



ARUBA KEY - UNINA

MANUALE D'USO



ARUBA PEC



UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II



1 Indice

- 1 Indice 2
- 2 Informazioni sul documento 3
 - 2.1 Scopo del documento 3
- 3 Caratteristiche del dispositivo 3
 - 3.1 Prerequisiti 3
- 4 Installazione della smart card 4
- 5 Avvio di Aruba Key 5
- 6 Firmare digitalmente un file in formato P7M 7
 - 6.1 Firmare digitalmente più file in formato P7M 9
 - 6.2 Firmare digitalmente una intera cartella 12
 - 6.3 Funzione di Firma Multipla 15
 - 6.4 Funzione di Firma Enveloped 17
 - 6.5 Funzione di Firma Enveloped e Firma Multipla di una cartella 18
- 7 Verifica di file firmati 22
 - 7.1 Verifica di file contenuti in una cartella 24
- 8 Firmare digitalmente un file in formato PDF 27
 - 8.1 Firmare digitalmente più file in formato PDF 31
- 9 Gestione smart card 34
 - 9.1 Cambio del pin 34
 - 9.2 Sblocco del PIN 35
 - 9.3 Cambio del PUK 36
 - 9.4 Lettura informazioni carta 37
 - 9.5 Codici di errore gestione carta 38
- 10 Autodiagnosi del dispositivo Aruba Key 39
- 11 "Import" certificato 41
- 12 Cifratura File 43
- 13 Decifratura File 46
- 14 Utilizzo di una cartella cifrata 48
- 15 Opzioni 51
 - 15.1 Impostazioni del proxy 51
 - 15.2 Impostazioni della lingua 53
- 16 Visualizzazione dei certificati su FireFox Portable 55
- Appendice A 57
 - Apposizione di marche temporali 57
 - Verifica Marche Temporali 59
 - Verifica Marche Temporali in formato .TSD 62



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 Temporalmente
4. Verifica di Firme Digitali in formato .P7M e .PDF
5. Verifica di Marche Temporalmente
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.

Il dispositivo, quando è collegato ad un PC connesso ad internet, verifica automaticamente gli aggiornamenti disponibili, proponendo al titolare l'esecuzione degli stessi. In tal modo, il software della Aruba KEY sarà sempre aggiornato all'ultima versione disponibile.

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, Win 8, Win 8 PRO, in versione 32 bit e 64 bit
- Mac Os X Tiger (10.4 - Intel), Leopard (10.5 - Intel), Snow Leopard (10.6 - Intel), Lion (10.7 - Intel) (32 bit e 64 bit)
- Linux Ubuntu 12.0.4 e 12.10, Debian 6.0, Mint 13 e 14

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 (raccomandata ai fini della verifica dei documenti firmati, ma non obbligatoria).
2. Possibilità di poter instaurare connessioni HTTP, HTTPS e LDAP.



3.1.3 Antivirus

In caso di presenza di antivirus, installato sul PC, è necessario verificare che lo stesso consenta l'esecuzione di file da dispositivi esterni, consenta l'esecuzione di aggiornamenti e, più in generale, non blocchi le funzionalità principali del dispositivo di firma digitale.

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.

Passo 1:

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.

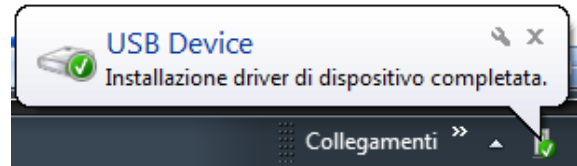




5 Avvio di Aruba Key

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.

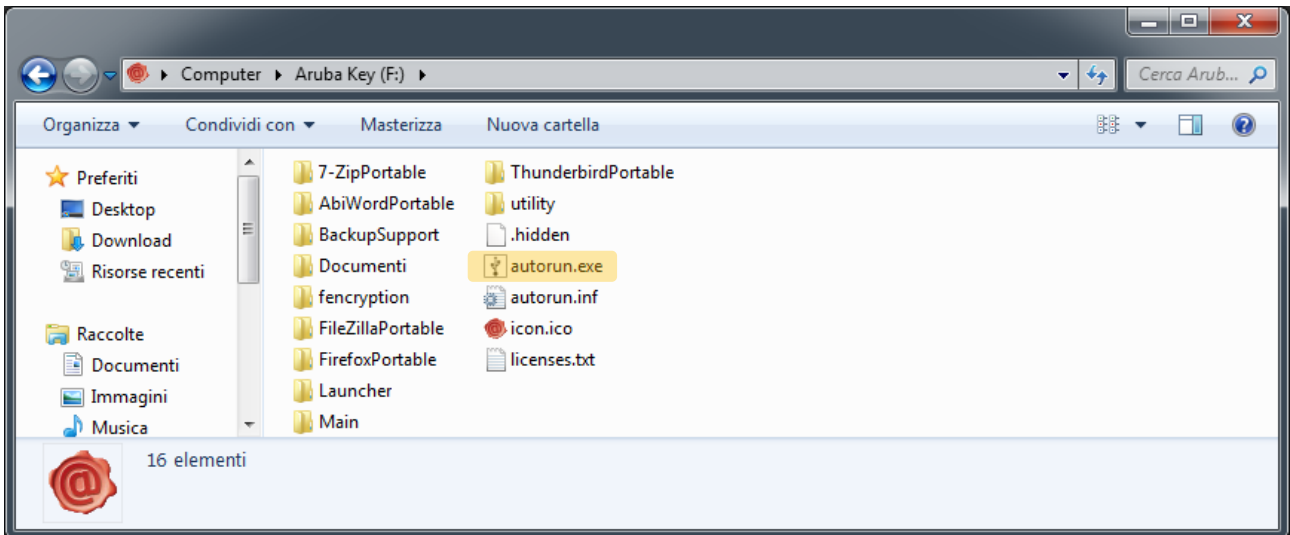


Se nella postazione è attiva la funzione di esecuzione automatica (Autorun) al momento del collegamento dell'Aruba Key verrà avviata automaticamente la Barra degli strumenti come quella riportata nella figura seguente.



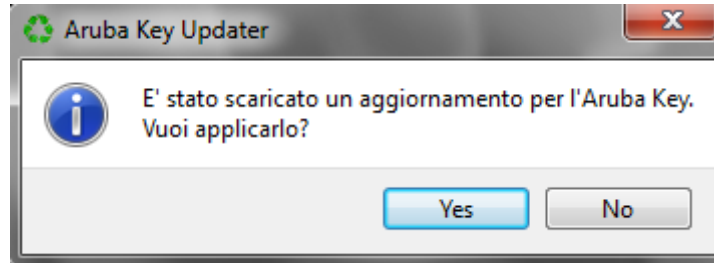
Se, invece, al momento dell'inserimento del dispositivo, non viene avviata la Barra degli strumenti di Aruba Key, è probabile allora che la funzione di esecuzione automatica sia disattivata.

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





Ad ogni collegamento del dispositivo al computer, si avvia la verifica sulla presenza di aggiornamenti software. Tale funzione necessita di collegamento internet.



In caso di disponibilità di un aggiornamento, è molto importante applicarlo, dal momento che la nuova versione del software potrebbe riguardare:

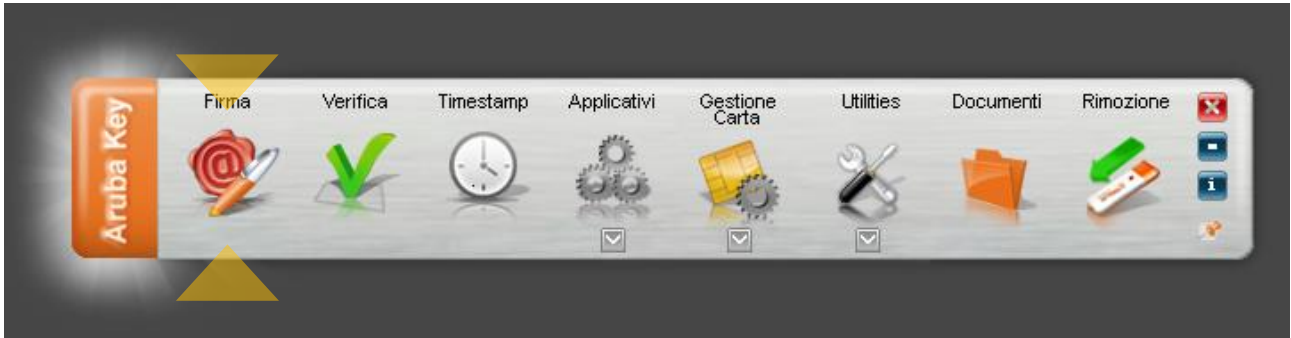
1. Adeguamenti normativi
2. Aggiunta di nuove funzionalità
3. Risoluzione di bug



6 Firmare digitalmente un file in formato P7M

Passo 1

Trascinare il file sopra l'icona "Firma". Ricordiamo che il file, per disposizioni normative, non deve avere contenuti attivi, pertanto si raccomanda l'esclusivo utilizzo di file in formato PDF.



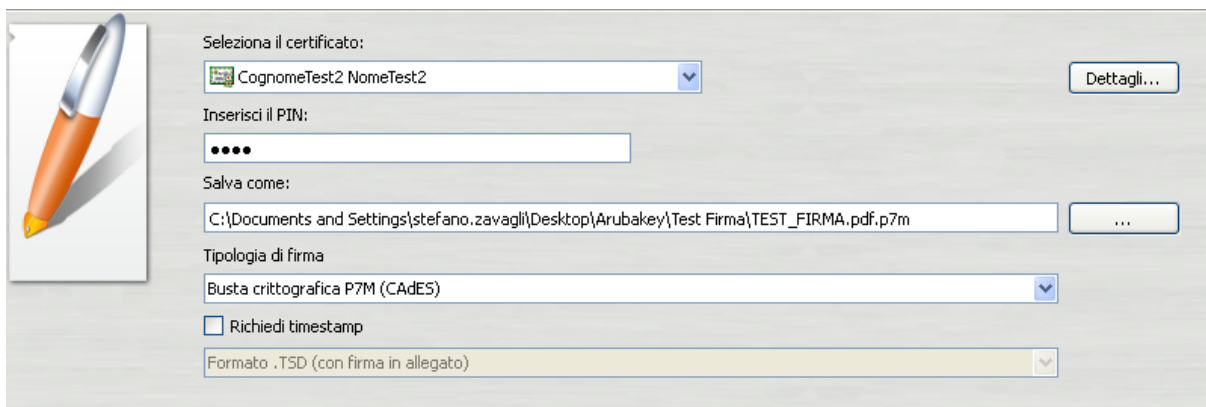
Passo 2

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



Passo 3

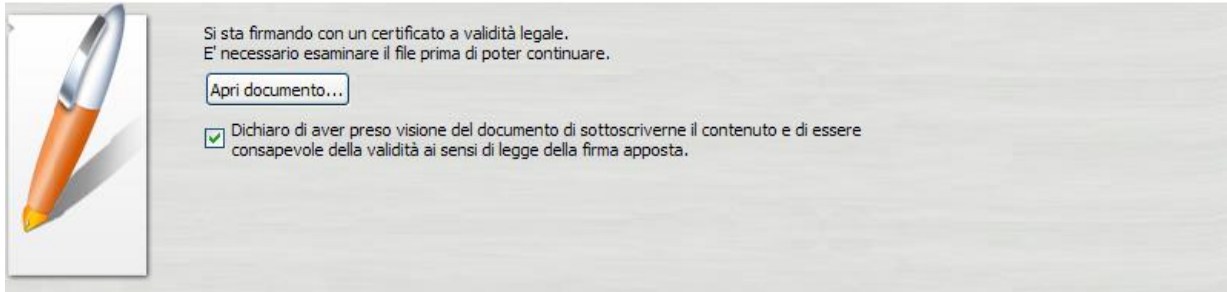
- Assicurarsi che sia selezionato il certificato per la firma digitale (Cognome Nome);
- Inserire il PIN di protezione della smart card;
- Selezionare l'opzione "Firma come busta crittografica P7M";
- Verificare che il percorso utilizzato per salvare il file firmato sia quello desiderato. Di default il percorso indicato è quello di partenza.
- 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.

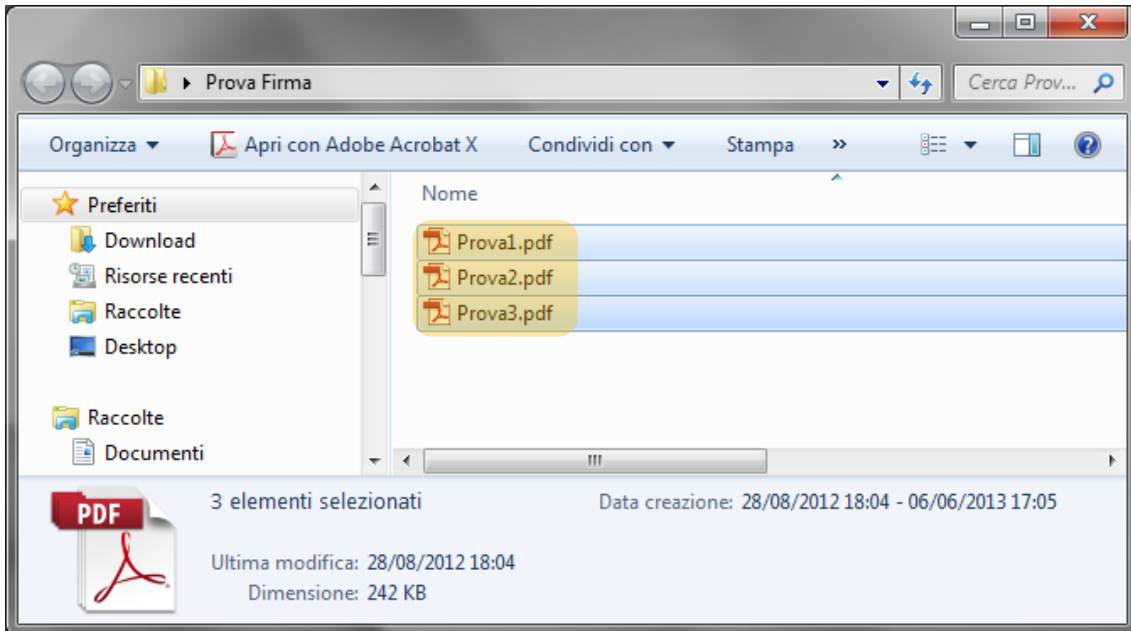




6.1 Firmare digitalmente più file in formato P7M

Passo 1

Selezionare tutti i documenti da firmare.



Passo 2

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



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 "Firma come busta crittografica P7M";
- d. Verificare che il percorso utilizzato per salvare il file firmato sia quello desiderato. Di default il percorso indicato è quello di partenza.
- e. Cliccare sul pulsante **Next >**

Seleziona il certificato:
CognomeTest2 NomeTest2 Dettagli...

Inserisci il PIN:
.....

Salva in:
C:\Documents and Settings\Admin\Desktop\Nuova cartella ...

Tipologia di firma
Busta crittografica P7M (CAES)

Richiedi timestamp

Formato .TSD (con firma in allegato)

Passo 5

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

Si sta firmando con un certificato a validità legale.
E' necessario esaminare i documenti prima di poter continuare.

Dichiaro di aver preso visione dei documenti di sottoscrivere il contenuto e di essere consapevole della validità ai sensi di legge della firma apposta.

Passo 6

Attendere il completamento dell'operazione di firma.

Firma in corso...



Passo 7

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

Operazione conclusa

Il file C:\Documents and Settings\stefano.zavagli\Desktop\Arubakey\New Folder\file di prova.txt è stato firmato correttamente

- Salvato in: [C:/Documents and Settings/stefano.zavagli/Desktop/Arubakey/New Folder/file di prova.txt.p7m](#)
- Firmatario: [CognomeTest2 NomeTest2](#) (il certificato ha validità legale)

Il file C:\Documents and Settings\stefano.zavagli\Desktop\Arubakey\New Folder\file di prova1.txt è stato firmato correttamente

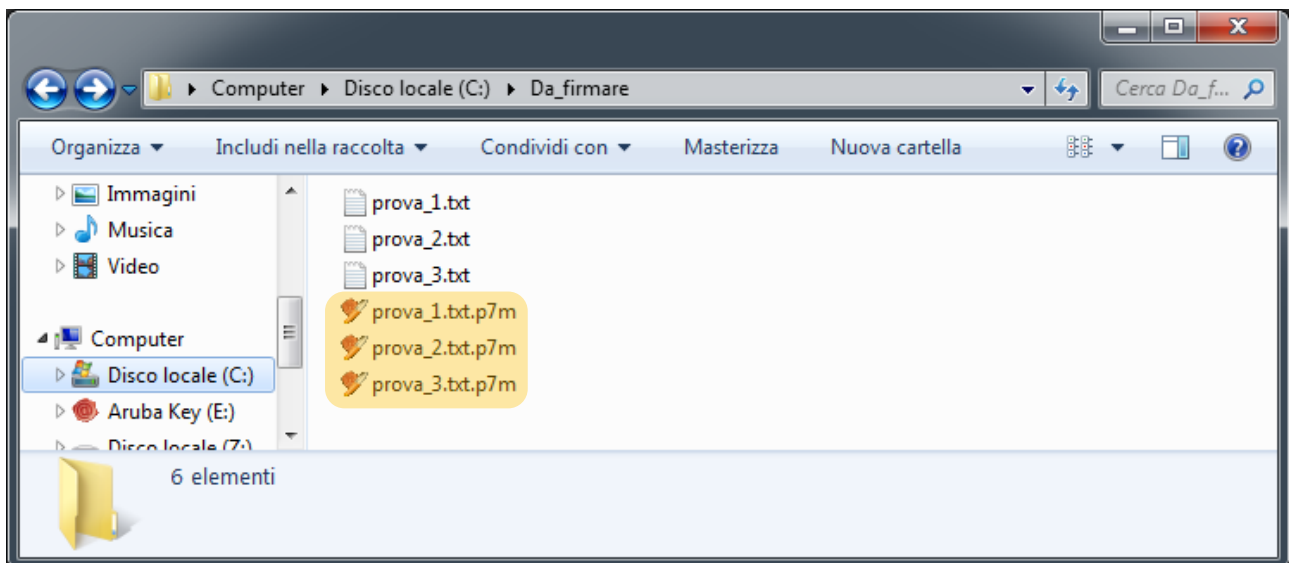
- Salvato in: [C:/Documents and Settings/stefano.zavagli/Desktop/Arubakey/New Folder/file di prova1.txt.p7m](#)
- Firmatario: [CognomeTest2 NomeTest2](#) (il certificato ha validità legale)

Il file C:\Documents and Settings\stefano.zavagli\Desktop\Arubakey\New Folder\file di prova2.txt è stato firmato correttamente

- Salvato in: [C:/Documents and Settings/stefano.zavagli/Desktop/Arubakey/New Folder/file di prova2.txt.p7m](#)
- Firmatario: [CognomeTest2 NomeTest2](#) (il certificato ha validità legale)

Passo 8

I documenti firmati, come indicato al passo 4.d, verranno salvati nella stessa cartella dove risiedono i documenti originali aggiungendo al nome l'estensione .p7m.





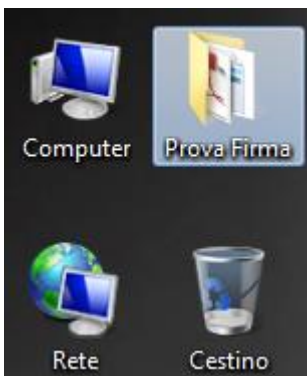
6.2 Firmare digitalmente una intera cartella

Trascinando sopra il pulsante di firma una cartella, contenente documenti elettronici, anche in formati diversi tra loro, è possibile, mediante unico inserimento del PIN, apporre la firma all'intero contenuto della cartella stessa. Di seguito sono illustrati i passaggi necessari.

Specifichiamo che il numero di documenti che la cartella può contenere, anche in riferimento alla loro dimensione (mb), è strettamente connesso alle prestazioni del computer utilizzato (soprattutto in termini di memoria RAM).

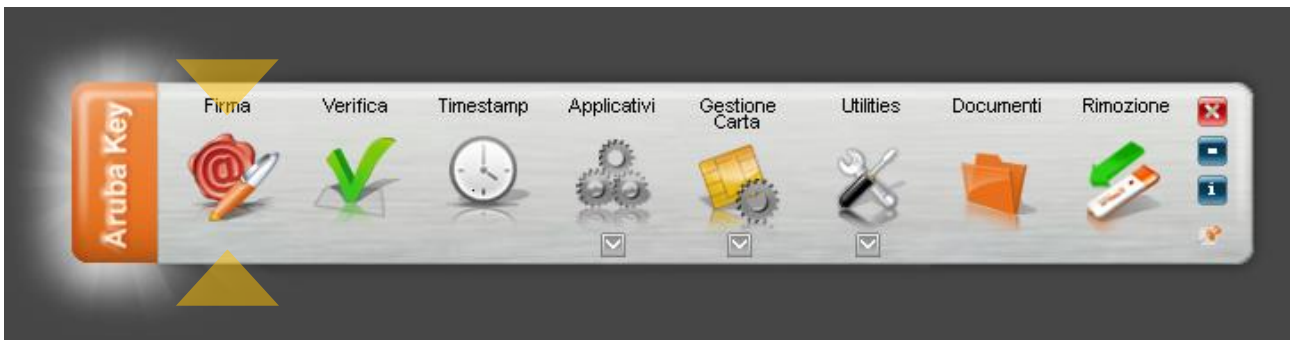
Passo 1

Selezionare la cartella contenente i file da firmare.



Passo 2

Trascinare la cartella sopra l'icona "firma" e rilasciare il mouse.



Passo 3

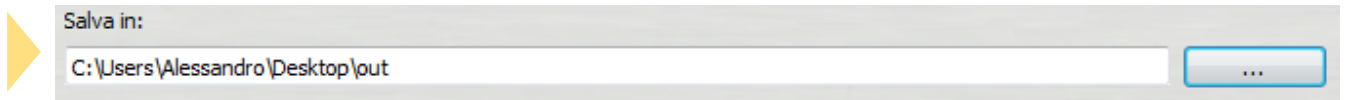
Attendere che Aruba Key recuperi le informazioni relative ai certificati contenuti nella smart card.



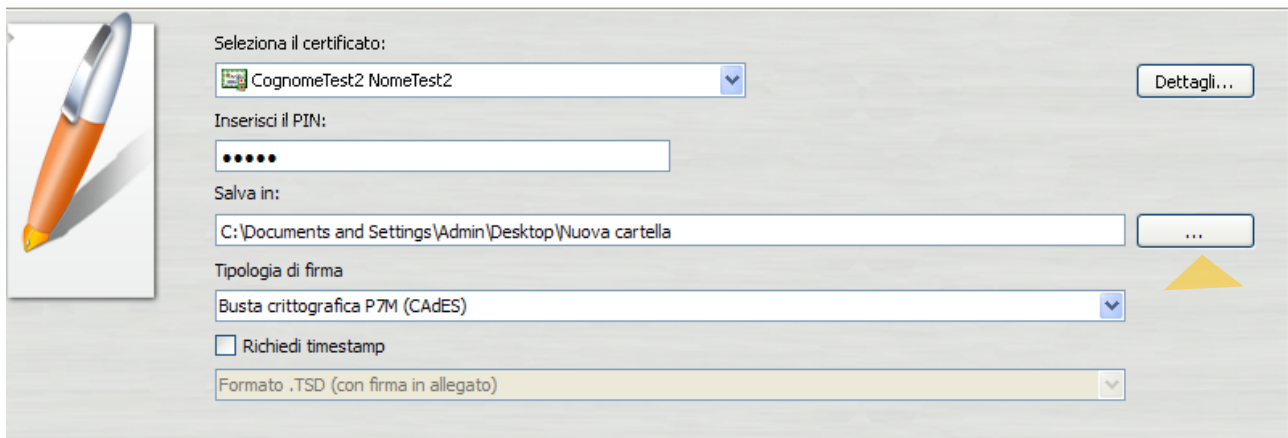


Passo 4

- 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 "Firma come busta crittografica P7M";
- d. Verificare che il percorso utilizzato per salvare il file firmato sia quello desiderato, in alternativa, selezionare la cartella di destinazione di proprio interesse, mediante il relativo pulsante:

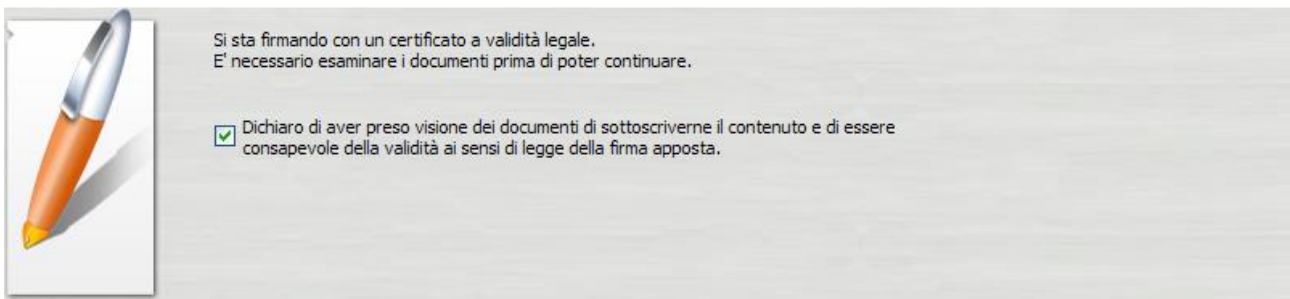


- e. Cliccare sul pulsante **Next >**



Passo 5

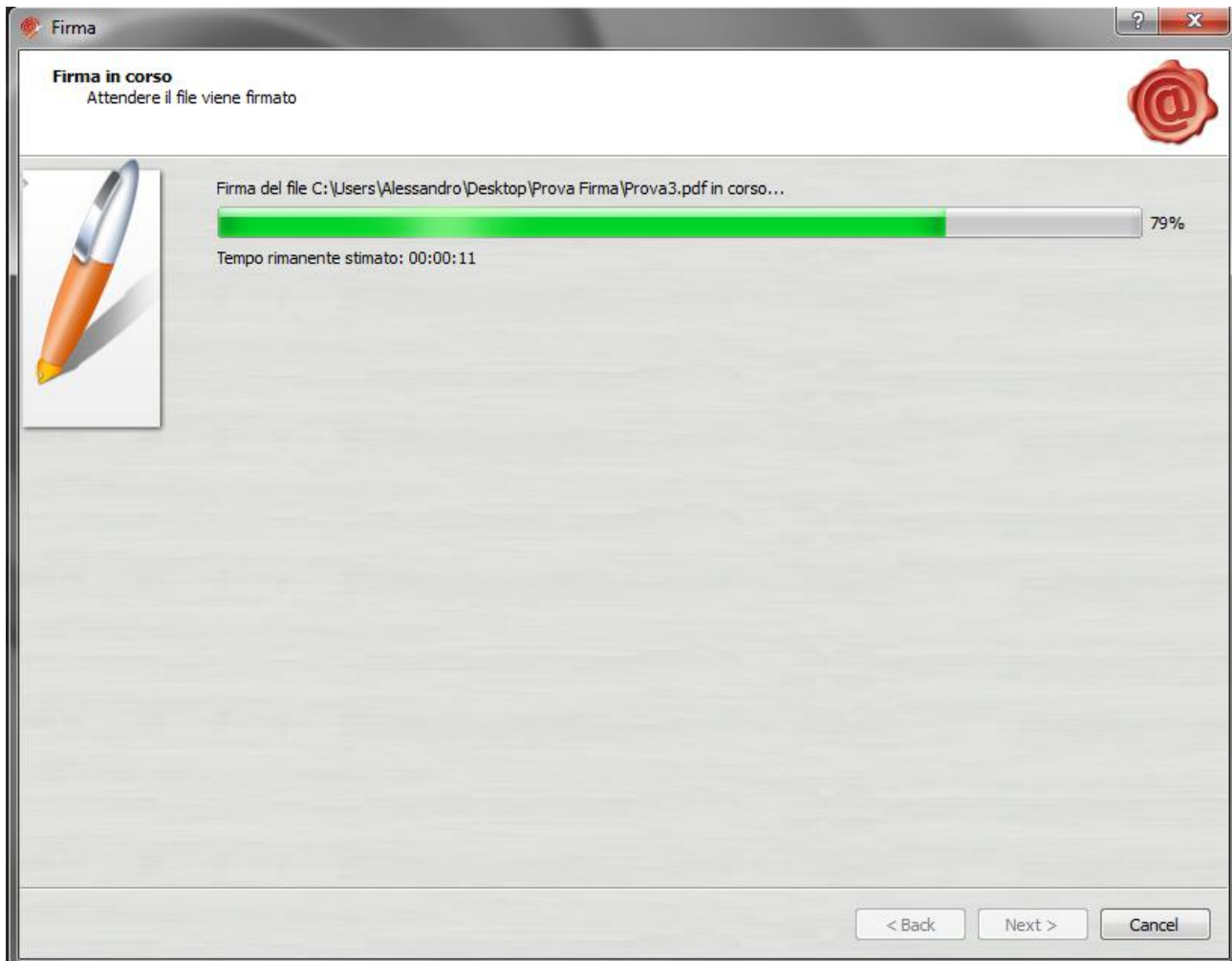
- a. Selezionare l'opzione relativa alla presa visione dei documenti;
- b. Cliccare sul pulsante **Next >**





Passo 6

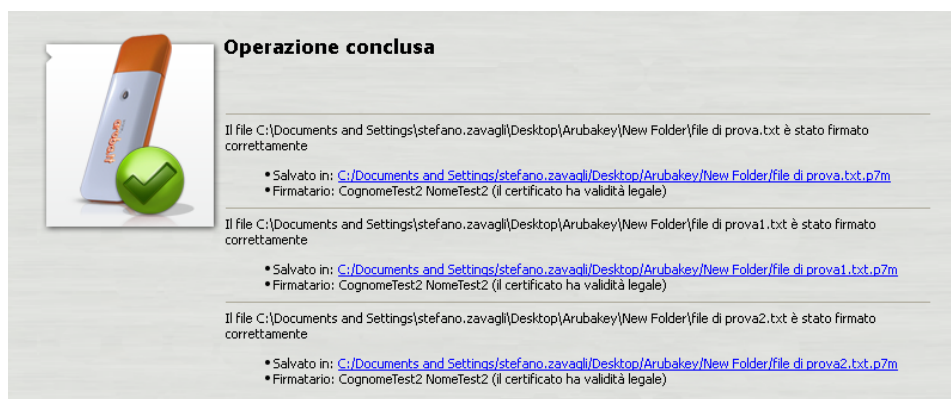
Attendere il completamento dell'operazione di firma.



Il tempo necessario per la conclusione dell'operazione varia in base al numero dei file da firmare.

Passo 7

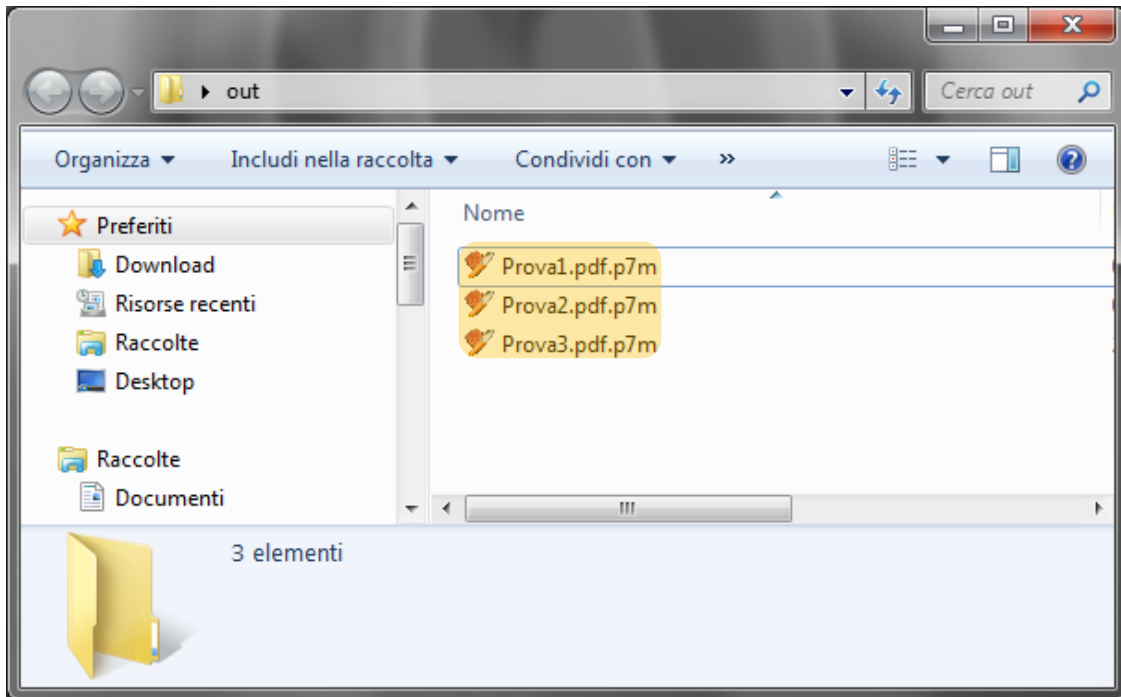
Verificare che al termine della operazione, venga riportata una schermata che notifica la correttezza delle firma su ogni singolo documento.





Passo 8

Nel caso non sia stata selezionata alcuna specifica cartella di destinazione, i documenti firmati verranno salvati nella cartella "out", che verrà creata sul desktop.

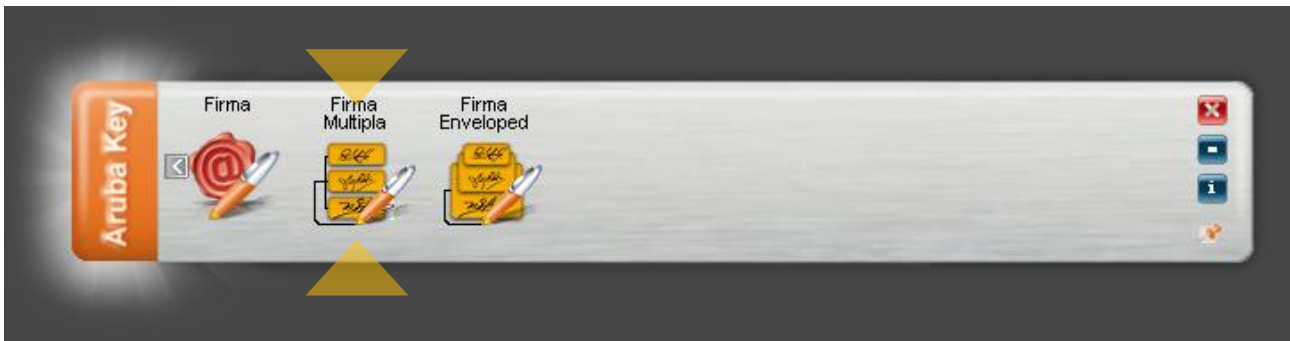


6.3 Funzione di Firma Multipla

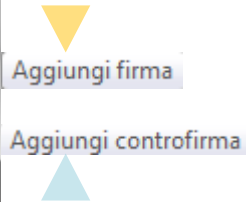
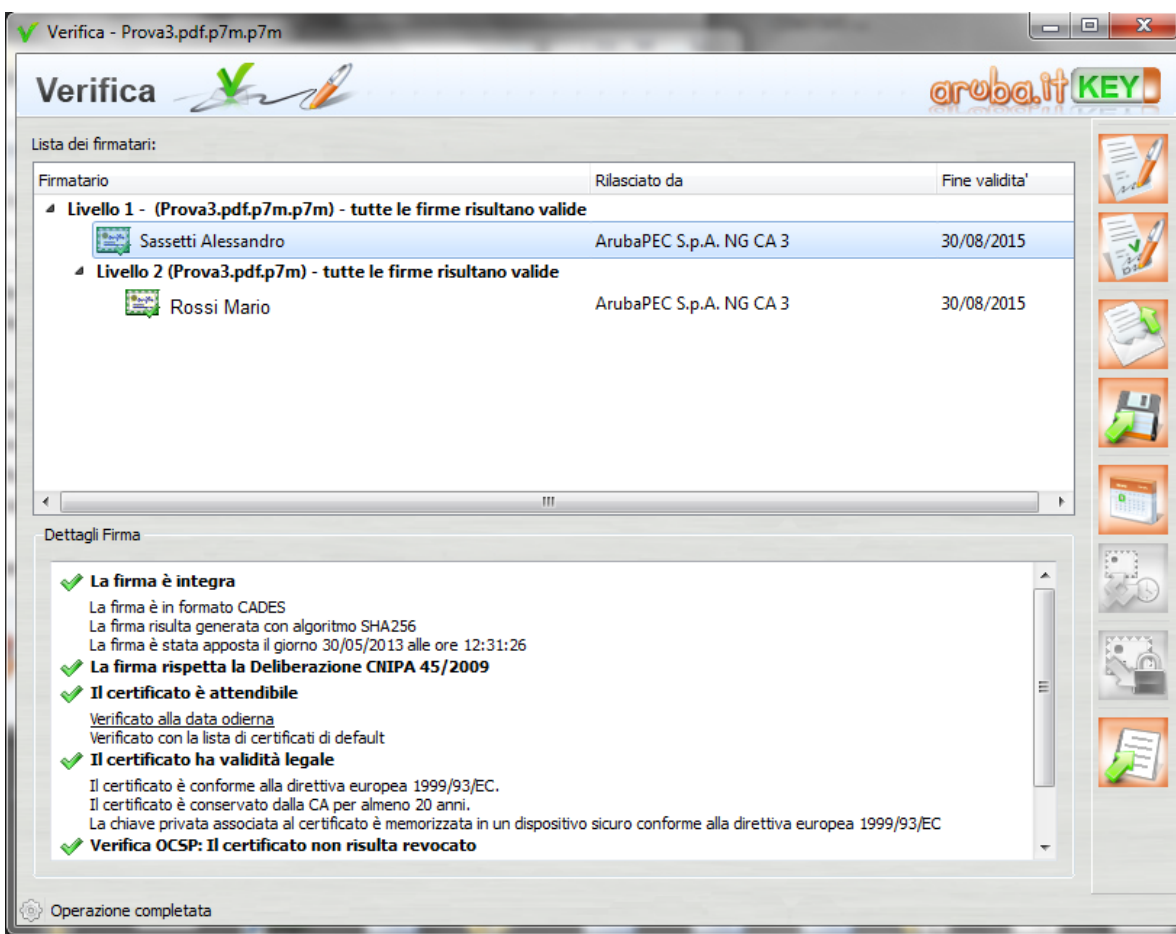
Trascinando sopra il pulsante di firma un file già firmato in formato p7m è possibile accedere alle funzioni di **Firma Multipla**, vedi figure seguenti:



NOTA: Per attivare le funzioni appena citate è necessario 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.



6.4 Funzione di Firma Enveloped

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)



Tale tipologia di firma digitale, comporta la creazione di file firmati al cui nome viene aggiunta una estensione .p7m ad ogni firma apposta. Nel caso un file sia firmato da tre soggetti, troveremo, pertanto un file il cui nome è prova.pdf.p7m.p7m.p7m.

Data la particolare tipologia di firma (cosiddetta a matryoska, in quanto ogni p7m contiene un altro p7m, e così via), si sconsiglia vivamente il ricorso alla Firma Enveloped, che potrebbe generare una difficile interpretazione in fase di verifica di un file firmato da più soggetti.



6.5 Funzione di Firma Eveloped e Firma Multipla di una cartella

E' possibile sottoporre a firma digitale un'intera cartella contenente file già in formato p7m. Per eseguire questa operazione, è necessario compiere i sottostanti passaggi.

Passo 1

Selezionare la cartella contenente i file in formato p7m (se dovessero essere presenti file in formato .pdf, essi subirebbero un normale processo di firma in formato p7m), quindi trascinarla sul pulsante firma



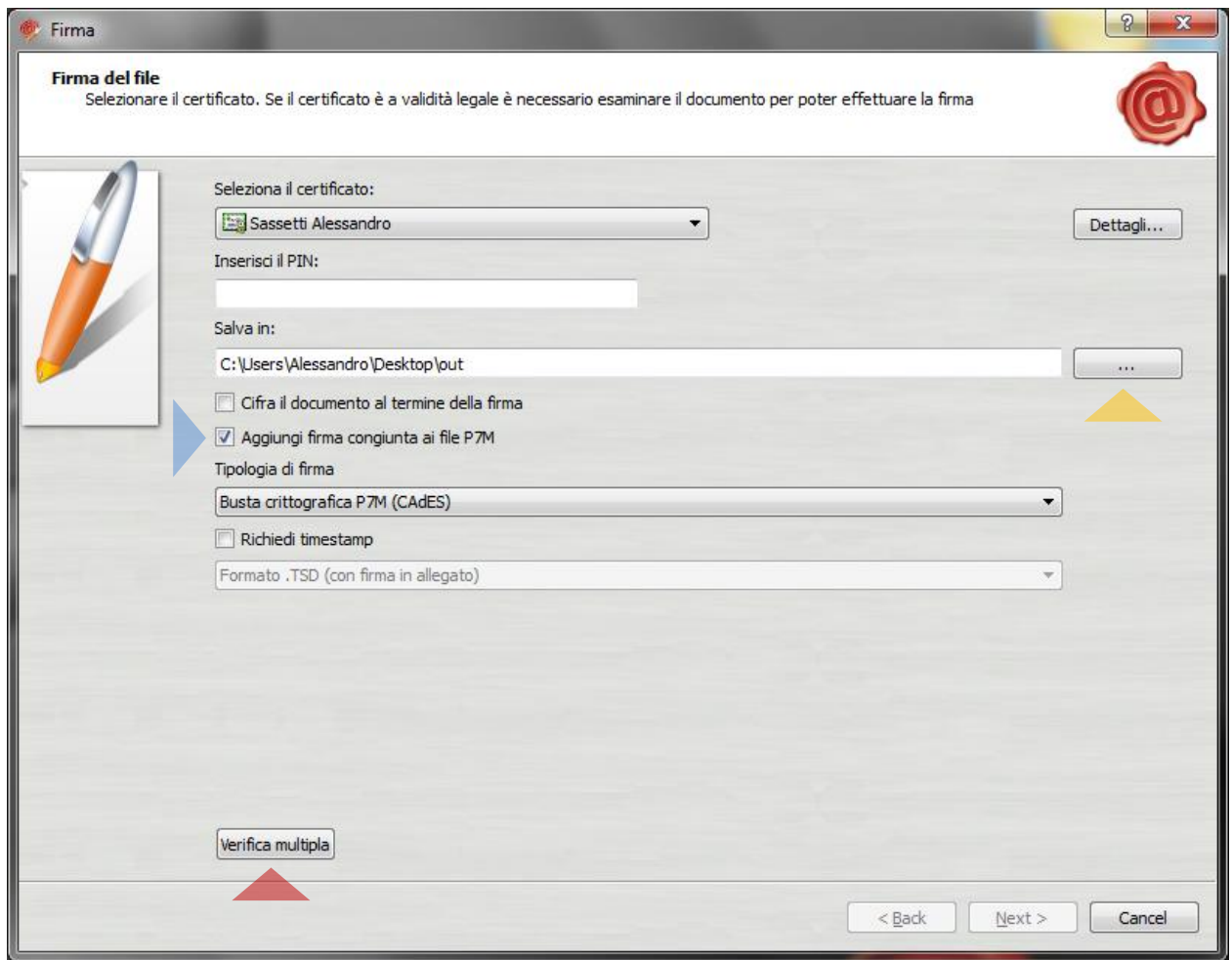
Passo 2

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

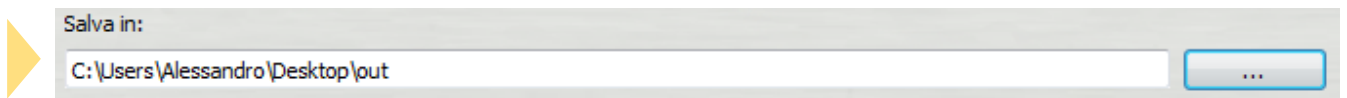




Passo 3



- a. Assicurarsi che sia selezionato il certificato per la firma digitale (Cognome Nome);
- b. Inserire il PIN di protezione della smart card;
- c. Selezionare l'opzione "Firma come busta crittografica P7M";
- d. Verificare che il percorso utilizzato per salvare il file firmato sia quello desiderato, in alternativa, selezionare la cartella di destinazione di proprio interesse, mediante il relativo pulsante:

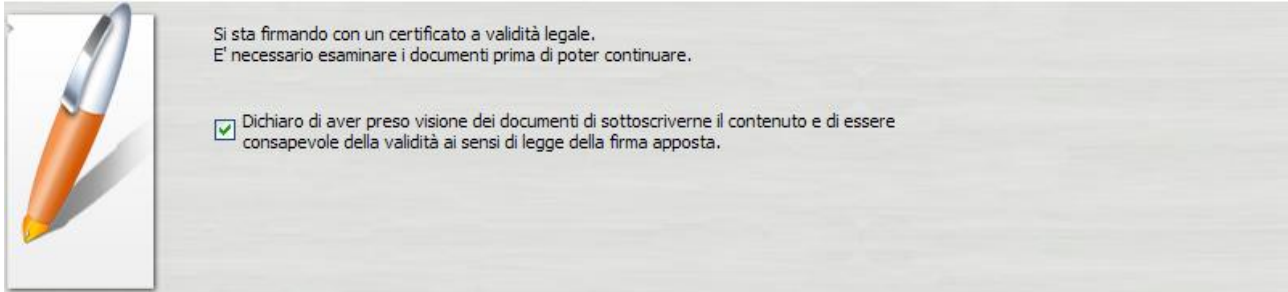


- e. Lasciando selezionata la voce **Aggiungi firma congiunta ai file P7M** verranno create firme multiple su ciascun file incluso nella cartella. Deselezionando il flag, verranno create firme enveloped per ciascun file incluso nella cartella.
- f. Prima di apporre le firme è possibile, mediante il pulsante avviare la verifica di tutti i file presenti nella cartella.
- g. Cliccare sul pulsante **Next >**



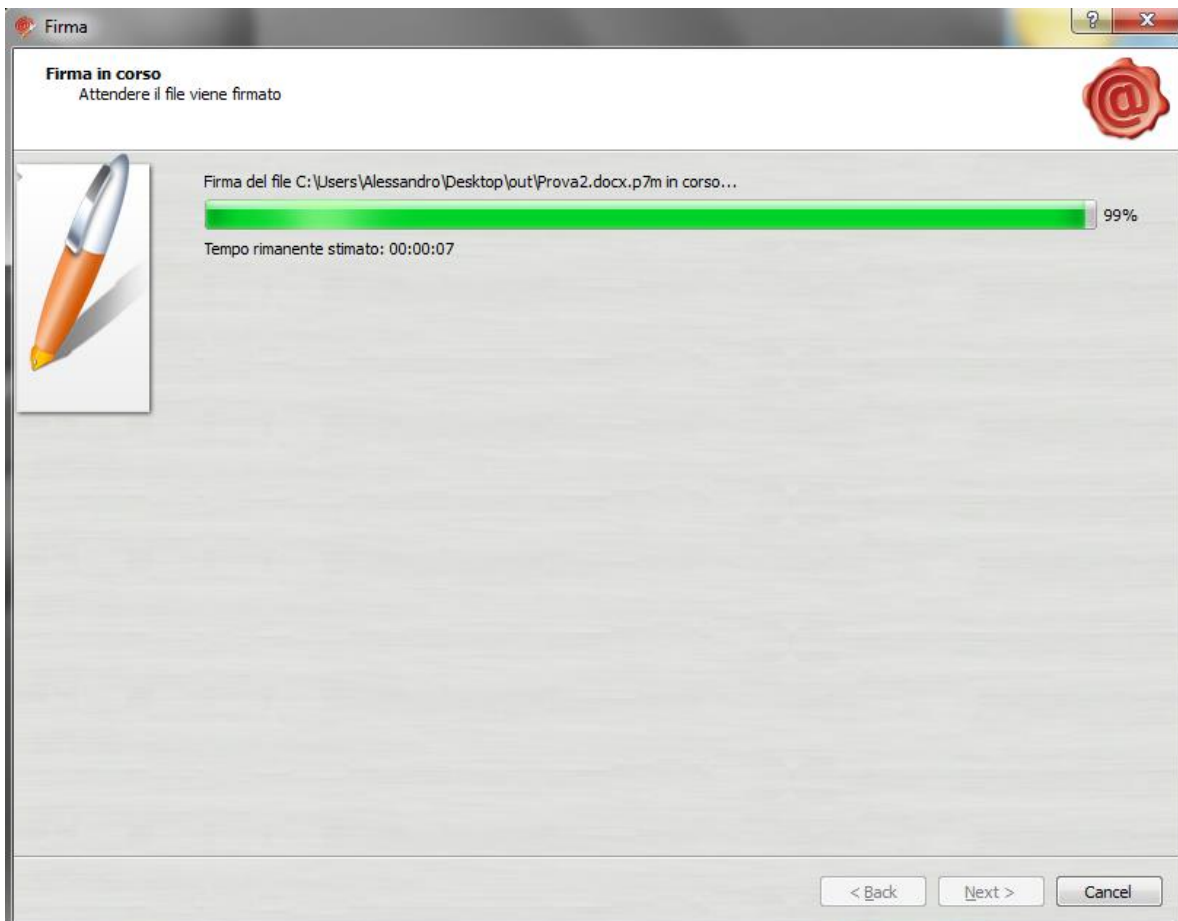
Passo 4

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



Passo 5

Attendere il completamento dell'operazione di firma.

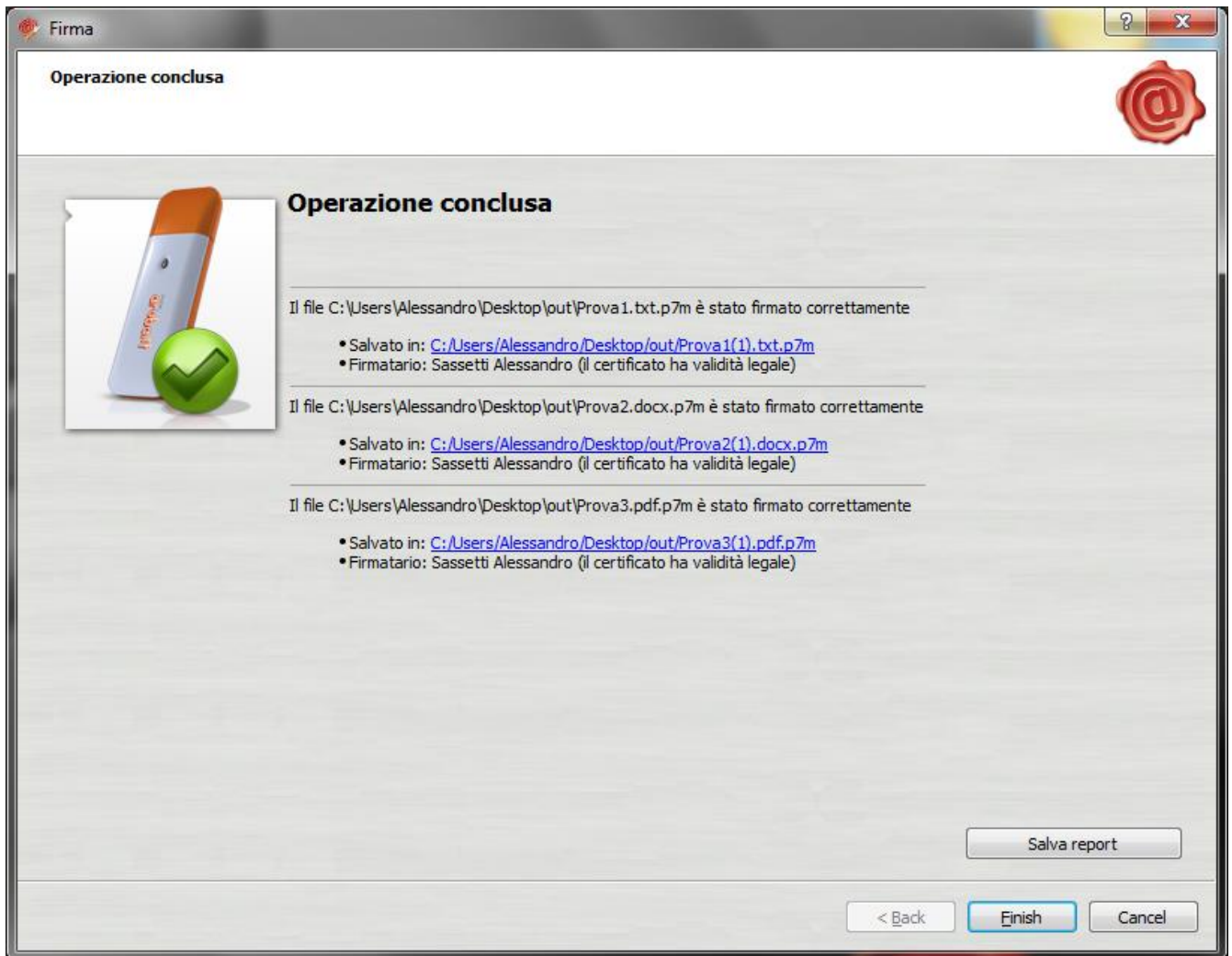


Il tempo necessario per la conclusione dell'operazione varia in base al numero dei file da firmare.



Passo 6

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



La funzione “salva report” consente di salvare, nella stessa cartella dove risiede il file firmato, un file .txt riepilogativo dell’operazione svolta.

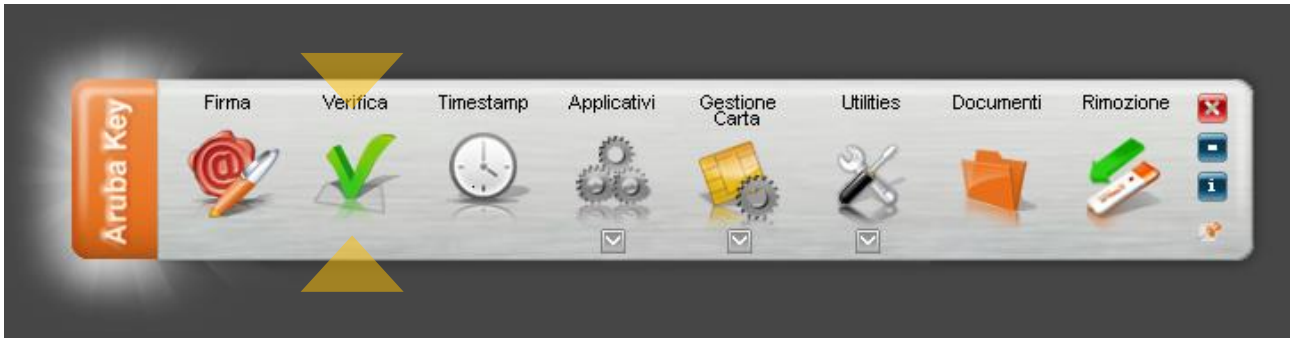


7 Verifica di file firmati

Passo 1

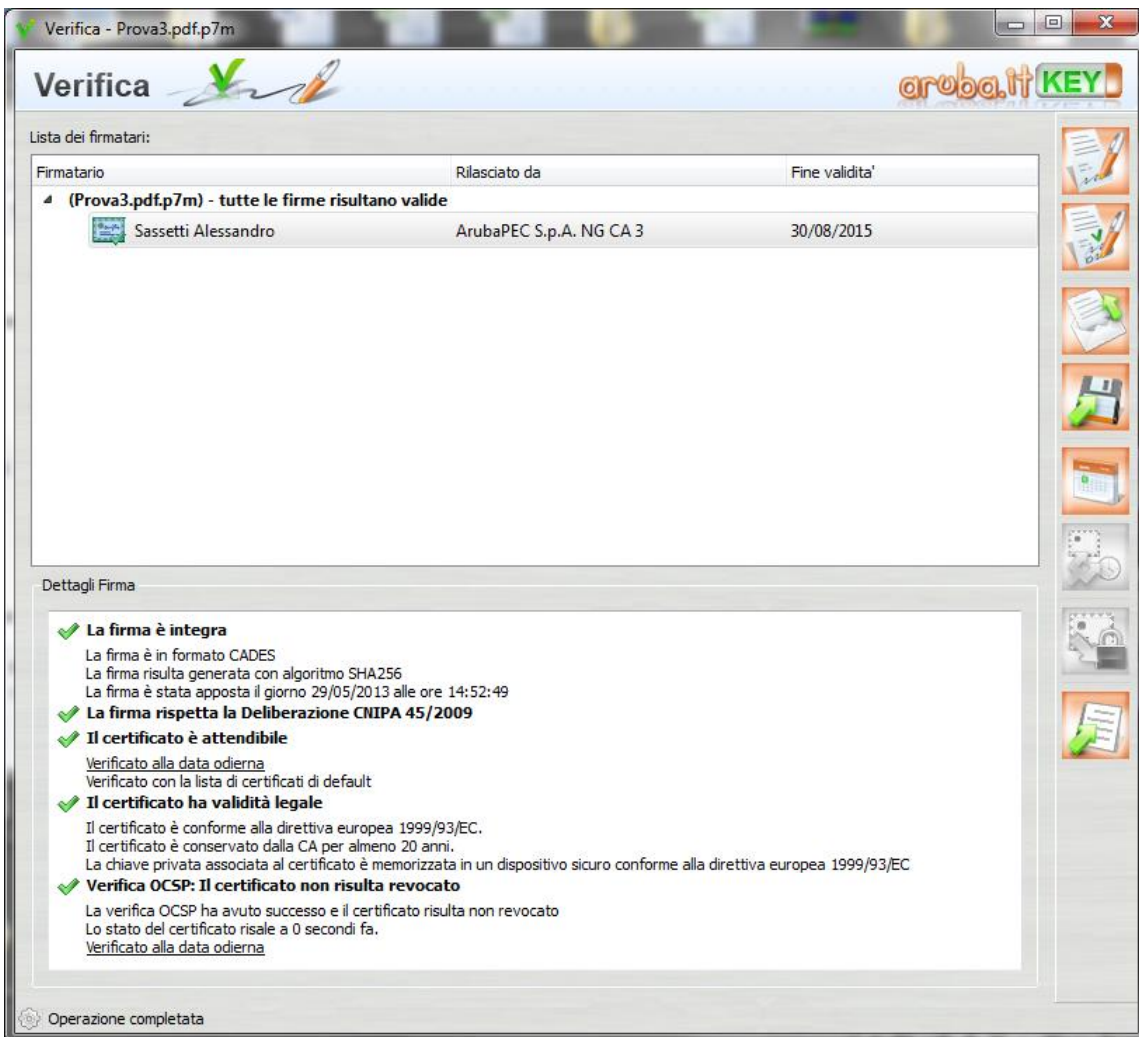
Trascinare il file da verificare sopra il pulsante "Verifica".

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:





Di seguito viene specificato il significato delle voci di riepilogo della verifica:

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

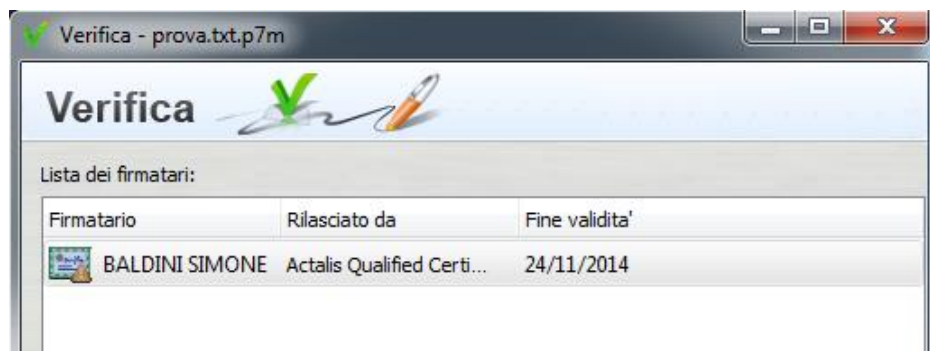
Questa sezione contiene dettagli aggiuntivi sugli algoritmi utilizzati oltre ad indicare dettagli sugli standard utilizzati per la generazione.
- ✓ **La firma rispetta la Deliberazione CNIPA 45/2009.**
Notifica circa il rispetto delle previsioni contenute negli ultimi aggiornamenti normativi
- ✓ **Il 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".



7.1 Verifica di file contenuti in una cartella

Passo 1

Trascinare la cartella contenente uno o più 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:

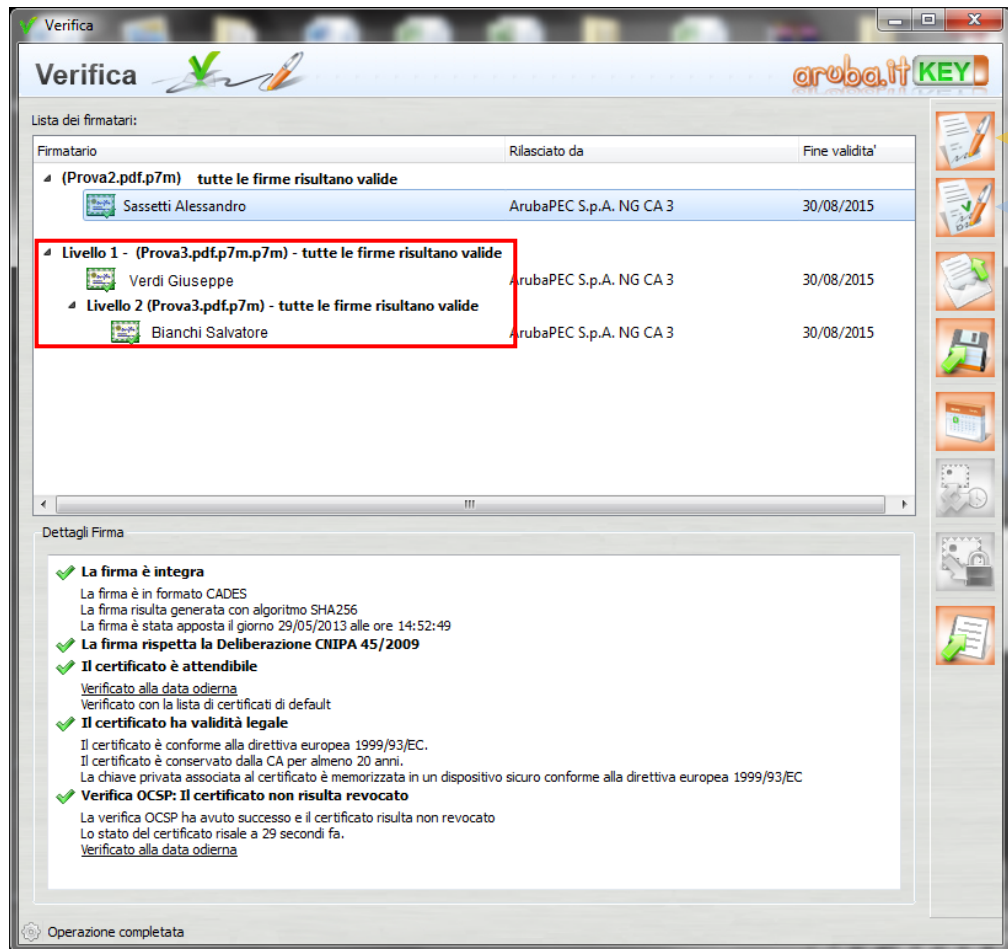


Le voci presenti nella sezione Dettagli Firma sono analoghe a quelle visualizzate durante la verifica di un singolo file.

Selezionando un firmatario, si abilitano o meno i pulsanti di apposizione di:

-  Aggiunta Firma
-  Controfirma

Come visibile nell'esempio evidenziato in rosso, in caso di firma + controfirma il firmatario del documento viene indicato al livello 1, mentre il controfirmatario viene indicato al livello 2.



The screenshot shows the 'Verifica' window with the following data:

Firmatario	Rilasciato da	Fine validita'
(Prova2.pdf.p7m) - tutte le firme risultano valide		
Sassetti Alessandro	ArubaPEC S.p.A. NG CA 3	30/08/2015
Livello 1 - (Prova3.pdf.p7m.p7m) - tutte le firme risultano valide		
Verdi Giuseppe	ArubaPEC S.p.A. NG CA 3	30/08/2015
Livello 2 (Prova3.pdf.p7m) - tutte le firme risultano valide		
Bianchi Salvatore	ArubaPEC S.p.A. NG CA 3	30/08/2015

Dettagli Firma

- ✓ **La firma è integra**
La firma è in formato CADES
La firma risulta generata con algoritmo SHA256
La firma è stata apposta il giorno 29/05/2013 alle ore 14:52:49
- ✓ **La firma rispetta la Deliberazione CIIPA 45/2009**
- ✓ **Il certificato è attendibile**
Verificato alla data odierna
Verificato con la lista di certificati di default
- ✓ **Il certificato ha validità legale**
Il certificato è conforme alla direttiva europea 1999/93/EC.
Il certificato è conservato dalla CA per almeno 20 anni.
La chiave privata associata al certificato è memorizzata in un dispositivo sicuro conforme alla direttiva europea 1999/93/EC
- ✓ **Verifica OCSP: Il certificato non risulta revocato**
La verifica OCSP ha avuto successo e il certificato risulta non revocato
Lo stato del certificato risale a 29 secondi fa.
Verificato alla data odierna

Operazione completata

Per una più semplice visualizzazione delle verifiche, soprattutto in caso di molteplici file, i livelli sono espandibili e comprimibili, mediante i triangoli neri, posti alla sinistra del nome file:

▲ **(Prova3-signed.pdf) - tutte le firme risultano valide**

Livelli compressi



The screenshot shows the 'Verifica' window with a compressed list of signatories:

- ▶ **(Prova3-signed.pdf) - tutte le firme risultano valide**
- ▶ **(Prova3.pdf.p7m) - tutte le firme risultano valide**
- ▶ **Livello 1 - (Prova3.pdf.p7m.p7m) - tutte le firme risultano valide**



Livelli espansi

✓ Verifica

Verifica

Lista dei firmatari:

Firmatario	Rilasciato da
▲ (Prova3-signed.pdf) - tutte le firme risultano valide	
Sassetti Alessandro	ArubaPEC S.p.A. NG CA 3
▲ (Prova3.pdf.p7m) - tutte le firme risultano valide	
Sassetti Alessandro	ArubaPEC S.p.A. NG CA 3
▲ Livello 1 - (Prova3.pdf.p7m.p7m) - tutte le firme risultano valide	
Sassetti Alessandro	ArubaPEC S.p.A. NG CA 3
▲ Livello 2 (Prova3.pdf.p7m) - tutte le firme risultano valide	
Sassetti Alessandro	ArubaPEC S.p.A. NG CA 3



8 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”**.



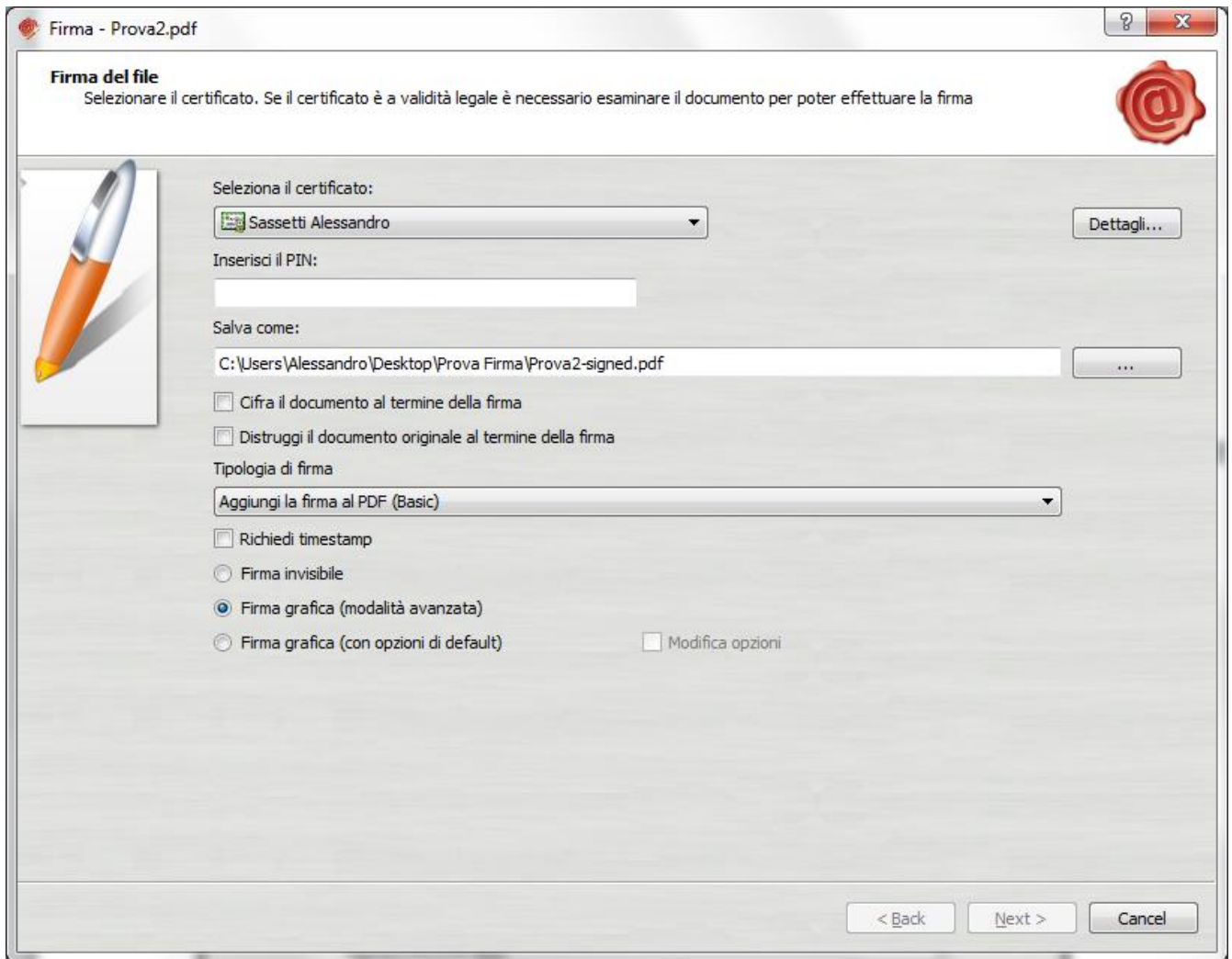
Passo 2

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



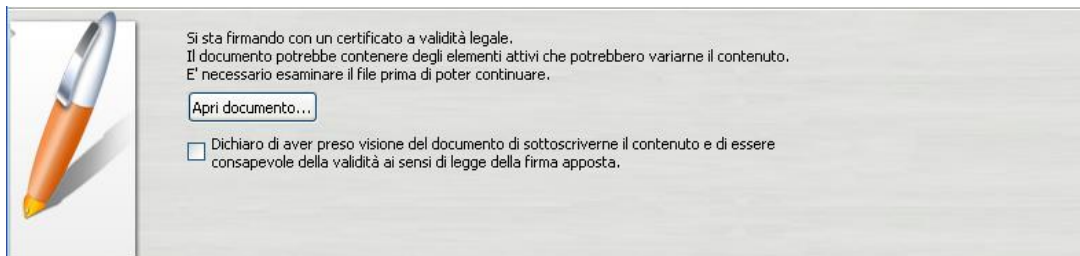
Passo 3

- Assicurarsi che sia selezionato il certificato per la firma digitale (Cognome Nome);
- Inserire il PIN di protezione della smart card;
- Selezionare *“Aggiungi la firma al PDF”* e attivare l’opzione *“Firma grafica (modalità avanzata)”*;
- Cliccare sul pulsante **Next >**



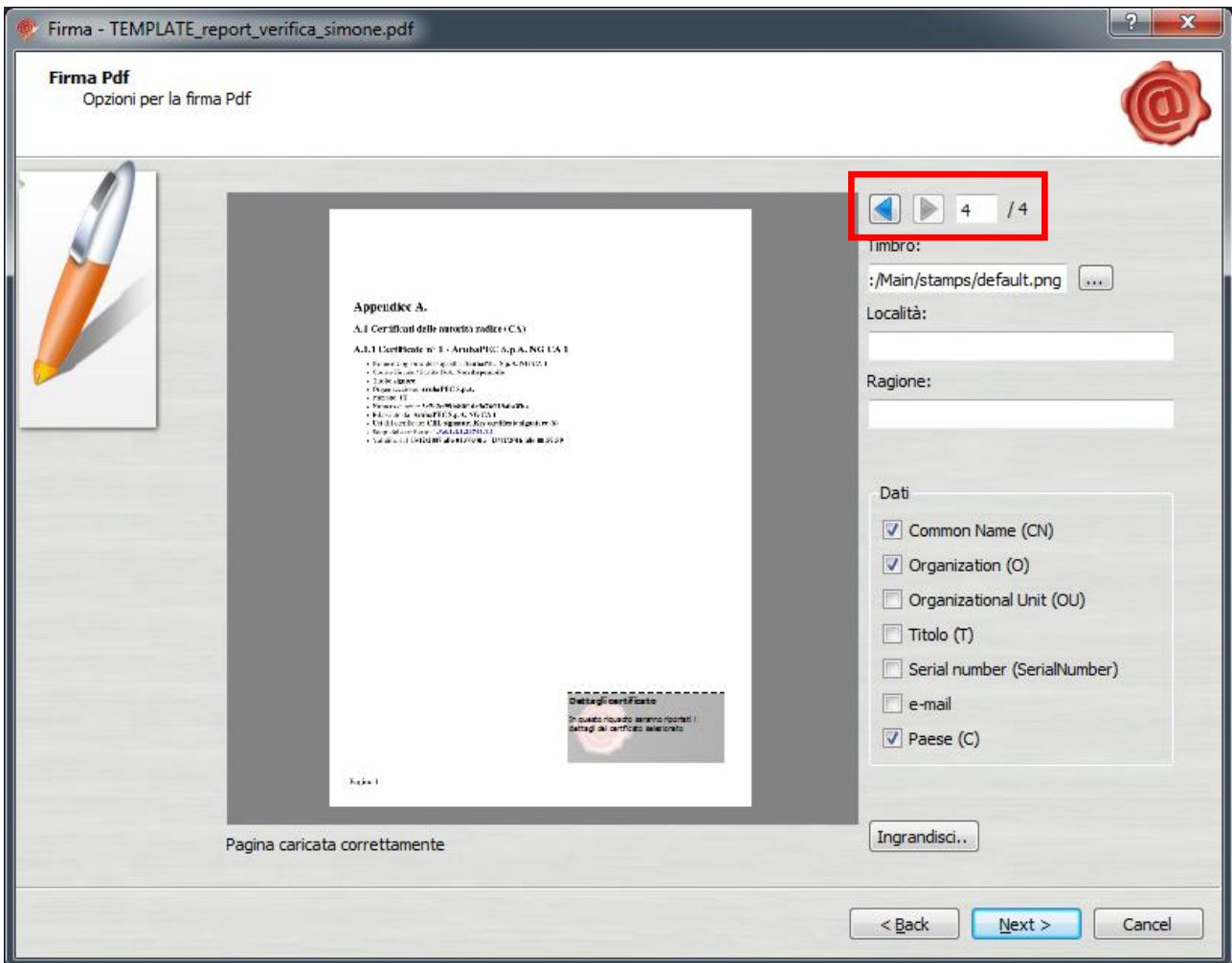
Passo 4

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



Passo 5

- Definire, attraverso la finestra di anteprima, la posizione, la dimensione e il logo del campo che ospiterà il contrassegno, contenente i dati del sottoscrittore;
- Cliccare sul pulsante **Next >**



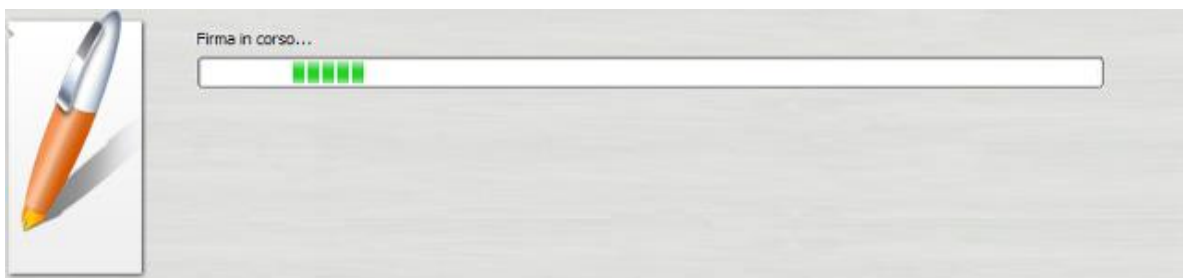
Il timbro può essere posizionato in una delle pagine del documento PDF, mediante le frecce evidenziate nella immagine di cui sopra.

Il timbro è ridimensionabile, agendo con il mouse sul timbro stesso, e la sua posizione può essere variata all'interno della pagina selezionata.

Alla destra dell'anteprima, sono evidenziate le voci che è possibile inserire nelle diciture incluse nel timbro. Tali informazioni, vengono prelevate dal certificato con il quale si sta firmando digitalmente.

Passo 6

Attendere il completamento dell'operazione di firma.





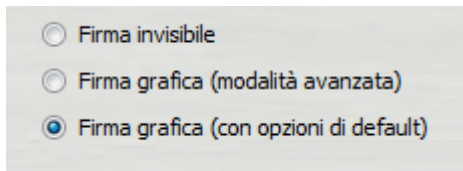
Passo 7

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



Oltre alla firma grafica avanzata, è possibile apporre altri due tipi di firma digitale in format pdf:

- firma grafica con opzioni di default
- firma invisibile



Le impostazioni di default comportano l'apposizione di un timbre, a pagina 1 del document PDF in alto a sinistra. Le informazioni contenute nel timbro sono relative a :

- Nome e cognome del firmatario
- Organizzazione di appartenenza
- Paese di origine

La firma invisibile, invece, crea un pdf firmato digitalmente, senza alcuna apposizione di timbre grafici.

IMPORTANTE

In fase di firma digitale in format pdf, il software della Aruba KEY aggiunge un suffisso "signed" al nome file.

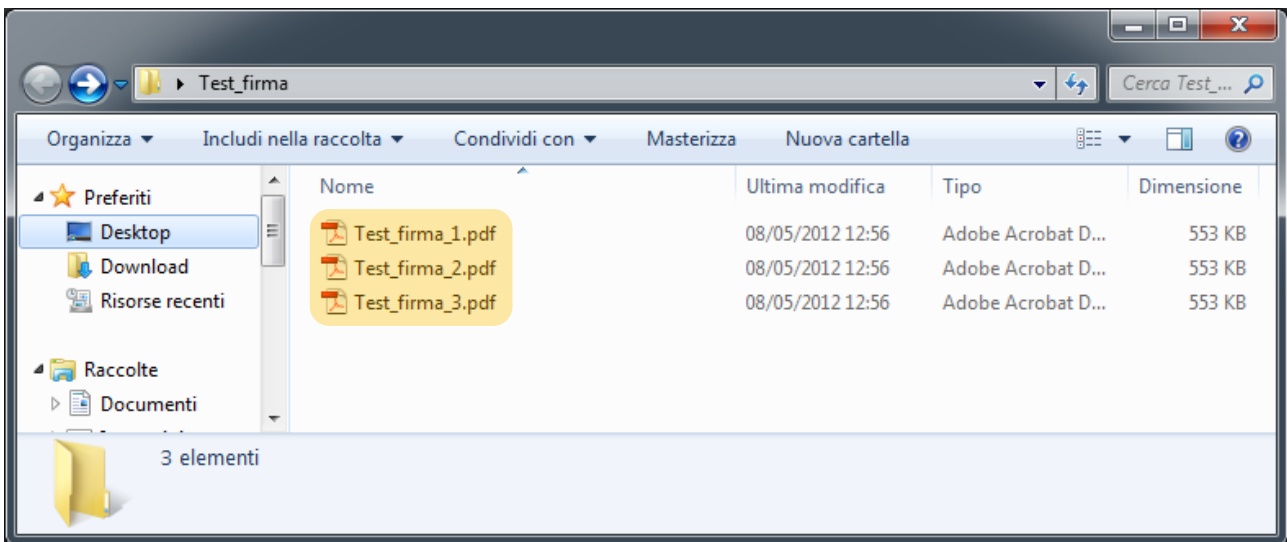
Firmando il document Prova2.pdf, avremo pertanto un file con nome Prova2-signed.pdf.



8.1 Firmare digitalmente più file in formato PDF

Passo 1

Selezionare tutti i documenti PDF da firmare.



Nell'esempio sono indicate file pdf non firmati.

Se nella cartella sono presenti anche file pdf firmati (quindi con suffisso "signed") ad essi verrà apposta una firma multipla.

Pertanto, nella cartella possono coesistere file pdf e file pdf già firmati (in formato signed.pdf).

Passo 2

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



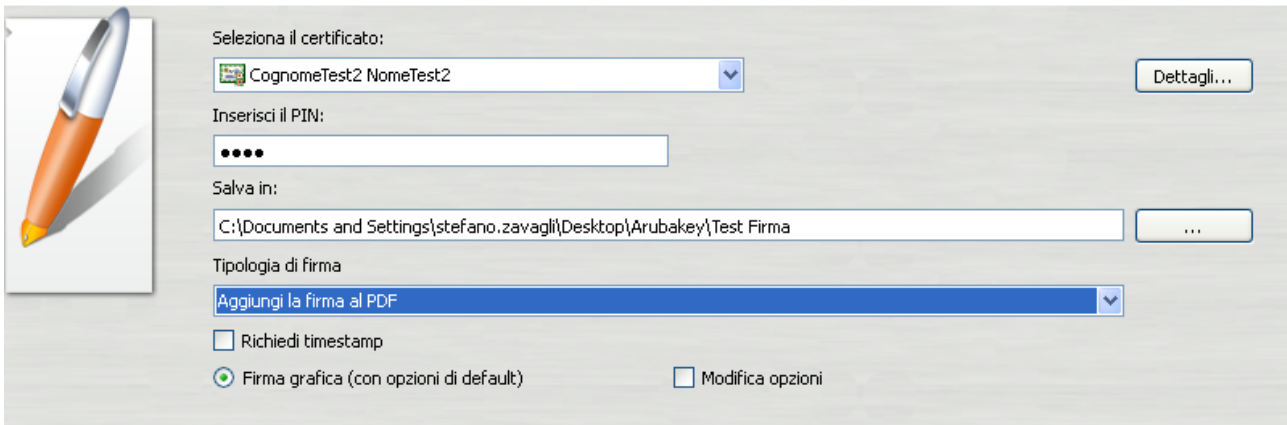
Passo 3

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



Passo 4

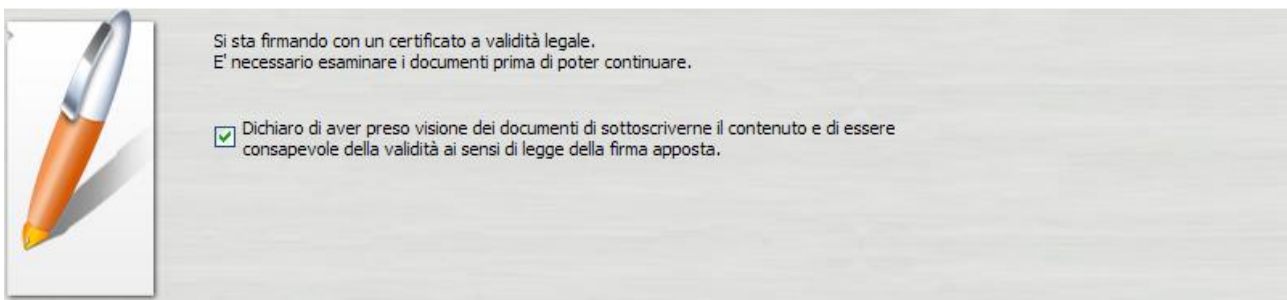
- a. Assicurarsi che sia selezionato il certificato per la firma digitale (Cognome Nome);
- b. Inserire il PIN di protezione della smart card;
- c. Selezionare l'opzione "Aggiungi la firma al PDF";
- d. Cliccare sul pulsante **Next >**



Attraverso l'opzione "salva in" è possibile selezionare una diversa cartella di destinazione dei file firmati, rispetto a quella proposta di default (cartella di partenza).

Passo 5


- a. Selezionare l'opzione relativa alla presa visione dei documenti;
- b. 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.



Operazione conclusa

Il file C:\Documents and Settings\stefano.zavagli\Desktop\Arubakey\Test Firma\TEST_FIRMA1.pdf è stato firmato correttamente

- Salvato in: [C:/Documents and Settings/stefano.zavagli/Desktop/Arubakey/Test Firma/TEST_FIRMA1-signed.pdf](#)
- Firmatario: CognomeTest2 NomeTest2 (il certificato ha validità legale)

Il file C:\Documents and Settings\stefano.zavagli\Desktop\Arubakey\Test Firma\TEST_FIRMA2.pdf è stato firmato correttamente

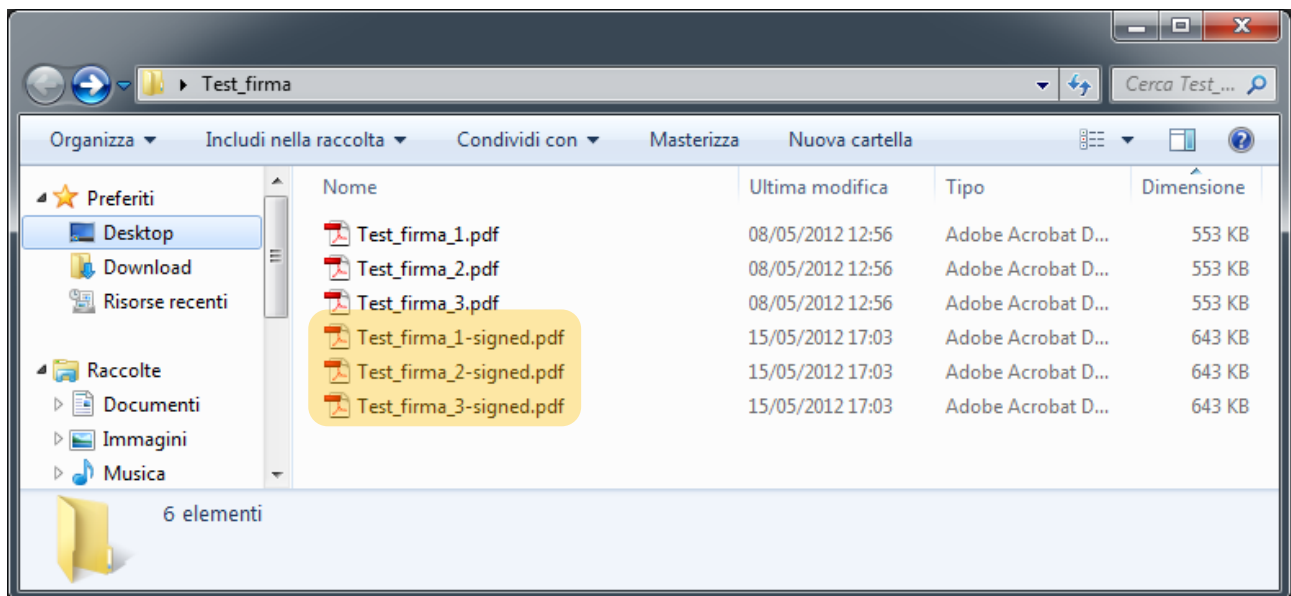
- Salvato in: [C:/Documents and Settings/stefano.zavagli/Desktop/Arubakey/Test Firma/TEST_FIRMA2-signed.pdf](#)
- Firmatario: CognomeTest2 NomeTest2 (il certificato ha validità legale)

Il file C:\Documents and Settings\stefano.zavagli\Desktop\Arubakey\Test Firma\TEST_FIRMA3.pdf è stato firmato correttamente

- Salvato in: [C:/Documents and Settings/stefano.zavagli/Desktop/Arubakey/Test Firma/TEST_FIRMA3-signed.pdf](#)
- Firmatario: CognomeTest2 NomeTest2 (il certificato ha validità legale)

Passo 7

I documenti firmati verranno salvati nella stessa cartella dove risiedono i documenti originali (se non diversamente indicato, come da passo 4) aggiungendo al nome il suffisso "signed".



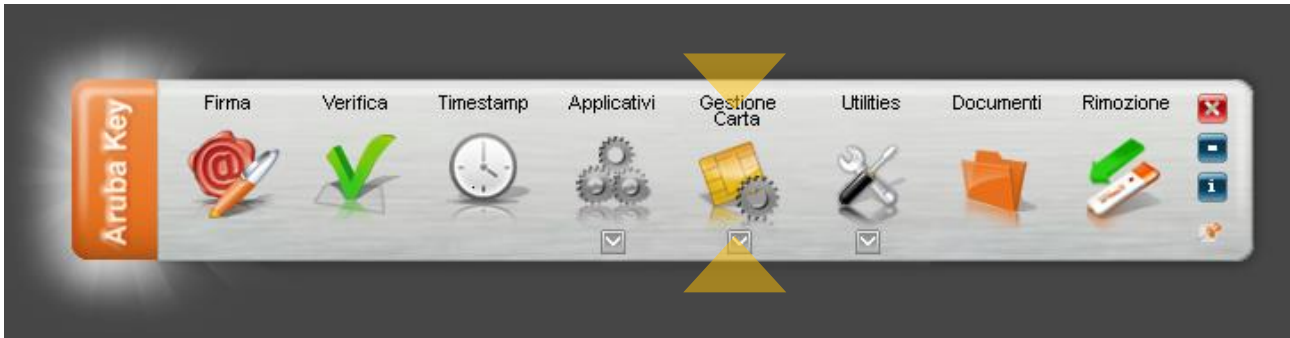


9 Gestione smart card

9.1 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".

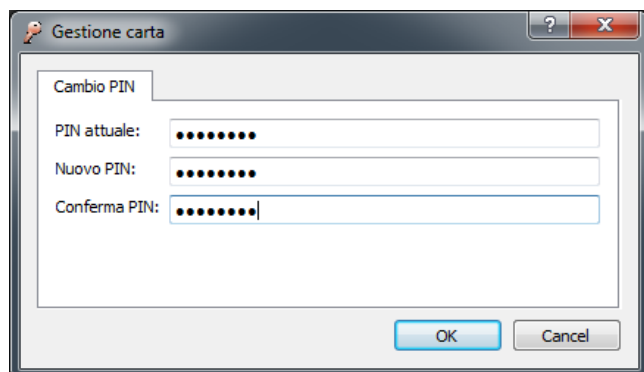


Passo 3

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.



Il numero massimo di tentativi consecutivi di inserimento del PIN è pari a 5.



9.2 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".

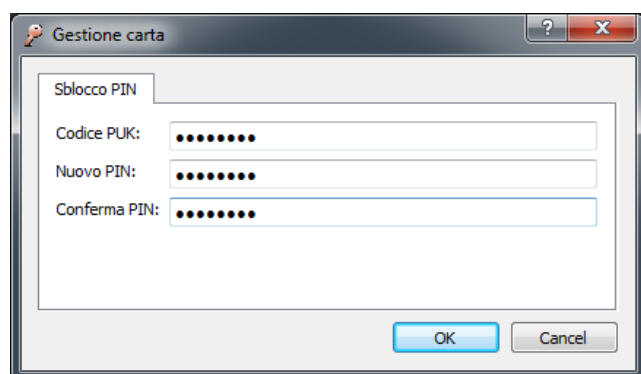


Passo 3

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.



Il numero massimo di tentativi consecutivi di inserimento del PUK è pari a 5.

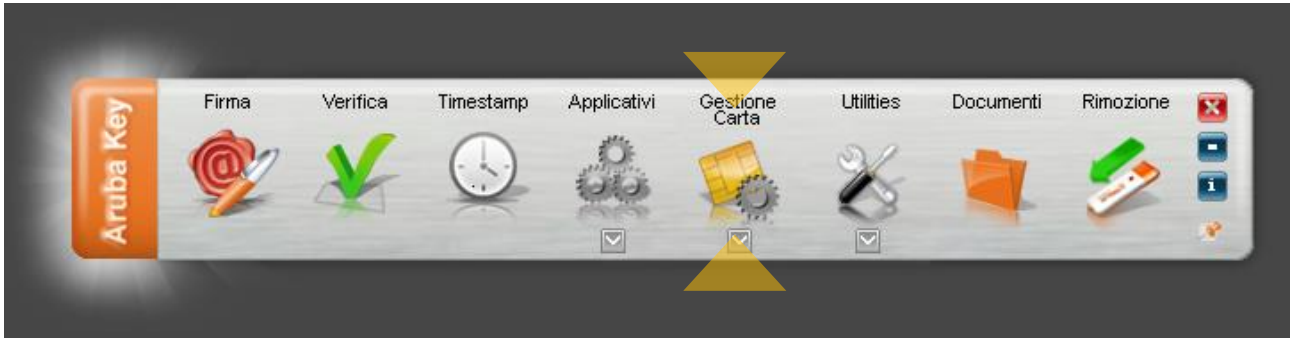
In caso di inserimenti consecutivi di un PUK errato per un numero di volte maggiori a 5, la smart card si blocca. In tal caso deve essere inviata una segnalazione al CSI mediante l'applicazione <http://www.cerdi.unina.it/Ticket>.



9.3 Cambio del PUK

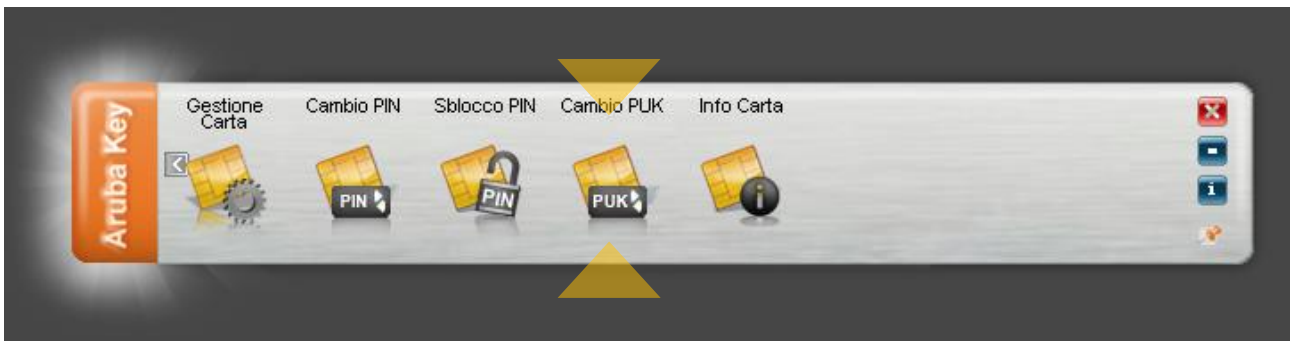
Passo 1

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".

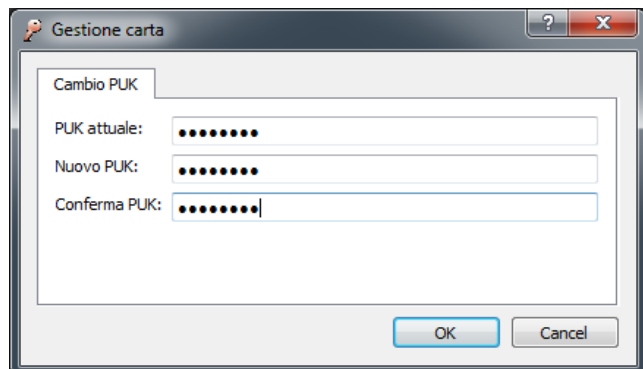


Passo 3

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.



Il numero massimo di tentativi consecutivi di inserimento del PUK è pari a 5.

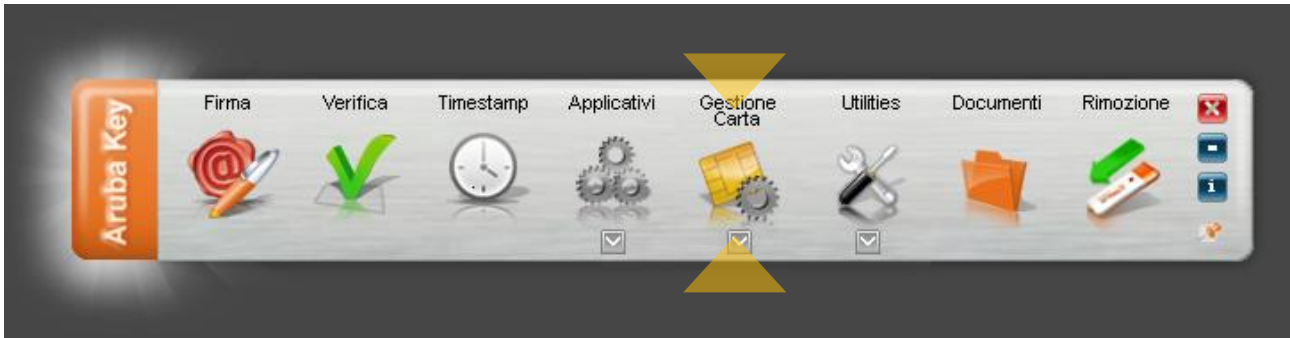
In caso di inserimenti consecutivi di un PUK errato per un numero di volte maggiori a 5, la smart card si blocca. In tal caso, contattare il CSI.



9.4 Lettura informazioni carta

Passo 1

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



Passo 2

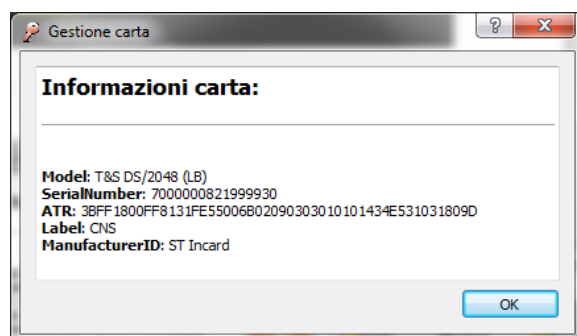
Cliccare su "Info Carta".



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





9.5 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:

<p>Errore: Il Pin attuale è errato. Attenzione: troppi tentativi errati possono bloccare il PIN.</p>	<p>Questo messaggio indica che il campo "Vecchio Pin" della finestra "Cambio Pin", non è corretto.</p> <p>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.</p>
<p>Errore: Il PIN è bloccato.</p>	<p>Questo messaggio indica che il PIN della carta è bloccato.</p> <p>E' necessario procedere con lo sblocco del PIN seguendo le indicazioni contenute nel paragrafo "Sblocco PIN".</p>
<p>Errore: Il Codice PUK è errato.</p> <p>Attenzione: troppi tentativi errati potrebbero bloccare il PUK!</p>	<p>Questo messaggio indica che il campo "Puk" della finestra "Sblocco Pin", non è corretto.</p> <p>In questo caso l'utente deve tener ben presente il fatto che l'inserimento ripetuto di PUK non validi può causare il blocco <u>definitivo</u> della carta.</p>
<p>Errore: Il PUK attuale è errato.</p> <p>Attenzione: troppi tentativi errati potrebbero bloccare il PUK!</p>	<p>Questo messaggio indica che il campo "Puk" della finestra "Cambio Puk", non è corretto.</p> <p>In questo caso l'utente deve tener ben presente il fatto che l'inserimento ripetuto di PUK non validi può causare il blocco <u>definitivo</u> della carta.</p>
<p>Errore: Il PUK è bloccato.</p>	<p>Questo messaggio indica che il PUK della carta è bloccato.</p> <p>E' necessario inviare una segnalazione al CSI, per far revocare e richiedere l'emissione di un nuovo certificato di firma, tramite l'applicazione http://www.cerdi.unina.it/Ticket</p>



10 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

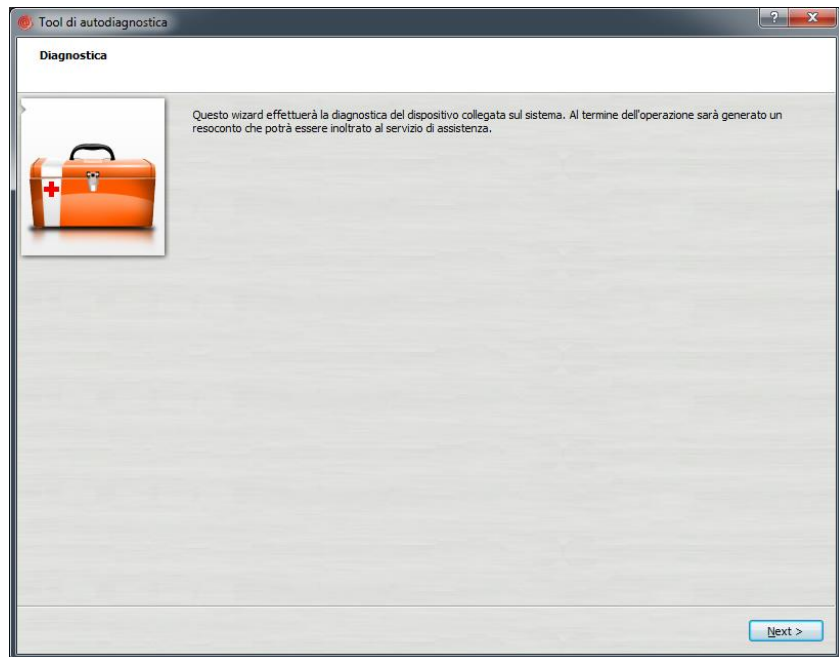
Cliccare su "Auto-diagnostica".





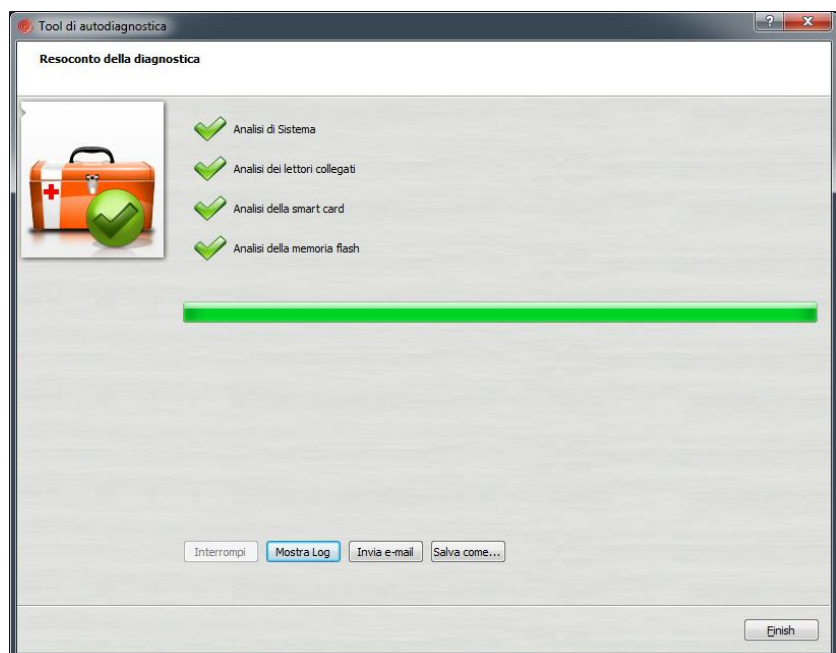
Passo 3

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.



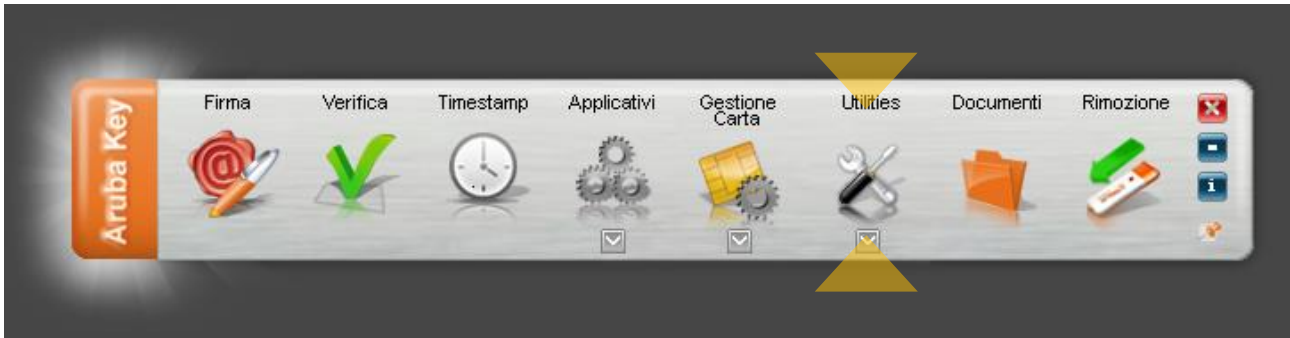
11 "Import" certificato

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

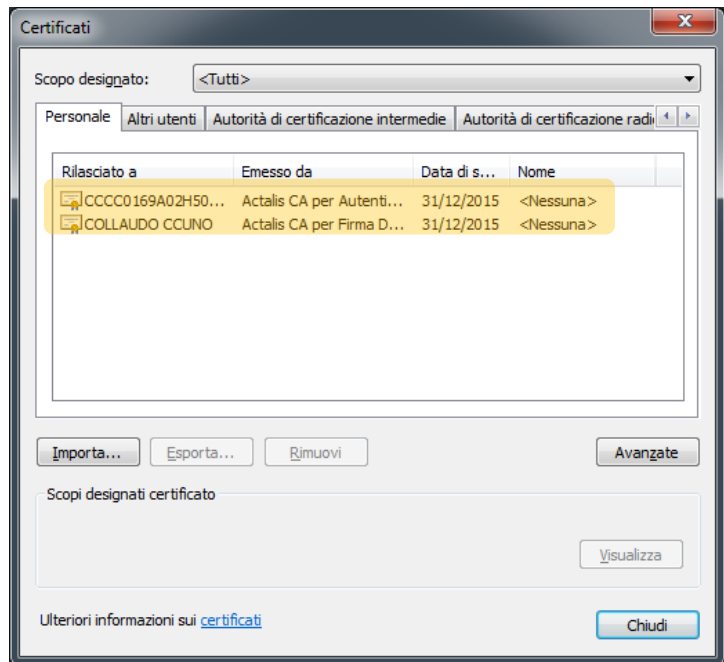
Seguire il wizard di installazione accettando le condizioni di contratto e cliccando su OK ad ogni schermata.

Passo 4

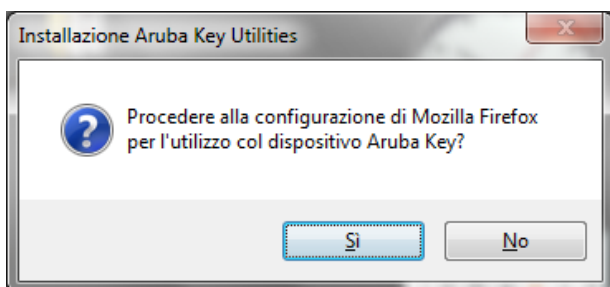
Verificare la corretta installazione del certificato tramite la seguente procedura

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



La funzione di Import Certificato consente la configurazione automatic di Mozilla FireFox per l’utilizzo con Aruba KEY. Al fine di procedere con tale configurazione, è sufficiente cliccare su Sì quando richiesto:





12 Cifratura File

PREMESSA

L'operazione di cifratura di un file, benchè utile in talune circostanze, è molto delicata e potenzialmente pericolosa, dal momento che per cifrare/decifrare i file si utilizzano i certificate a bordo della SIM card.

Nel caso la SIM card si guasti o venga smarrita, infatti, non sarà più possibile decifrare un file precedentemente cifrato, rendendone impossibile la successive visualizzazione/stampa.

Per tale ragione, si sconsiglia di ricorrere a tale forma di protezione dei file.

Passo 1

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



Passo 2

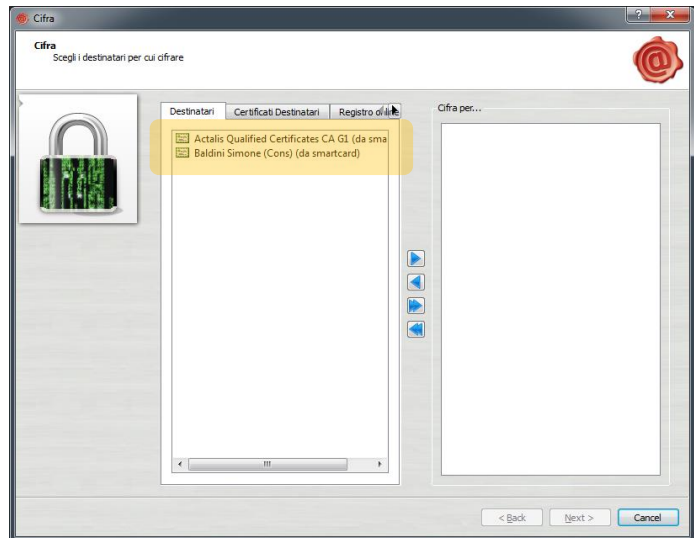
Trascinare il file da cifrare sopra il pulsante **"Cifra"**.



Passo 3

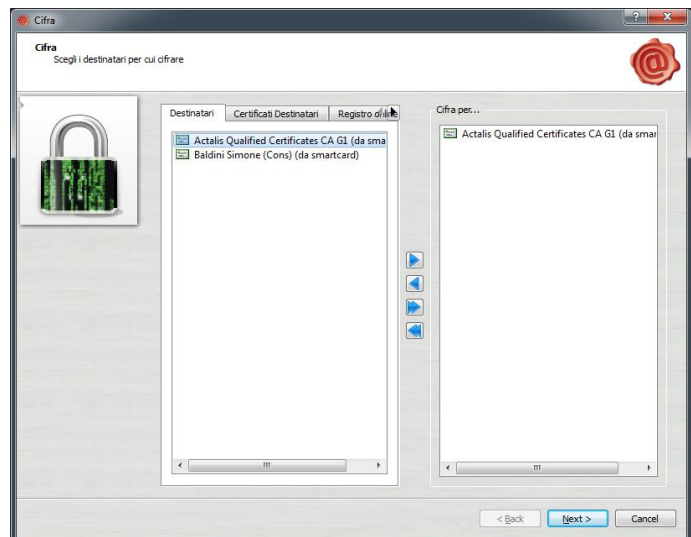


All'interno della finestra di cifratura selezionare, dalla sezione di sinistra, l'elenco dei destinatari del file cifrato e cliccare su "Aggiungi".



Passo 4

Cliccare su "Next".



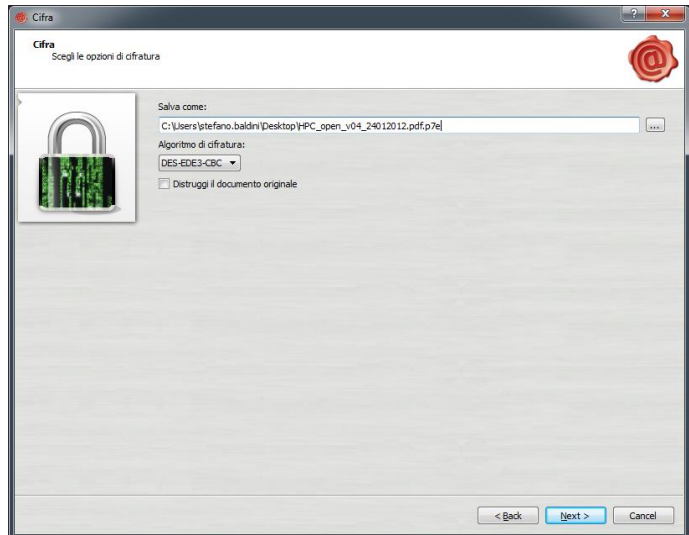
Passo 5



Selezionare la cartella di destinazione dove salvare il file cifrato e cliccare su “Next”.

NOTE:

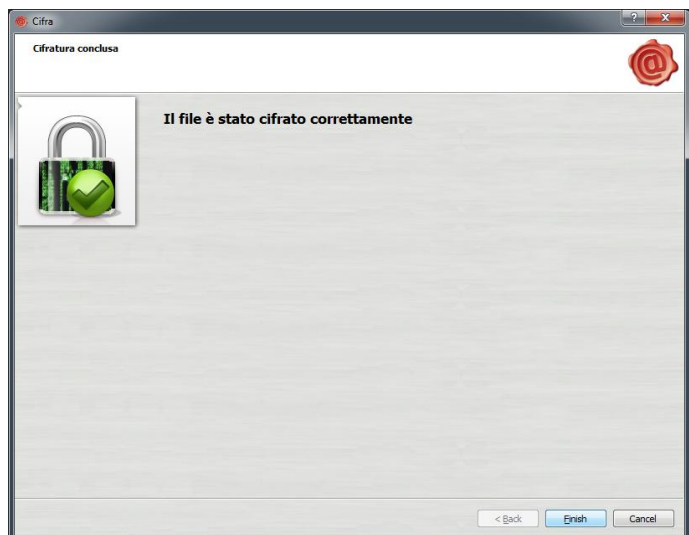
- *Se vengono selezionati più certificati per la cifratura del file, il risultato sarà un unico file decifrabile da ogni singolo titolare dei certificati selezionati.*
- *In fase di cifratura del file l’Aruba key propone automaticamente, nell’area “destinatari”, il proprio certificato di autenticazione, 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.





13 Decifratura File

Passo 1

Per cifrare un file selezionare "Utilities".



Passo 2

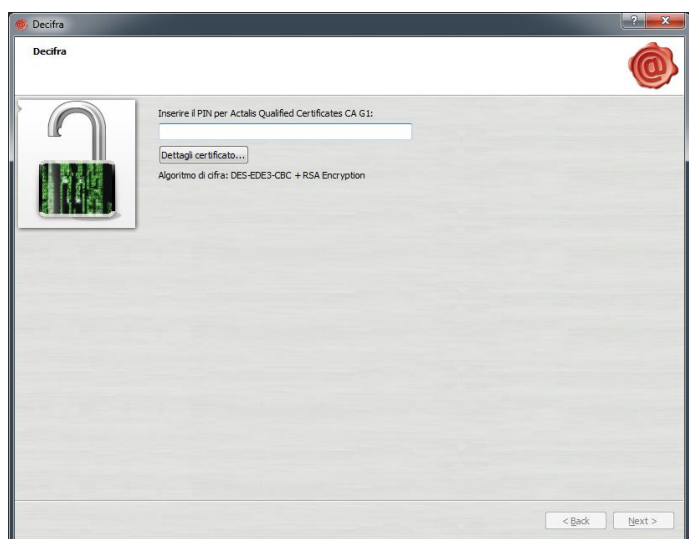
Trascinare il file ".p7e" sull'icona "Decifra".



Passo 3

L'Aruba key verifica che nella SIM sia presente almeno uno dei certificati indicati nella fase di cifratura.

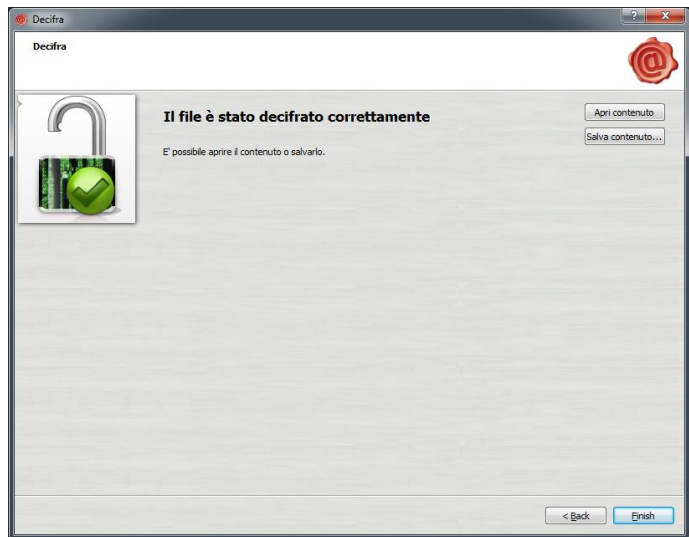
In questa fase viene richiesto il PIN della SIM inserita in Arubakey.





Passo 4

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





14 Utilizzo di una cartella cifrata

Passo 1

Per cifrare un file selezionare "Utilities".



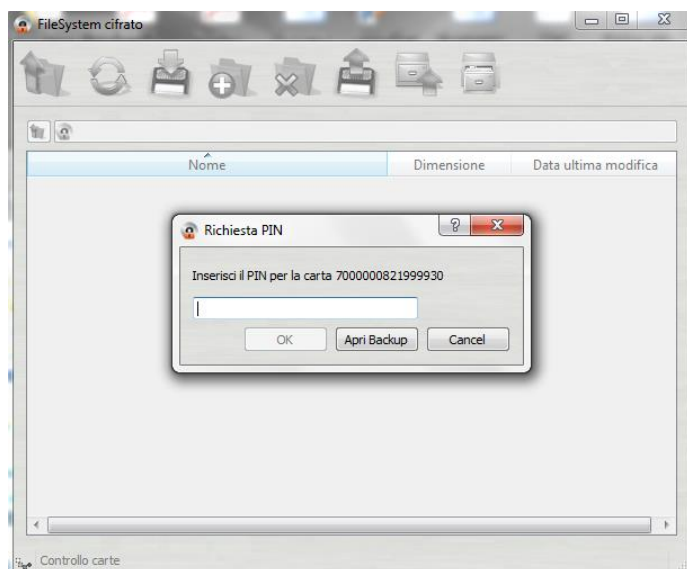
Passo 2

Selezionare il pulsante "Cartella Cifrata".



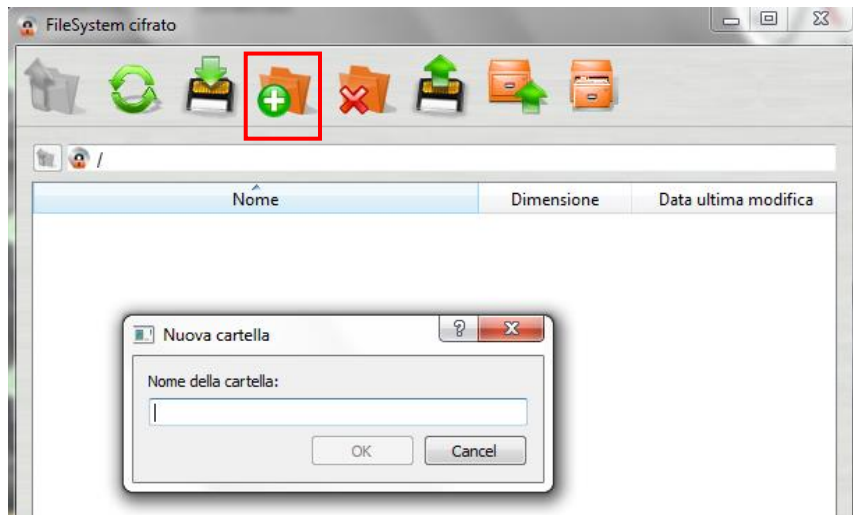
Passo 3

Inserire il PIN della smart card





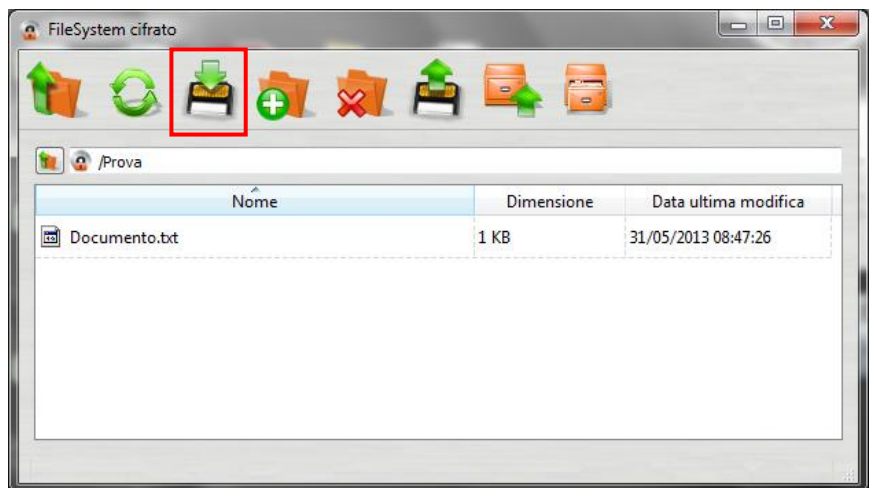
Cliccare il pulsante “Crea nuova cartella” e, quando richiesto, inserire il nome della cartella.







Eseguire il doppio click sulla cartella selezionata e trascinarvi, all’interno, i file di proprio interesse.

Automaticamente, il file verrà salvato nella cartella cifrata.

E’ possibile aggiungere file, trascinandoli all’interno della cartella, oppure cliccando sul pulsante “Aggiungi File”, evidenziato in rosso.

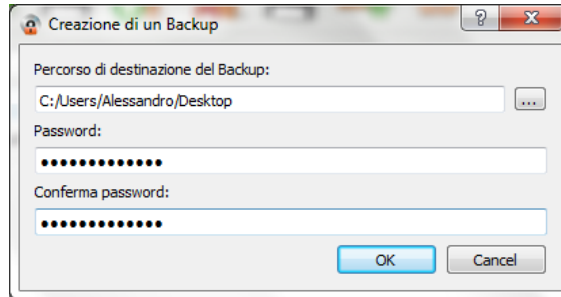


Di seguito viene specificato il significato delle restanti icone/pulsanti, presenti sulla barra degli strumenti della funzione “Cartella Cifrata”:

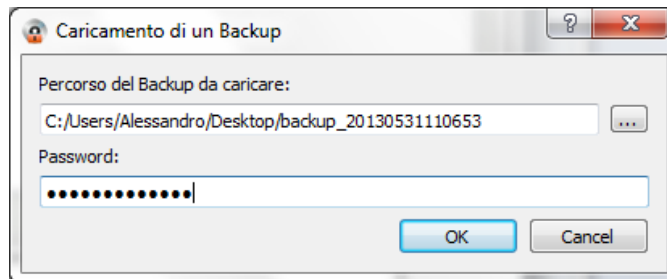
	Se si è all’interno di una cartella, creata come da precedenti indicazioni, tale pulsante consente di salire di un livello, fino a tornare nella cartella principale del FileSystem Cifrato.
	Pulsante “aggiorna”, utile per aggiornare la visualizzazione delle cartelle.
	Pulsante “rimuovi selezionati”, utile per eliminare file e/o cartelle preventivamente selezionate.
	Pulsante “esporta selezionati”, utile per esportare, ad esempio sul desktop del PC, file presenti all’interno di una cartella cifrata. Una volta esportato il file, esso potrà essere aperto con il programma associato alla sua estensione (es. file .doc verrà aperto con Word).



Pulsante “crea backup del disco cifrato”, utile per creare una cartella di backup dell’intero FileSystem Cifrato. Per creare la cartella di backup è necessario specificare il percorso ove salvarla, ed inserire una password, come di seguito indicato:



Pulsante “apri backup”, utile per aprire una cartella soggetta a preventivo backup, come sopra indicato. Per aprire una cartella precedentemente sottoposta a backup è necessario richiamare il percorso ove è stata memorizzata ed inserire la password scelta in fase di backup, come di seguito indicato:





15 Opzioni

15.1 Impostazioni del proxy

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

Passo 1

Selezionare il pulsante “Utilities”.



Passo 2

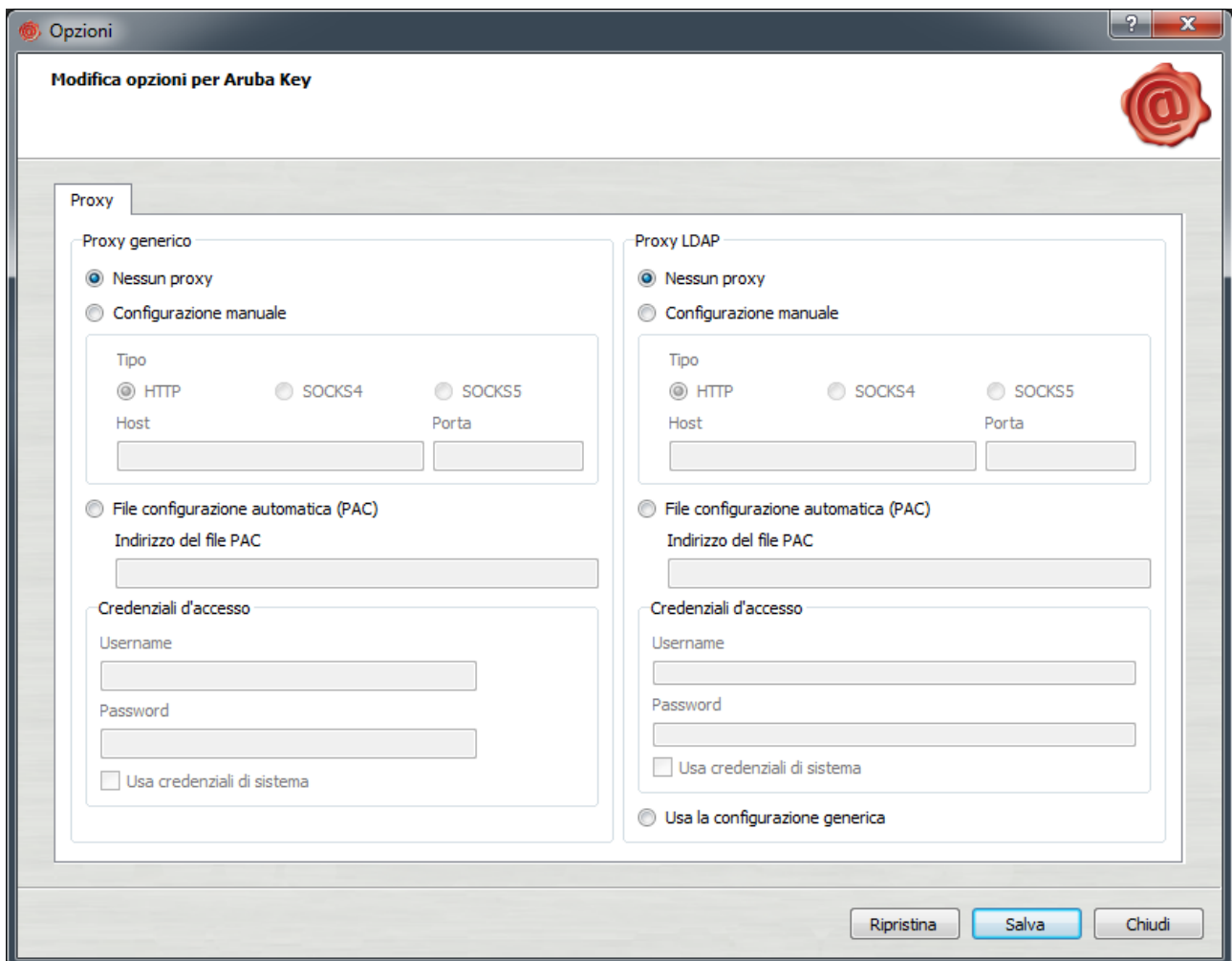
Cliccare su “Opzioni e Proxy”.





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.

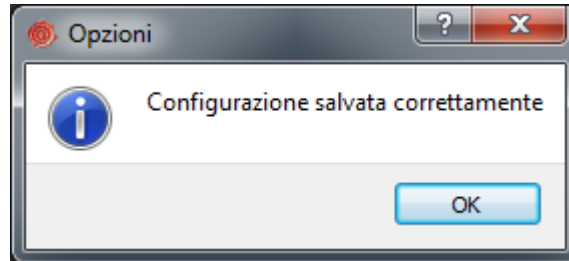
Per la configurazione 'Proxy LDAP' è possibile inoltre selezionare anche l'opzione **Usa la configurazione generica** in modo tale che per indirizzi LDAP venga utilizzata la stessa configurazione specificata in 'Proxy generico'.

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.

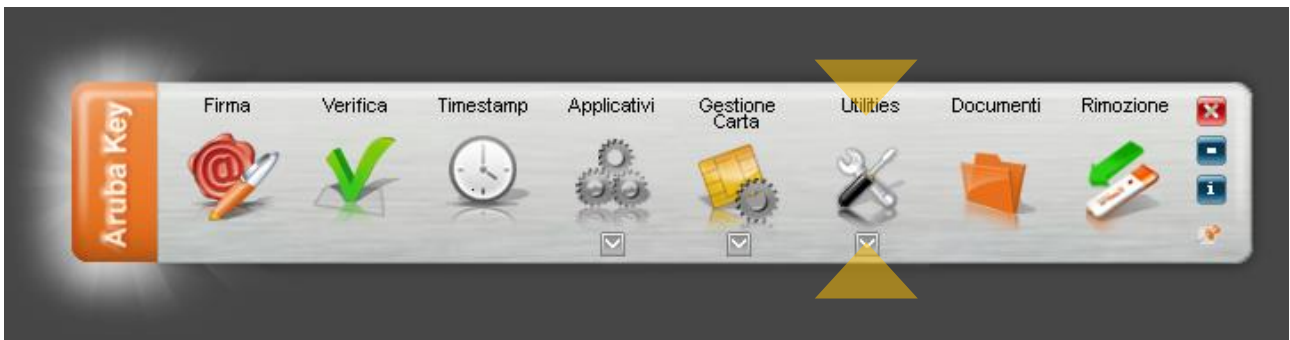


15.2 Impostazioni della lingua

Per cambiare la lingua dell'Aruba Key svolgere le seguenti operazioni:

Step 1

Selezionare "Utilities".



Step 2

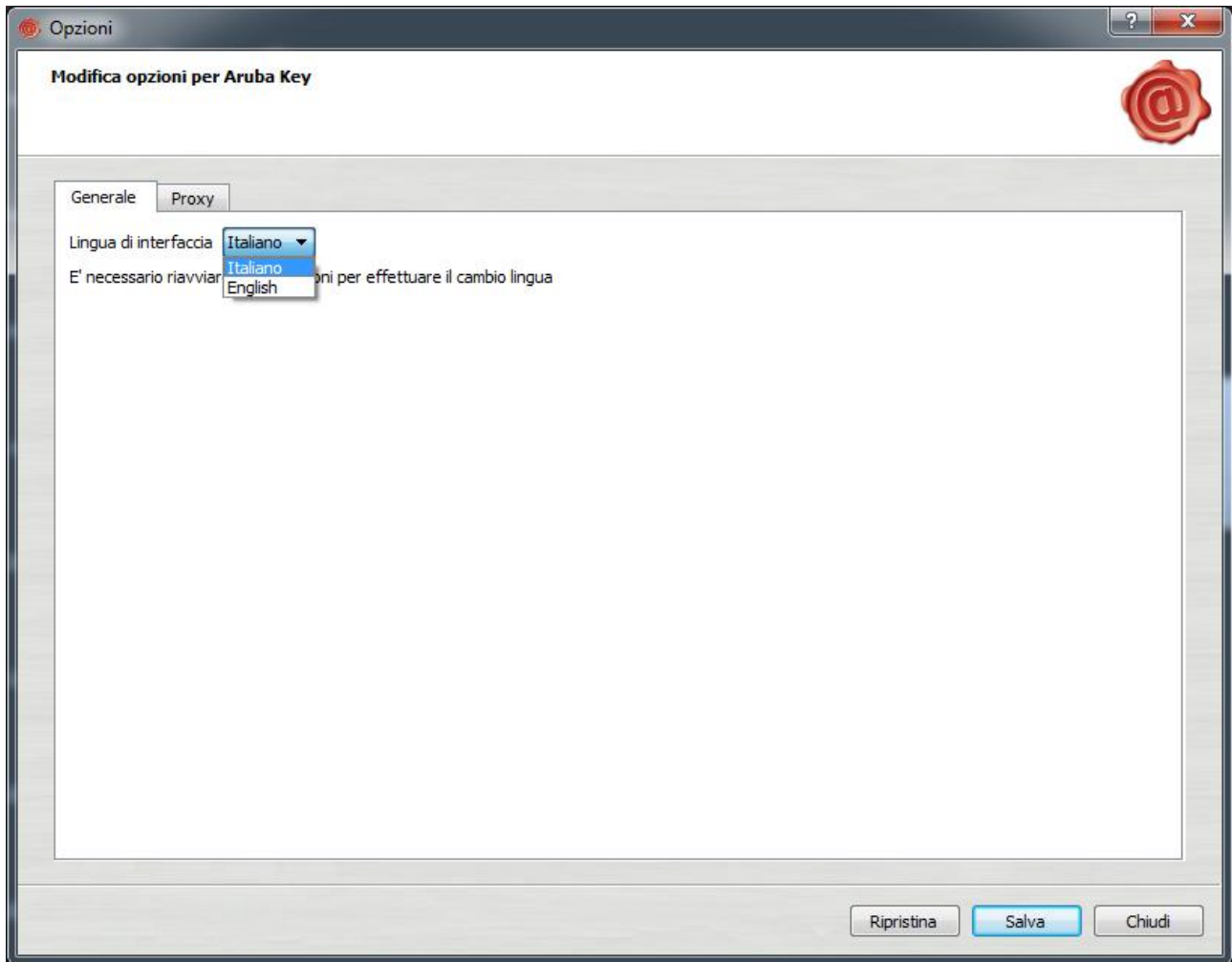
Cliccare sul pulsante "Opzioni e Proxy".



Step 3



Selezionare la lingua prescelta



NOTA: Una volta che è stata selezionata la lingua è necessario riavviare l'Aruba Key per rendere operative le modifiche.

NOTE 2: Questa versione del software non supporta l'impostazione dinamica della lingua nelle seguenti applicazioni:

- Firefox portable
- Thunderbird portable
- Filezilla portable
- AbiWord portable
- 7Zip

Per configurare sulla propria Aruba Key la versione completa del software in lingua inglese è necessario formattare il dispositivo ed estrarre nell'unità di memoria tutto il contenuto dello zip scaricabile da: https://ca.arubapec.it/downloads/AK_EN_VERSION.zip.



16 Visualizzazione dei certificati su FireFox Portable.

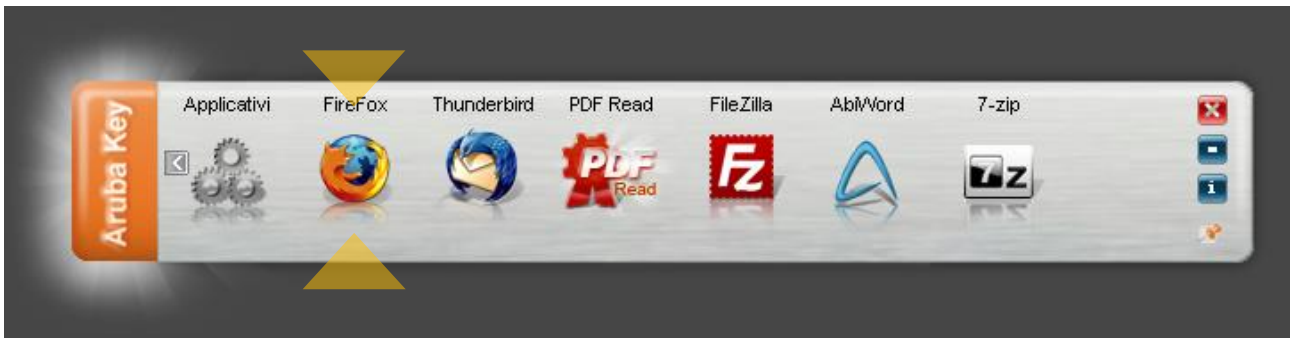
Passo 1

Per accedere a “Mozilla FireFox Portable Edition” presente a bordo dell’Aruba Key cliccare sopra il pulsante “Applicativi”.



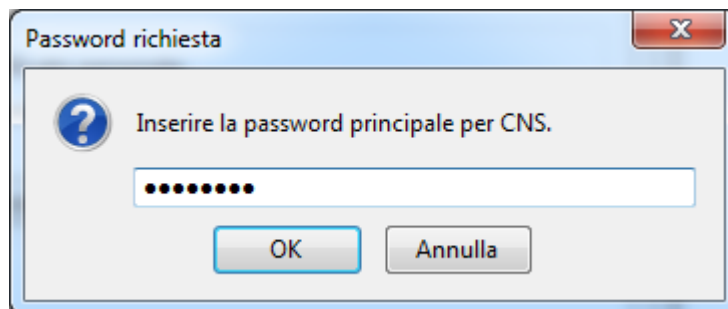
Passo 2

Cliccare sul pulsante “Firefox”.



Passo 3

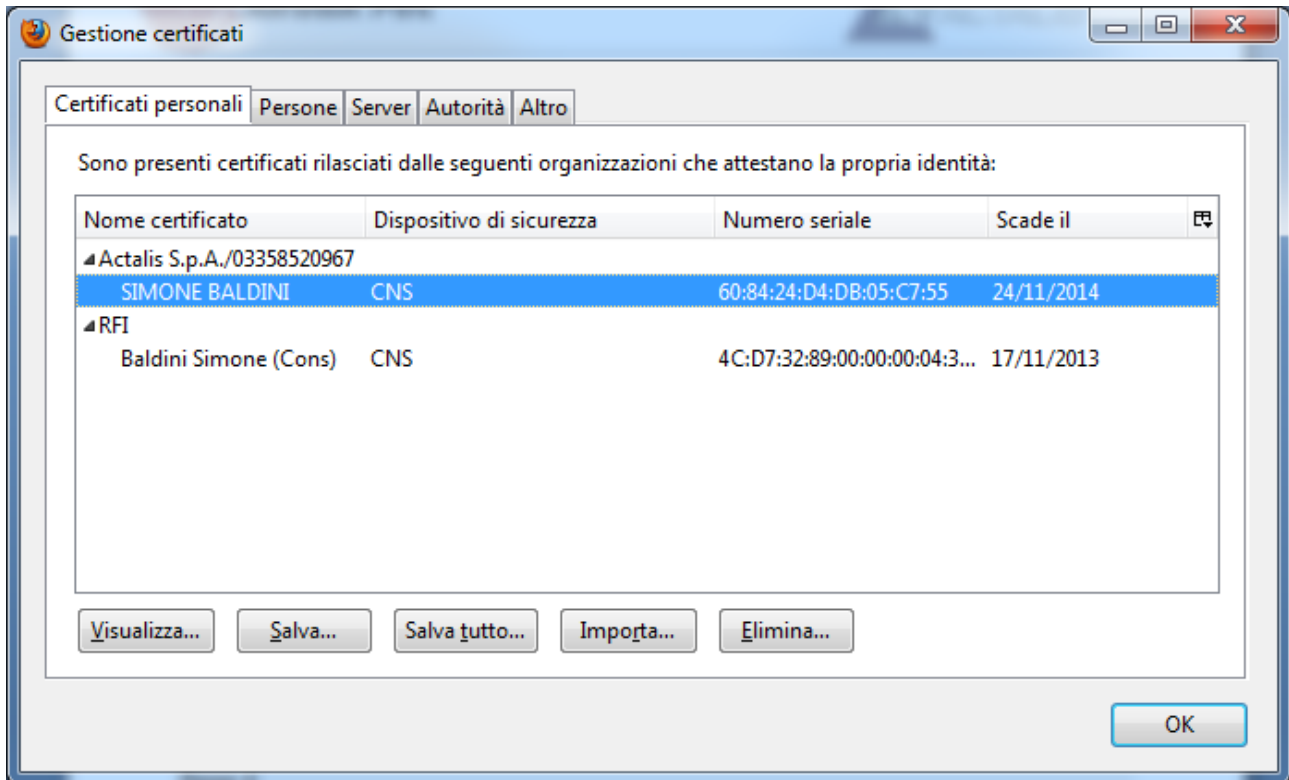
Selezionare Strumenti → Opzioni → Avanzate → Cifratura → “Mostra Certificati” ed inserire il PIN quando richiesto



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.



Appendice A

Apposizione di marche temporali

La marca temporale è un riferimento temporale certo, associato ad un documento (firmato o non digitalmente), opponibile a terzi.

Il servizio di marcatura temporale è opzionale rispetto alla firma digitale e non è parte della attuale fornitura.

Al fine di illustrare le funzionalità associate all'icona "Marca Temporale", vengono di seguito riportati i passaggi necessari per eseguire la marca di un file non firmato e di un file firmato digitalmente.

Passo 1

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



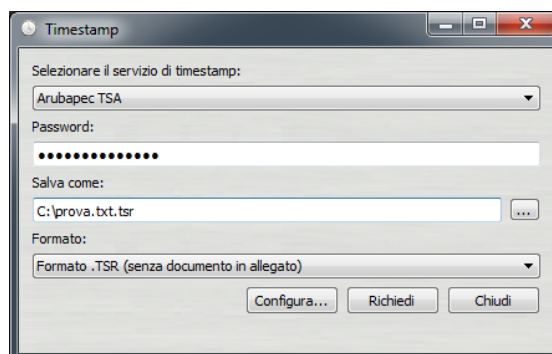
Passo 2

- Selezionare l'account da utilizzare per la richiesta di marcatura temporale;
- 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);

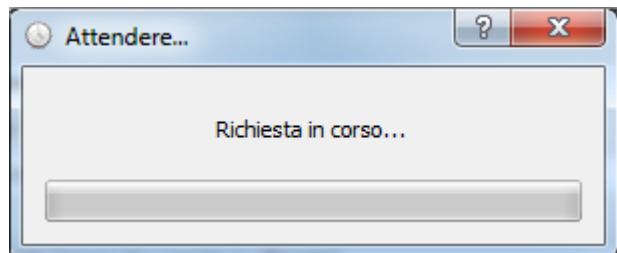
- Verificare che il percorso utilizzato per salvare il file marcato sia quello desiderato;
- Selezionare il formato di salvataggio della marca temporale;





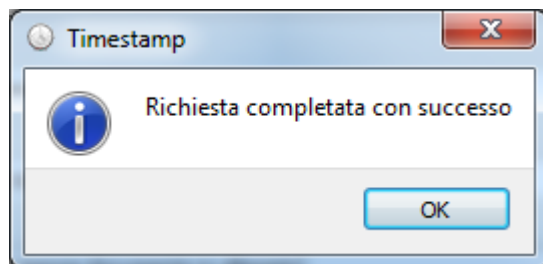
Passo 3

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.



Verifica Marche Temporali

Passo 1

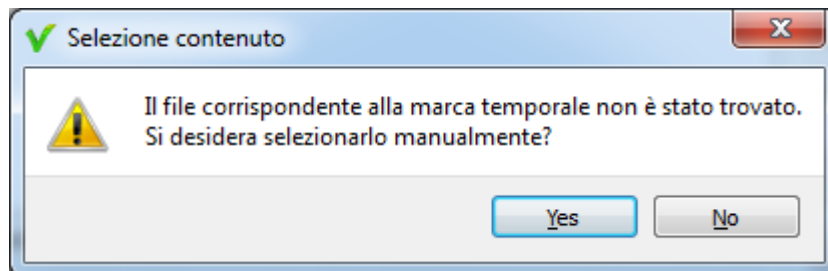
Trascinare la marca temporale da verificare sopra il pulsante “Verifica”.



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

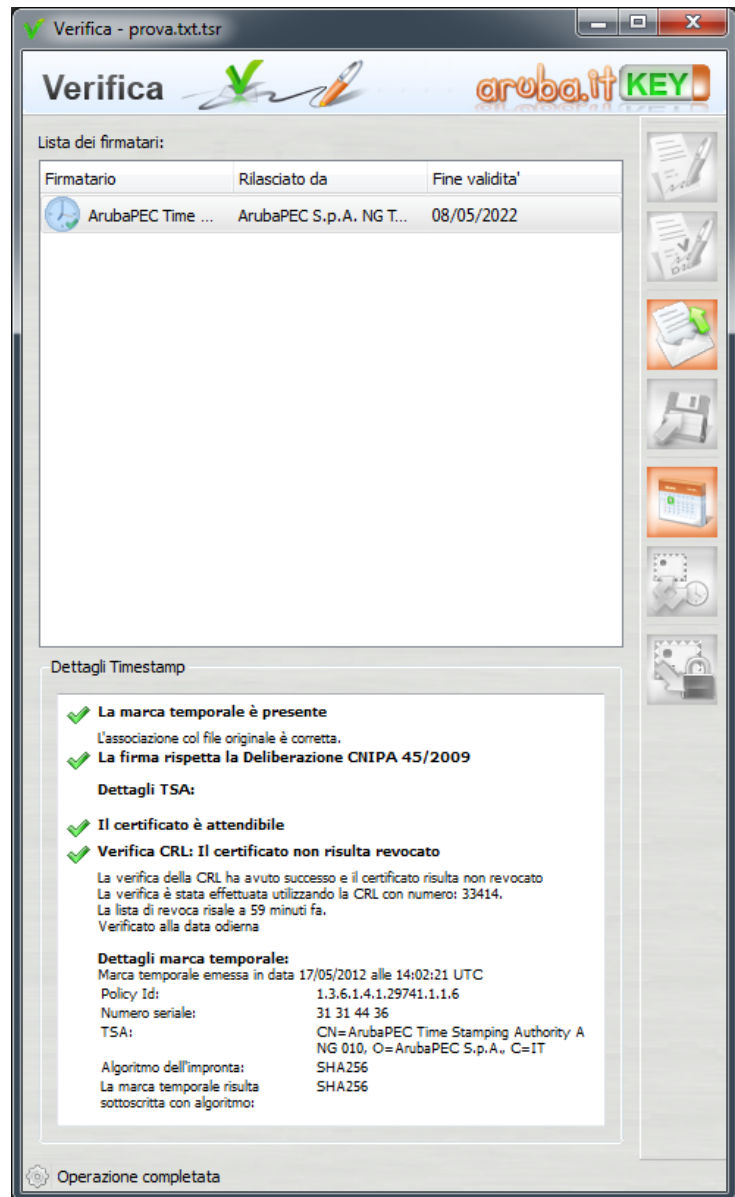
Questo messaggio sta ad indicare che la Marca Temporale è rilasciata da un'Autorità di Certificazione inclusa nell'Elenco Pubblico dei Certificatori

Il certificato non risulta revocato

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

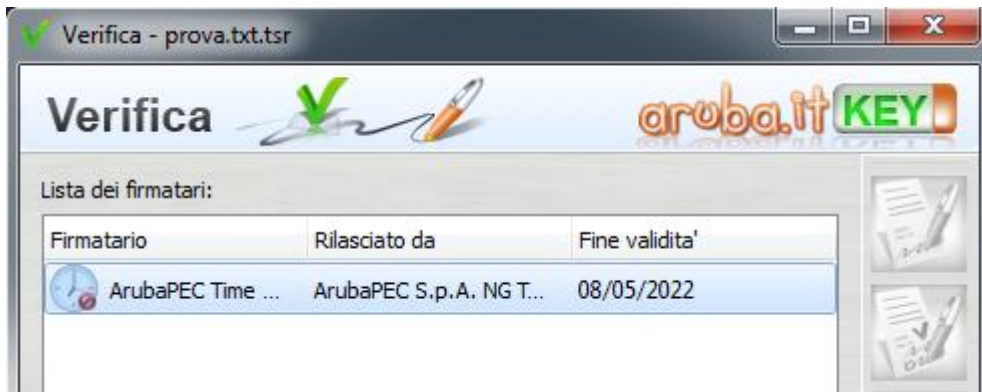
Dettagli marca temporale

Sotto questa voce sono riportati i dettagli della marca temporale.



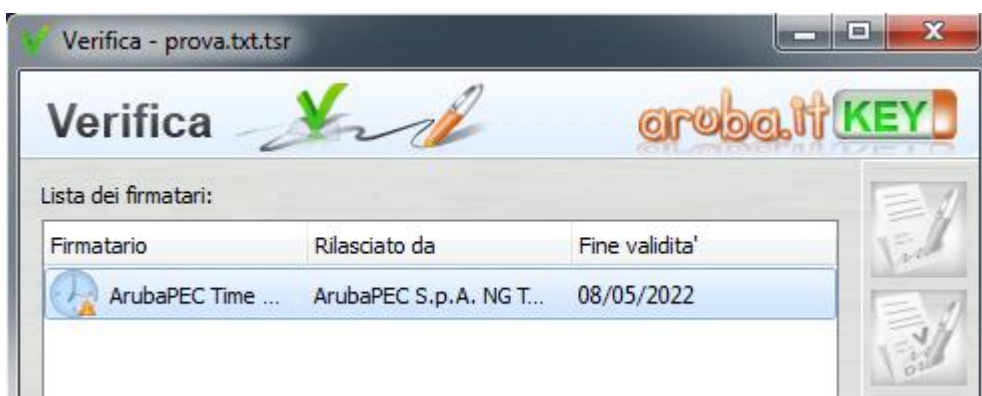


Qualora la finestra di riepilogo dovesse mostrare un esito simile al seguente:



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".



Verifica Marche Temporalì 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.

