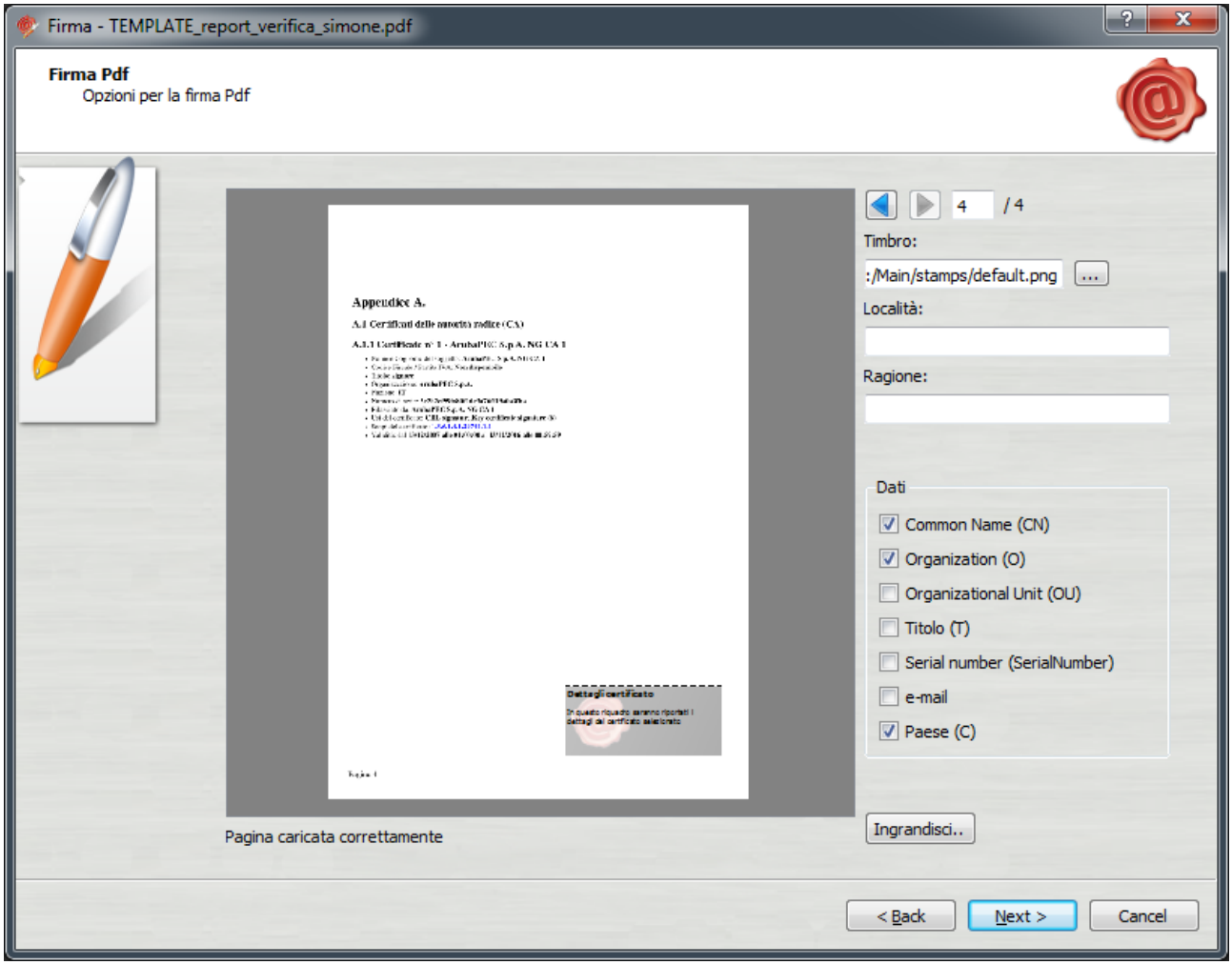
c. Cliccare sul pulsante **Next >**



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.

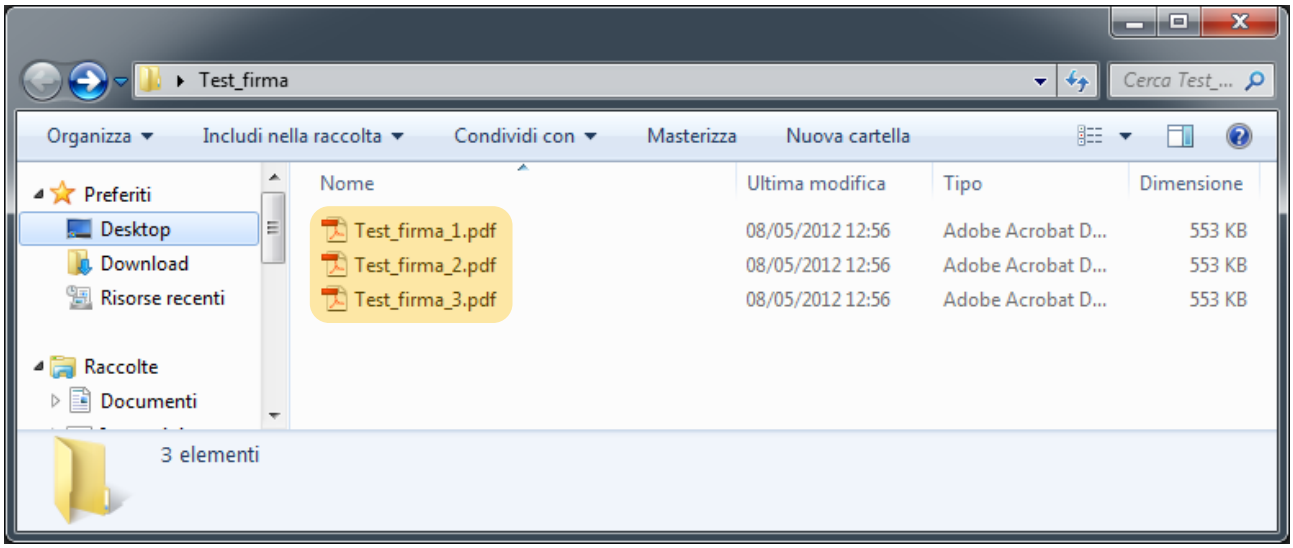
Passo 7

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

7.1 Firmare digitalmente più file in formato PDF

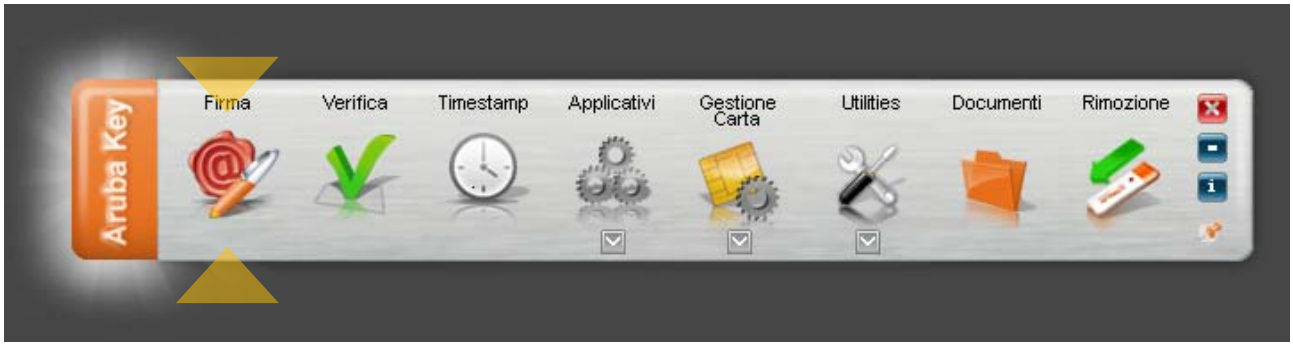
Passo 1

Selezionare tutti i documenti PDF da firmare.



Passo 2

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

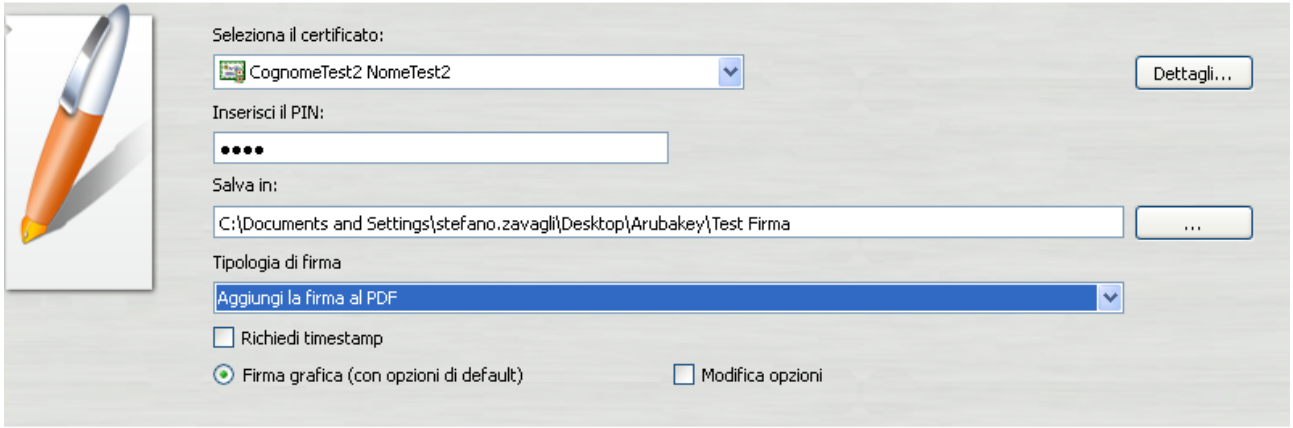


Passo 3

Attendere che Aruba Key recuperi le informazioni relative ai certificati contenuti nella smart card.

Passo 4

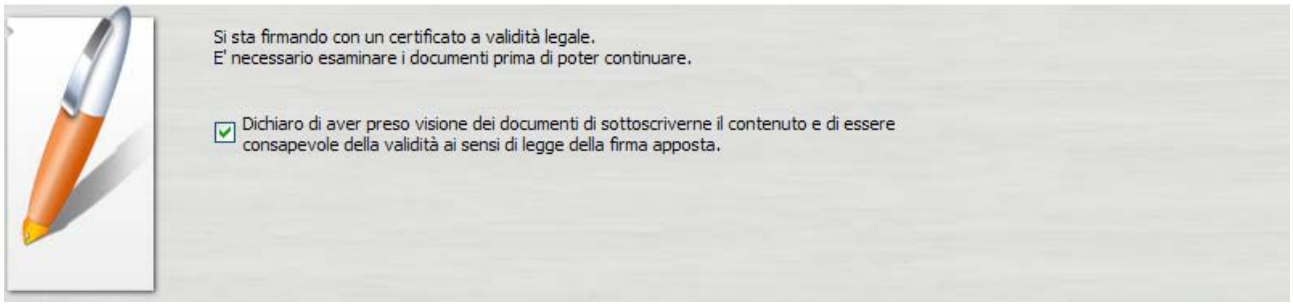
a. Assicurarsi che sia selezionato il certificato per la firma digitale (Cognome Nome);
b. Inserire il PIN di protezione della smart card;
c. Selezionare l'opzione *"Aggiungi la firma al PDF";*
d. Cliccare sul pulsante **Next >**



Passo 5

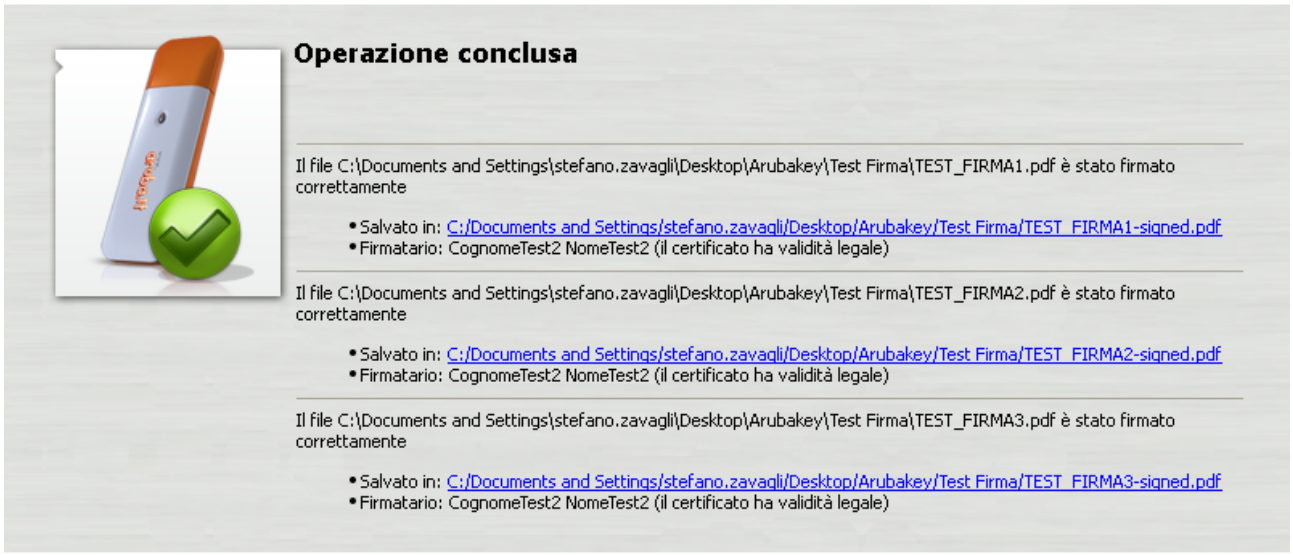
c. Selezionare l'opzione relativa alla presa visione dei documenti;

d. Cliccare sul pulsante **Next >**



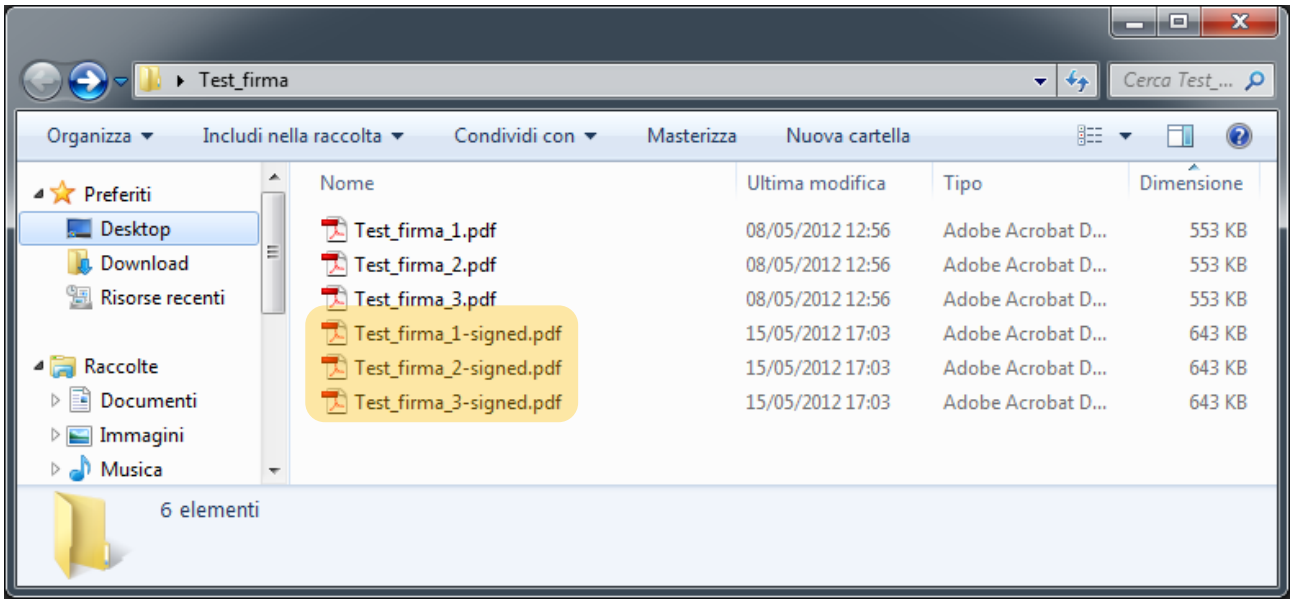
Passo 6

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



Passo 7

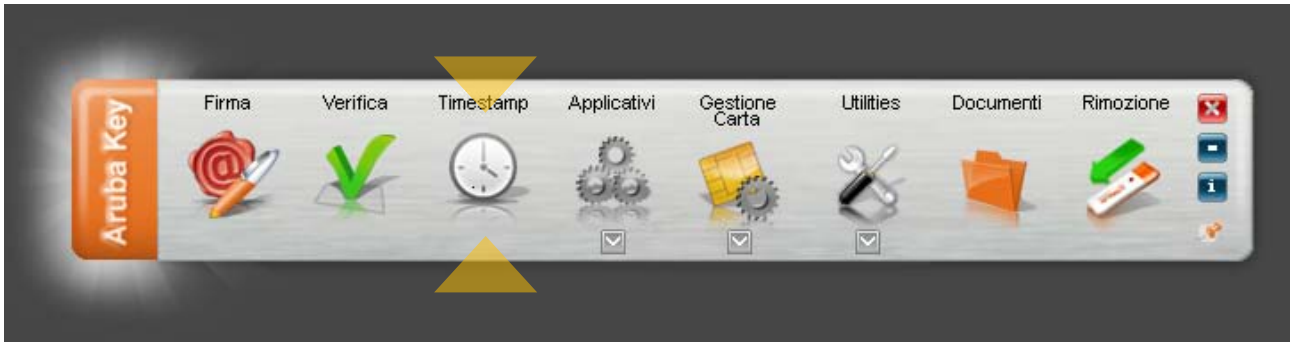
I documenti firmati verranno salvati nella stessa cartella dove risiedono i documenti originali aggiungendo al nome il suffisso “signed”.



8 Apposizione di marche temporali

Passo 1

Trascinare il file da marcare sopra il pulsante **"Timestamp".**



Passo 2

a. Selezionare l'account da utilizzare per la richiesta di marcatura temporale;

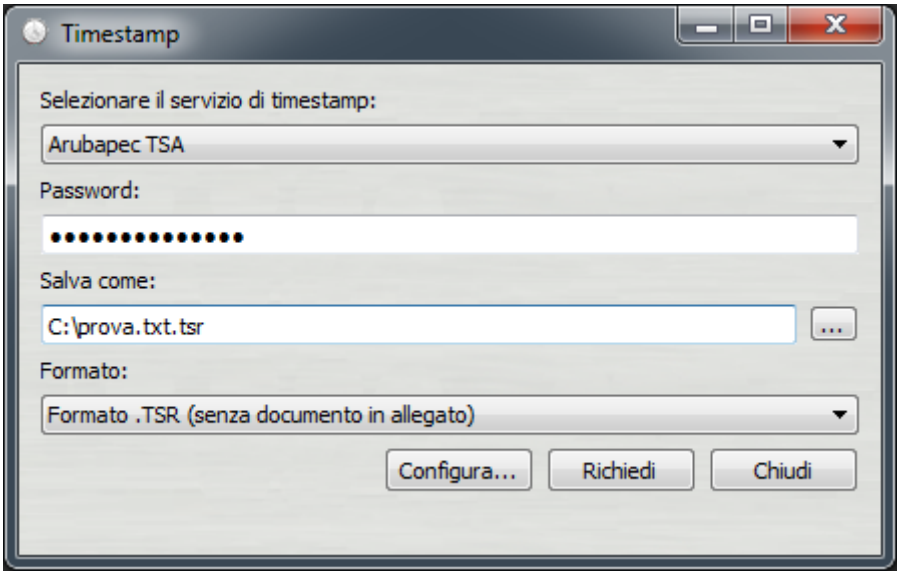
b. Inserire la password per l'accesso al servizio di marcatura temporale;

ATTENZIONE: La password che deve essere inserita in questo step è quella ottenuta a seguito dell'acquisto e attivazione di un lotto di marche temporali.

In questa fase quindi NON deve essere inserito alcun codice di sicurezza contenuto nella busta ricevuta assieme alla smart card (ad esempio PIN PUK o Codice Utente);

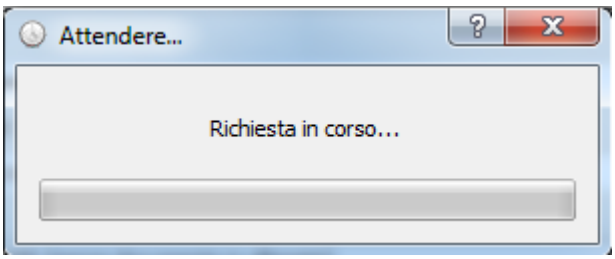
c. Verificare che il percorso utilizzato per salvare il file marcato sia quello desiderato;

d. Selezionare il formato di salvataggio della marca temporale;



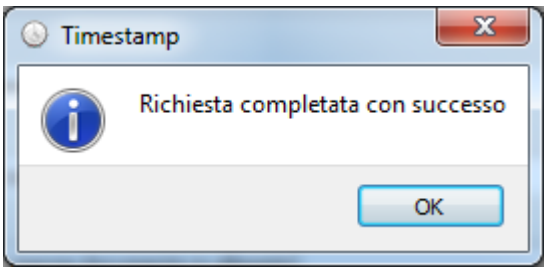
Passo 3

Attendere il completamento dell'operazione di marcatura temporale.



Passo 4

Cliccare OK al messaggio che notifica la corretta marcatura del file.



Passo 5

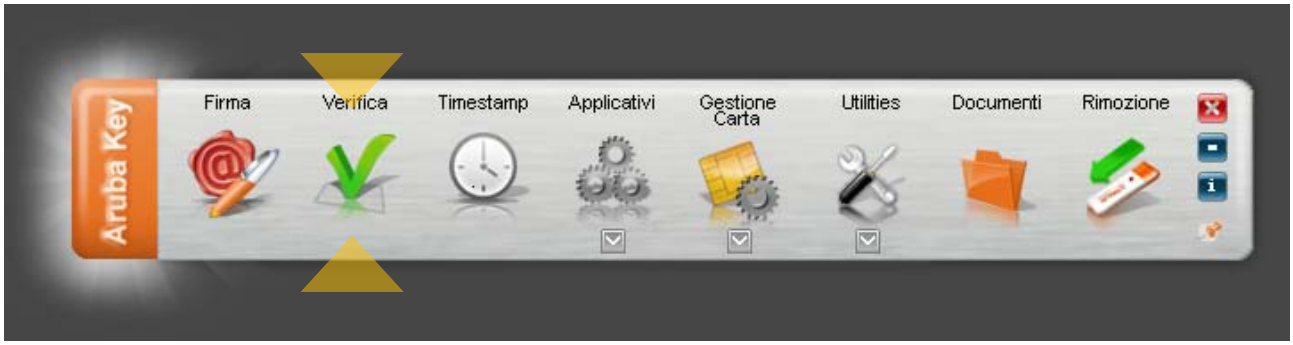
Recuperare il file marcato memorizzato nel percorso indicato al Passo 2.

9 Verifica di file firmati

Passo 1

Trascinare il file da verificare sopra il pulsante **“Verifica”.**

NOTA: Le indicazioni riportate di seguito sono applicabili ai file firmati in formato p7m (CAdES) e pdf (PAdES).



Passo 2

Completate le verifiche Aruba Key restituirà una finestra di riepilogo simile alla seguente:

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

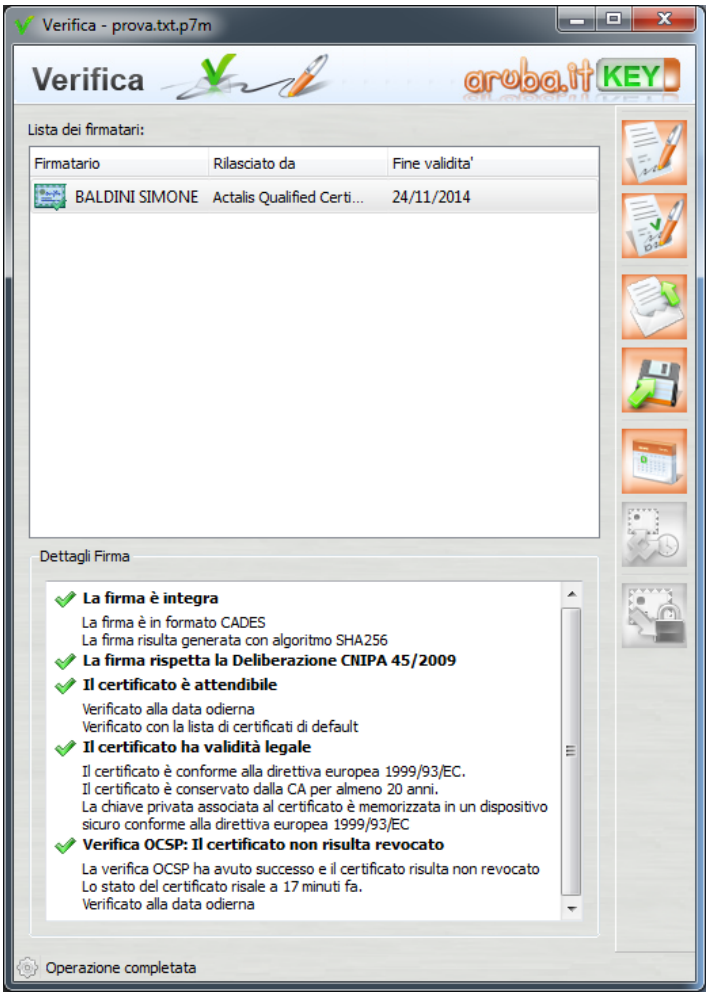
Questa sezione contiene dettagli aggiuntivi sugli algoritmi utiliz oltre ad indicare dettagli sugli standard utilizzati per la generazione

La firma rispetta la Deliberazione CNIPA 45/2009.
Notifica circa il rispetto delle previsioni contenute negli ultimi aggiornamenti normativi

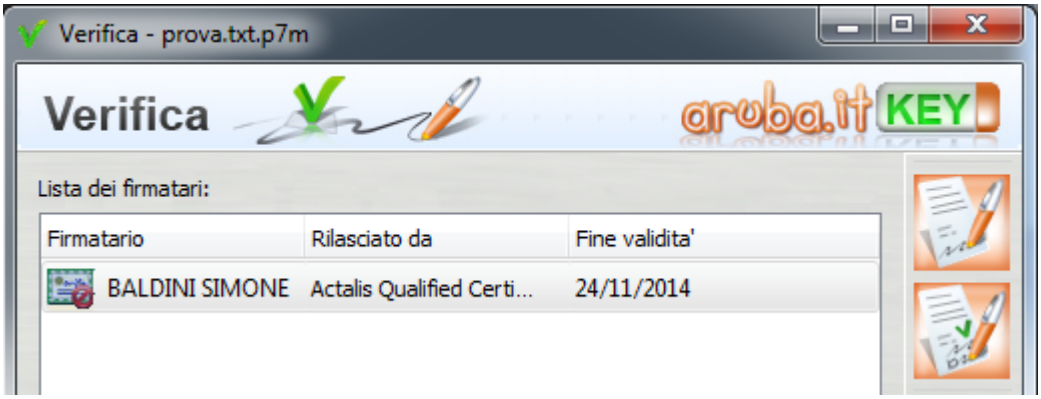
Il certificato è attendibile.
Il messaggio indica che il certificato del sottoscrittore è garantito da una Autorità di Certificazione inclusa nell’Elenco Pubblico dei Certificatori e che non risulta scaduto alla data della verifica.

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.

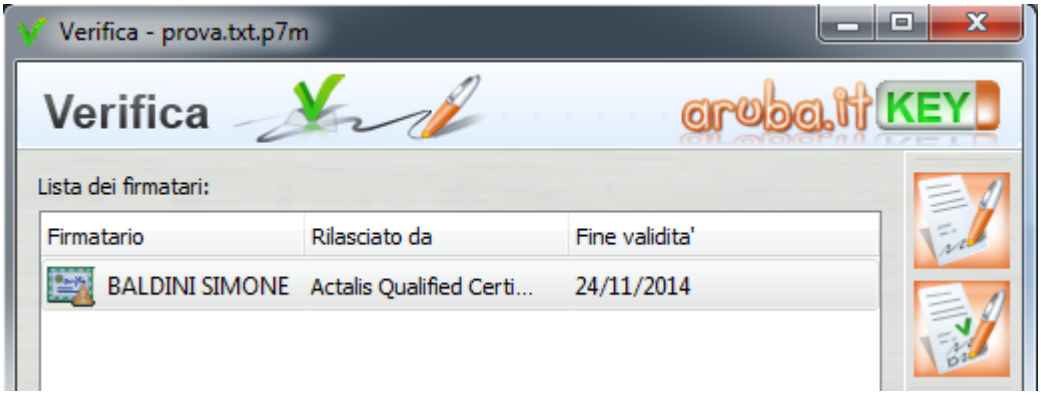


Qualora la finestra di riepilogo dovesse mostrare un esito simile al seguente:



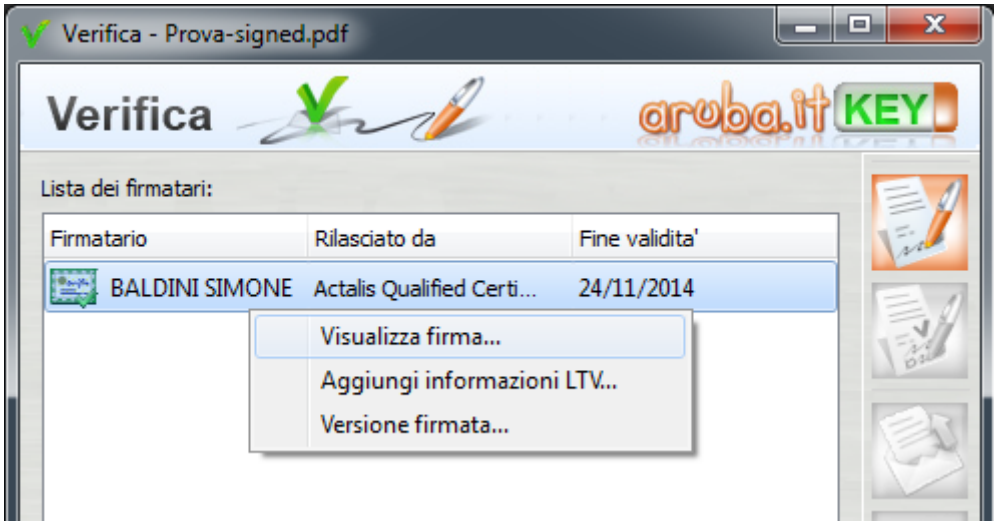
Allora ciò sta ad indicare che sono stati portati a termine tutti i controlli previsti per la verifica della validità della firma, ma qualcuno di questi non è andato a buon fine. Per analizzare meglio il tipo di errore riscontrato è sufficiente visualizzare i messaggi restituiti dall'applicativo all'interno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

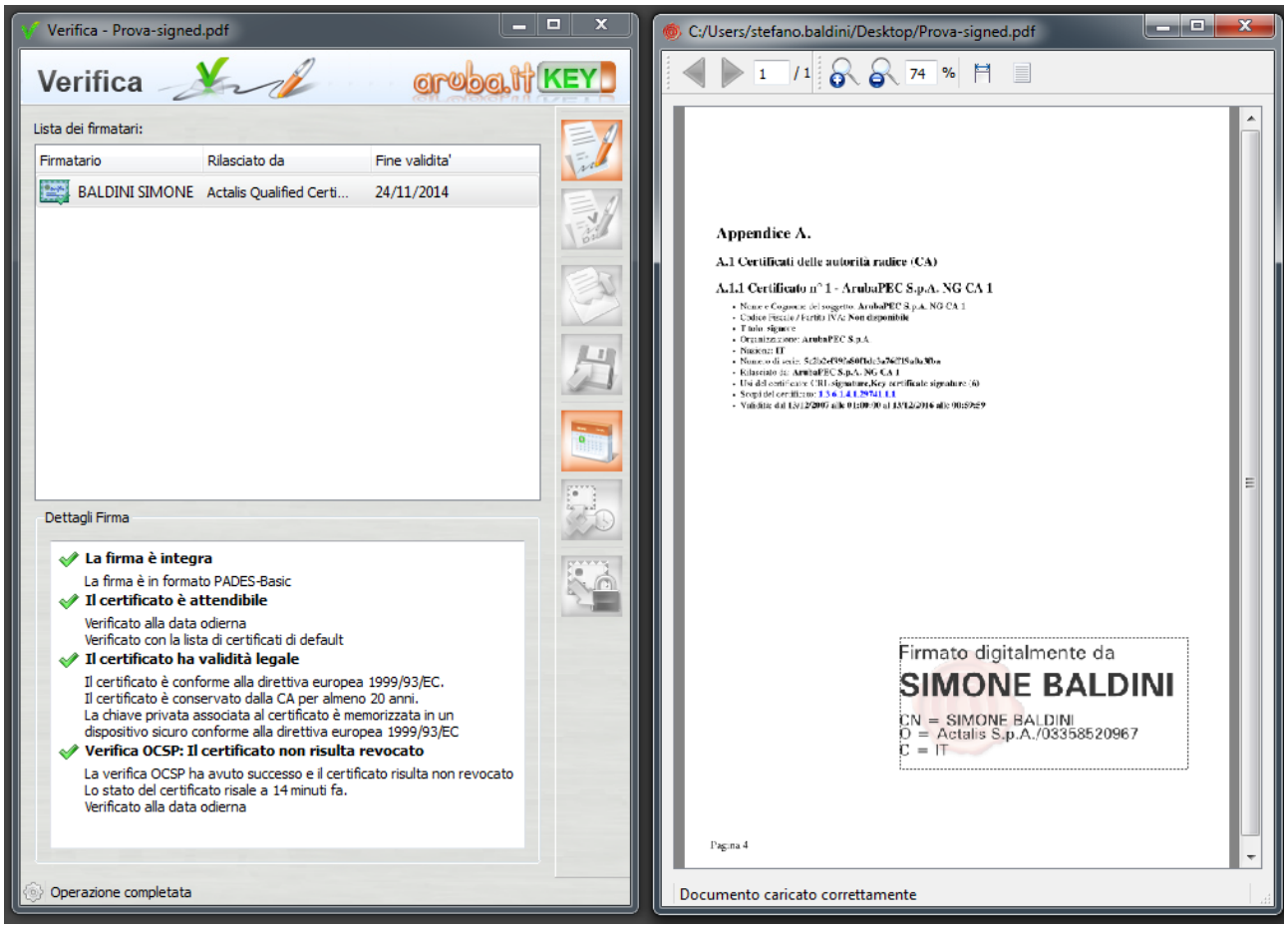
Qualora invece la finestra di riepilogo dovesse mostrare un messaggio simile al seguente:



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".

Nel caso in cui si stia verificando un file pdf firmato (identificabile dal tipo firma pari a **PADES-Basic** o **PADES-BES**) è possibile visualizzare il documento cliccando con il tasto destro del mouse sulla particolare firma e selezionando **Visualizza Firma.**

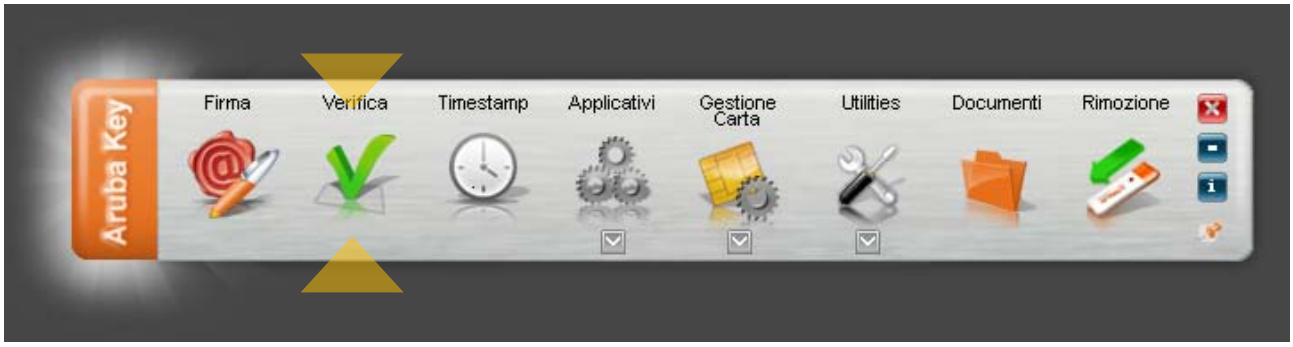




10 Verifica marche temporali

Passo 1

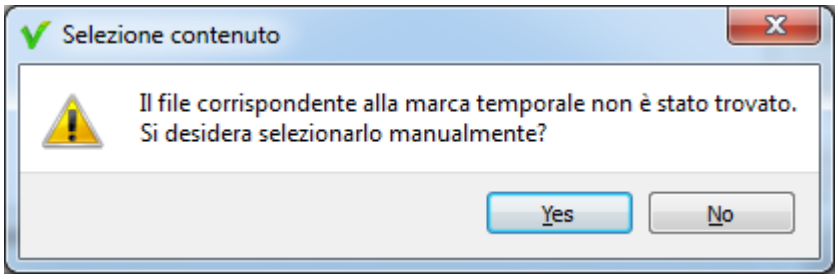
Trascinare la marca temporale da verificare sopra il pulsante **“Verifica”.**



Passo 2

Il software, come primo passo, esegue l’associazione Marca Temporale <-> File Marcato.

Durante questa fase viene automaticamente verificata la presenza del file associato alla marca all’interno della stessa cartella dalla quale quest’ultima è stata selezionata e, nel caso in cui la ricerca dia esito negativo, viene richiesto all’utente se intende selezionare manualmente il file associato alla marca che sta verificando (vedi figura seguente).



Selezionare il file e cliccare su Apri.

Passo 3

Il software attiva la verifica e, terminate le operazioni, mostra una finestra di riepilogo simile alla seguente:

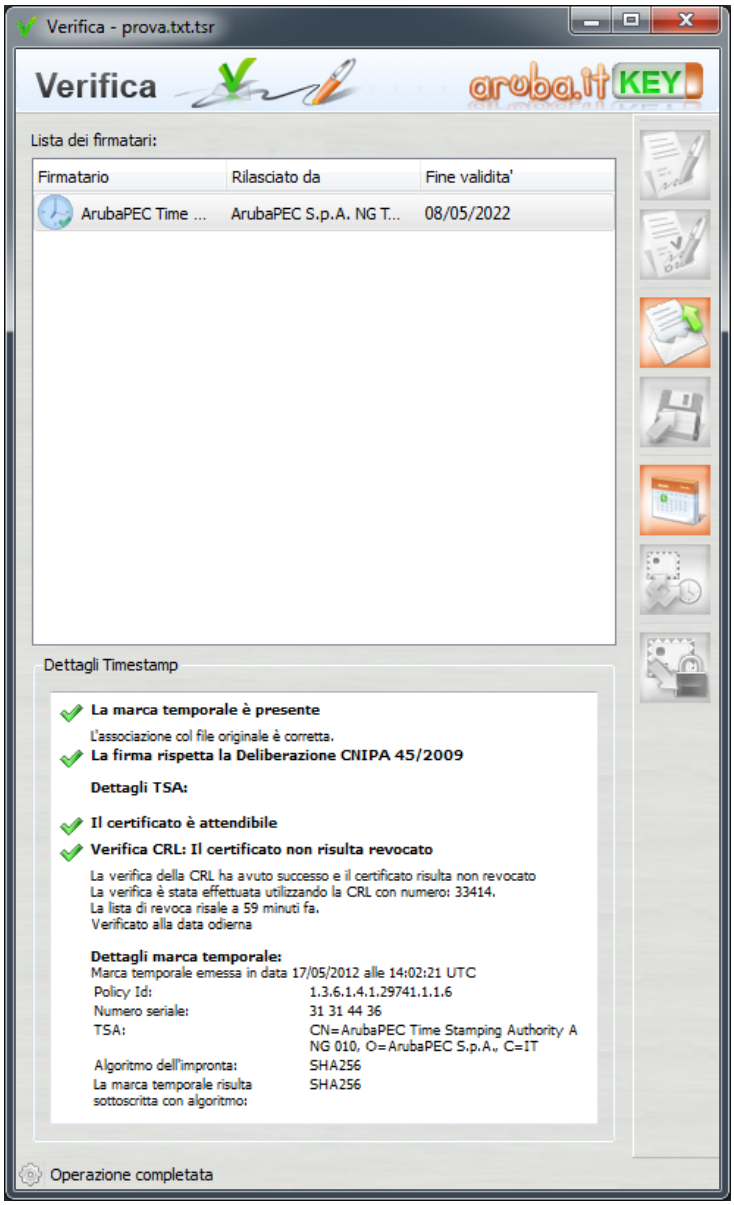
La marca temporale è presente
Questo messaggio indica che la marca temporale è integra ed è correttamente associata al documento selezionato.

La firma rispetta la Deliberazione CNIPA 45/2009.
Notifica circa il rispetto delle previsioni contenute negli ultimi aggiornamenti normativi

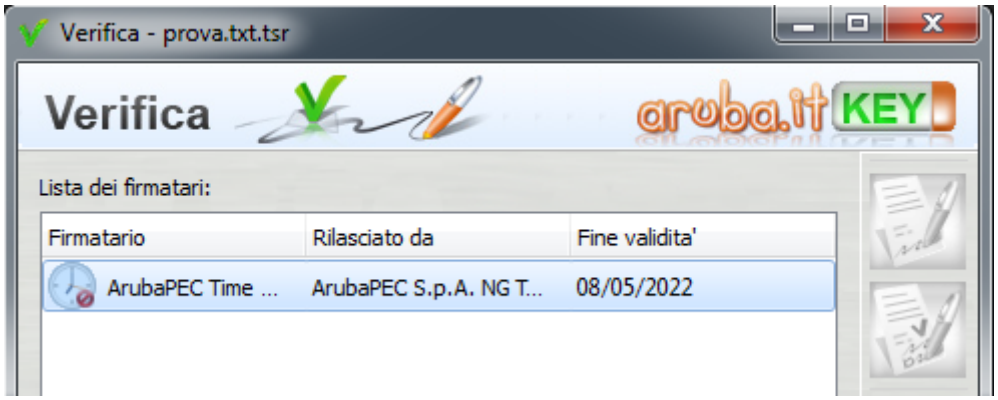
Il certificato è attendibile
Questo messaggio sta ad indicare che la Marca Temporale è rilasciata da un'Autorità di Certificazione inclusa nell'Elenco Pubblico dei Certificatori

Il certificato non risulta revocato
Questo messaggio sta ad indicare che il certificato del Sistema di Marcatura Temporale non risulta nè revocato nè sospeso.

Dettagli marca temporale
Sotto questa voce sono riportati i dettagli della marca temporale.

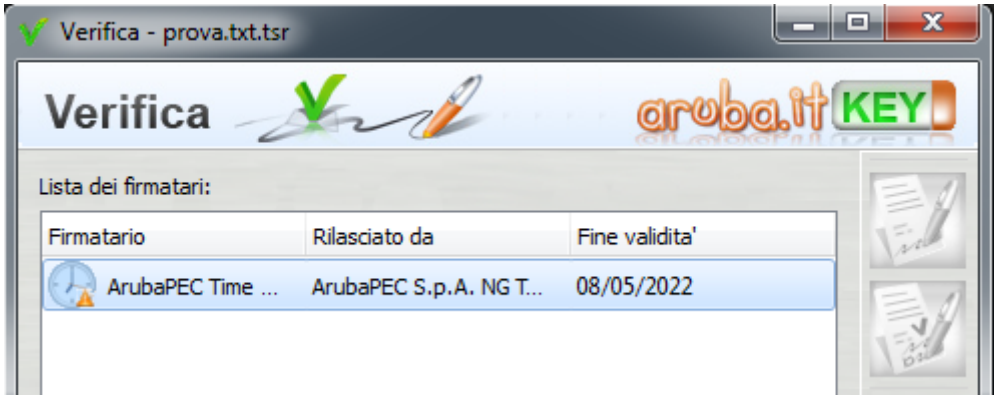


Qualora la finestra di riepilogo dovesse mostrare un esito simile al seguente:



Allora ciò sta ad indicare che sono stati portati a termine tutti i controlli previsti per la verifica della validità della marca, 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 Timestamp".

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

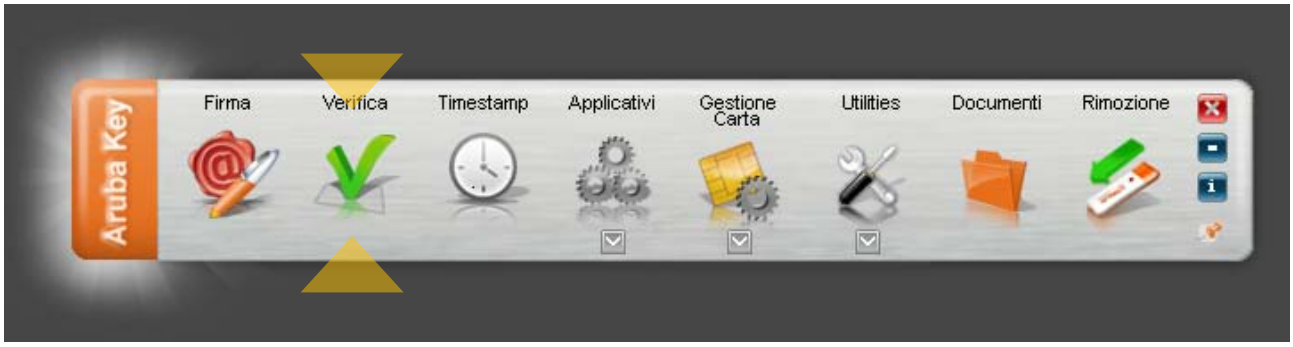


Allora ciò sta ad indicare che non è stato possibile portare a termine tutti i controlli previsti per verificare la validità della marca ed è necessario analizzare meglio il tipo di errore riscontrato visualizzando i messaggi restituiti dall'applicativo all'interno della sezione "Dettagli Timestamp".

11 Verifica di Marche Temporali in formato .TSD

Passo 1

Trascinare la marca temporale da verificare sopra il pulsante **"Verifica".**



Passo 2

Il software inizia la verifica e, finite le operazioni, mostra una finestra di riepilogo simile alla seguente:

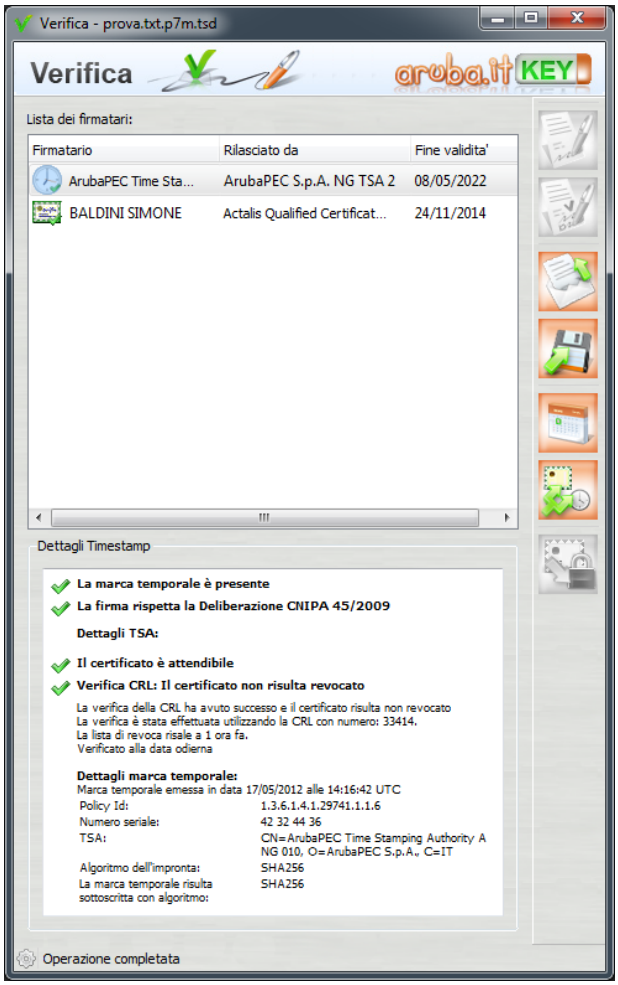
La marca temporale è presente
Questo messaggio indica che la marca temporale è integra ed è correttamente associata al documento selezionato.

La firma rispetta la Deliberazione CNIPA 45/2009.
Notifica circa il rispetto delle previsioni contenute negli ultimi aggiornamenti normativi

Il certificato è attendibile
Questo messaggio sta ad indicare che la Marca Temporale è rilasciata da un'Autorità di Certificazione inclusa nell'Elenco Pubblico dei Certificatori

Il certificato non risulta revocato
Questo messaggio sta ad indicare che il certificato del Sistema di Marcatura Temporale non risulta nè revocato nè sospeso.

Dettagli marca temporale
Sotto questa voce sono riportati i dettagli della marca temporale.



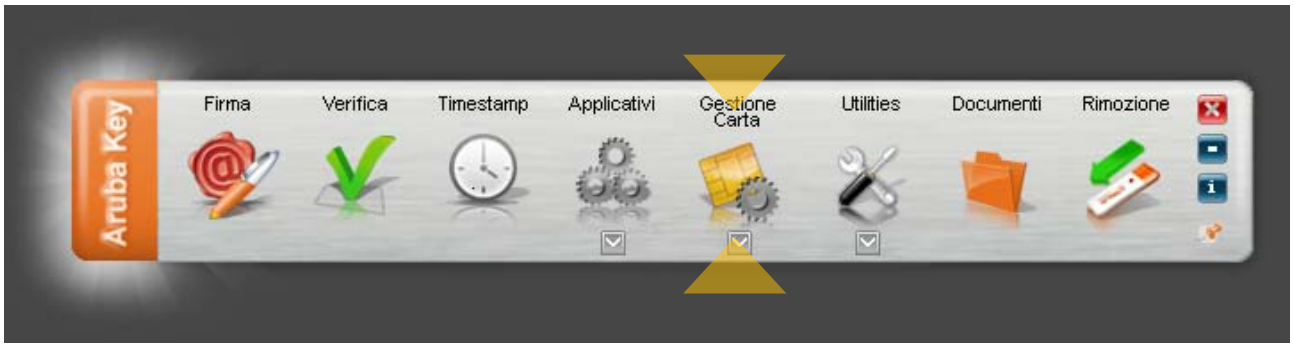
NOTA:
Qualora la finestra di riepilogo dovesse mostrare un delle spunte di errore (rosse) o di avviso (gialle) collegate alla marca temporale, valgono le stesse considerazioni riportate al Capitolo 10.

12 Gestione smart card

12.1 Cambio del pin

Passo 1

Per cambiare il codice PIN della carta inserita a bordo dell'Aruba Key cliccare sopra il pulsante "**Gestione Carta" .**

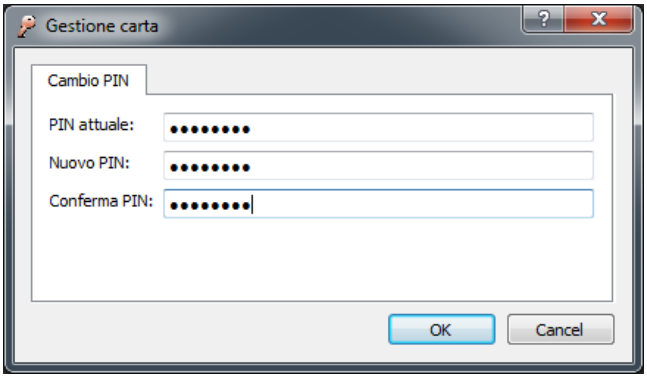


Passo 2

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

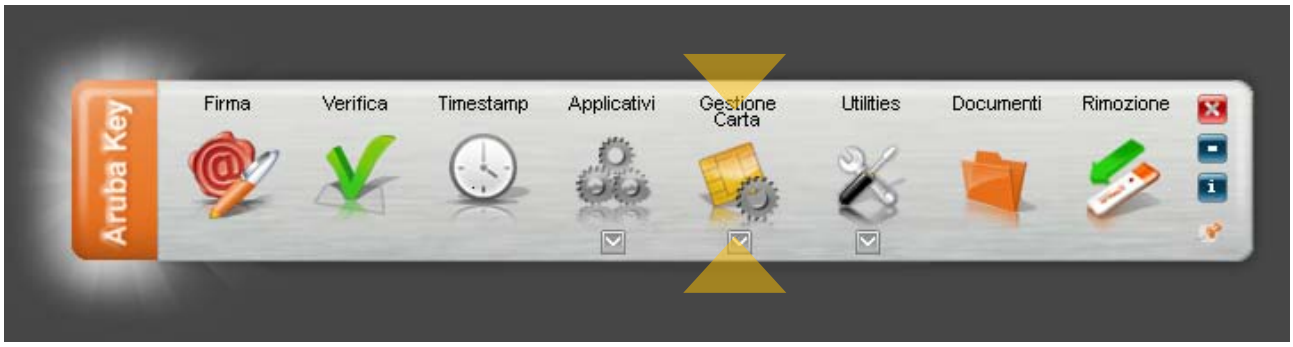


ATTENZIONE:
Per il codice PIN non sono ammessi caratteri alfabetici (a,b,A,B, etc..) ma solo numerici (0,1,2,3,4,5,6,7,8 e 9). Ai fini della sicurezza si consiglia l'utilizzo di codici PIN composti almeno da 8 numeri.

12.2 Sblocco del PIN

Passo 1

Per sbloccare il codice PIN della carta inserita a bordo dell'Aruba Key cliccare sopra il pulsante **"Gestione Carta".**

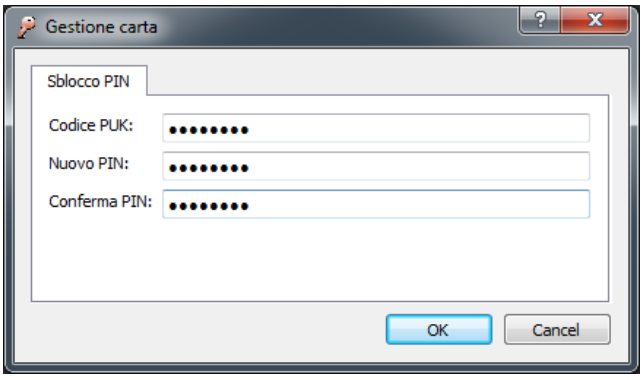


Passo 2

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.

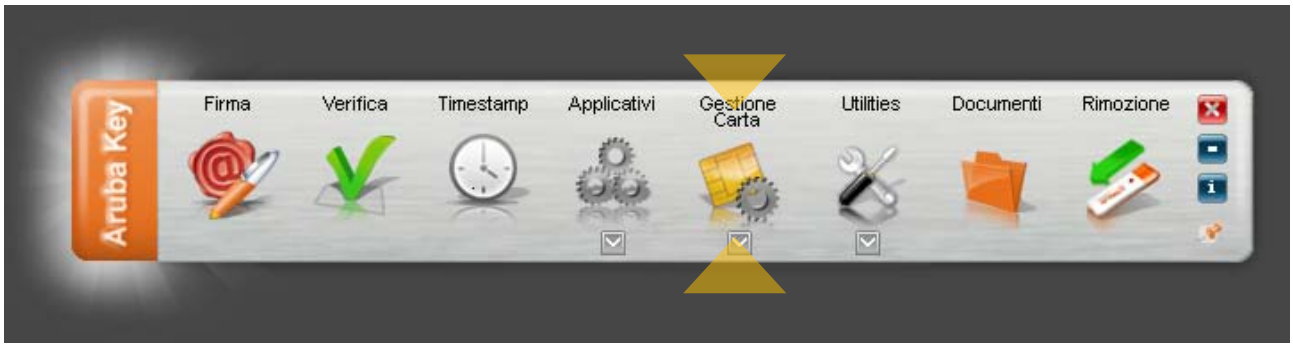


ATTENZIONE:
Per il codice PIN non sono ammessi caratteri alfabetici (a,b,A,B, etc..) ma solo numerici (0,1,2,3,4,5,6,7,8 e 9). Ai fini della sicurezza si consiglia l'utilizzo di codici PIN composti almeno da 8 numeri.

12.3 Cambio del PUK

Passo 1

Per cambiare il codice PUK della carta inserita a bordo dell'Aruba Key cliccare sopra il pulsante "**Gestione Carta".**



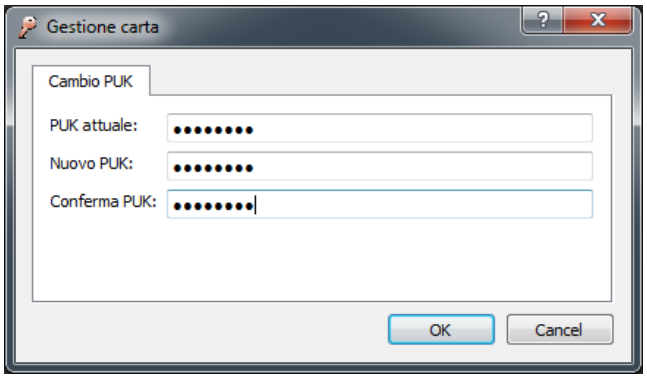
Passo 2

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.

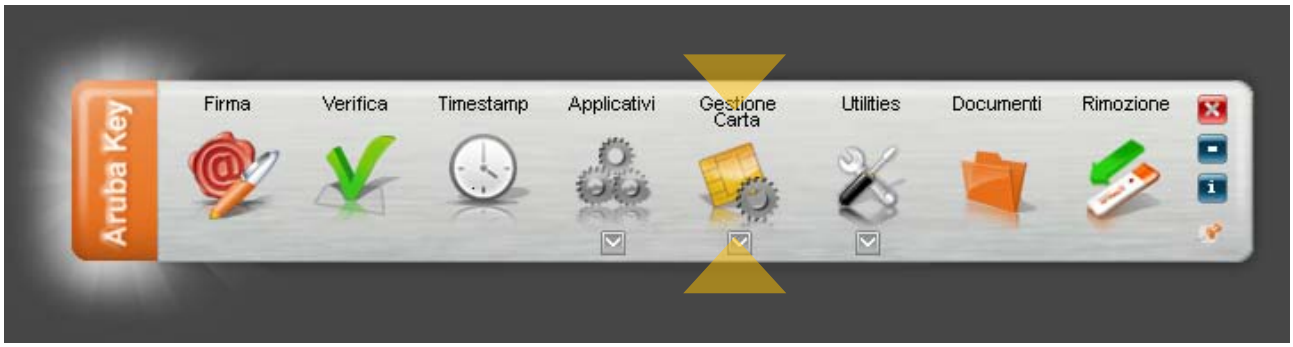
ATTENZIONE:
Per il codice PUK non sono ammessi caratteri alfabetici (a,b,A,B, etc..) ma solo numerici (0,1,2,3,4,5,6,7,8 e 9). Ai fini della sicurezza si consiglia l'utilizzo di codici PUK composti almeno da 8 numeri.



12.4 Lettura informazioni carta

Passo 1

Per recuperare le informazioni relative alla carta presente a bordo dell'Arubakey cliccare su "**Gestione Carta".**



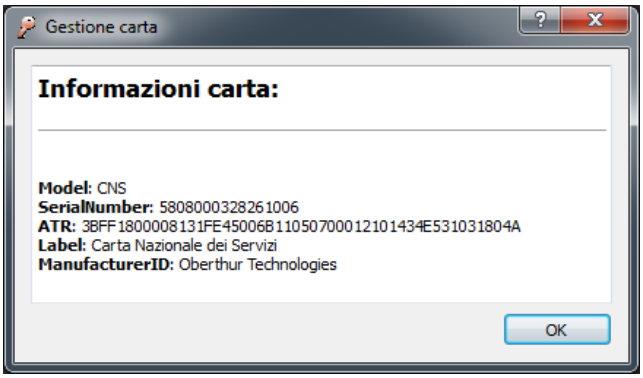
Passo 2

Cliccare su **"Info Carta"**.

Passo 3

All'interno della finestra "Gestione Carta" sono riportate le seguenti informazioni:

- Modello;
- Numero Seriale della smart card;
- ATR della smart card;
- Eventuale Label associata alla smart card;
- Produttore della smart card



12.5 Codici di errore gestione carta

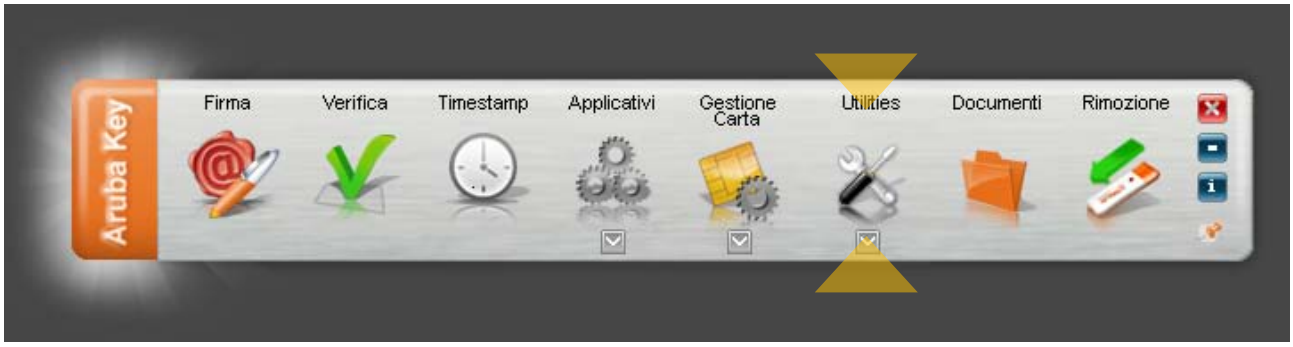
Durante l'operazione di **cambio del PIN**, **sblocco PIN** e **cambio PUK** Arubakey può restituire i seguenti messaggi d'errore:

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".
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 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 Aruba Key

Passo 1

Per accedere all'applicazione di auto-diagnosi presente a bordo dell'Aruba Key cliccare su "**Utilities".**



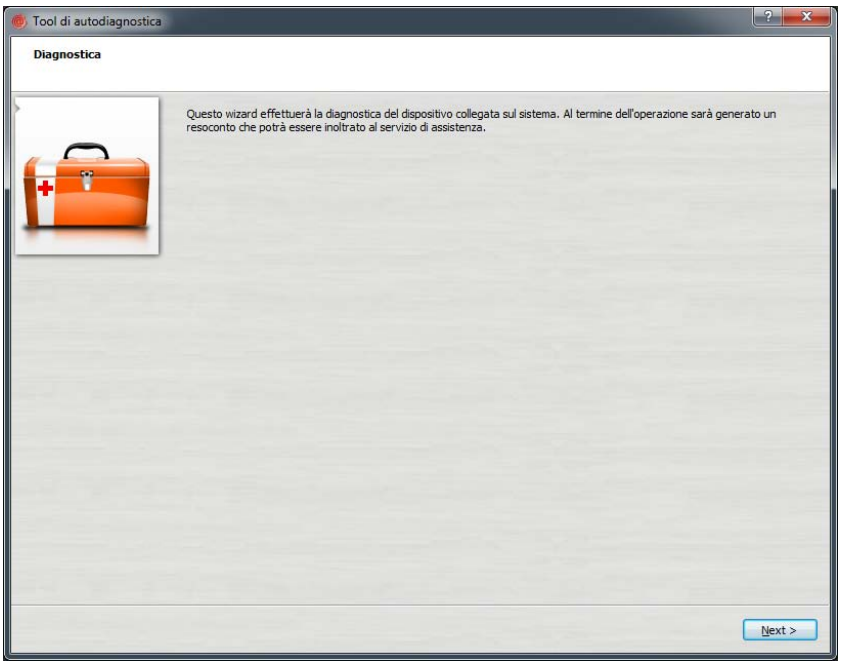
ATTENZIONE: Su piattaforma Macosx è necessario avere a disposizione la password di amministratore della postazione per consentire al software di effettuare l'analisi della memoria del dispositivo.

Passo 2

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

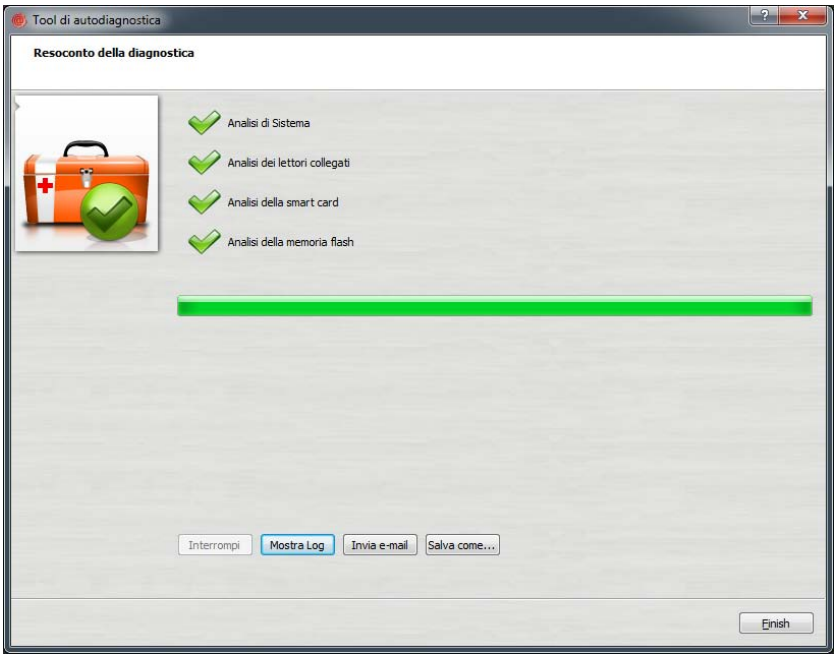
Passo 3

Cliccare su "**Next**" ed attendere che l'Arubakey complete l'analisi del dispositivo



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 di Aruba key l'utente deve avere i privilegi di amministratore.*

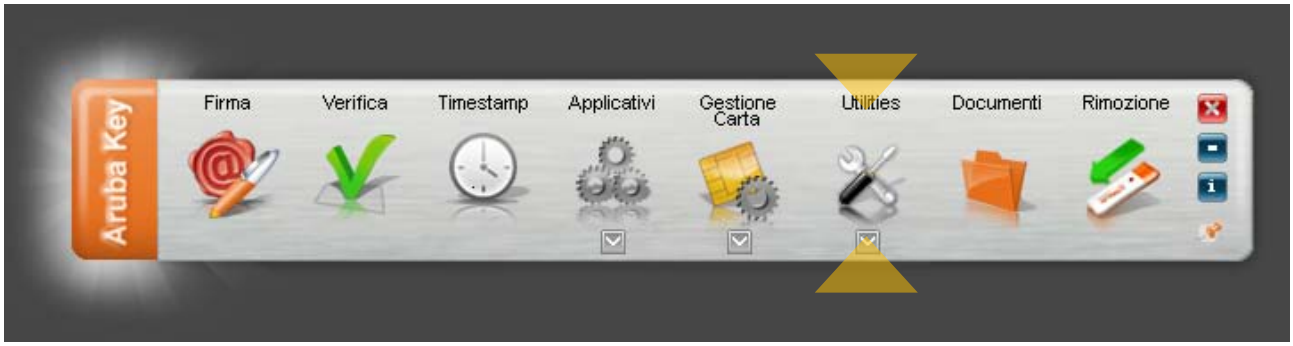
14 "Import" certificato

La funzione di “Import” certificato consente l’importazione dei certificati dell’Aruba Key all’interno dello store locale rendendo possibile l’interfacciamento del dispositivo anche da parte di quelle applicazioni già presenti nel pc host come ad esempio: Internet Explorer, Adobe Reader (Professional), Safari, software di Firma Digitale, etc…

NOTA: Per attivare questa funzionalità è necessario avere i privilegi di amministratore del PC.

Passo 1

Per attivare l’ “import” del certificato, cliccare su “**Utilities”.**



Passo 2

Cliccare su “**Import” Certificato**.

Passo 3

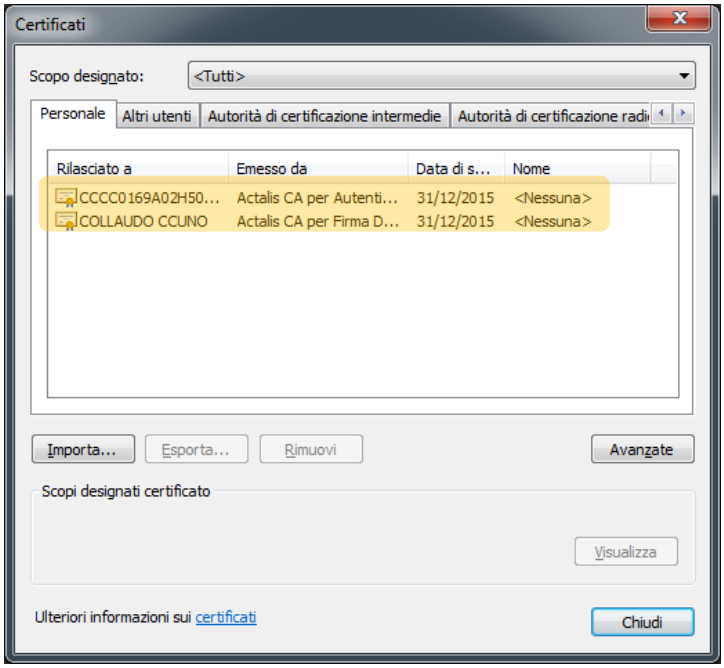
Seguire il wizard di installazione accettando le condizioni di contratto e cliccando su OK ad ogni schermata.

Passo 4

Verificare la corretta installazione del certificato tramite la seguente procedura

1. Avvio di Microsoft Internet Explorer;
2. Selezionare Strumenti → Opzioni Internet;
3. Selezionare la scheda Contenuto, cliccare il pulsante Certificati e quindi scheda Personale.
4. Verificare che siano visibili i certificati installati su Arubakey
5. Cliccare su "Chiudi

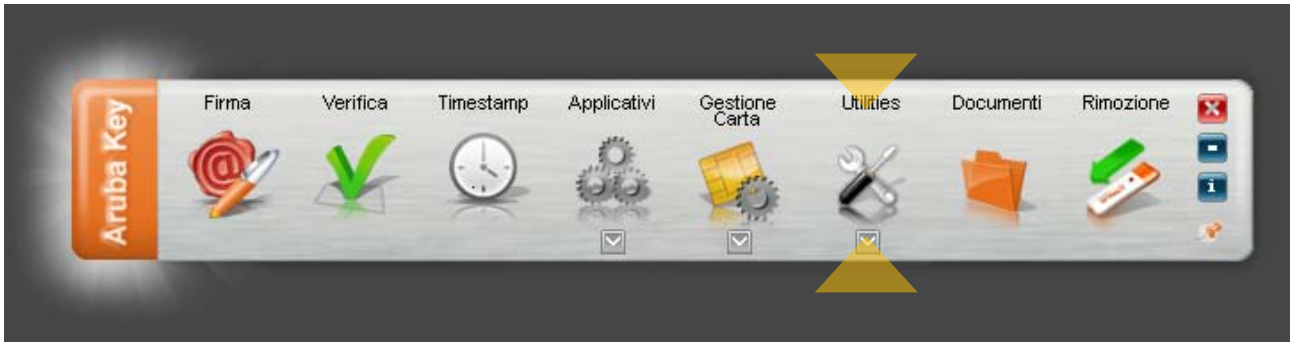
Seguire l'analoga procedura con il portachiavi di Macosx per verificare la corretta installazione in ambiente Apple



15 Cifratura File

Passo 1

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

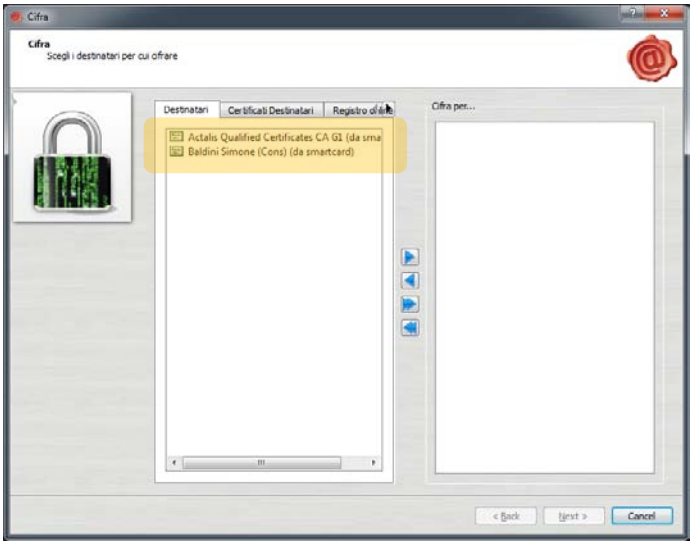


Passo 2

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

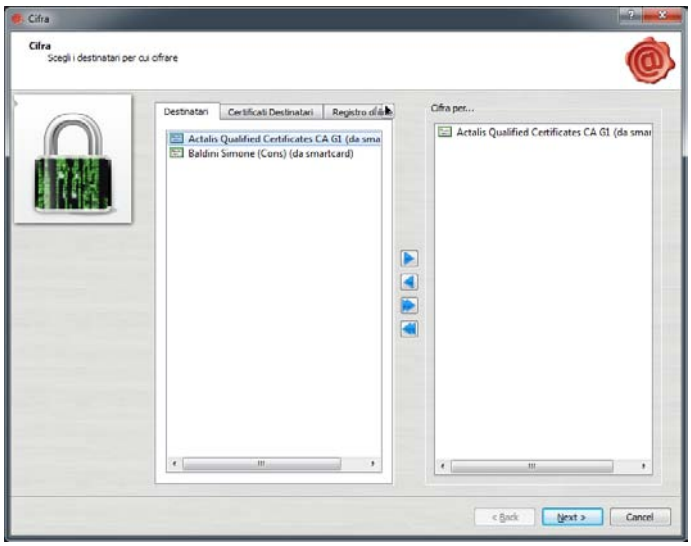
Passo 3

All’interno della finestra di cifratura selezionare, dalla sezione di sinistra, l’elenco dei destinatari del file cifrato e cliccare su “**Aggiungi**”.



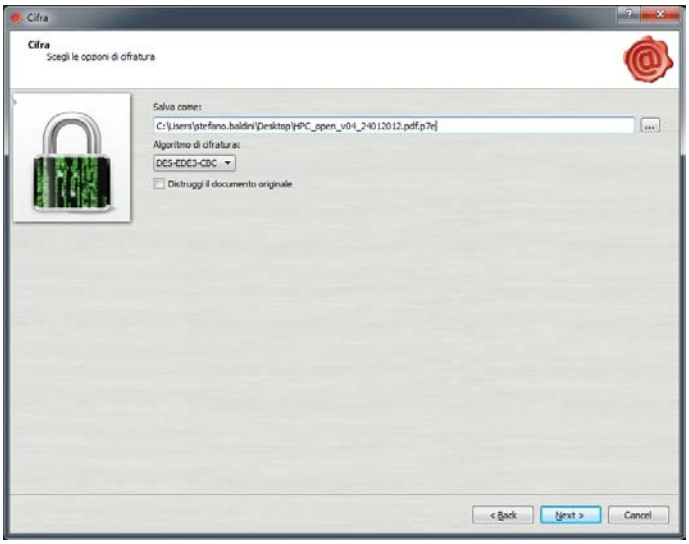
Passo 4

Cliccare su "**Next**".



Passo 5

Selezionare la cartella di destinazione dove salvare il file cifrato e cliccare su "**Next**".

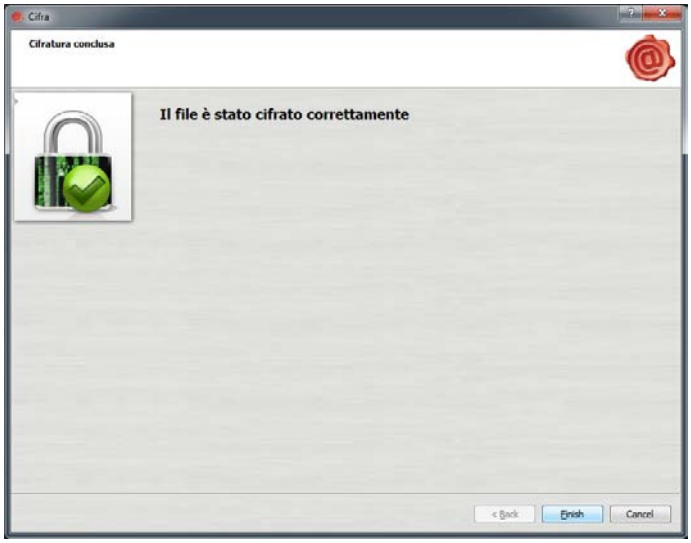


NOTE:

- *Se vengono selezionati più certificati per la cifratura del file, il risultato sarà un unico file decifrabile da ogni singolo titolare dei certificati selezionati.*
- *In fase di cifratura del file l'Aruba key propone automaticamente, nell'area "destinatari", il proprio certificato di autenticazione, quello presente cioè nella SIM inserita in Aruba Key.*

Passo 6

Al termine della procedura verrà mostrata la seguente schermata, cliccare su **"Finish"**.

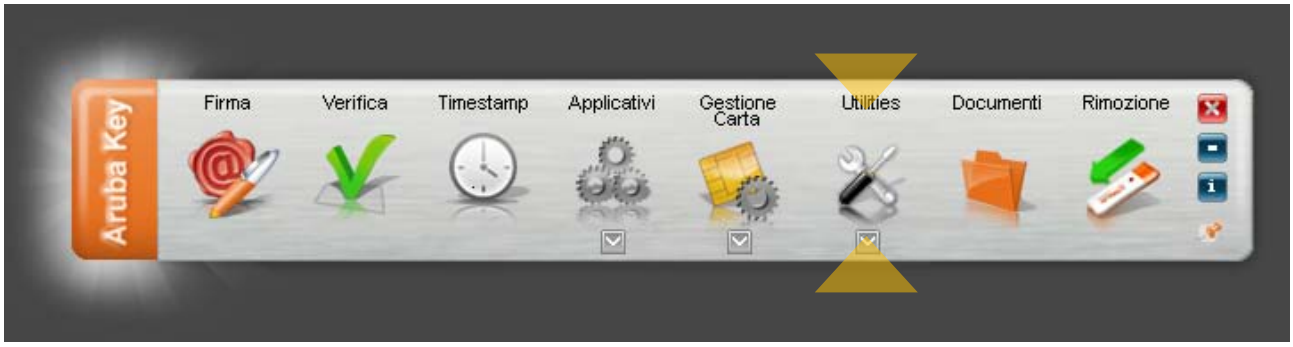


NOTA: Il file cifrato prodotto dall'operazione di cifratura avrà l'ulteriore estensione ".p7e" ed includerà il file originale.

16 Decifratura File

Passo 1

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

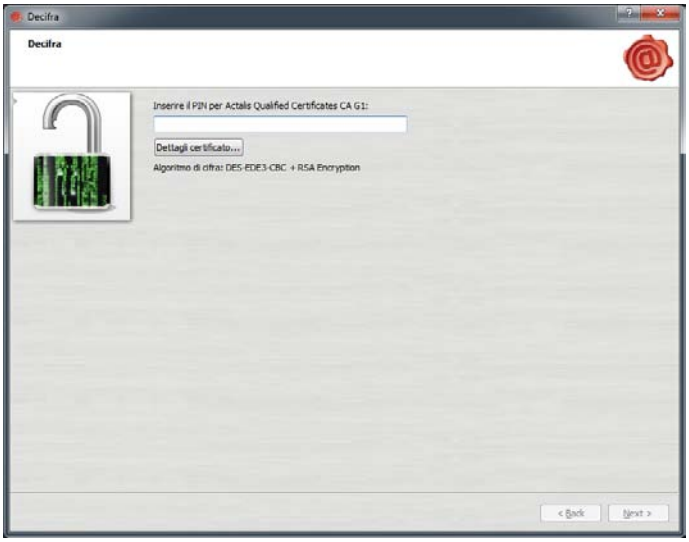


Passo 2

Trascinare il file **“.p7e”** sull’icona **“Decifra”**.

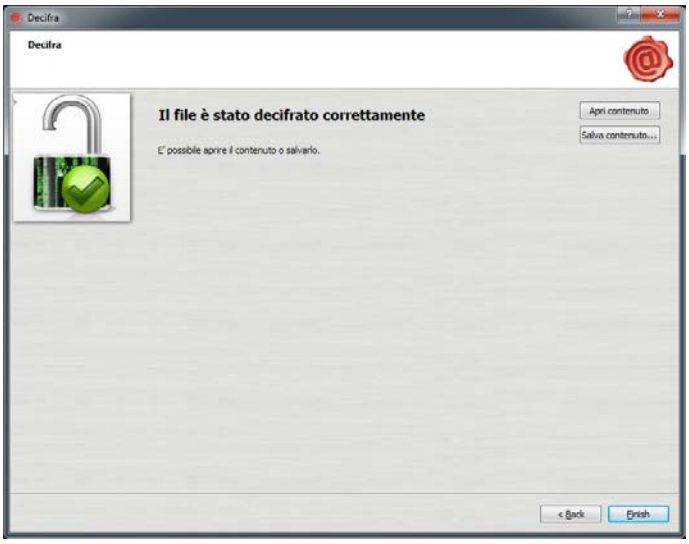
Passo 3

L’Aruba key verifica che nella SIM sia presente almeno uno dei certificati indicati nella fase di cifratura.
In questa fase viene richiesto il PIN della SIM inserita in Arubakey.



Passo 4

Arubakey, dopo aver completato il processo di decifratura del file, propone all'utente l'apertura o il salvataggio dello stesso.

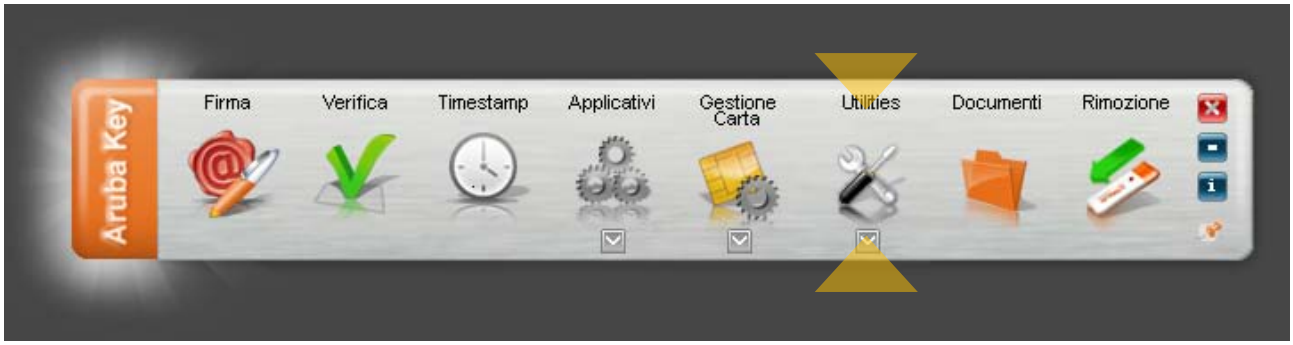


17 Impostazione Proxy

Per utilizzare Aruba key in una rete protetta da Proxy, far riferimento alle seguenti istruzioni:

Passo 1

Selezionare il pulsante "**Utilities".**

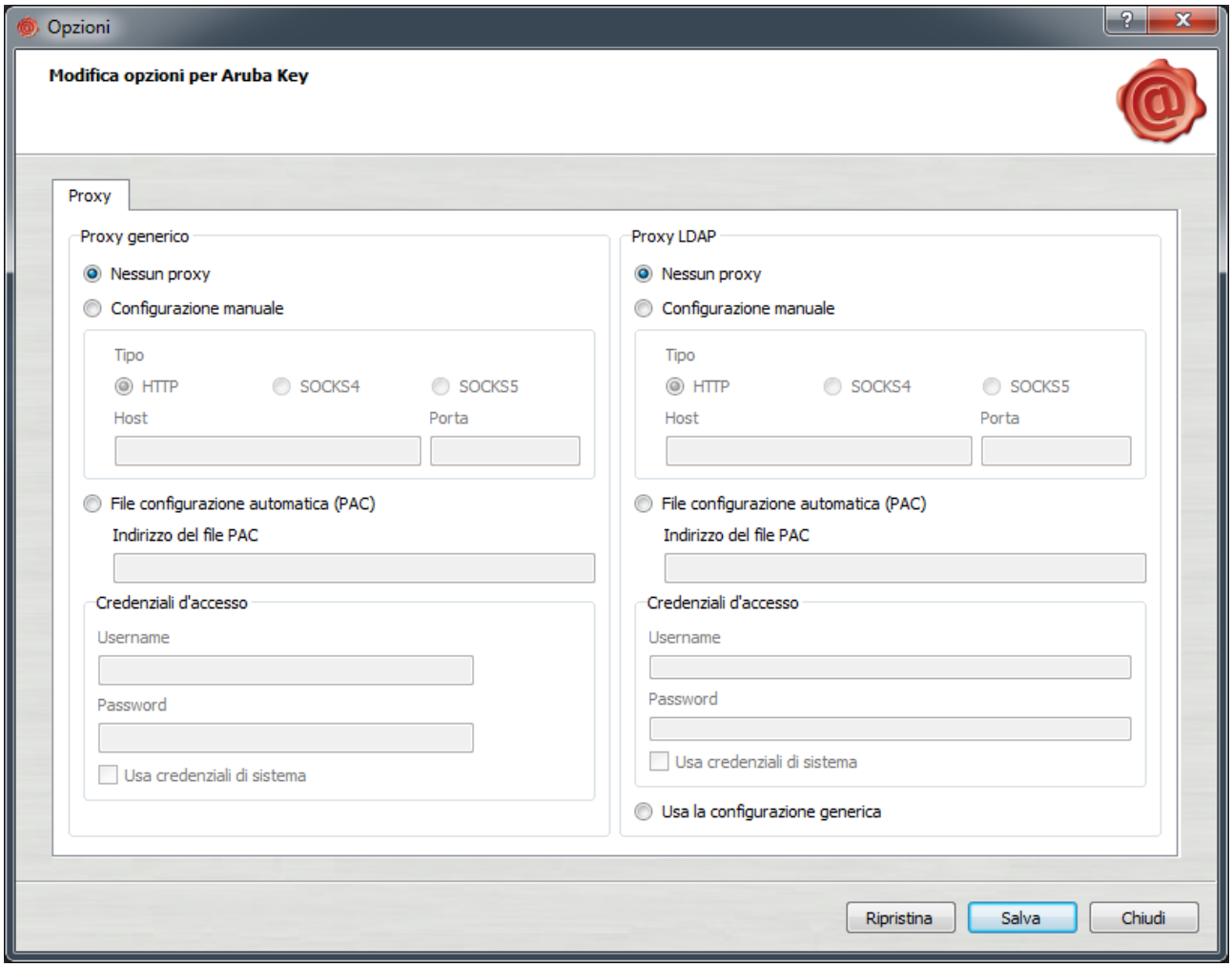


Passo 2

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.

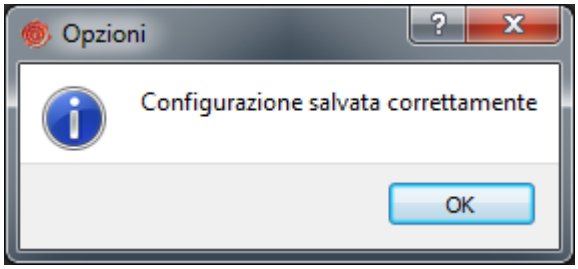
Le credenziali di accesso specificano nome utente e password da utilizzare per l'autenticazione proxy.
Se non specificate su sistemi operativi Windows, verranno utilizzate, se possibile, le credenziali dell'utente attualmente autenticato sul sistema. Se le credenziali non dovessero essere valide per 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

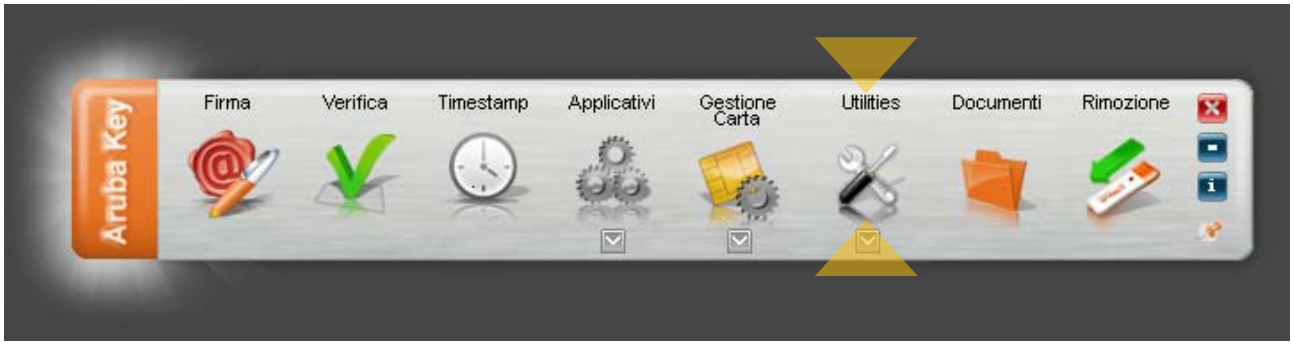
Se le configurazione è stata salvata correttamente comparirà la seguente finestra.



18 Visualizzazione dei certificati su FireFox Portable.

Passo 1

Per accedere a **"Mozilla FireFox Portable Edition"** presente a bordo dell'Aruba Key cliccare sopra il pulsante **"Applicativi".**

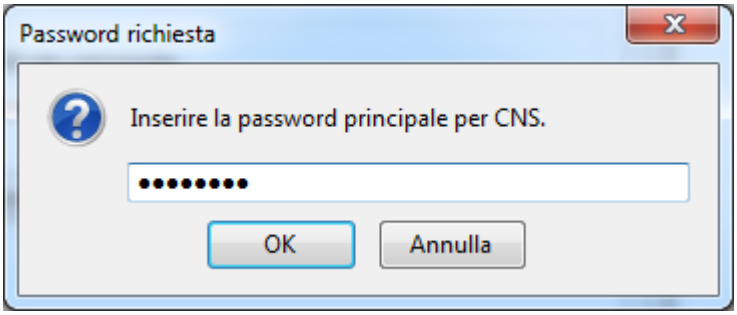


Passo 2

Cliccare sul pulsante **"Firefox".**

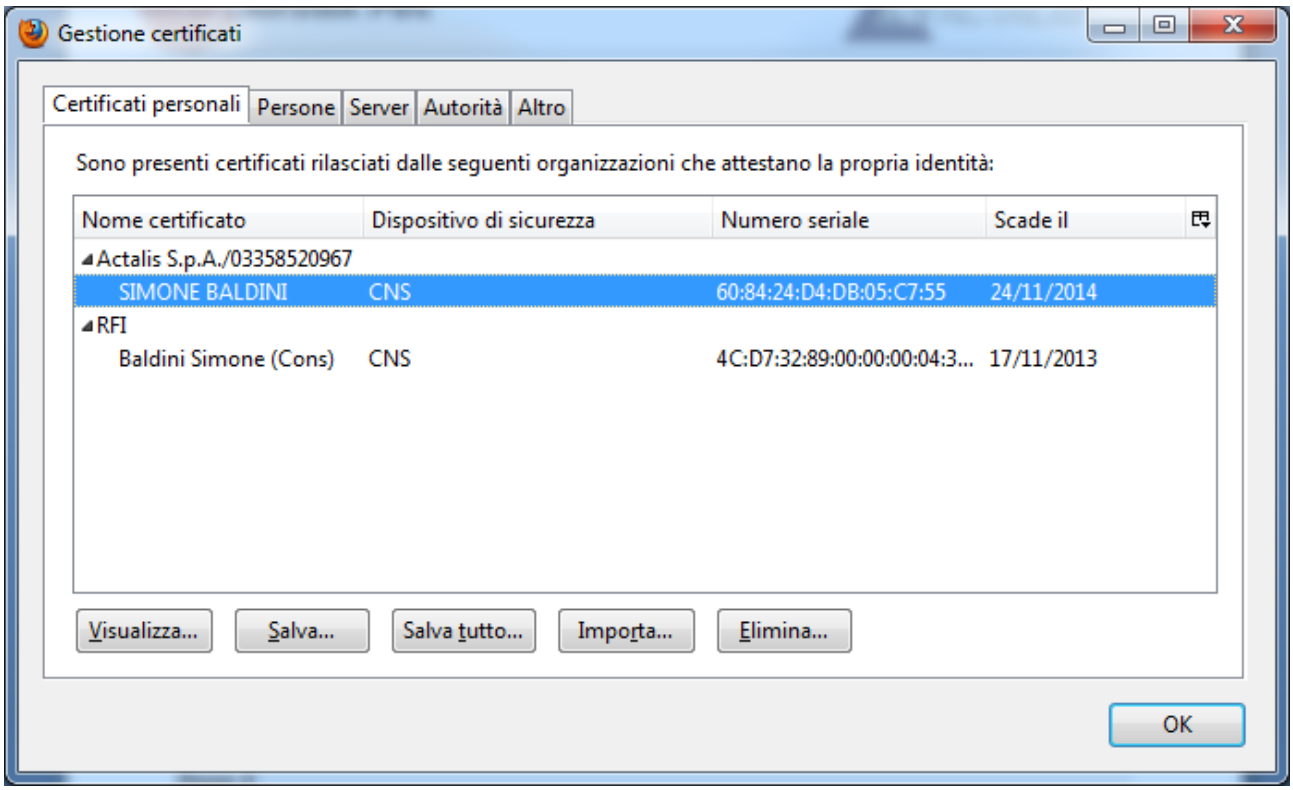
Passo 3

Selezionare Strumenti → Opzioni → Avanzate → Cifratura → **"Mostra Certificati"** ed inserire il PIN quando richiesto



Passo 4

I propri certificati, residenti nell'Arubakey, sono visualizzati all'interno della scheda 'Certificati personali'



ATTENZIONE: Nel caso in cui i certificati di firma e CNS vengano importati all'interno dello Store di Mozilla FireFox è doveroso non cliccare sul pulsante" Elimina..". Questo azione potrebbe causare l'eliminazione dei certificati CNS e Firma digitale all'interno della smartcard e l'impossibilità di recupero degli stessi.

19 Procedura di caricamento del certificato ACTALIS

In generale la smart card contiene già a bordo il certificato di firma digitale. Esiste tuttavia la possibilità, **nel caso in cui l'Aruba Key sia stata acquistata dal circuito Actalis**, che la smart card sia stata fornita senza certificati a bordo. Il titolare dovrà quindi seguire la seguente procedura per effettuare il caricamento dei certificati e rendere Aruba Key operativa.
In questo caso al titolare, in seguito o contestualmente al processo di identificazione effettuato da un Operatore di Registrazione, viene consegnata una busta chiusa con un **Codice Riservato Personale** (chiamato codice **CRP**).
Per ottenere il caricamento del certificato è necessario seguire i passi sotto riportati.

Passo 1

Accedere a "Mozilla FireFox Portable Edition" presente a bordo dell'Aruba Key cliccando prima sul pulsante **"Applicativi"** e quindi sul pulsante **"Firefox".**

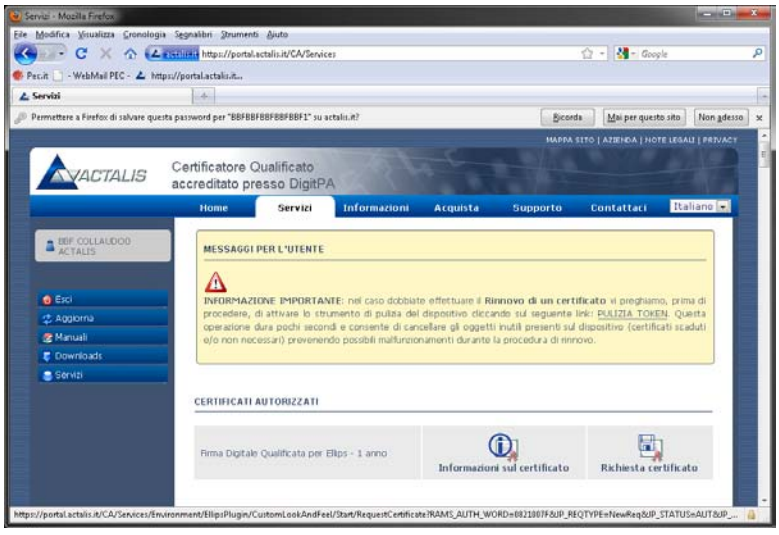
Passo 2

Collegarsi con il browser al sito https://portal.actalis.it

Nell'area **"ACCESSO CLIENTI",** posta in alto a sinistra, digitare in caratteri maiuscoli il **codice fiscale** del titolare ed il **codice CRP** consegnato in fase di identificazione del titolare. Quindi cliccare su "**LOGIN**".

Passo 3

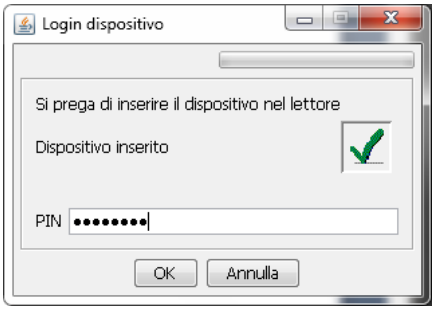
Si accede così alla pagina in cui sono disponibili i **"CERTIFICATI AUTORIZZATI"** per il titolare. Cliccare su "**Richiesta certificato".**



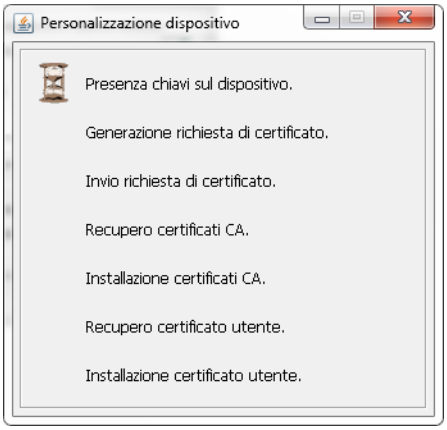
Si avvia così una procedura automatica che chiede al titolare l'inserimento del codice PIN per accedere al dispositivo.

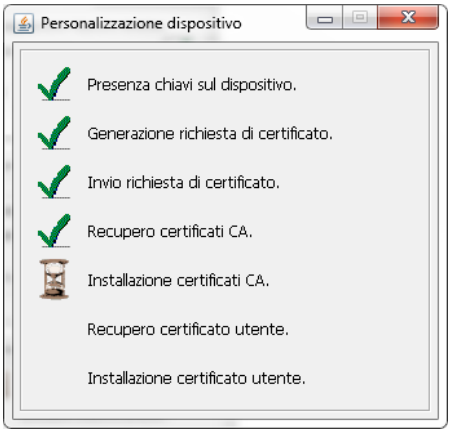
Passo 4

Inserire quando richiesto il PIN ricevuto con Aruba Key e cliccare sul pulsante "**OK**".



Il sistema provvede ad eseguire i passi necessari per ottenere il certificato.

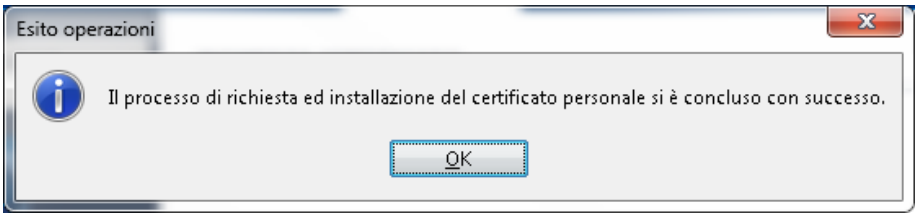


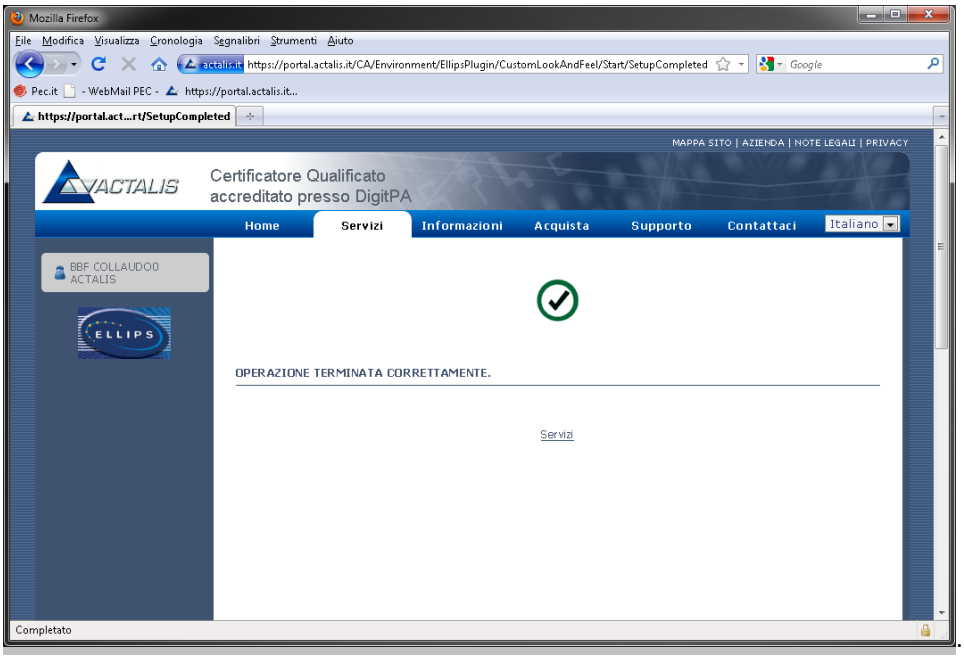


Al termine dell'operazione viene fornito un **Codice di Revoca,** utilizzabile dal titolare qualora volesse invalidare il certificato emesso. Tale operazione può essere eseguita collegandosi nuovamente al medesimo portale.

Il codice può essere salvato cliccando sul pulsante "**Salva**".

Il sistema comunica quindi l'esito del processo di caricamento del certificato





La procedura è così conclusa ed il titolare può chiudere il browser ed operare con tutte le funzioni di Aruba Key.