Aruba Sign 3

Guida rapida

Indice

Indice....2
1 Informazioni sul documento....3
1.1 Scopo del documento....3
2 Prerequisiti....4
2.1.1 Software....4
2.1.2 Rete....4
3 Installazione....5
Passo 2....5
4 Avvio di Aruba Sign2....5
5 Firmare digitalmente un file in formato P7M....7
5.1 Firmare digitalmente più file in formato P7M....10
6.1 Firmare digitalmente più file in formato PDF....17
8 Verifica di file firmati in P7M....23
9 Verifica di file firmati in PDF....25
11 Verifica di Marche Temporali in formato .TSD....30
12 Cambio PIN....33
13 Sblocco PIN....35
14 Cambio PUK....37
16 Decifratura File....41
17 Impostazione Proxy....42
17 Firma Remota....44
17.1 Configurazione Parametri Firma Remota....44

1 Informazioni sul documento

1.1 Scopo del documento

Il presente documento intende essere una guida rapida per lo svolgimento delle seguenti operazioni con il software di firma Aruba Sign 2:

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

2 Prerequisiti

Di seguito sono descritti i prerequisiti Hardware e Software che deve possedere la postazione a cui viene installato Aruba sign 2..

2.1.1 Software

Sistemi Operativi:

- MS Windows XP, Vista, Seven, Server 2003, Server 2008 (32 e 64 bit)
- Leopard (10.5 - Intel), Snow Leopard (10.6 - Intel)
- Linux

2.1.2 Rete

Di seguito sono riportati i parametri di rete che devono possedere le postazioni nella quali viene installata ArubaSign 2:

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

3 Installazione

Passo 1
Cliccare sull'icona ArubaSign2.exe ed attendere che si avvii il processo di installazione del software.

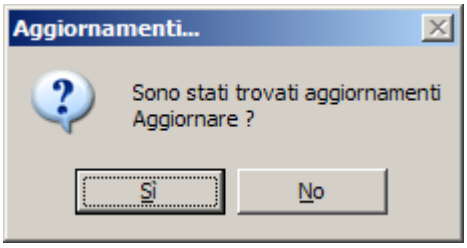
Passo 2
Cliccare sul pulsante avanti.

Passo 3
Accettare le condizioni di contratto e cliccare sul pulsante **"fine"**

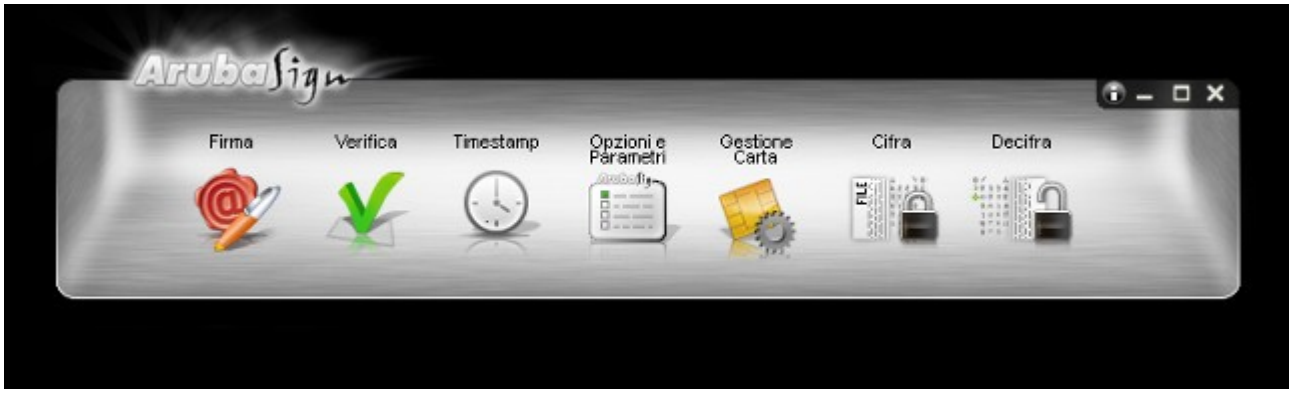
4 Avvio di Aruba Sign2

Completata l'installazione, sul desktop si presenta l'icona di Aruba Sign 2, che permette l'avvio del programma,

Al primo avvio, e ogni volta che è disponibile un aggiornamento,comparirà la finestra Pop-Up;
è sempre consigliabile effettuare al'aggiornamento del programma di firma.



Al termine del'aggiornamento verrà visualizzata la schermata principale del software di Firma Arubasign2.



5 Firmare digitalmente un file in formato P7M

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

Passo 2
Attendere che ArubaSign2 recuperi le informazioni relative ai certificati contenuti nella smart card.

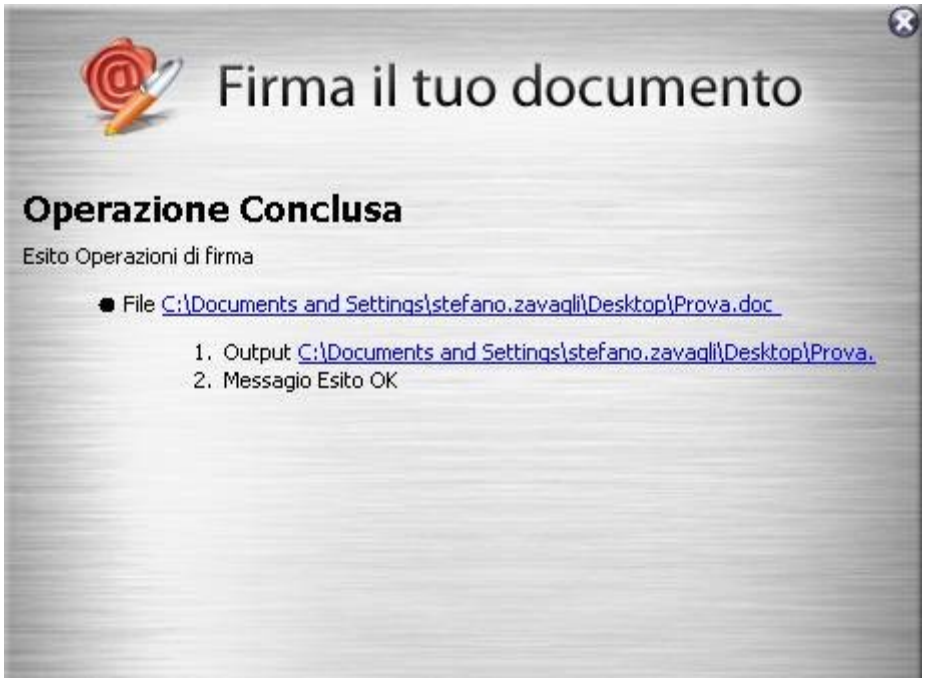
a. Assicurarsi che sia selezionato il certificato per la firma digitale (Cognome Nome);
b. Inserire il PIN di protezione della smart card;
c. Selezionare l'opzione *Tipo Busta "busta crittografica P7M";*
d. Verificare che il percorso utilizzato per salvare il file firmato sia quello desiderato.
e. Cliccare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

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 **Avanti >**

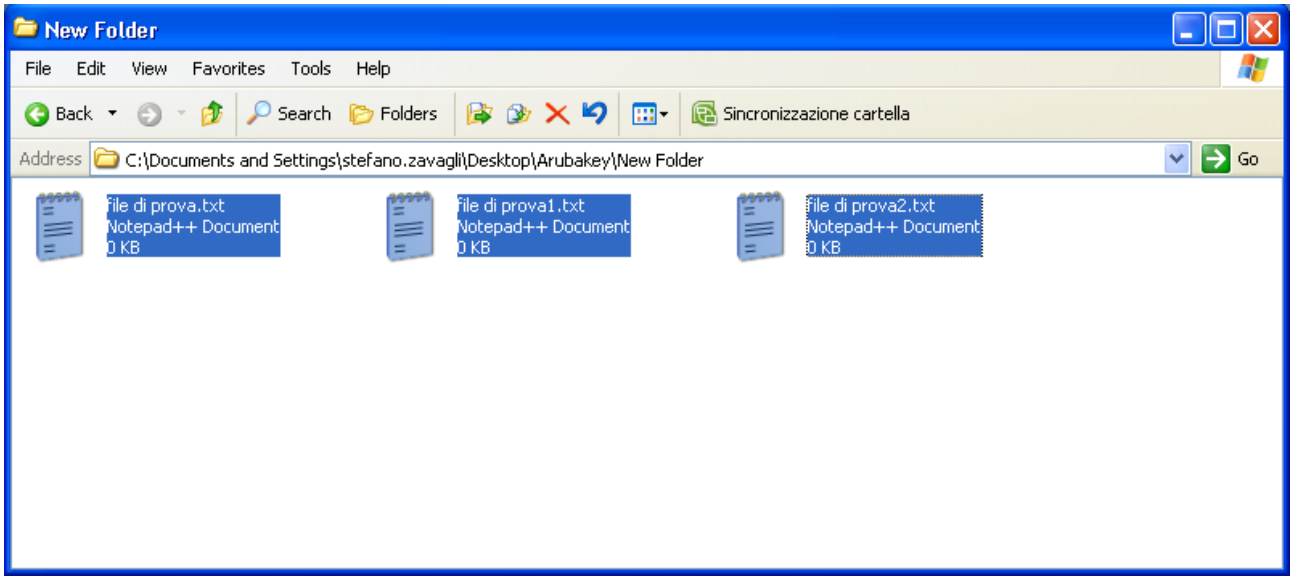
Passo 6

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

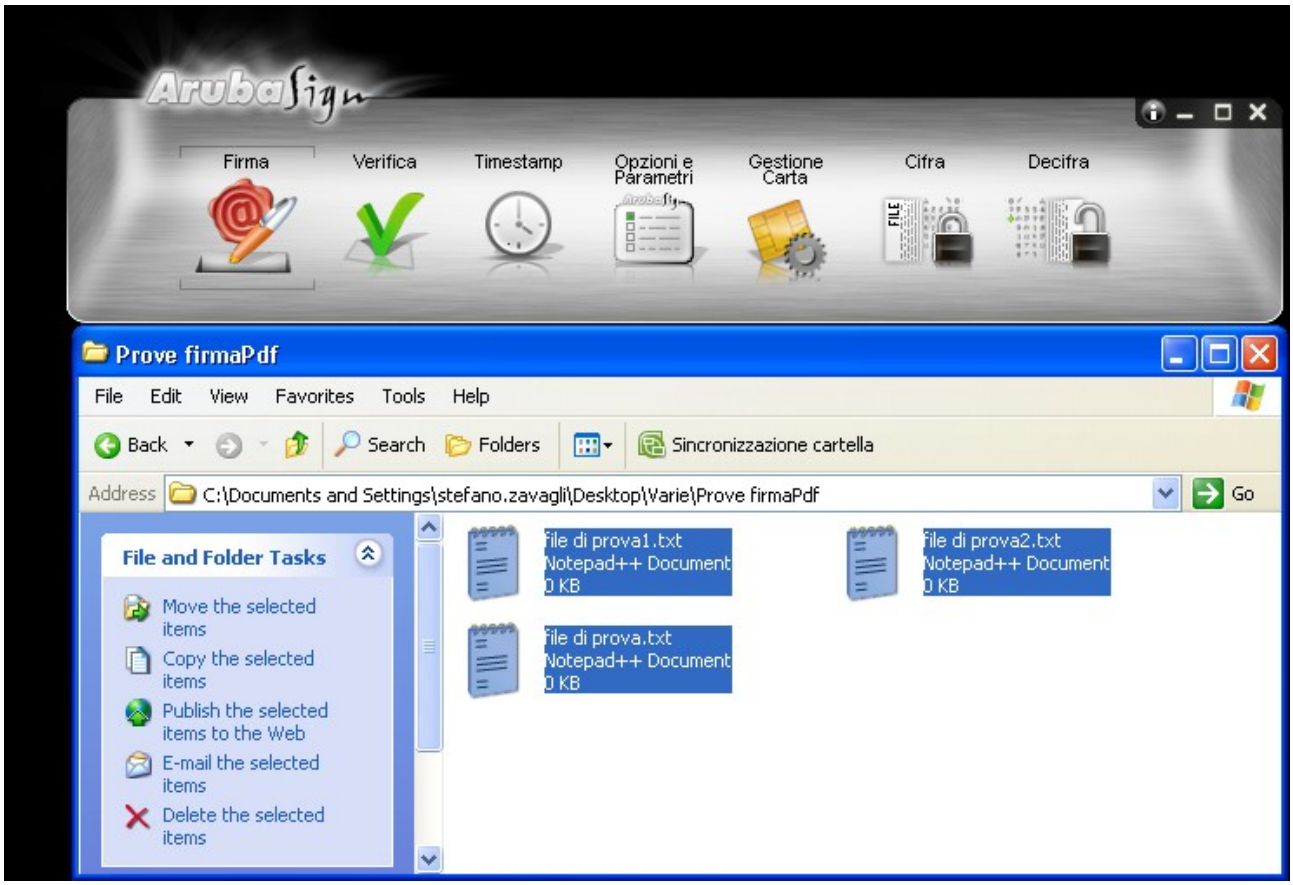


5.1 Firmare digitalmente più file in formato P7M

Passo 1
Selezionare tutti i documenti da firmare.



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



Passo 4

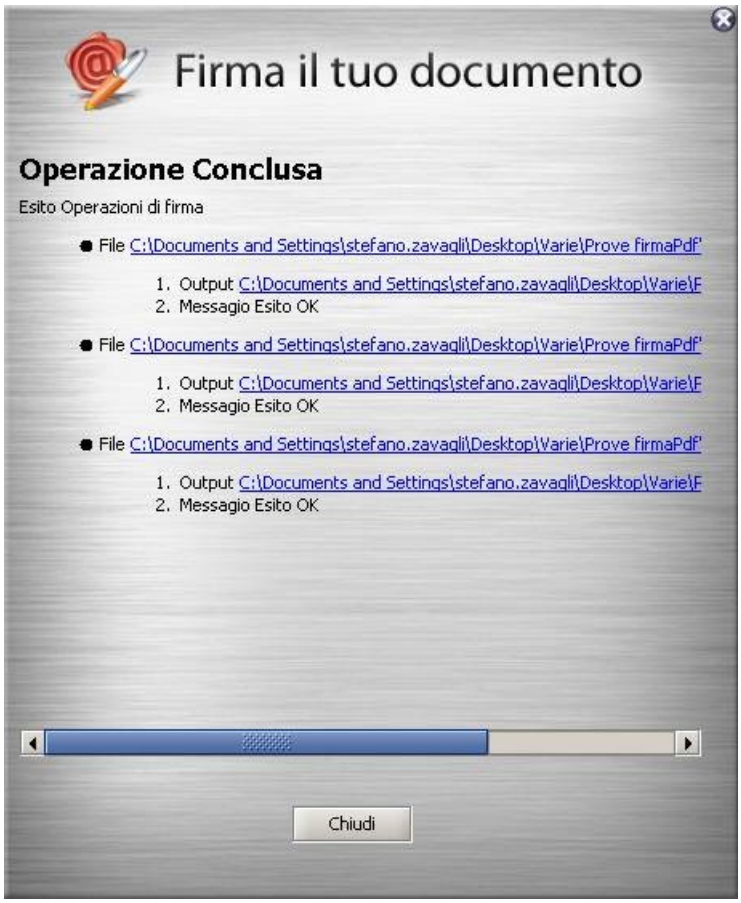
a. Assicurarsi che sia selezionato il certificato per la firma digitale (Cognome Nome);
b. Inserire il PIN di protezione della smart card;
c. Selezionare l'opzione "**tipo busta"** *busta crittografica P7M";*
d. Verificare che il percorso utilizzato per salvare il file firmato sia quello desiderato.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

Passo 5

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

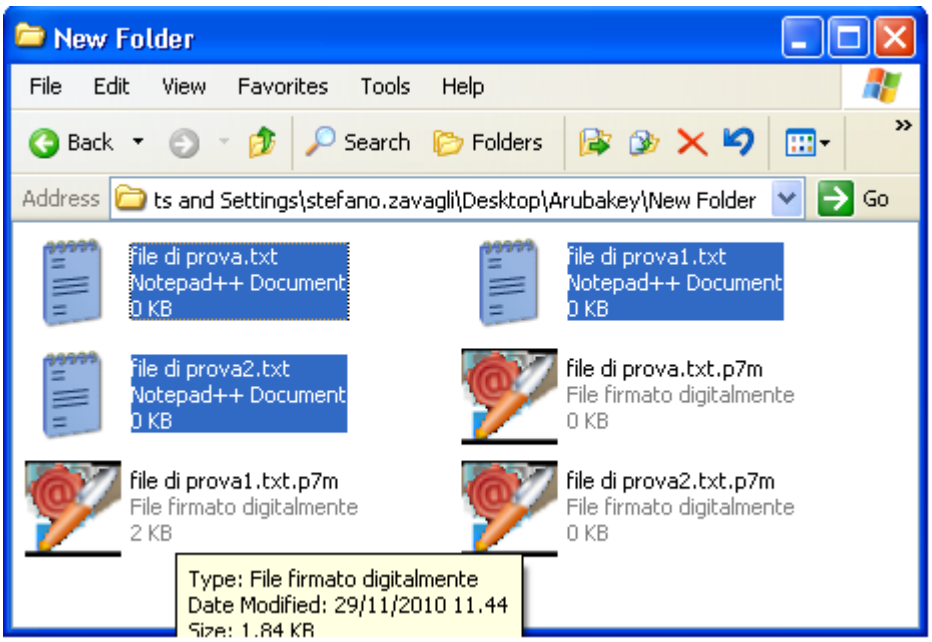
Passo 6

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



Passo 8

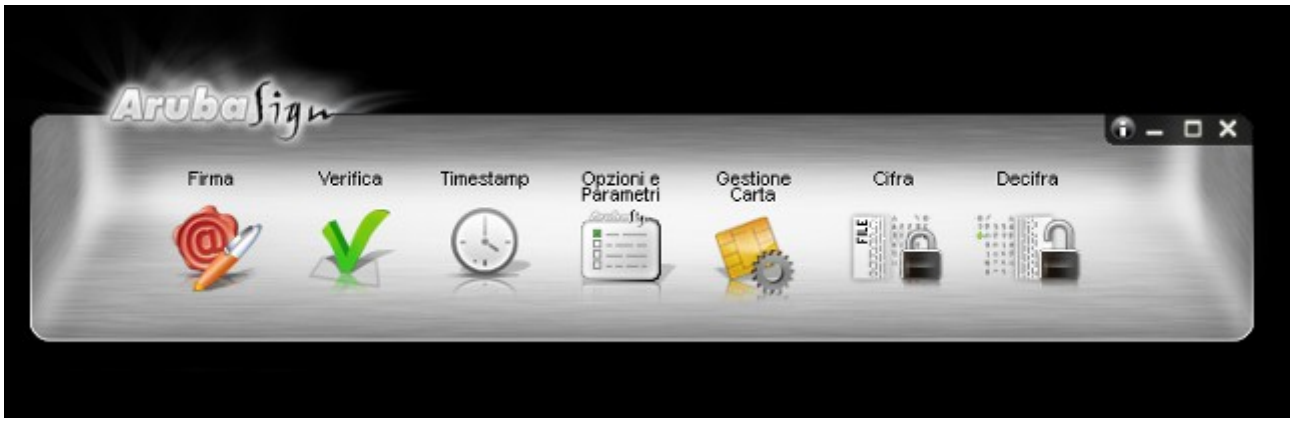
I documenti firmati verranno salvati nella stessa cartella dove risiedono i documenti originali aggiungendo al nome l'estensione .p7m.



6 Firmare digitalmente un file in formato PDF

La procedura di firma in formato PDF è applicabile ai soli file .PDF.
Non è quindi possibile, attraverso ArubaSign 2, firmare in PDF un file che non sia già stato convertito in questo formato.

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

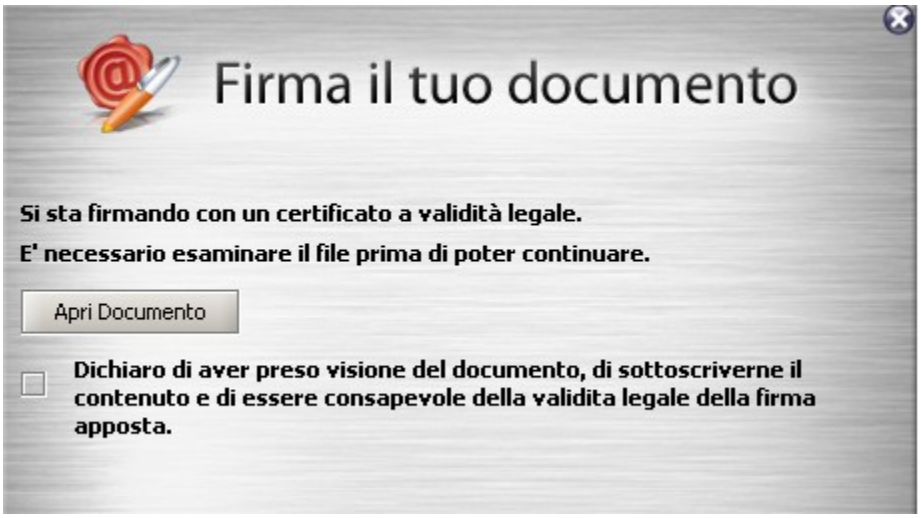


Passo 2

a. Assicurarsi che sia selezionato il certificato per la firma digitale (Cognome Nome);
b. Inserire il PIN di protezione della smart card;
c. Selezionare ***"Firma Grafica"***;
d. Cliccare sul pulsante **Avanti>**

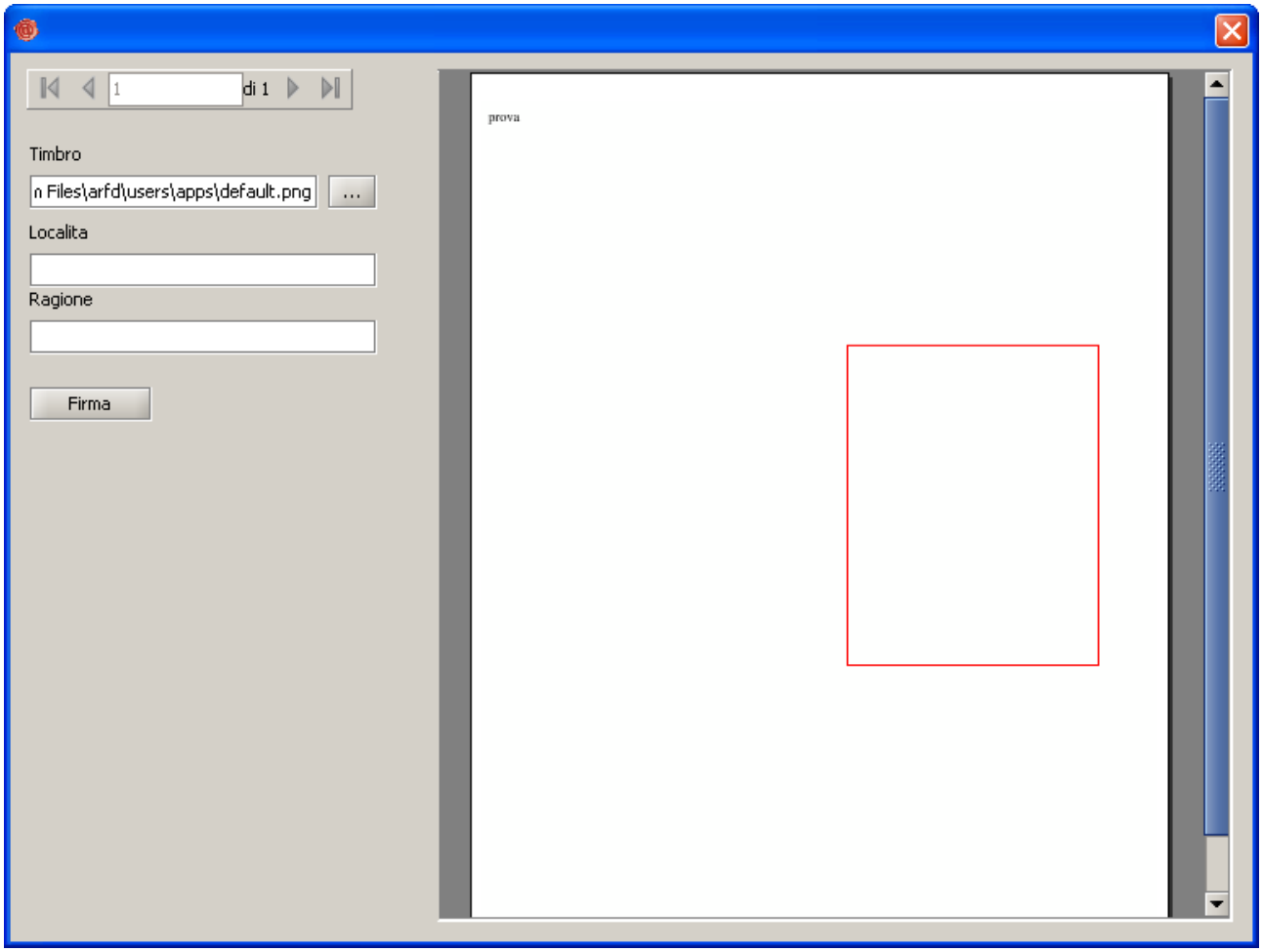
Passo 4

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 **Avanti>**



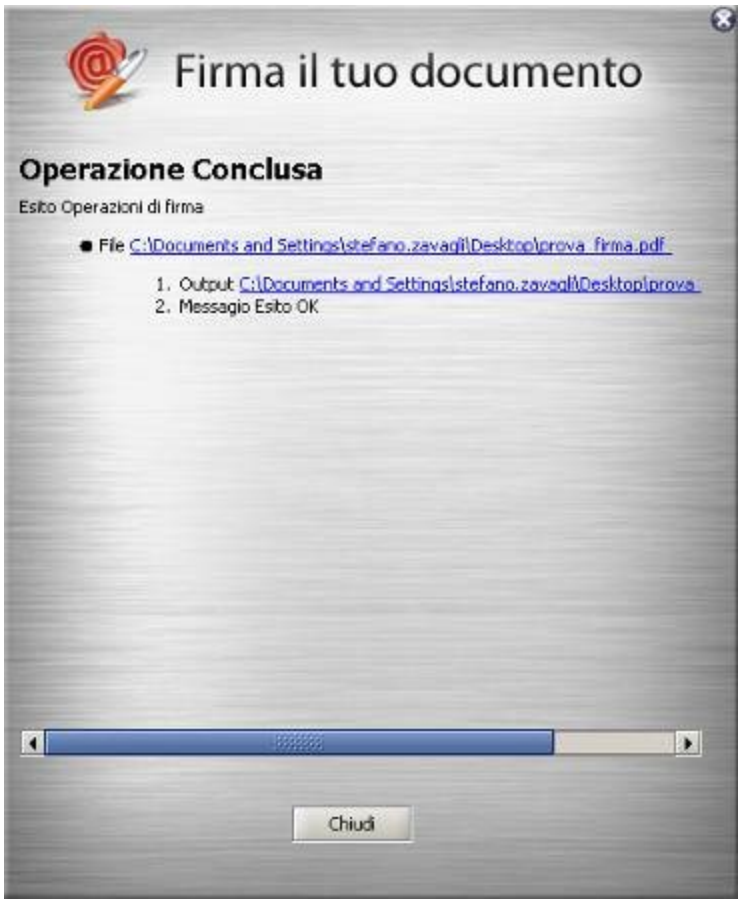
Passo 5

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



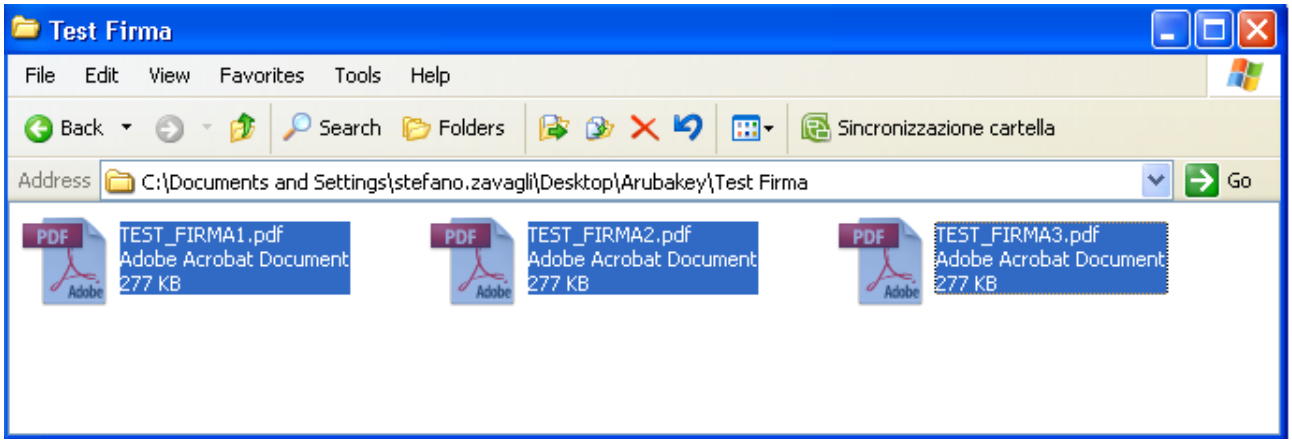
Passo 6

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

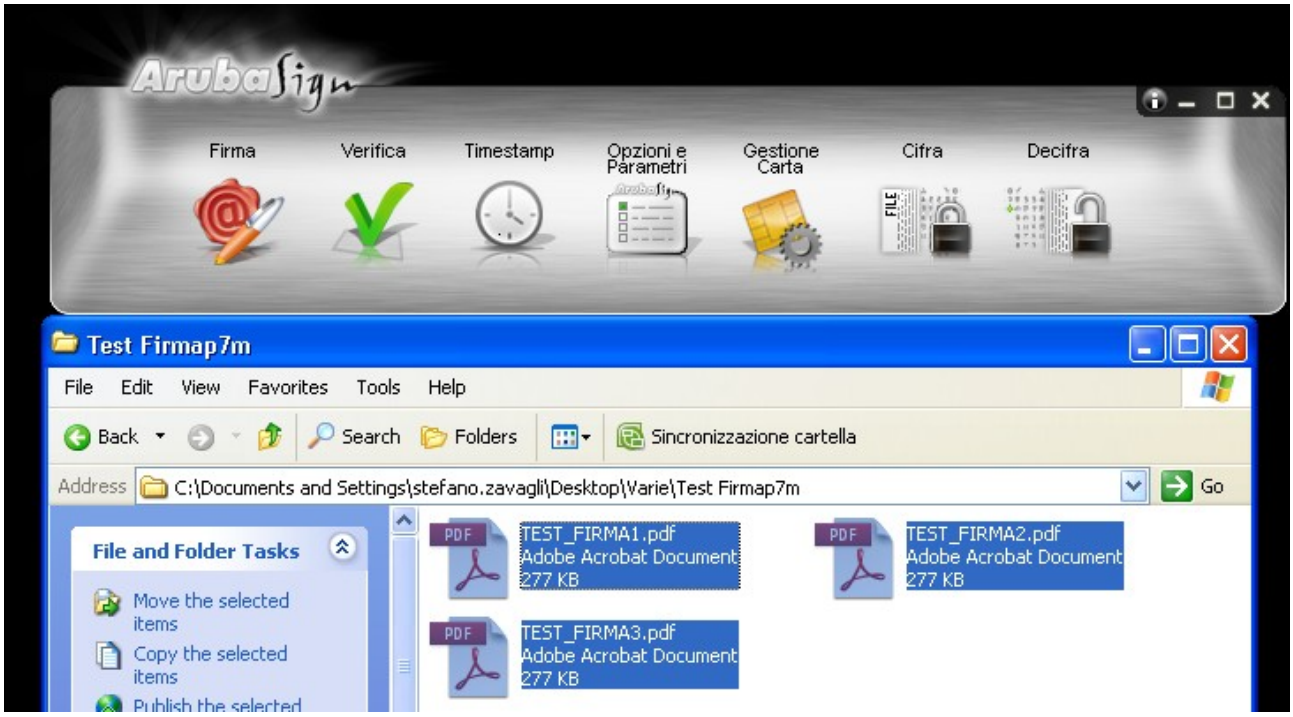


6.1 Firmare digitalmente più file in formato PDF

Passo1
Selezionare tutti i documenti PDF da firmare.



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



Passo 3

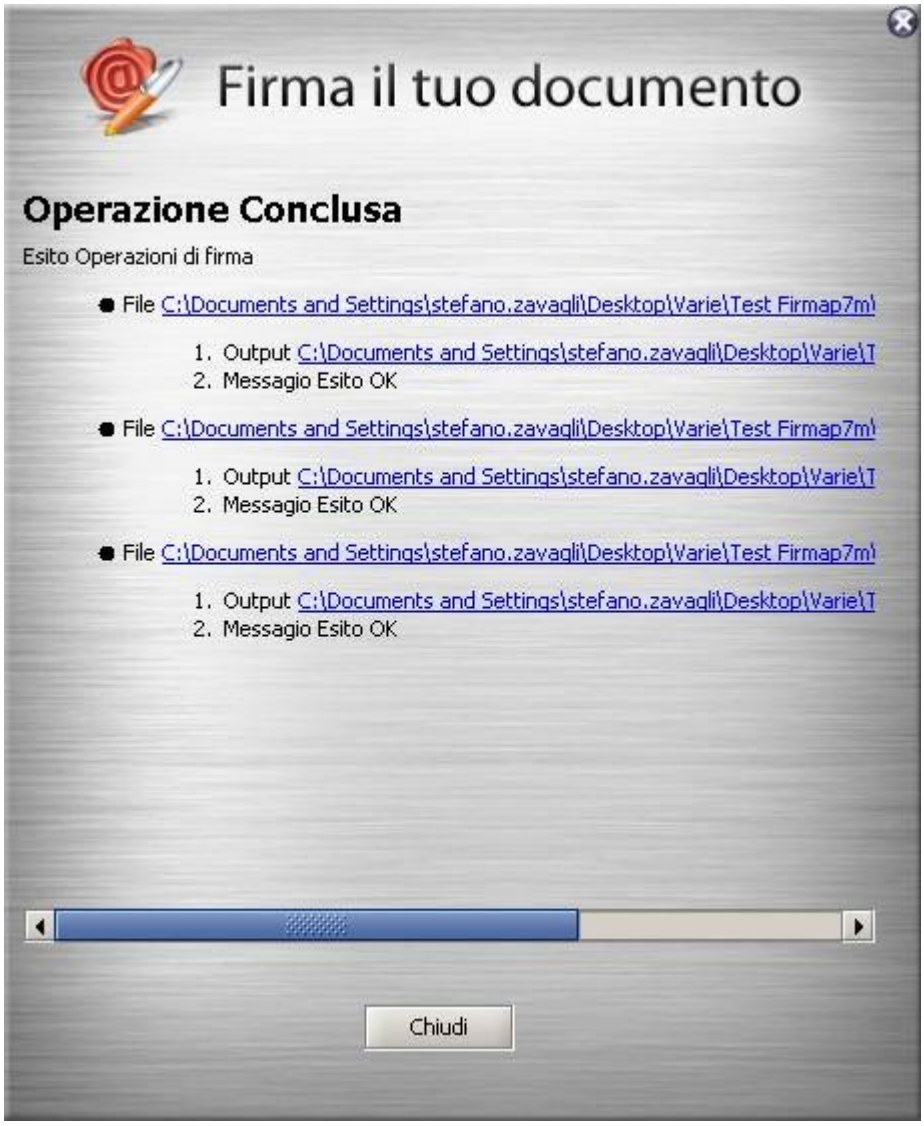
a. Assicurarsi che sia selezionato il certificato per la firma digitale (Cognome Nome);
b. Inserire il PIN di protezione della smart card;
c. Selezionare l'opzione ***"Firma Grafica"***;
d. Cliccare sul pulsante **Avanti >**

Passo 5

c. Selezionare l'opzione relativa alla presa visione dei documenti;
d. Cliccare sul pulsante **Avanti >**

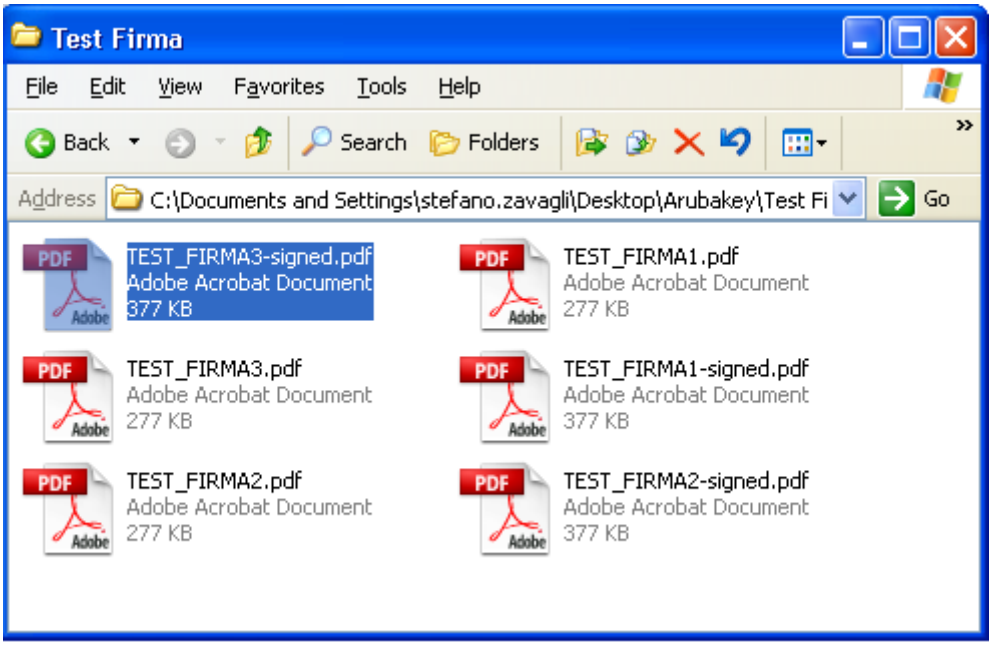
Passo 6

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



Passo 7

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



7 Apposizione di marche temporali

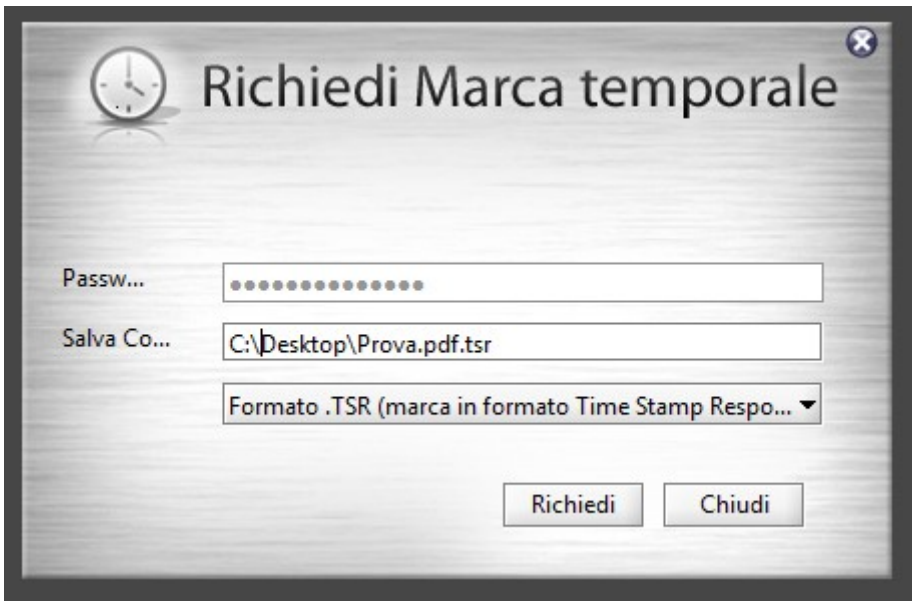
Passo 1
Trascinare il file da marcare sopra il pulsante **"Timestamp".**

Passo 2

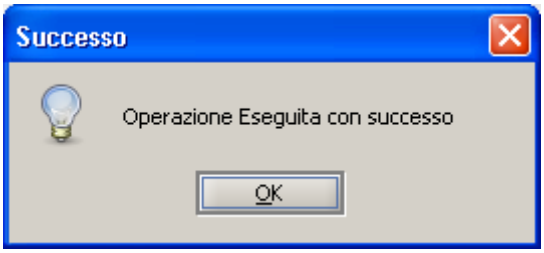
a. Selezionare l'account da utilizzare per la richiesta di marcatura temporale;
b. Inserire la password per l'accesso al servizio di marcatura temporale;

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



Passo 5
Recuperare il file marcato memorizzato nel percorso indicato al Passo 2.

8 Verifica di file firmati in P7M

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

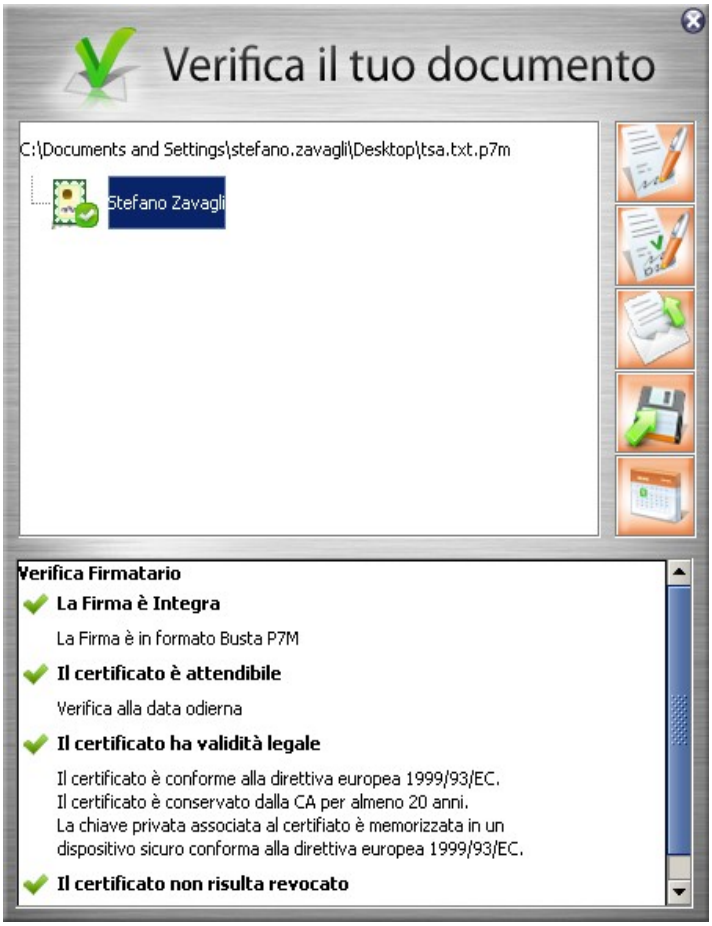
Passo 2
Completate le verifiche ArubaSign2 restituirà una finestra di riepilogo simile alla seguente:

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

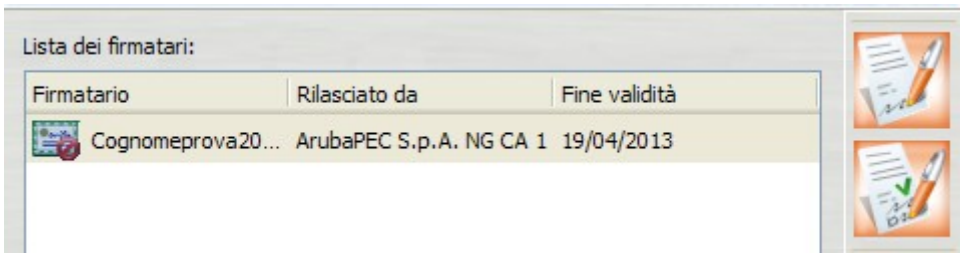
Il certificato è attendibile.
Il messaggio indica che il certificato del sottoscrittore è garantito da una Autorità di Certificazione inclusa nell'Elenco Pubblico dei Certificatori e che non risulta scaduto alla data della verifica.

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

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

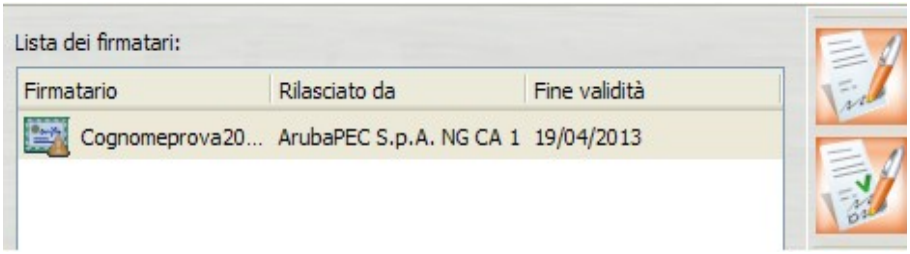


Qualora la finestra di riepilogo dovesse mostrare un esito simile al seguente:



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

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



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

9 Verifica di file firmati in PDF

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

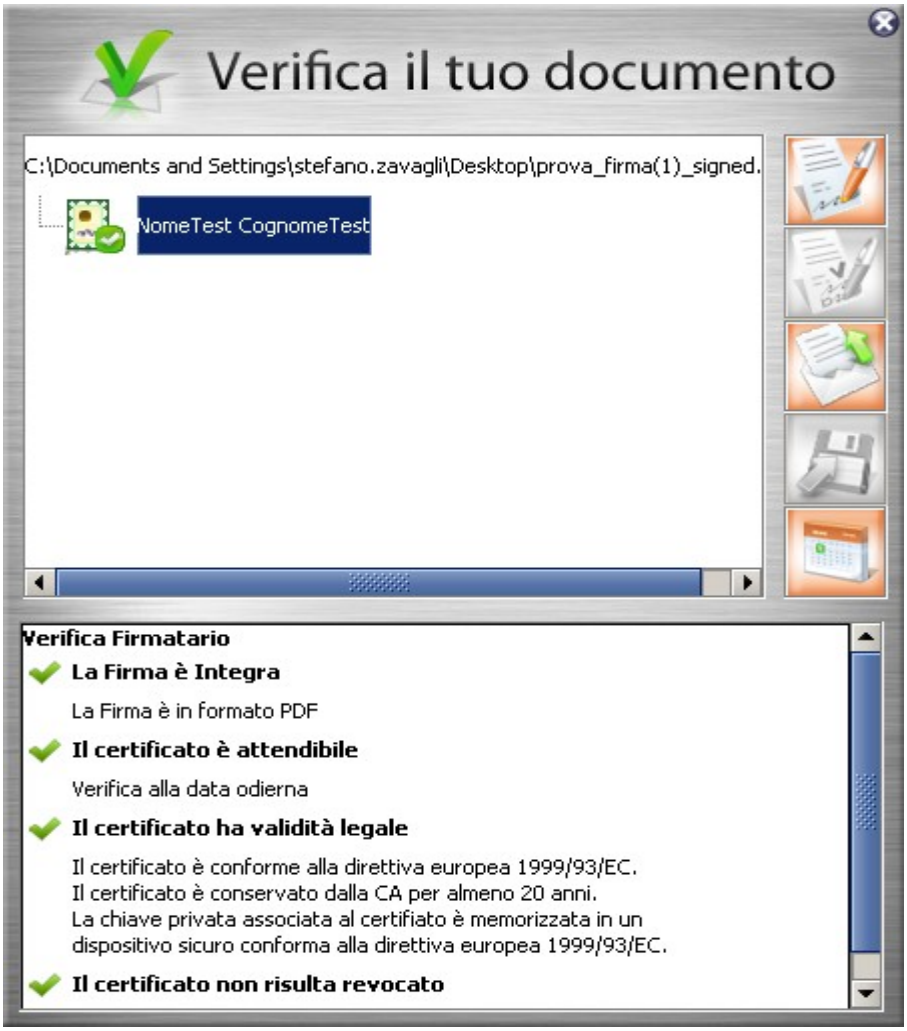
Passo 2
Completate le verifiche ArubaSign2 restituirà una finestra di riepilogo simile alla seguente:

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

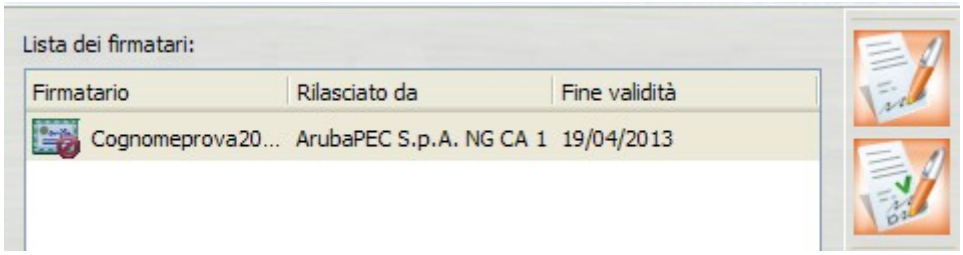
Il certificato è attendibile.
Il messaggio indica che il certificato del sottoscrittore è garantito da una Autorità di Certificazione inclusa nell'Elenco Pubblico dei Certificatori e che non risulta scaduto alla data della verifica.

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

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

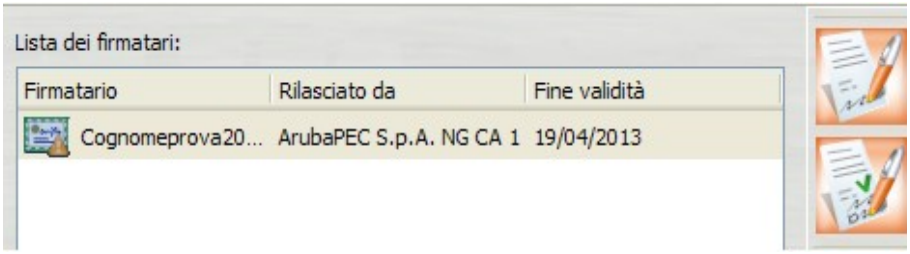


Qualora la finestra di riepilogo dovesse mostrare un esito simile al seguente:



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

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

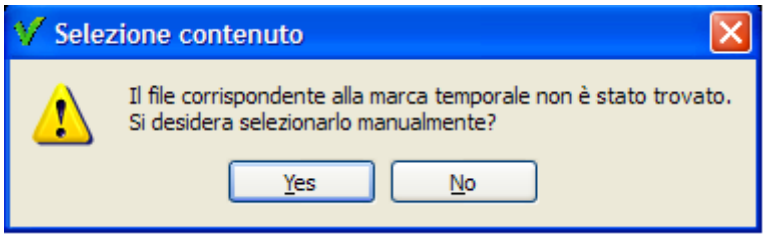


Allora ciò sta ad indicare che non è stato possibile portare a termine tutti i controlli previsti per verificare la validità della firma ed è necessario analizzare meglio il tipo di errore riscontrato visualizzando i messaggi

10 Verifica delle Marche Temporali in formato .TSR o .TST

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.

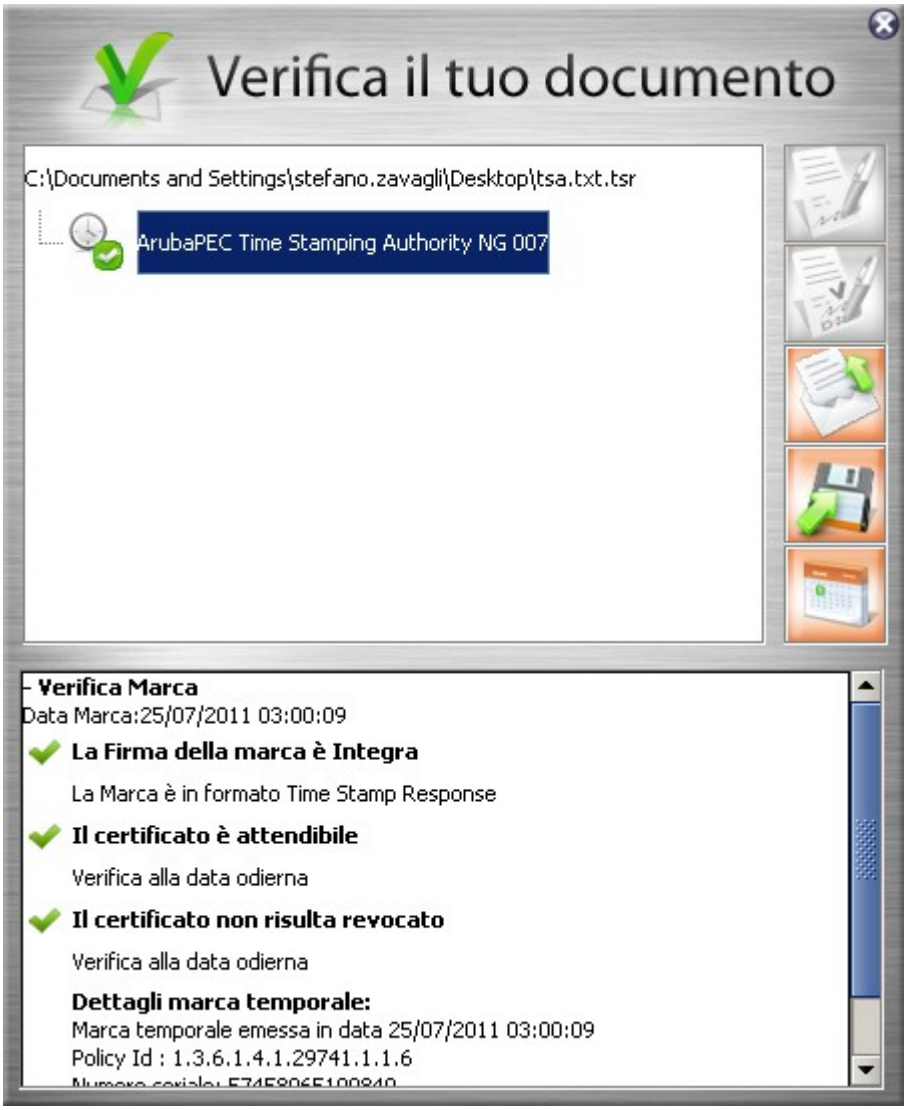
Passo 3
Il software inizia la verifica e, finite le operazioni, mostra una finestra di riepilogo simile alla seguente:

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

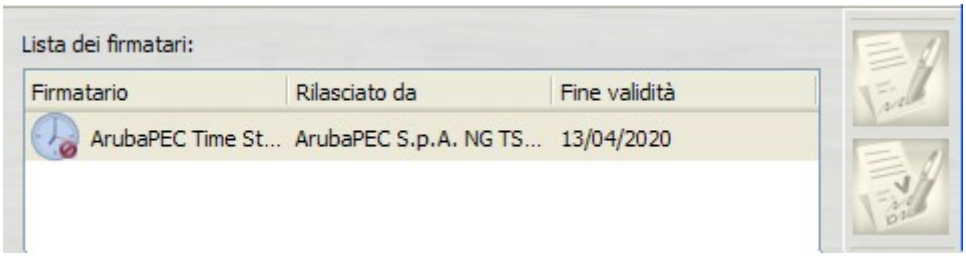
Il certificato è attendibile
Questo messaggio sta ad indicare che la Marca Temporale è rilasciata da un'Autorità di Certificazione inclusa nell'Elenco Pubblico dei Certificatori

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.

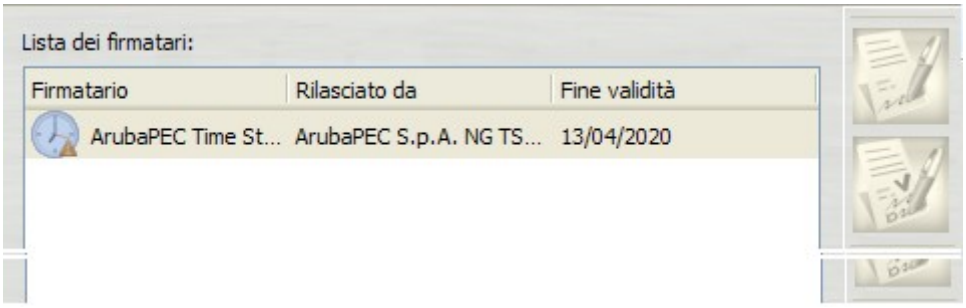


Qualora la finestra di riepilogo dovesse mostrare un esito simile al seguente:



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".

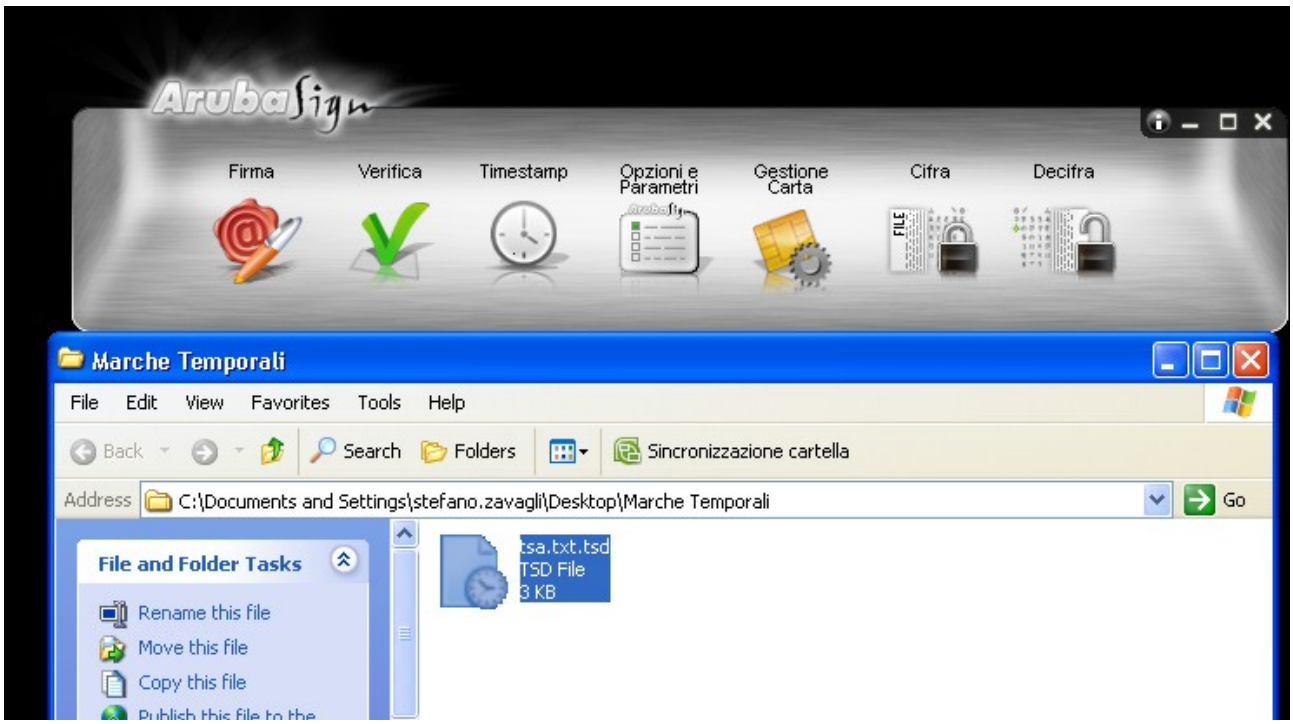
Qualora invece la finestra di riepilogo dovesse mostrare un messaggio simile al seguente:



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".**



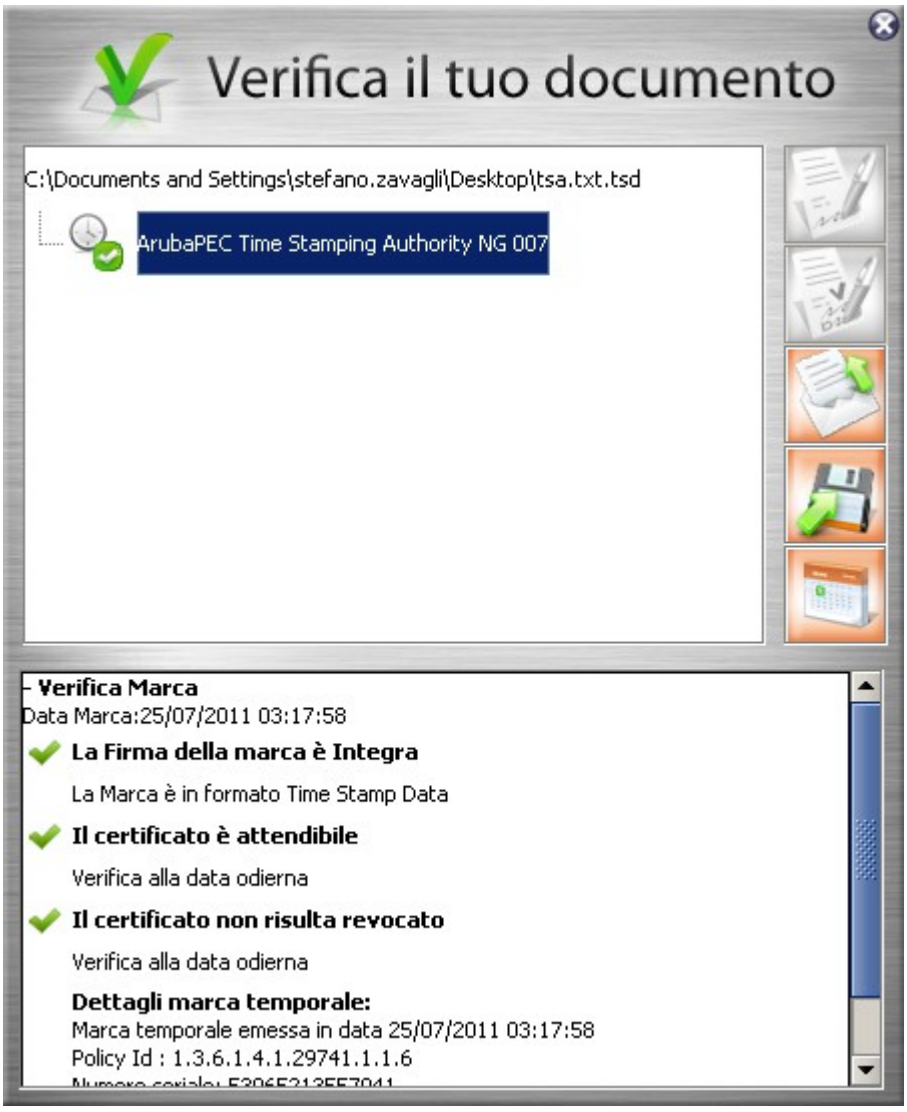
Passo 2
Il software inizia la verifica e, finite le operazioni, mostra una finestra di riepilogo simile alla seguente:

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

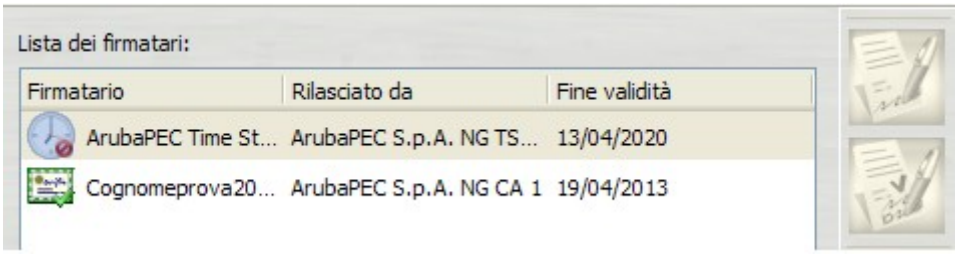
Il certificato è attendibile
Questo messaggio sta ad indicare che la Marca Temporale è rilasciata da un'Autorità di Certificazione inclusa nell'Elenco Pubblico dei Certificatori

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.

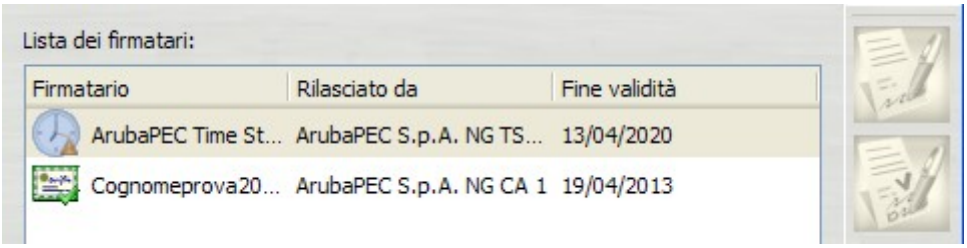


Qualora la finestra di riepilogo dovesse mostrare un esito simile al seguente:



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".

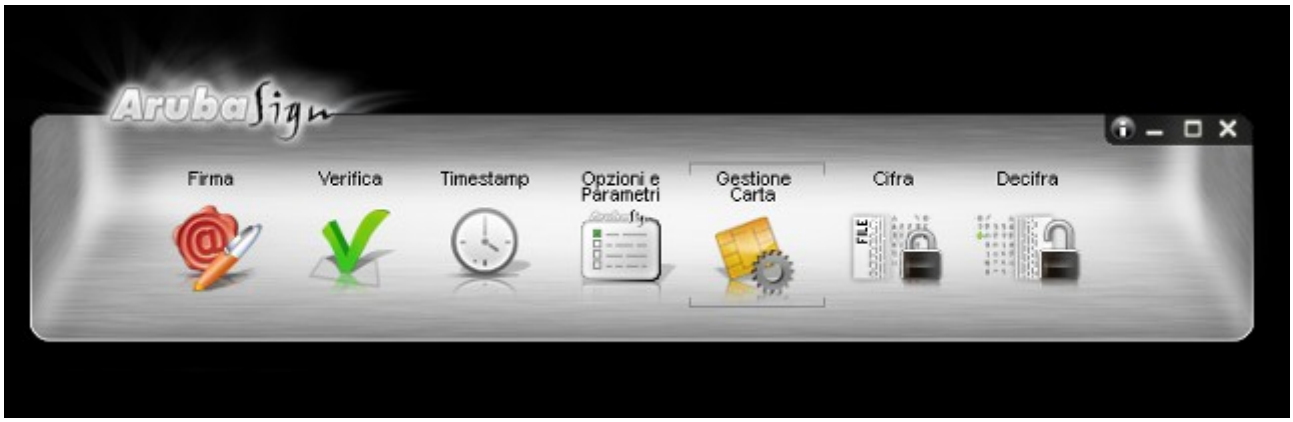
Qualora invece la finestra di riepilogo dovesse mostrare un messaggio simile al seguente:



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".

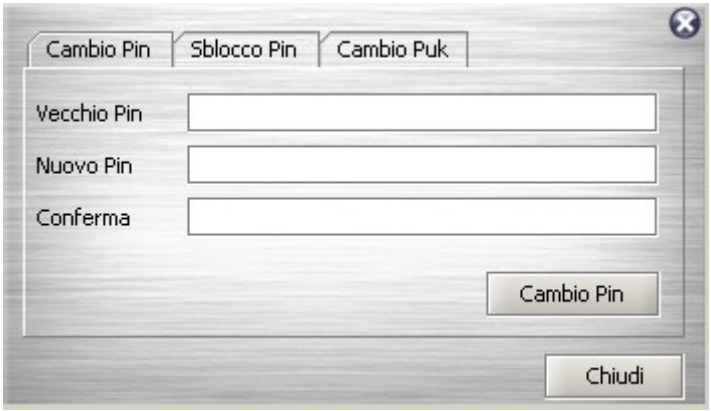
12 Cambio PIN

Passo 1
Per cambiare il codice PIN della carta inserita,cliccare sopra il pulsante "**Gestione Carta".**



Passo 2
All'interno del Tab "Cambio Pin" inserire il precedente PIN, impostare il nuovo valore e cliccare sul pulsante OK.

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

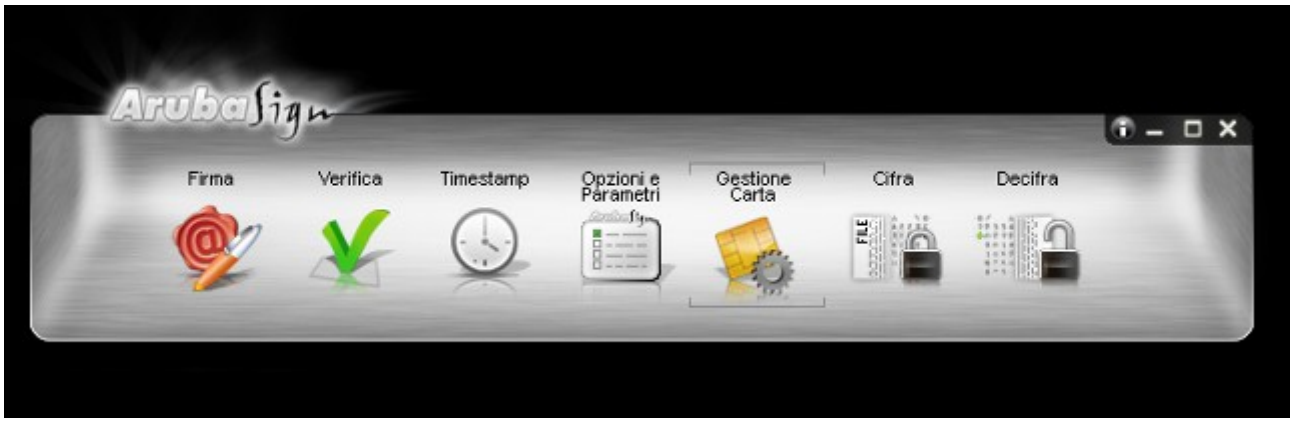


Durante l'operazione di cambio del PIN può restituire i seguenti messaggi d'errore:

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".

13 Sblocco PIN

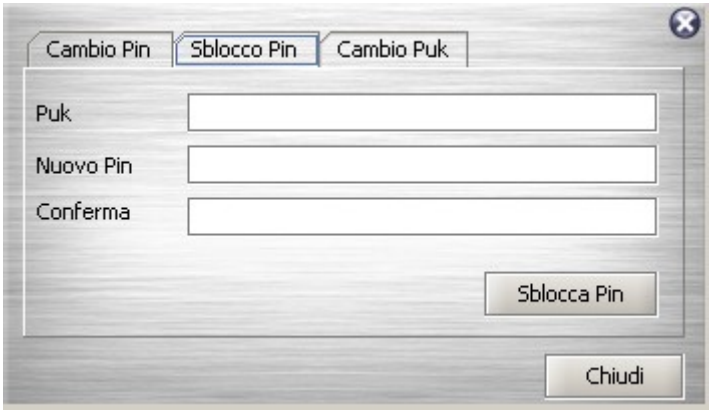
Passo 1
Per sbloccare il codice PIN della carta inserita,cliccare sopra il pulsante "**Gestione Carta".**



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

ATTENZIONE:

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

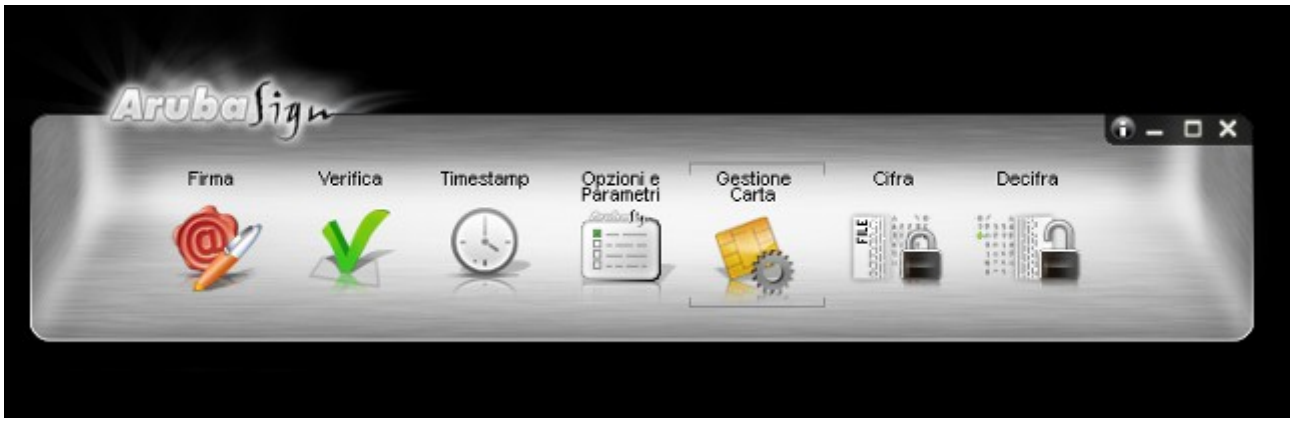


Durante l'operazione di sblocco del PIN può restituire i seguenti messaggi d'errore:

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

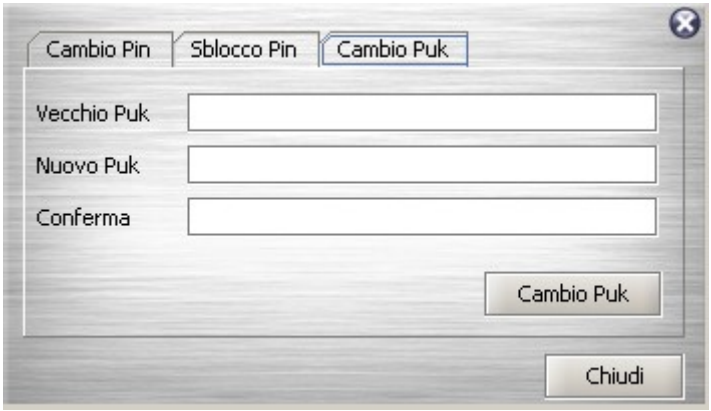
14 Cambio PUK

Passo 1
Per cambiare il codice PUK della carta inserita cliccare sopra il pulsante "**Gestione Carta".**



Passo 2
All'interno della finestra "Cambio PUK" inserire il precedente PUK, impostare il nuovo valore e cliccare sul pulsante OK.

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

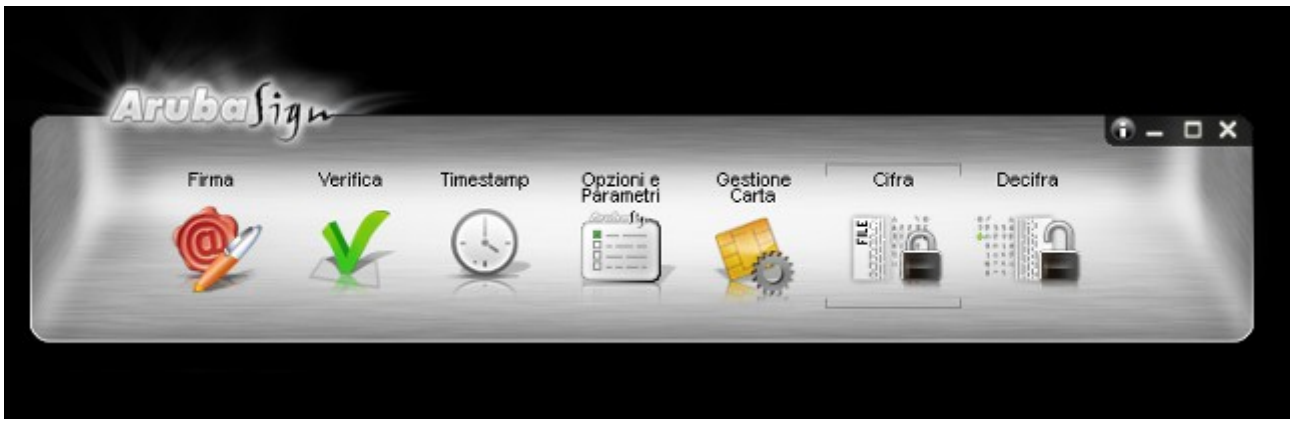


Durante l'operazione di Cambio del PUK Aruba Key può restituire i seguenti messaggi d'errore:

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

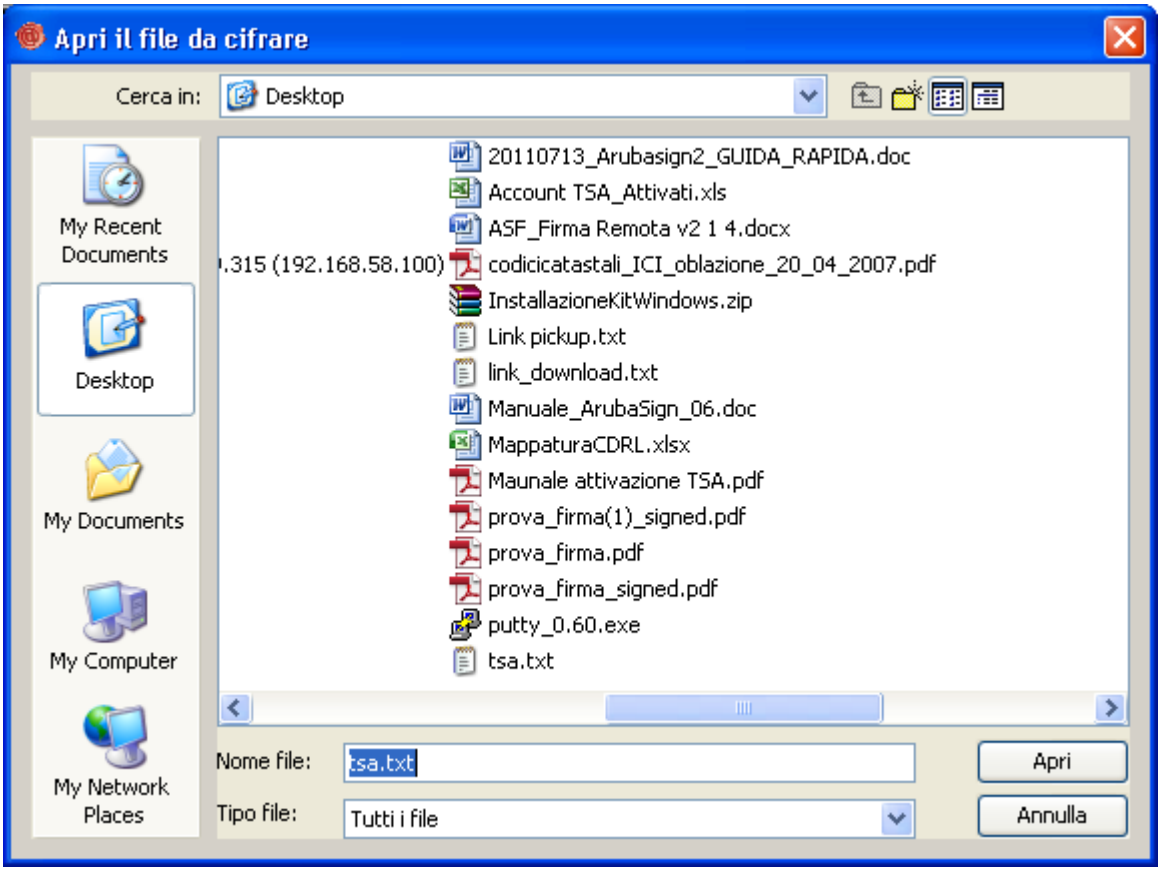
15 Cifratura File

Passo 1
Trascinare il file da cifrare sopra il pulsante **"Cifra"**.

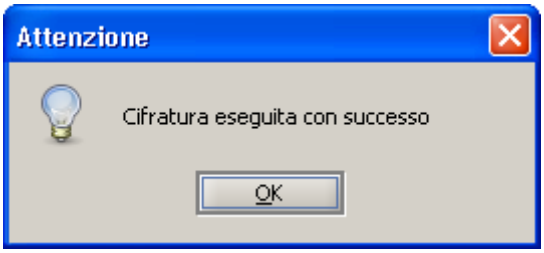


.

Passo 2
All'interno della finestra di cifratura selezionare, il file da cifrare e cliccare su "**Apri"**



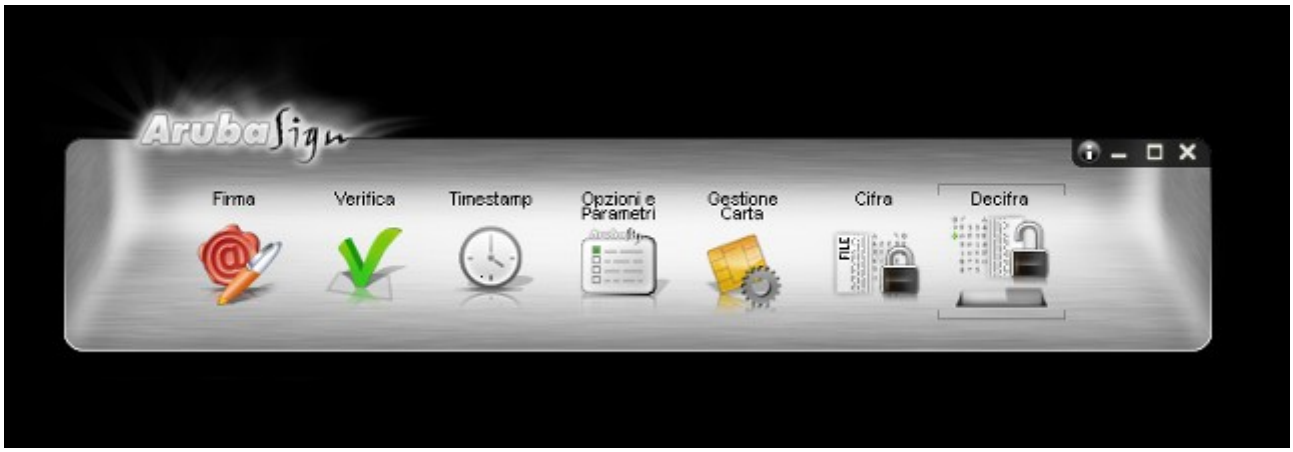
Passo 6
Se la procedura è andata a buon fine verrà mostrata la seguente schermata, cliccare su **"Ok"**.



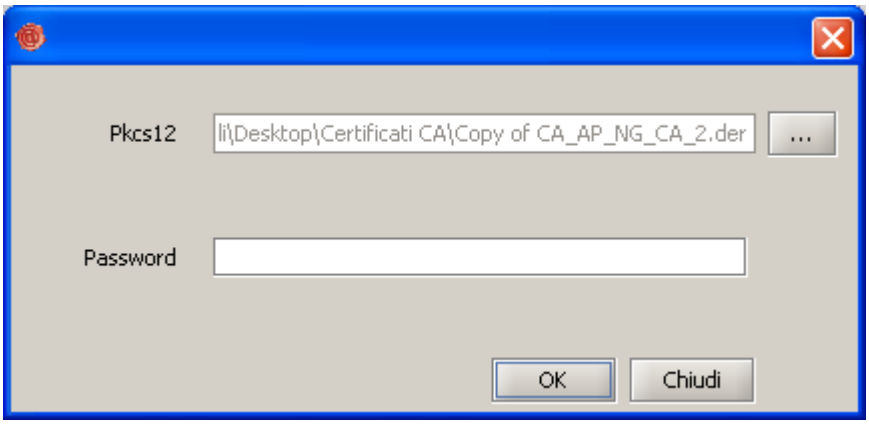
Nota: *Il programma di Cifratura crea un file con estensione ".p7e" che include il file originale.*

16 Decifratura File

Passo 1
Trascinare il file **".p7e"** sull'icona **"Decifra.**



Passo 3
LArubasign verifica che nella smartcard sia presente almeno uno dei certificati indicati nella fase di cifratura. Il programma in questa fase chiede il PIN della smartcard.

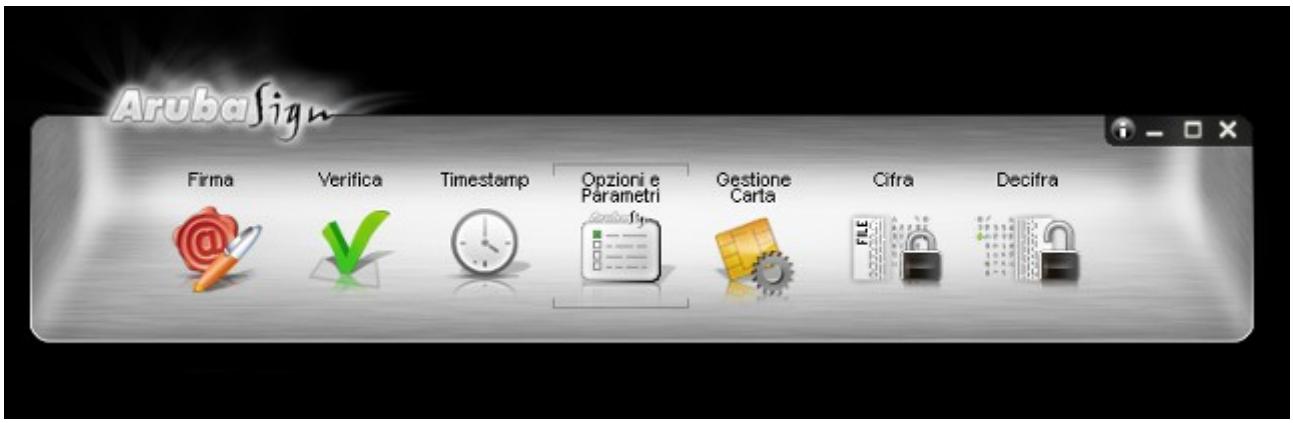


Passo 4
ArubaSign, dopo aver completato il processo di decifratura del file, propone all'utente l'apertura o il salvataggio dello stesso.

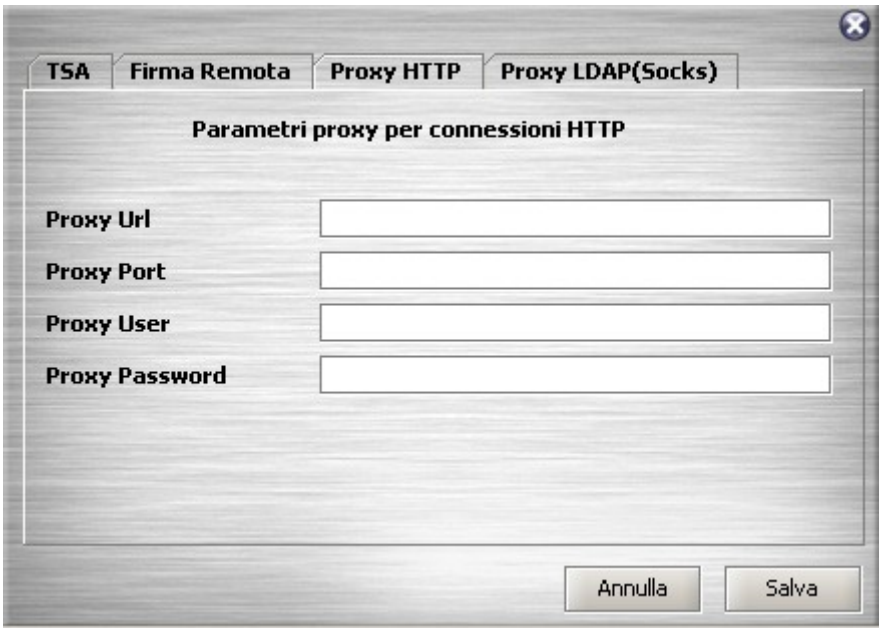
17 Impostazione Proxy

Per utilizzare Aruba Sign 2 in una rete protetta da Proxy, far riferimento alle seguenti istruzioni:

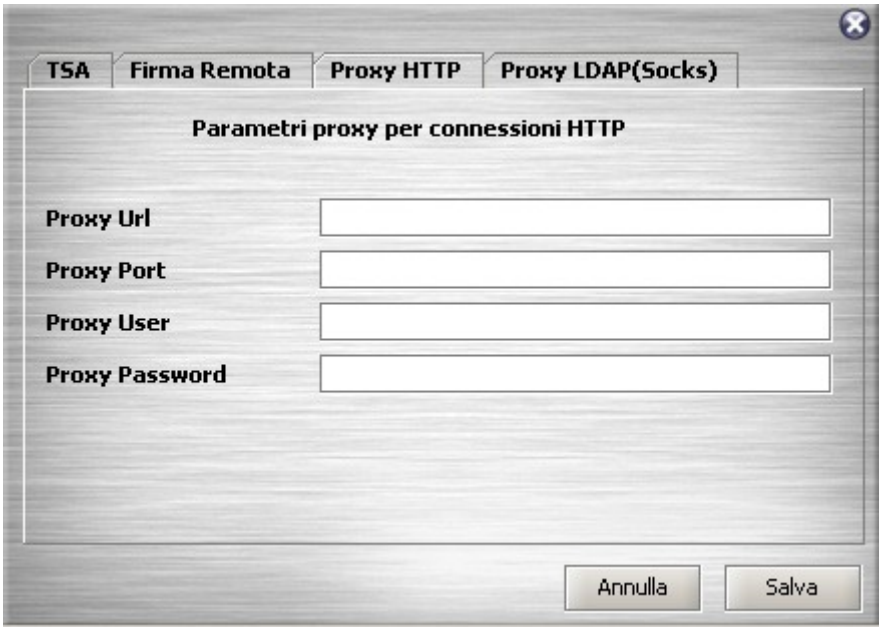
Passo 1
Selezionare il pulsante "**Opzioni e Parametri".**



Passo2
Cliccare su "**Proxy HTTP"**.



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



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.*

17 Firma Remota

17.1 Configurazione Parametri Firma Remota

Passo1

Prima di apporre una Firma Digitale utilizzando il servizio di Firma Remota, è necessario impostare su Aruba Sign 2 le proprie credenziali, secondo quanto indicato:

1. Selezionare il Tab “Firma Remota”
2. Scrivere il proprio User Name (scelto in fase di attivazione del servizio).

Nota: *I parametri dell’indirizzo server primario e secondario vengono valorizzati automaticamente e non devono essere modificati.*

Passo 2
Terminata la configurazione, cliccare su “Salva”.