Software Aruba Sign

Guida rapida

Scopo del Documento

Il presente documento vuole essere una guida rapida per lo svolgimento delle seguenti operazioni con il Software di Firma Aruba Sign e Dispositivi di Firma Digitale e/o Remota Aruba:

1. Prerequisiti di utilizzo e compatibilità;
2. Modalità di installazione e avvio del Software;
3. Modalità di Firma Documenti e formati di Firma disponibili;
4. Modalità di Apposizione di Marche Temporali;
5. Modalità di Verifica di File firmati e di Marche Temporali;
6. Principali funzioni della barra di menù di Aruba Sign.

Sommario

1. Installazione e avvio Aruba Sign – Firma Digitale

1.1 Prerequisiti hardware e software

La postazione cui viene collegato il **software Aruba Sign** deve possedere i seguenti prerequisiti Hardware e Software:

Software:

Sistemi Operativi:

- Windows 10, MS Windows XP, Vista, Seven, Server 2003, Server 2008 (32 e 64 bit)
- Mac OSX: Lion (10.7.4) e successive
- Linux Ubuntu 16.04 32/64bit, Xubuntu 16.04 32/64bit e Lubuntu 16.04 32/64bit

Rete:

Di seguito i **parametri di rete** che devono possedere le postazioni alle quali viene collegata **Aruba Sign**:
Disponibilità di connessione Internet senza presenza di Proxy

1. Possibilità di poter instaurare connessioni HTTP, HTTPS e LDAP

1.2 Installazione e avvio del Software – Firma Digitale

I Kit di Firma Digitale Aruba sono composti da **Token o lettori da tavolo**, **Smart Card** (in formato SIM e carta di credito) e **certificato di Firma e Autenticazione CNS**.

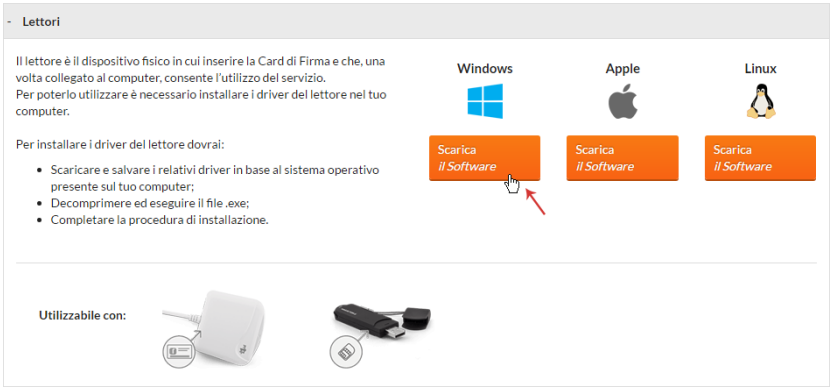
In caso di acquisto del Kit completo, prima di scaricare il Software Aruba Sign, installare i driver necessari al riconoscimento del lettore e della Smart Card acquistati. In caso di acquisto di una Smart Card, installare i soli driver relativi.

1.2.1 Installare i driver dei Lettori di Firma Digitale

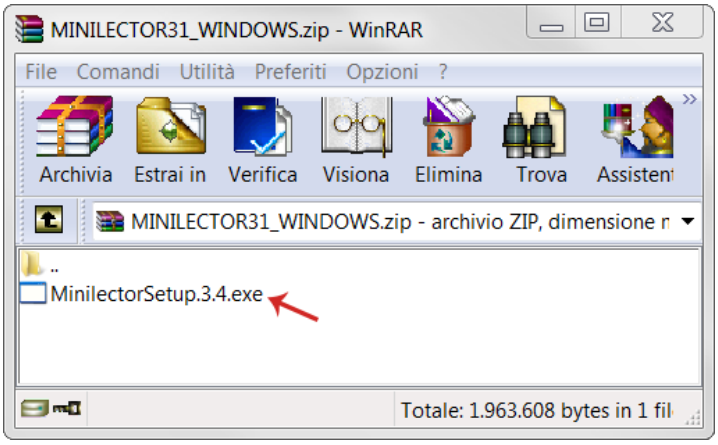
2. **Collegare il Lettore al PC** e attendere il riconoscimento del sistema, quindi **inserire la carta nel lettore** con il chip rivolto verso l'alto:

3. Dalla sezione "Download Software e Driver" del sito pec.it, al Form dedicato "**Driver Lettori**" cliccare su "**Scarica il Software**" a seconda del sistema operativo utilizzato (l'immagine esemplificativa di seguito indicata si riferisce a **Windows**):

DRIVER LETTORI

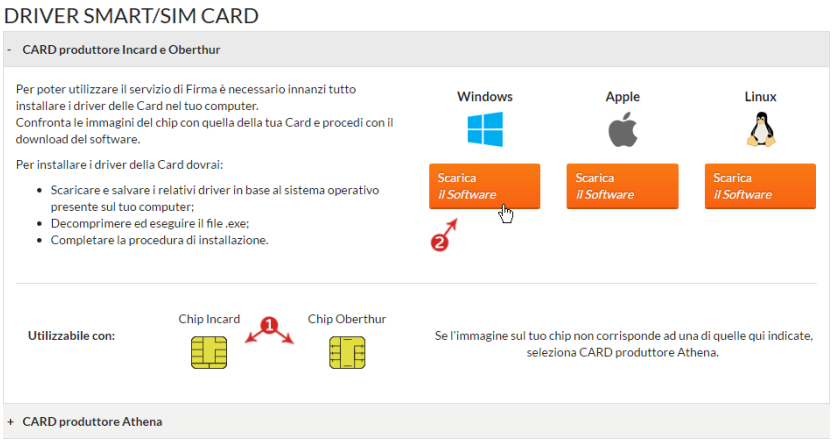


4. Dalla cartella creata a seguito dell'installazione, decomprimere ed eseguire il file .exe, quindi completare la procedura di installazione, seguendo i passaggi indicati dal sistema:

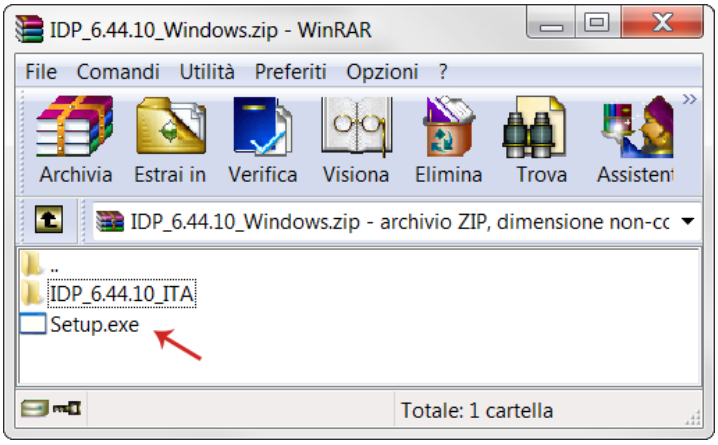


1.2.2 Installare i Driver Smart Card

1. **Confrontare l'immagine del chip della carta posseduta con quelle indicate nelle sezioni dedicate del sito** pec.it, visionabili dall'apposito menù a tendina al link https://www.pec.it/download-software-driver.aspx;
2. **Scaricare e salvare i relativi driver** cliccando sul pulsante "**Scarica il Software**" in base al sistema operativo presente sul proprio computer (l'immagini esemplificative di seguito indicata si riferisce a Chip Incard o Obertur e sistema operativo Windows):

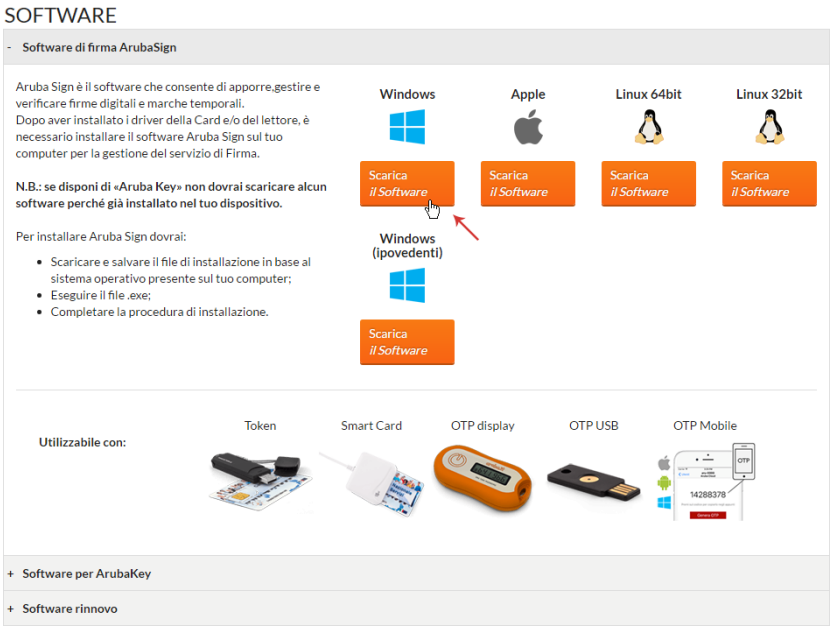


3. Dalla cartella creata a seguito dell'installazione, decomprimere ed eseguire il file .exe, quindi completare la procedura di installazione, seguendo i passaggi indicati dal sistema:



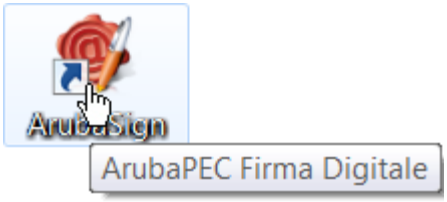
1.2.3 Installare il Software Aruba Sign

1. Collegarsi a https://www.pec.it/download-software-driver.aspx;
2. Dal menù a tendina "**Software**" → selezionare "**Software di Firma Aruba Sign**", quindi cliccare sul pulsante "**Scarica il Software**" **corrispondente al sistema operativo utilizzato** (l'esempio di seguito indicato si riferisce a Windows):

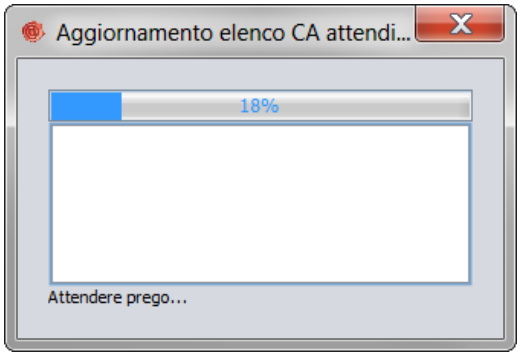


3. **Scaricare ed eseguire su locale il File di installazione**, quindi installare il Software utilizzando la procedura guidata:
   - Selezionare la "**Lingua di Installazione**";
   - Al Tab "**Installazione di Aruba Sign**", cliccare su "**Avanti**";
   - Selezionare la **cartella di destinazione** e cliccare su "**Avanti**";
   - Premere "**Installa**" per continuare l'installazione;
   - Attendere il completamento dell'installazione di Aruba Sign sul computer;
   - Premere "**Fine**" per completare l'installazione.

4. Completo il processo, **sul desktop si visualizza l'icona di Aruba Sign** che permette l'avvio del programma:



5. Il sistema effettua l'aggiornamento automatico del Database dei certificatori, come da immagine esemplificativa sottostante:



6. Completato l'aggiornamento, **si visualizza la schermata principale del Software**:

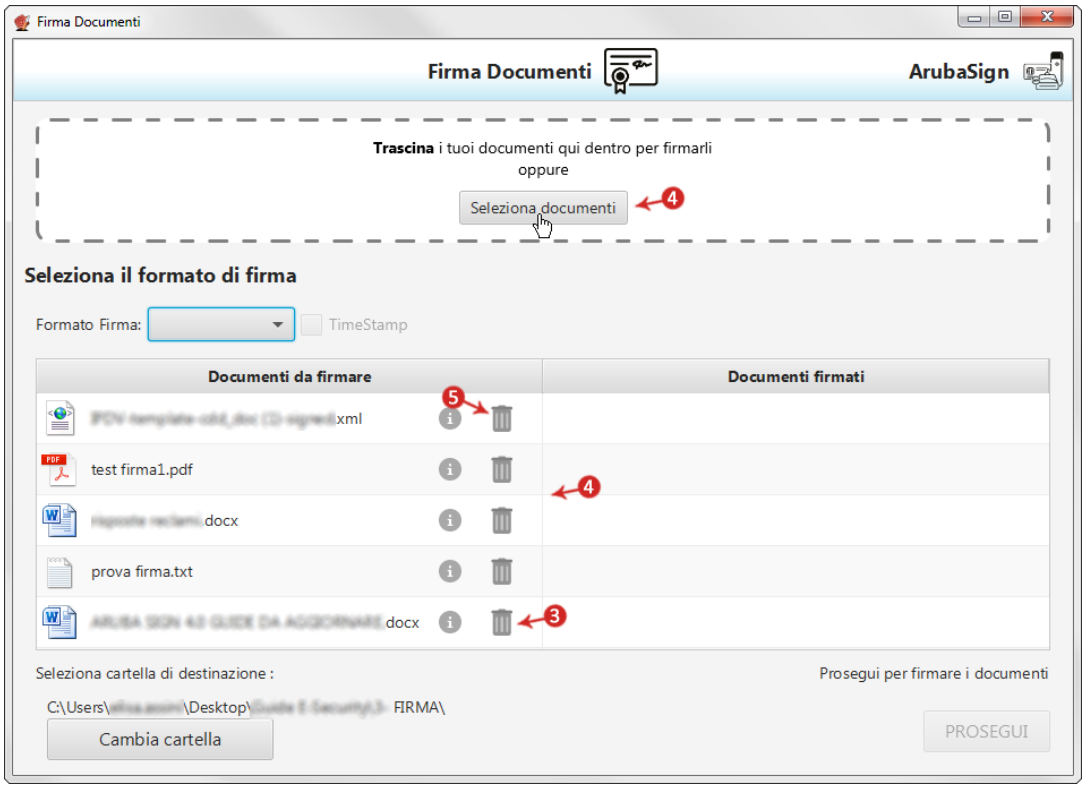
2. Firma e verifica file Aruba Sign - Firma Digitale

2.1 Caricamento documenti da firmare e/o cartelle su Aruba Sign

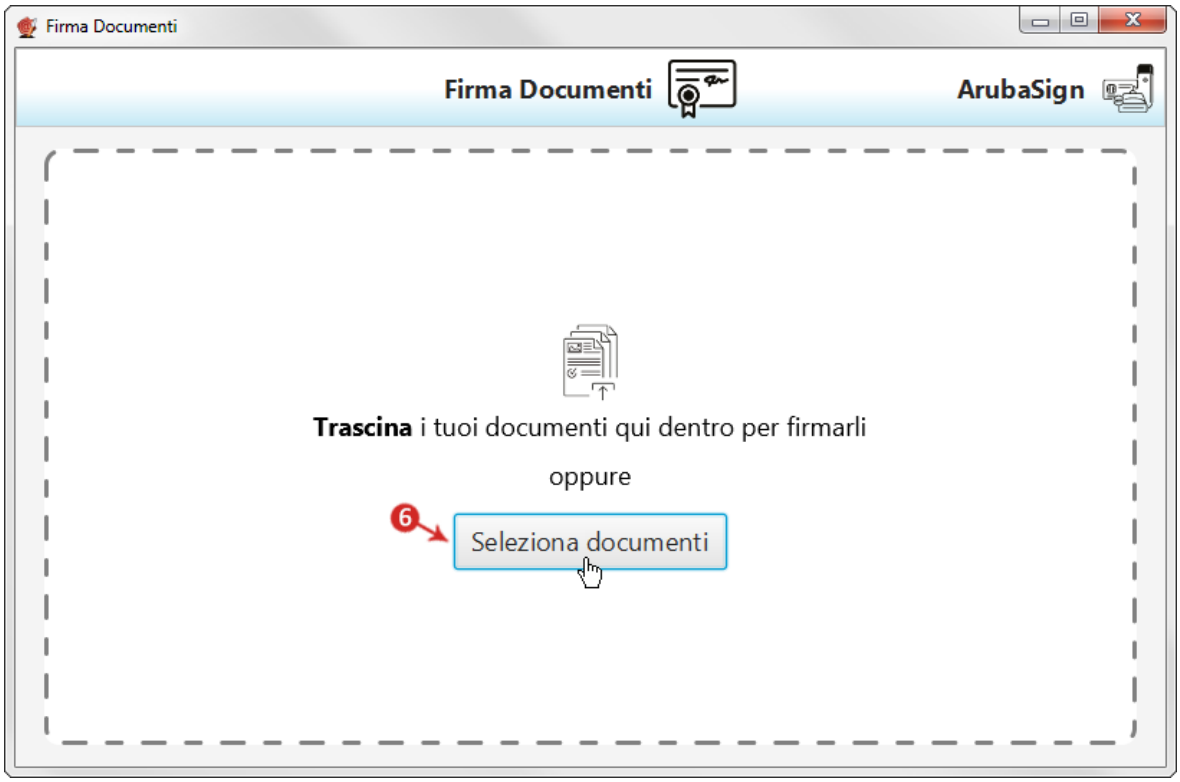
Per **caricare uno o più file su Aruba Sign** e/o una **intera cartella**:

1. Aprire il Software Aruba Sign;
2. Trascinare un qualsiasi documento e/o una cartella (sono accettate tutte le estensioni) sopra l'icona "**Firma**" e attendere che Aruba Sign recuperi le informazioni relative ai certificati contenute nella Smart Card:

3. Alla schermata "**Firma Documenti**", sono visibili i documenti importati in corrispondenza del Tab "**Documenti da firmare**";
4. Per aggiungere ulteriori documenti, cliccare su "**Seleziona Documenti**" e caricare i file desiderati da locale. Gli stessi sono visibili in elenco su "**Documenti da firmare**";
5. I documenti caricati possono essere rimossi in qualsiasi momento cliccando sull'icona "**Cestino**":



6. In alternativa, per uploadare file, cliccare su "**Firma**" dalla barra di menù di ArubaSign. Si visualizza la schermata "**Firma Documenti**", da cui caricare **file** e/o **cartelle** contenenti documenti da firmare cliccando su "**Seleziona Documenti**":



7. Completato il caricamento, si visualizza la schermata indicata agli step 3/4/5 ed è possibile compiere le operazioni descritte ai rispettivi punti.

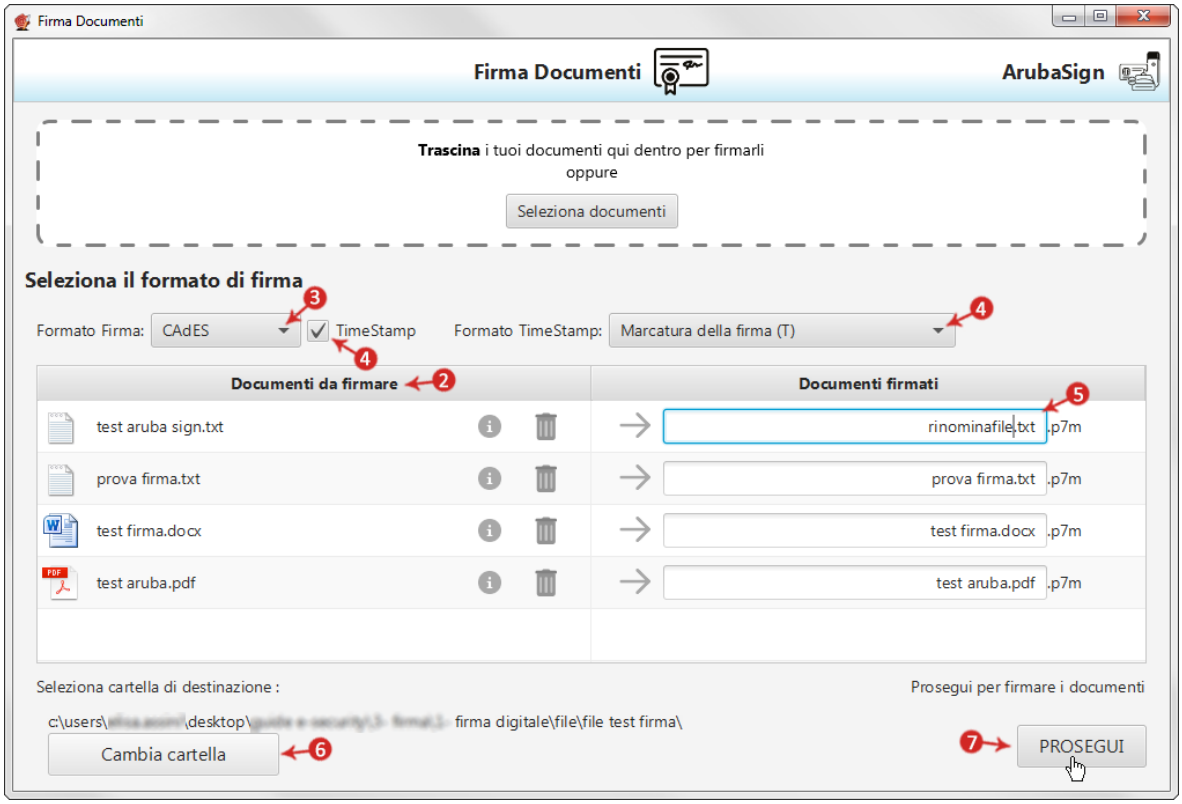
In caso di caricamento di una intera cartella vengono importati tutti i file contenuti nella cartella stessa e quelli eventualmente presenti in sottocartelle. Al momento della Firma, però, il sistema non consente di firmare documenti con identico nome. In questo caso si visualizza un messaggio di errore e la procedura è interrotta.

2.2 "Firma" uno o più file in formato .p7m - Firma Digitale

Un **file firmato digitalmente assume estensione .p7m**, che si somma all'estensione del file originario. Ad esempio, un **documento .txt**, al **termine del processo di Firma Digitale** diviene un **documento .txt.p7m** che rappresenta una **busta informatica** (**PKCS#7**). La busta incorpora al suo interno il documento originario, il certificato del sottoscrittore e un hash del documento firmato con il certificato del sottoscrittore. **Un documento sottoscritto digitalmente ha piena validità legale**.

Per **firmare digitalmente uno o più file in formato .p7m** (**Firma CAdES**) e/o una intera cartella **con Aruba Sign**:

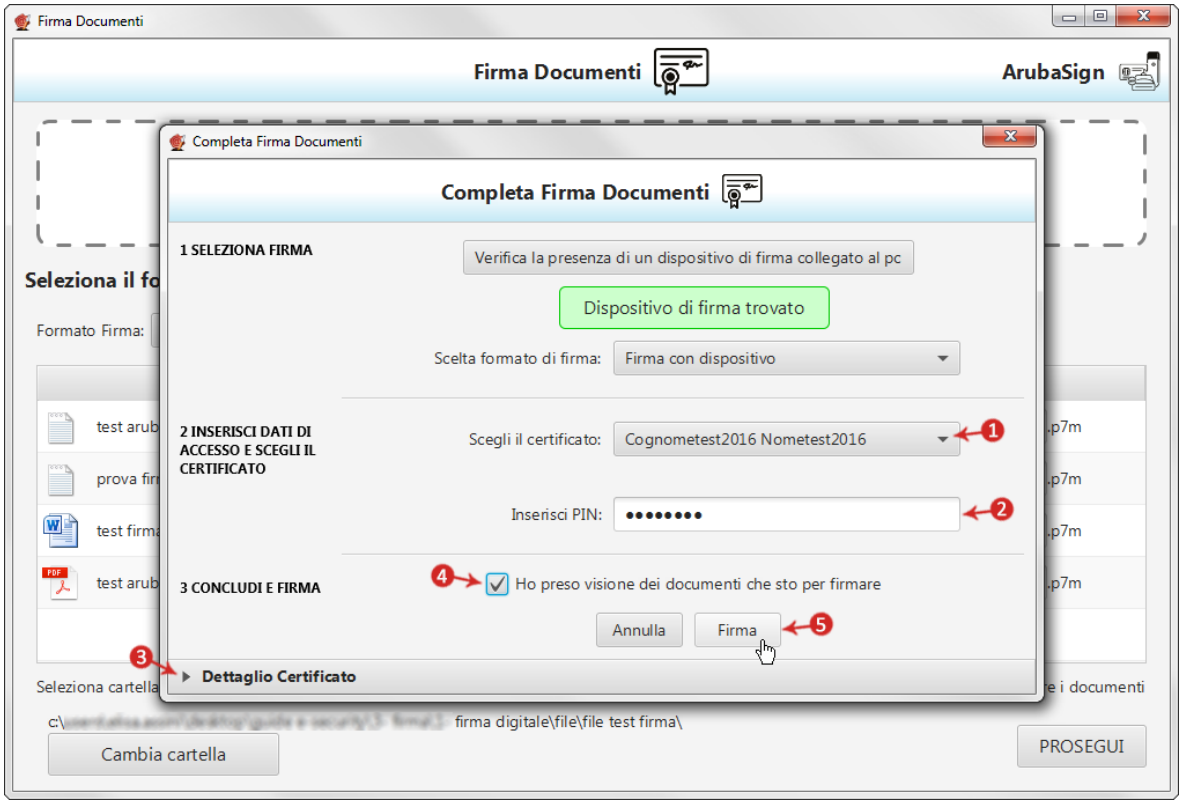
1. **Caricare uno o più documenti e/o una intera cartella**;
2. Il **singolo/i documenti caricati/o** sono visibili all'apposita schermata "**Documenti da firmare**";
3. Dall'apposito menù a tendina "**Formato Firma**" selezionare come tipologia di Firma "**CAdES**" per firmare il file in formato .p7m;
4. Inserire il Flag in corrispondenza della voce "**TimeStamp**" per apporre al file una marcatura temporale nel formato scelto dall'apposito menù a tendina "**Formato TimeStamp**" (lo stesso è visibile solo dopo aver selezionato la voce "**TimeStamp**");
5. Dalla finestra "**Documenti firmati**" rinominare, se desiderato, eventuali file prima di apporre la firma;
6. Da "**Cambia cartella**" verificare che il percorso utilizzato per salvare il/i file firmato/i sia quello desiderato, o selezionarne uno nuovo utilizzando il pulsante indicato;
7. Cliccare su "**Prosegui**" per continuare. Sono firmati tutti i documenti presenti alla finestra "**Documenti da firmare**":



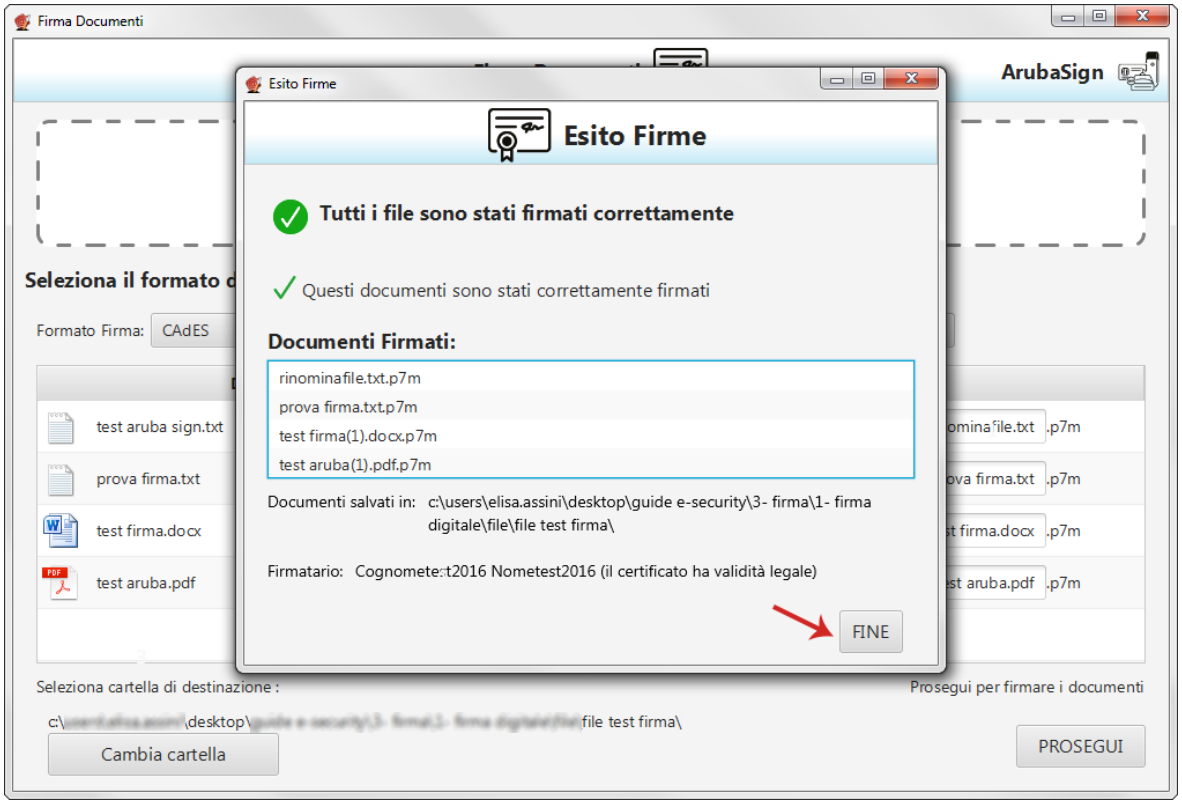
Alla schermata "**Completa Firma Documenti**":

1. Assicurarsi che sia selezionato il **Certificato per la firma digitale** (in formato Cognome - Nome);

2. Inserire il **PIN** di protezione della **Smart Card**. **Nel caso in cui non vi siano Dispositivi di Firma Digitale collegati al pc, il sistema lo indica con apposito messaggio in giallo** "**Nessun Dispositivo trovato**" e, da "**Scelta Formato di Firma**", è possibile impostare la firma con Firma Remota.
3. Da "**Dettagli Certificato**" visionare, qualora desiderato, le caratteristiche e la validità del Certificato stesso;
4. Dichiarare di aver preso visione del documento/i e di essere consapevole della validità ai sensi di legge della Firma apposta;
5. Cliccare su "**Firma**" per concludere il processo:



Al termine dell'operazione si visualizza la seguente schermata che notifica la corretta firma del file. Cliccare su "**FINE**" per chiudere la schermata:



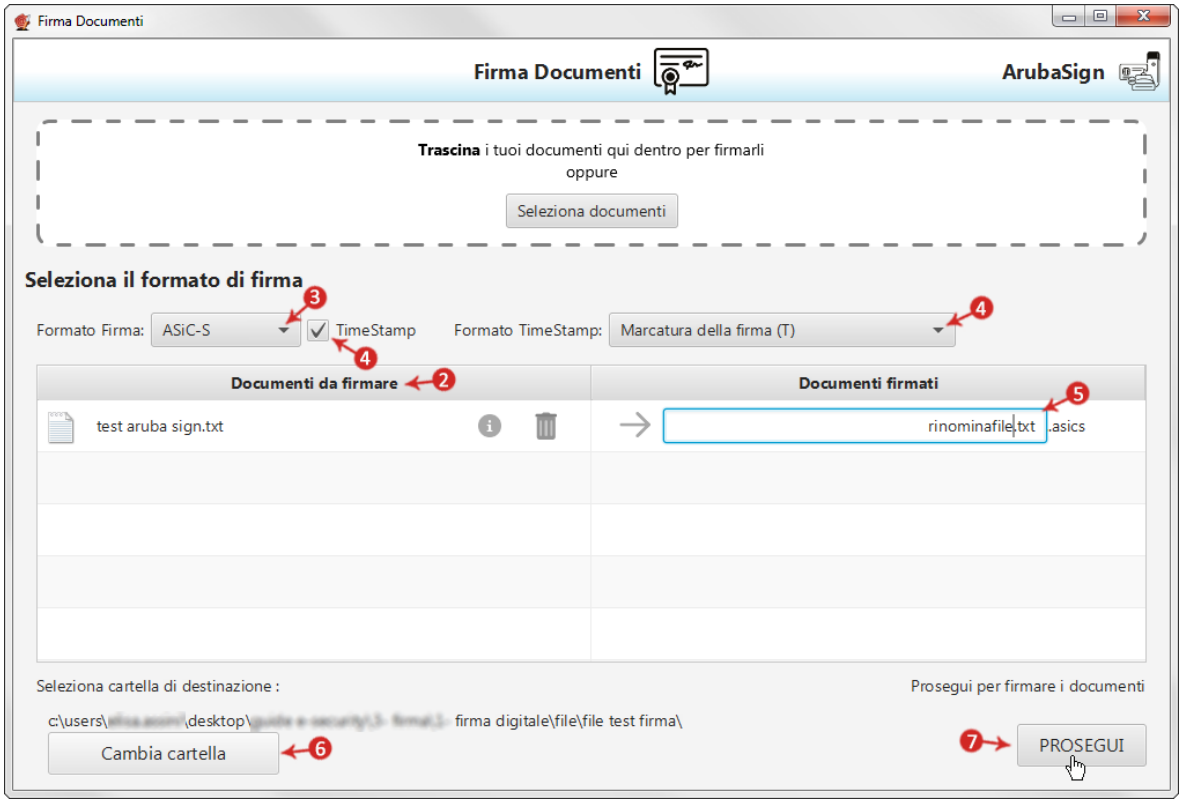
Il **documento/i firmato/i sono salvati in formato .p7m nella cartella indicata in fase di Firma**.

2.3 "Firma" un singolo file in formato ASiC-S - Firma Digitale

Il formato di firma **asic-s** (**Associated Signature Containers** "**ASiC simple**") è un **contenitore di dati che raggruppa un file e le relative firme digitali detached e/o marche temporali associate**, utilizzando il formato **.zip**.

Per **firmare digitalmente un file in formato ASiC-S con Aruba Sign**:

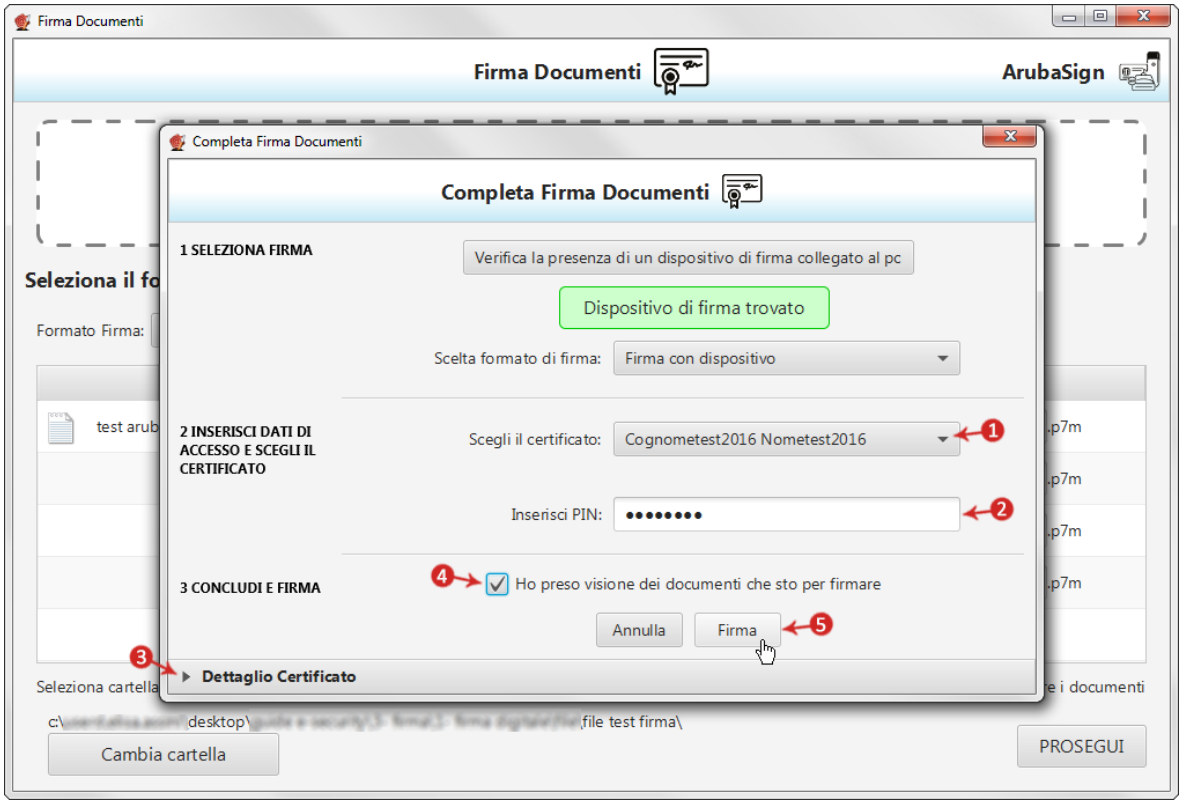
1. **Caricare il documento. Questo formato di Firma è applicabile solo in caso di caricamento su Aruba Sign di un singolo File**, per firmare più file in formato ASiC, selezionare la specifica voce ASiC-E;
2. Il **singolo/i documenti caricati/o** sono visibili all'apposita schermata "**Documenti da firmare**";
3. Dall'apposito menù a tendina "**Formato Firma**" selezionare come tipologia di Firma "**ASiC-S**";
4. Inserire il Flag in corrispondenza della voce "**TimeStamp**" per apporre al file una marcatura temporale nel formato scelto dall'apposito menù a tendina "**Formato TimeStamp**" (lo stesso è visibile solo dopo aver selezionato la voce "**TimeStamp**");
5. Dalla finestra "**Documenti firmati**" rinominare, se desiderato, il file;
6. Da "**Cambia cartella**" verificare che il percorso utilizzato per salvare il file firmato sia quello desiderato, o selezionarne uno nuovo utilizzando il pulsante indicato;
7. Cliccare su "**Prosegui**" per continuare:



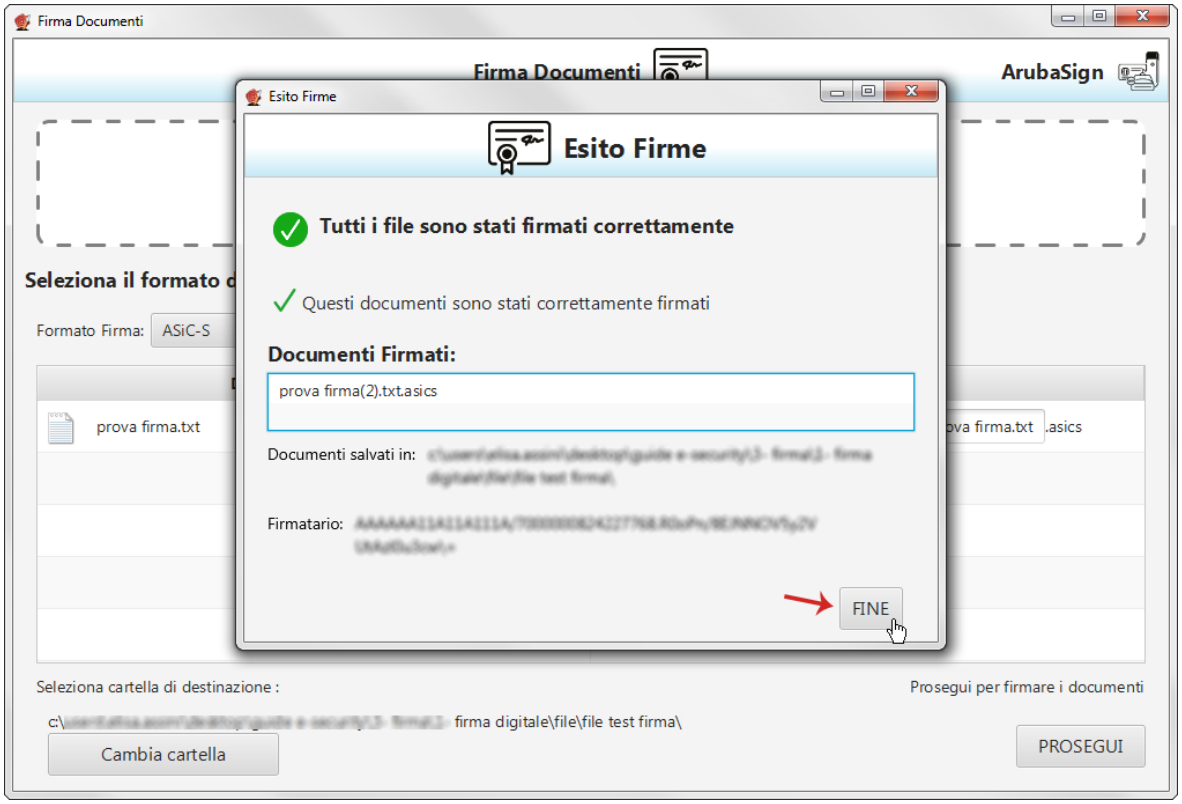
Alla schermata "**Completa Firma Documenti**":

1. Assicurarsi che sia selezionato il **Certificato per la firma digitale** (in formato Cognome - Nome);
2. Inserire il **PIN** di protezione della **Smart Card**. **Nel caso in cui non vi siano Dispositivi di Firma Digitale collegati al pc, il sistema lo indica con apposito messaggio in giallo** "**Nessun Dispositivo trovato**" e, da "**Scelta Formato di Firma**", è possibile impostare la firma con Firma Remota.

2. Da "**Dettagli Certificato**" visionare, qualora desiderato, le caratteristiche e la validità del Certificato stesso;
3. Dichiarare di aver preso visione del documento e di essere consapevole della validità ai sensi di legge della Firma apposta;
4. Cliccare su "**Firma**" per concludere il processo:



Al termine dell'operazione si visualizza la seguente schermata che notifica la corretta firma del file. Cliccare su "**FINE**" per chiudere la schermata:



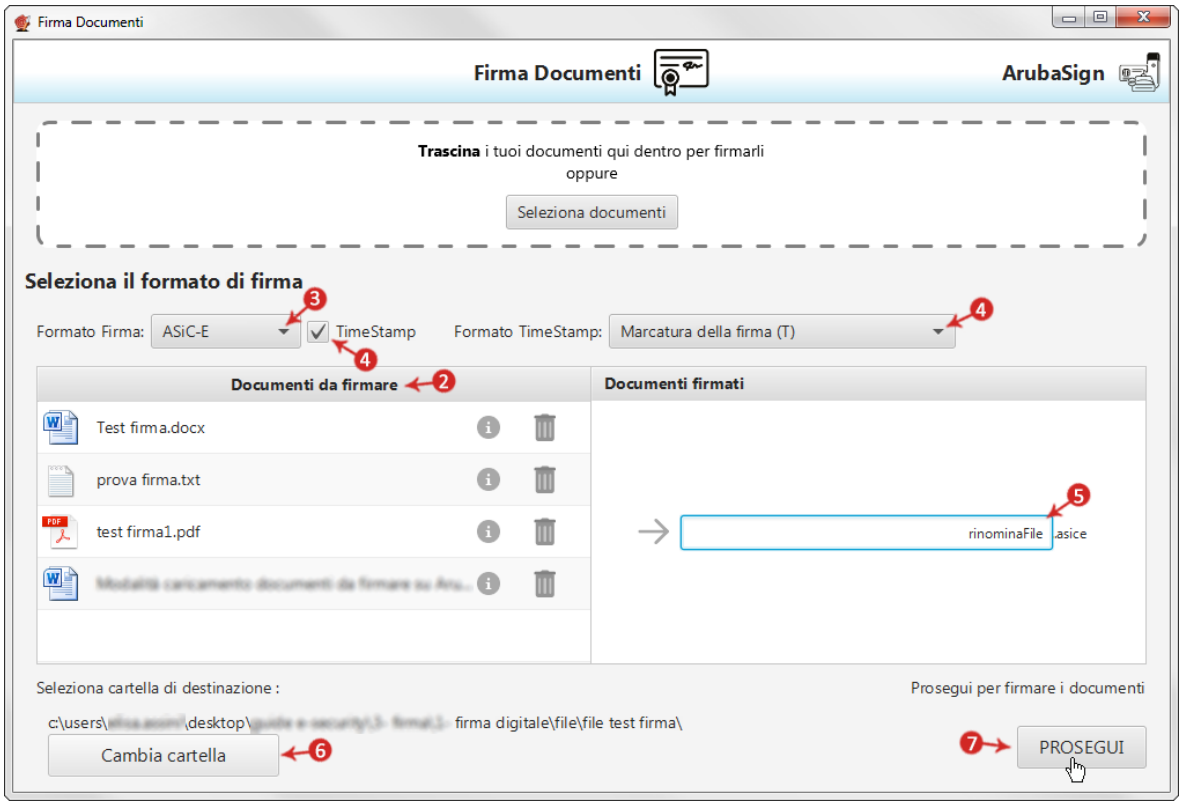
Il documento firmato in **formato ASiC-S** è salvato nella cartella indicata in fase di Firma.

2.4 "Firma" di più file in formato ASiC-E - Firma Digitale

Il formato di firma ASiC-E (**Associated Signature Containers** "**ASiC simple**") è un **contenitore di dati che raggruppa più file e le relative firme digitali detached e/o marche temporali associate**, utilizzando il formato **.zip**.

Per **firmare digitalmente più file in formato ASiC-E con Aruba Sign**:

1. **Caricare i documenti e/o una intera cartella**. **Questo formato di Firma è applicabile solo in caso di caricamento su Aruba Sign di più documenti**, per firmare un solo file in formato ASiC, selezionare dall'apposito menù a tendina "**Formato Firma**" ASiC-S.
2. I **documenti caricati** sono visibili all'apposita schermata "**Documenti da firmare**";
3. Dall'apposito menù a tendina "**Formato Firma**" selezionare come tipologia di Firma "**ASiC-E**";
4. Inserire il Flag in corrispondenza della voce "**TimeStamp**" per apporre ai file una marcatura temporale nel formato scelto dall'apposito menù a tendina "**Formato TimeStamp**" (lo stesso è visibile solo dopo aver selezionato la voce "**TimeStamp**");
5. Dalla finestra "**Documenti firmati**" rinominare, se desiderato, il contenitore dei file;
6. Da "**Cambia cartella**" verificare che il percorso utilizzato per salvare i file firmati sia quello desiderato, o selezionarne uno nuovo utilizzando il pulsante indicato;
7. Cliccare su "**Prosegui**" per continuare. Sono firmati tutti i documenti presenti alla finestra "**Documenti da firmare**":

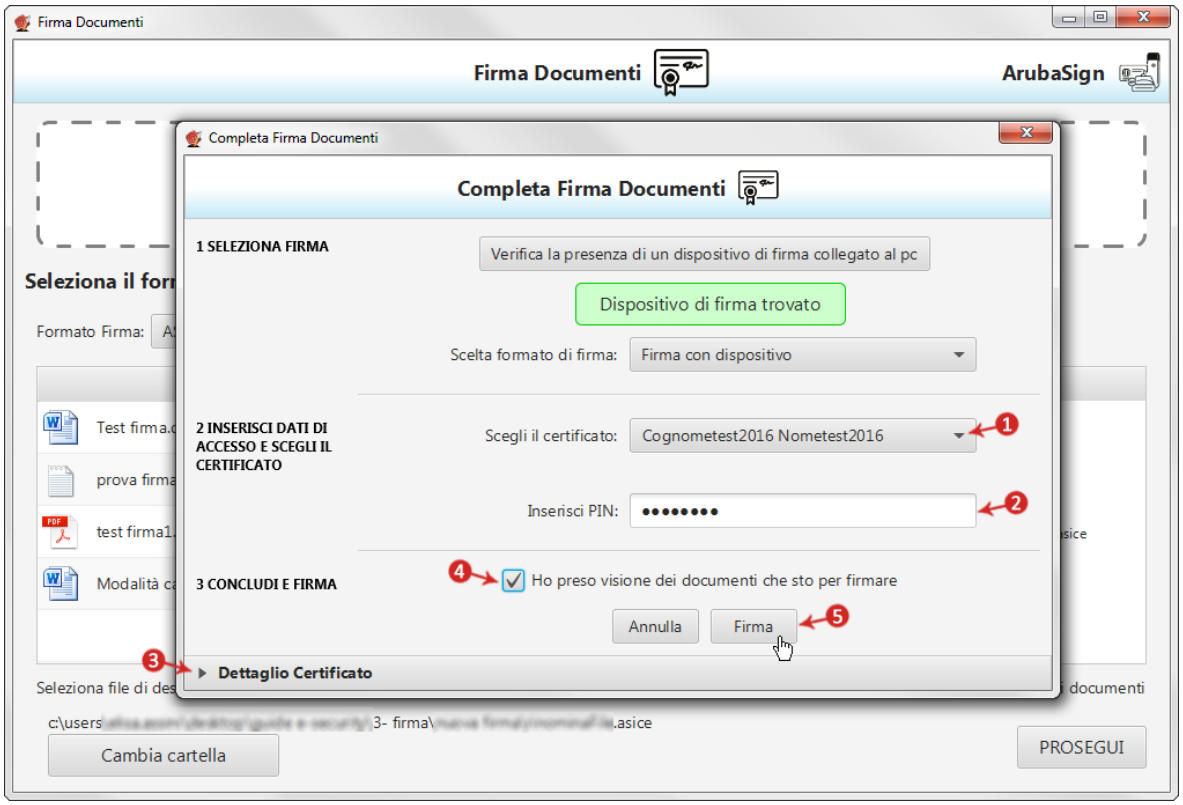


Alla schermata "**Completa Firma Documenti**":

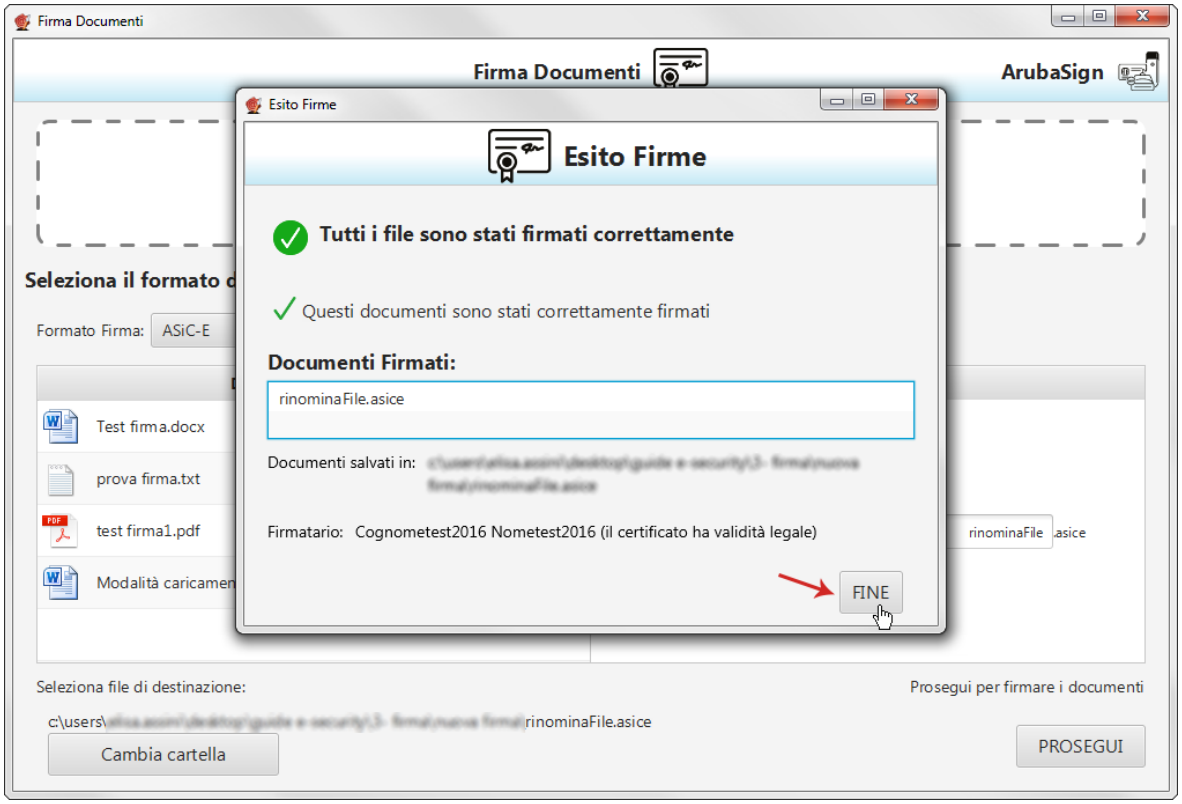
1. Assicurarsi che sia selezionato il **Certificato per la firma digitale** (in formato Cognome - Nome);
2. Inserire il **PIN** di protezione della **Smart Card**. **Nel caso in cui non vi siano Dispositivi di Firma Digitale collegati al pc, il sistema lo indica con apposito messaggio in giallo** "**Nessun**

Dispositivo trovato" e, da "**Scelta Formato di Firma**", è possibile impostare la firma con Firma Remota.

3. Da "**Dettagli Certificato**" visionare, qualora desiderato, le caratteristiche e la validità del Certificato stesso;
4. Dichiarare di aver preso visione dei documenti e di essere consapevole della validità ai sensi di legge della Firma apposta;
5. Cliccare su "**Firma**" per concludere il processo:



Al termine dell'operazione si visualizza la seguente schermata che notifica la corretta firma dei file. Cliccare su "**FINE**" per chiudere la schermata:



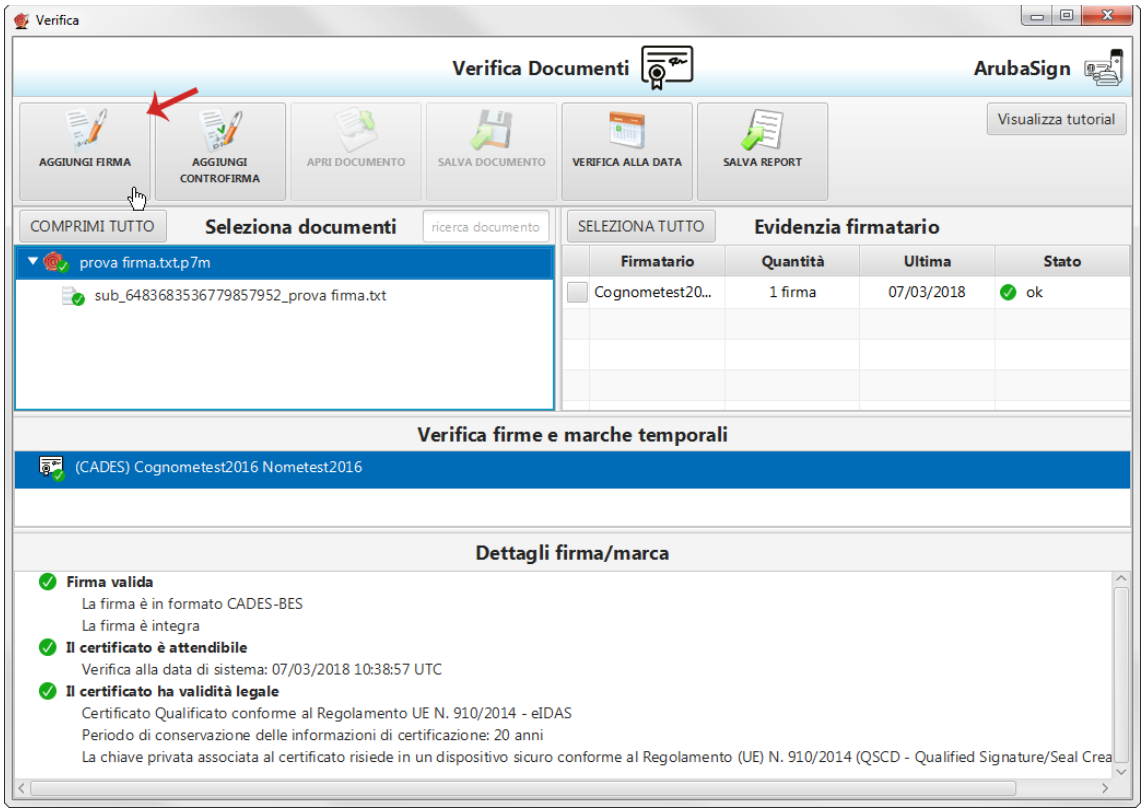
Il contenitore di documenti in **formato ASiC-E** è **salvato nella cartella indicata in fase di Firma**. In fase di verifica del contenitore è possibile visionare il dettaglio delle Firme apposte a ogni singolo documento.

2.5 Apposizione "Firma Parallela" - Firma Digitale

La funzione "**Firma Parallela**" è accessibile trascinando sopra il pulsante di verifica del Software Aruba Sign **uno o più file già firmati in formato .p7m (CAdES) o .PDF (PAdES)**. E' aggiunta allo stesso livello e allo stesso contenuto di una firma preesistente e viene di norma utilizzata per aggiungere firme ad un documento già firmato in formato .p7m in quei flussi documentali che ne prevedono l'utilizzo.

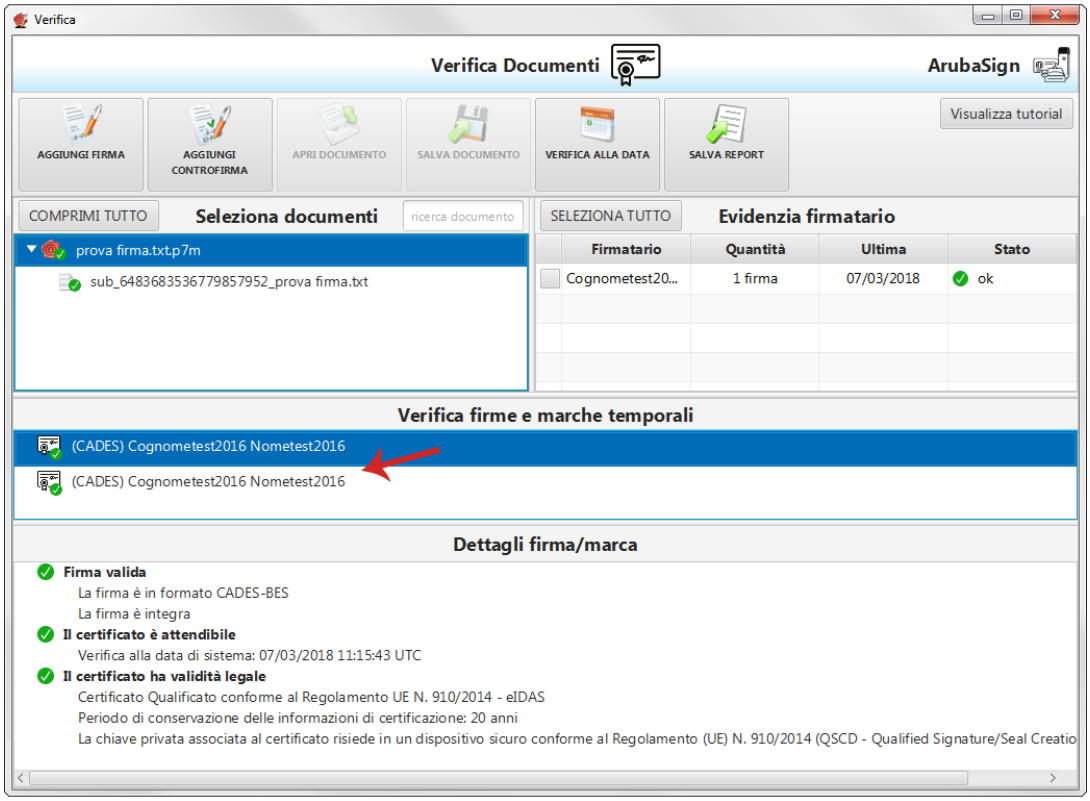
Per crearla **trascinare un file .p7m (CAdES)** o **.PDF (PAdES)**, sopra il menù "**Verifica**" di **Aruba Sign**:

Da "**Verifica documenti**" selezionare il documento (anche in caso di caricamento di un solo file) su cui apporre la **Firma Parallela** poi cliccare su "**Aggiungi Firma**":



Firmare digitalmente il file. **Il sistema non consente di selezionare il formato della Firma.** In caso di File **.p7m** la "**Firma Parallela**" è apposta in tale formato; per i file .PDF è possibile apporre una Firma Grafica o Invisibile. **La nuova firma è apposta allo stesso livello di quella preesistente**. **Il sistema** sovrascrive il documento già esistente e salvato nella cartella indicata in fase di Firma del documento stesso.

Trascinando il file sul pulsante "Verifica" è possibile visionare la presenza della Firma Parallela, come da immagine esemplificativa sottostante:

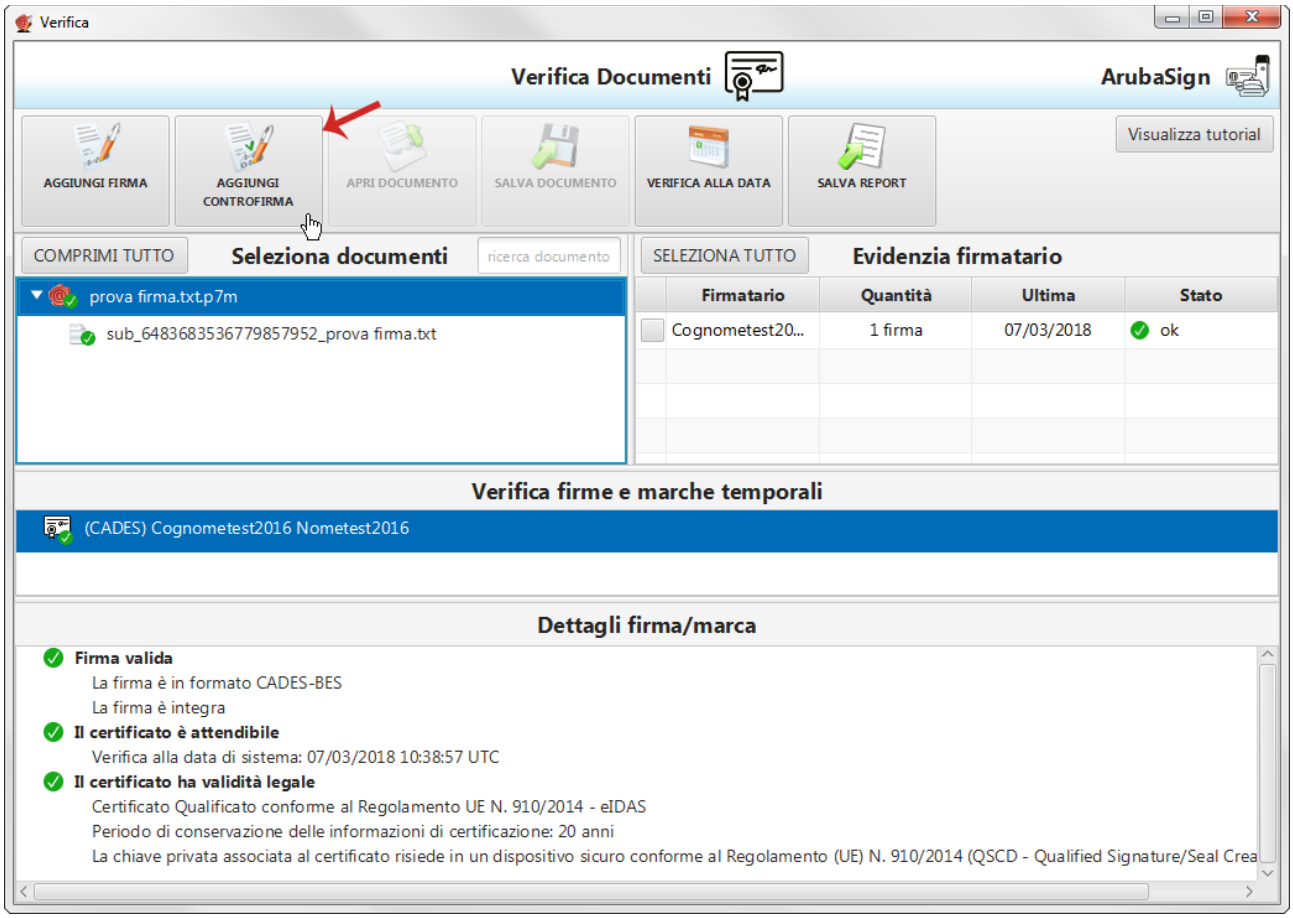


2.6 Apposizione "Controfirma" - Firma Digitale

La funzione "**Controfirma**" è accessibile trascinando sopra il pulsante di verifica del Software Aruba Sign **uno o più file già firmati in formato .p7m**. E' apposta a un livello sottostante di una firma preesistente e sottoscrive quest'ultima. E' più annidata rispetto alla firma a cui si riferisce (aspetto evidenziato da una rappresentazione ad albero delle firme stesse).

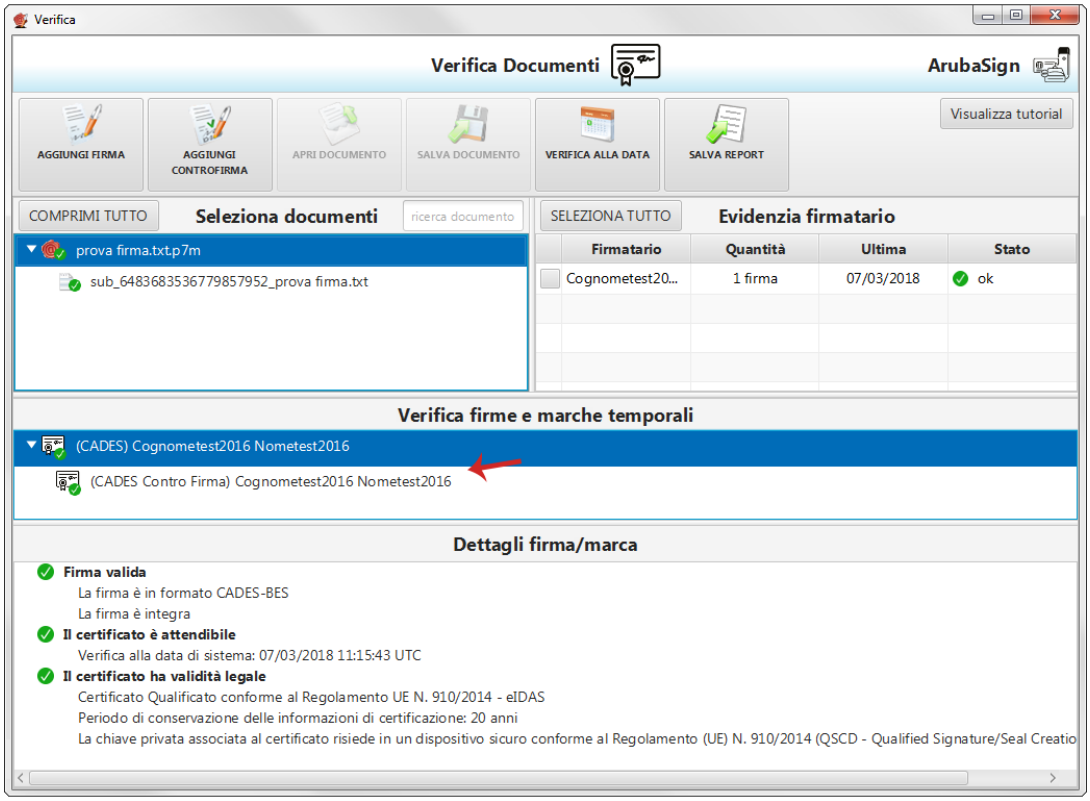
Per crearla **trascinare un file .p7m (CAdES)**, sopra il menù "**Verifica**" di **Aruba Sign**:

Da "**Verifica documenti**" selezionare il documento (anche in caso di caricamento di un solo file) su cui apporre la **Controfirma** poi cliccare su "**Aggiungi Controfirma**":



Firmare digitalmente il file in formato .p7m. **La nuova Firma è apposta a un livello sottostante della firma preesistente**. Il sistema sovrascrive il documento già esistente e salvato nella cartella indicata in fase di Firma del documento stesso.

Trascinando il file sul pulsante "Verifica" è possibile visionare la presenza della Controfirma, come da immagine esemplificativa sottostante:

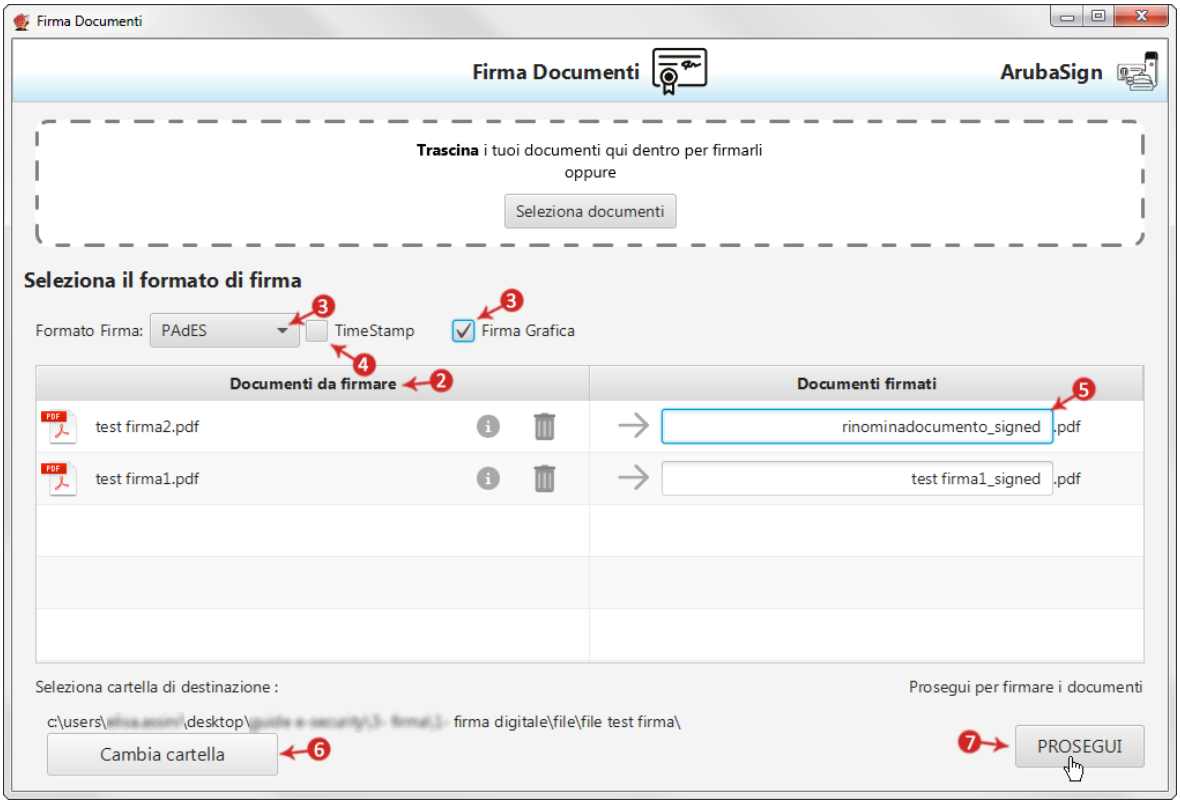


2.7 Apposizione Firma PDF - Grafica (Firma Digitale)

Il Formato di Firma PAdES è applicabile ai soli file già convertiti in formato .PDF, ed **è visibile solo se nel menù "Firma Documenti" di Aruba Sign sono caricati esclusivamente file con questa estensione**. Se sono caricati più file con estensioni diverse tra loro, la firma **PAdES** non risulta tra i formati selezionabili da menù "**Firma**". Un documento sottoscritto digitalmente ha piena validità legale.

La Firma PAdES - Firma Grafica permette di scegliere la posizione e la dimensione del campo che ospita la Firma Digitale. Per **firmare digitalmente uno o più file in formato .PDF in formato PAdES - Firma Grafica** e/o una intera cartella **con Aruba Sign**:

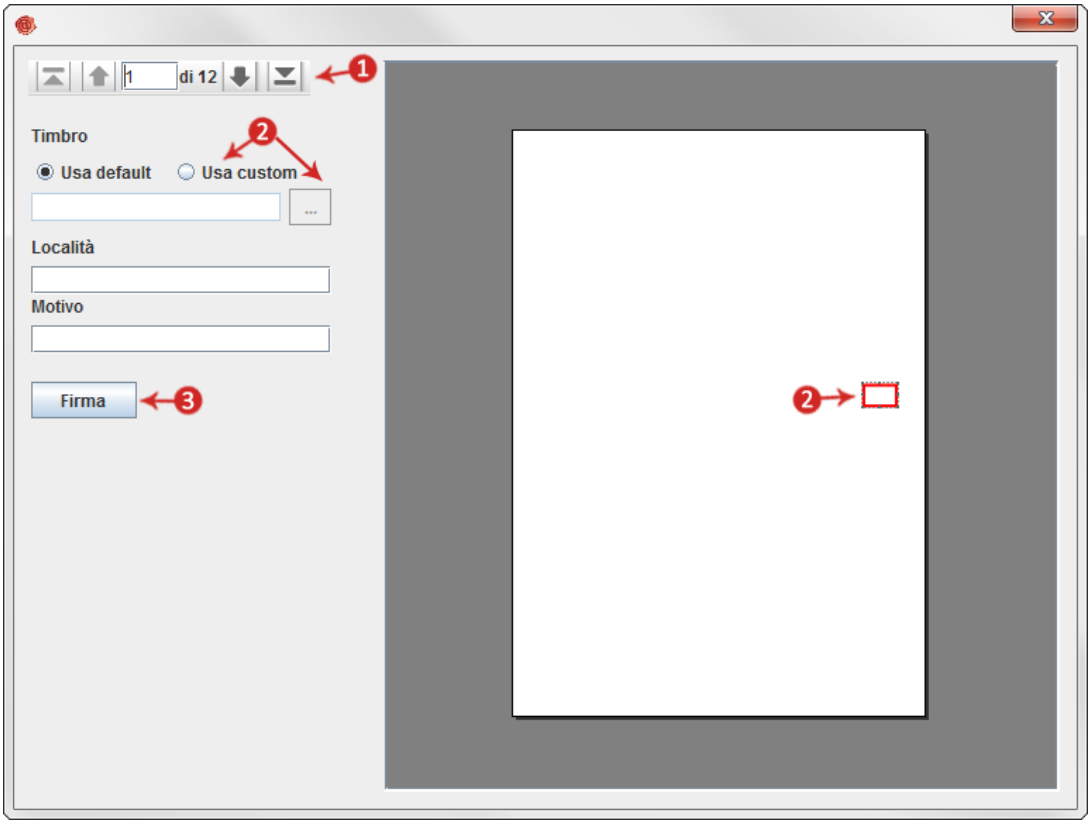
1. **Caricare uno o più documenti e/o una intera cartella**;
2. Il **singolo/i documenti caricati/o** sono visibili all'apposita schermata "**Documenti da firmare**";
3. Dall'apposito menù a tendina "**Formato Firma**" selezionare come tipologia di Firma "**PAdES**" per firmare il file in formato .PDF e lasciare il Flag su "**Firma Grafica**";
4. Inserire il Flag in corrispondenza della voce "**TimeStamp**" per apporre al file una marcatura temporale nel formato scelto dall'apposito menù a tendina "**Formato TimeStamp**" (lo stesso è visibile solo dopo aver selezionato la voce "**TimeStamp**");
5. Dalla finestra "**Documenti firmati**" rinominare, se desiderato, eventuali file prima di apporre la firma;
6. Da "**Cambia cartella**" verificare che il percorso utilizzato per salvare il/i file firmato/i sia quello desiderato, o selezionarne uno nuovo utilizzando il pulsante indicato;
7. Cliccare su "**Prosegui**" per continuare. Sono firmati tutti i documenti presenti alla finestra "**Documenti da firmare**":



Alla schermata "**Firma PDF**":

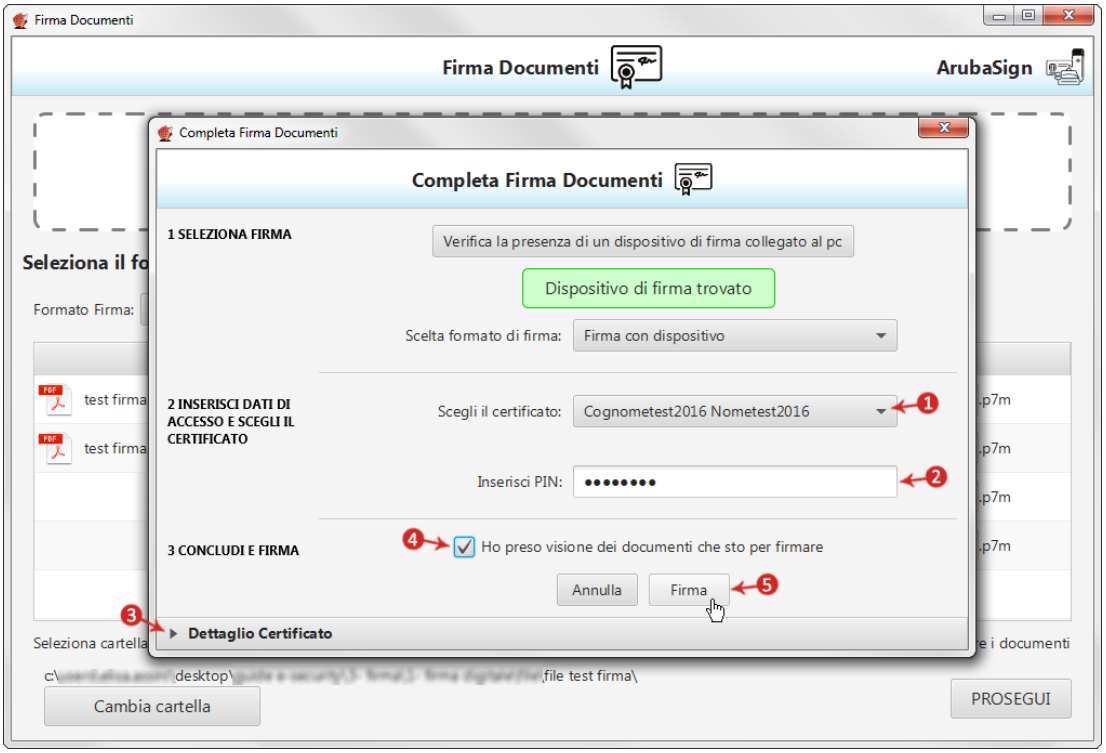
1. Indicare, dal menù in alto, il numero di pagina dove far comparire il timbro;

2. Definire, attraverso la finestra di anteprima, la **posizione** e la **dimensione del campo** che ospiterà la Firma Digitale. Al campo "**Timbro**", è possibile caricare da locale, spuntando "**Usa custom**" e utilizzando l'apposito pulsante indicato in figura, una img in formato .gif/.jpg/.png da sostituire a quella presente di default per il timbro. L'immagine caricata è ridimensionata in scala rispetto alle dimensione dell'area selezionata;
3. Cliccare su "**Firma**" per procedere:

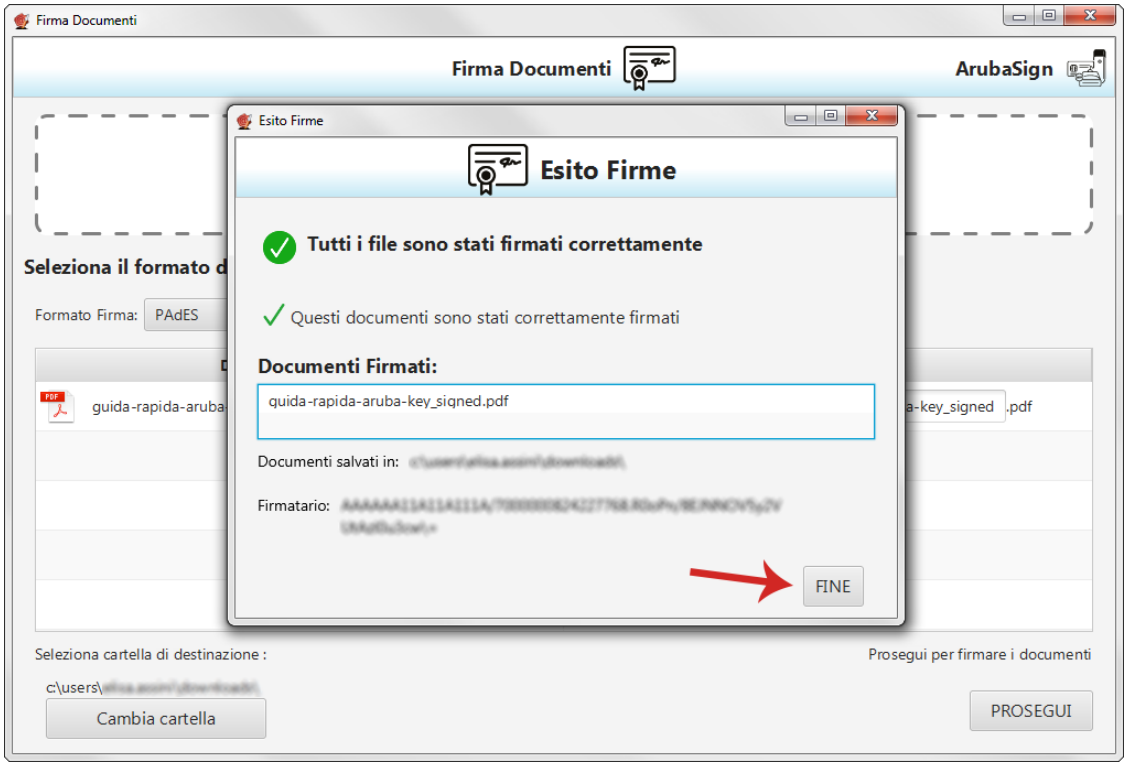


Alla schermata "**Completa Firma Documenti**":

1. Assicurarsi che sia selezionato il **Certificato per la firma digitale** (in formato Cognome - Nome);
6. Inserire il **PIN** di protezione della **Smart Card**. **Nel caso in cui non vi siano Dispositivi di Firma Digitale collegati al pc, il sistema lo indica con apposito messaggio in giallo** "**Nessun Dispositivo trovato**" e, da "**Scelta Formato di Firma**", è possibile impostare la firma con Firma Remota.
2. Da "**Dettagli Certificato**" visionare, qualora desiderato, le caratteristiche e la validità del Certificato stesso;
3. Dichiarare di aver preso visione del documento/i e di essere consapevole della validità ai sensi di legge della Firma apposta;
4. Cliccare su "**Firma**" per concludere il processo:



Al termine dell'operazione si visualizza la seguente schermata che notifica la corretta firma del file. Cliccare su "**FINE**" per chiudere la schermata:



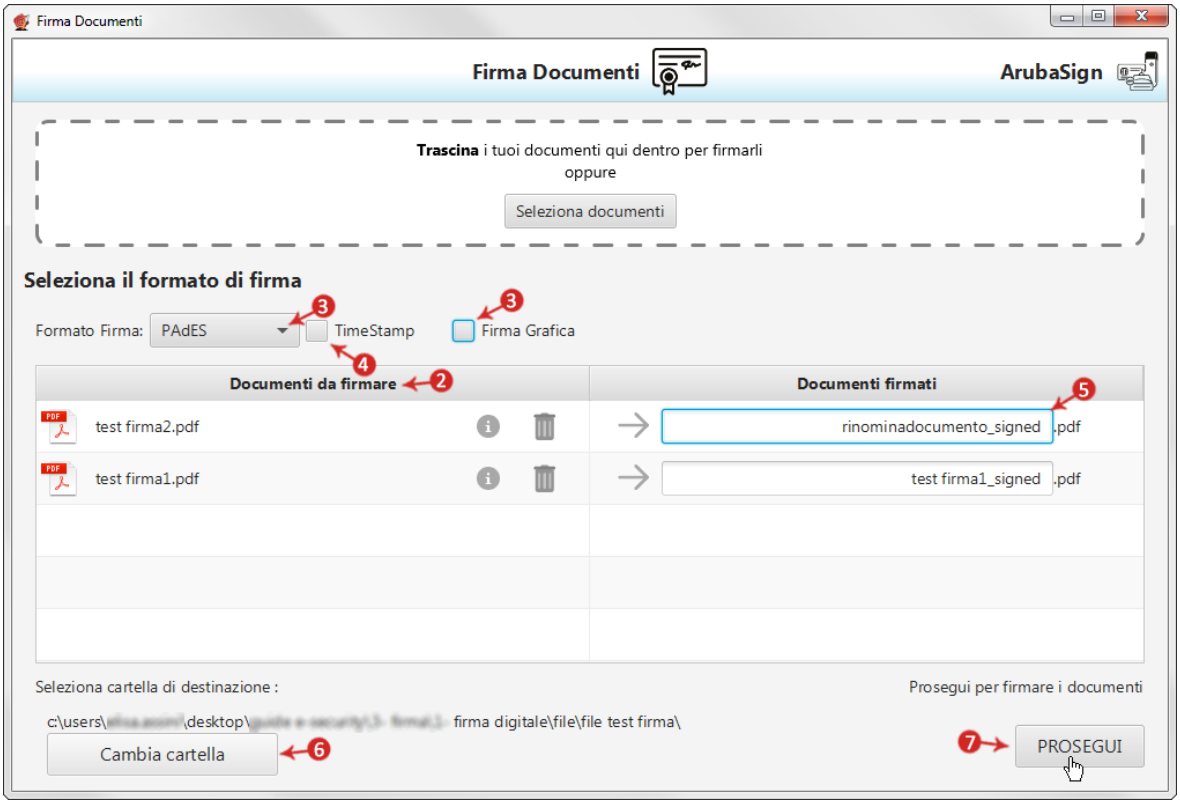
Il documento firmato è salvato nella cartella indicata durante il processo, aggiungendo al **nome originale l'estensione** "**signed.pdf**".

2.8 Apposizione Firma PDF - Invisibile (Firma Digitale)

Il Formato di Firma PAdES è applicabile ai soli file già convertiti in formato .PDF, ed **è visibile solo se nel menù "Firma Documenti" di Aruba Sign sono caricati esclusivamente file con questa estensione**. Se sono caricati più file con estensioni diverse tra loro, la firma **PAdES** non risulta tra i formati selezionabili da menù "**Firma**".

La Firma PAdES - Firma Invisibile consente di evitare l'inserimento dell'"**appearance**" (**campo firma visibile**) all'interno delle pagine del documento firmato. Per **firmare digitalmente uno o più file in formato .PDF in formato PAdES - Firma Grafica** e/o una intera cartella **con Aruba Sign**:

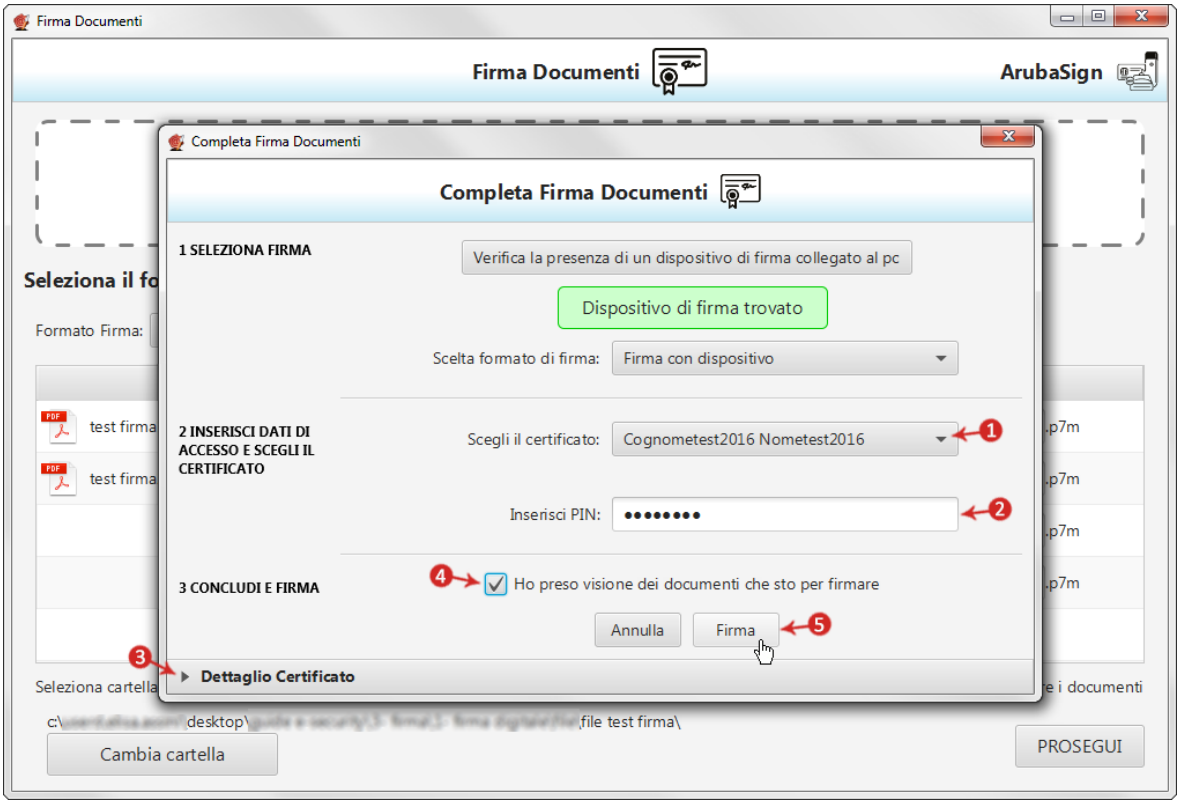
1. **Caricare uno o più documenti e/o una intera cartella**;
2. Il **singolo/i documenti caricati/o** sono visibili all'apposita schermata "**Documenti da firmare**";
3. Dall'apposito menù a tendina "**Formato Firma**" selezionare come tipologia di Firma "**PAdES**" per firmare il file in formato .PDF e rimuovere il Flag su "**Firma Grafica**";
4. Inserire il Flag in corrispondenza della voce "**TimeStamp**" per apporre al file una marcatura temporale nel formato scelto dall'apposito menù a tendina "**Formato TimeStamp**" (lo stesso è visibile solo dopo aver selezionato la voce "**TimeStamp**");
5. Dalla finestra "**Documenti firmati**" rinominare, se desiderato, eventuali file prima di apporre la firma;
6. Da "**Cambia cartella**" verificare che il percorso utilizzato per salvare il/i file firmato/i sia quello desiderato, o selezionarne uno nuovo utilizzando il pulsante indicato;
7. Cliccare su "**Prosegui**" per continuare. Sono firmati tutti i documenti presenti alla finestra "**Documenti da firmare**":



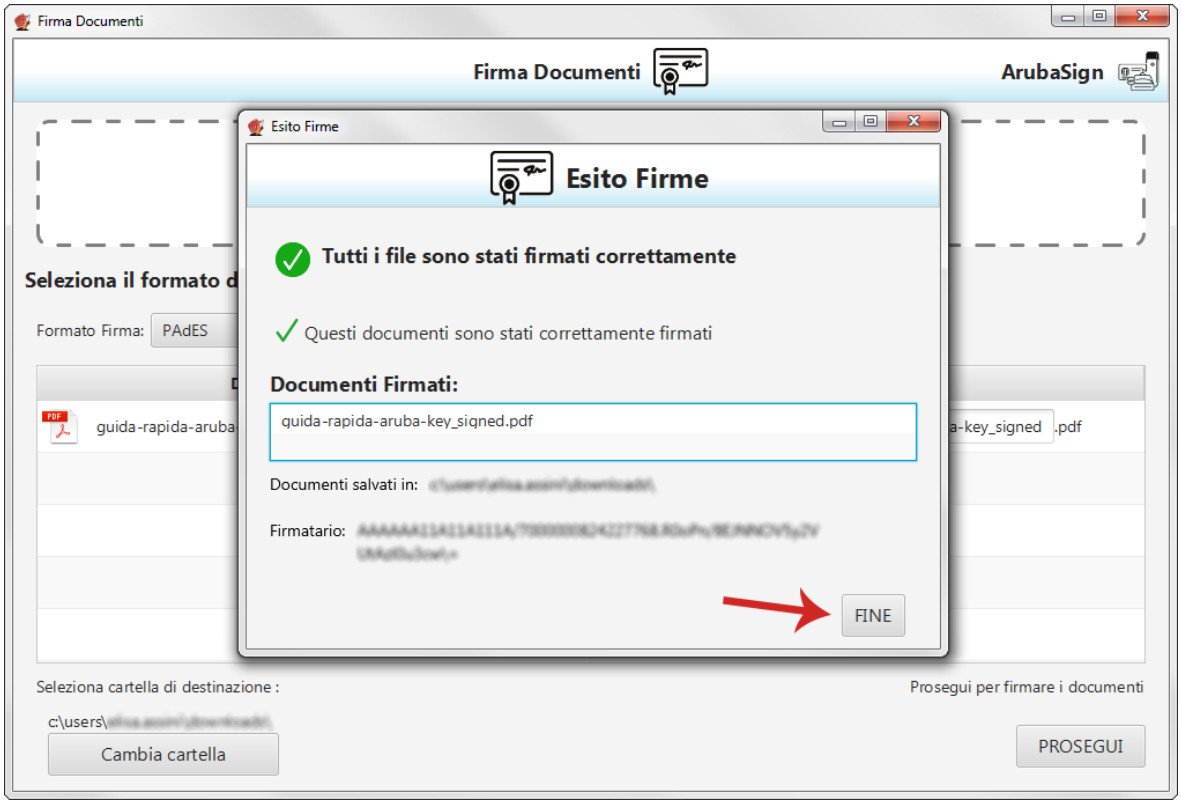
Alla schermata "**Completa Firma Documenti**":

1. Assicurarsi che sia selezionato il **Certificato per la firma digitale** (in formato Cognome - Nome);

2. Inserire il **PIN** di protezione della **Smart Card**. **Nel caso in cui non vi siano Dispositivi di Firma Digitale collegati al pc, il sistema lo indica con apposito messaggio in giallo** "**Nessun Dispositivo trovato**" e, da "**Scelta Formato di Firma**", è possibile impostare la firma con Firma Remota.
3. Da "**Dettagli Certificato**" visionare, qualora desiderato, le caratteristiche e la validità del Certificato stesso;
4. Dichiarare di aver preso visione del documento/i e di essere consapevole della validità ai sensi di legge della Firma apposta;
5. Cliccare su "**Firma**" per concludere il processo:



La Firma Invisibile è apposta automaticamente su tutte le pagine del documento che si intende firmare. In alcun modo il sistema permette di **selezionare le pagine su cui apporre la stessa o di firmarne solo alcune**. Al termine dell'operazione si visualizza la seguente schermata che notifica la corretta firma del file. Cliccare su "**FINE**" per chiudere la schermata:



Il documento firmato viene salvato nella cartella indicata durante il processo, aggiungendo al **nome originale l'estensione** "**signed.pdf**".

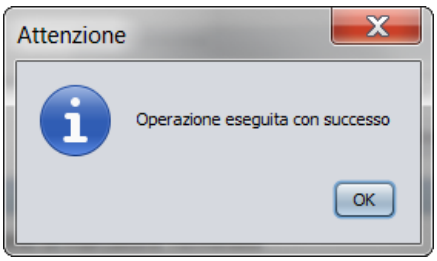
2.9 Apposizione di Marche Temporali (Aruba Sign e Firma Digitale)

Per apporre una marca temporale è sufficiente trascinare il file sopra il pulsante "**Timestamp**":

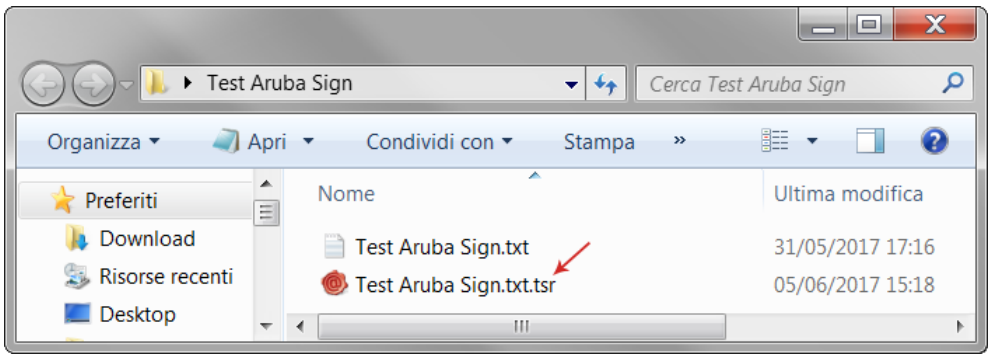
Alla pagina visualizzata:

1. **Selezionare il formato di salvataggio della marca temporale. E' possibile scegliere tra**:
   - **TSR**: Il File creato contiene solo l'impronta del file, non tutto il file, e **la marca temporale in formato TSR è separata dal documento**. Pertanto, per verifica il file TSR, è indispensabile possedere anche il documento sottoposto a marca temporale, e che ha generato il TSR stesso. Se si appone una marca temporale in formato TSR e si desidera inviarla a un destinatario, è necessario inviare anche il documento di origine.
   - **TSD**: Il File creato comprende sia **il file sottoposto a marcatura che la marcatura temporale stessa**. Se si appone una marca temporale in formato TSD e si desidera inviarla a un destinatario, non è necessario inviare anche il documento di origine.
   - **Gli altri dati (password e cartella di destinazione del file) sono indicati automaticamente del sistema**:
     - La **password** è preimpostata a seguito della configurazione dell'Account di marcatura Temporale;
     - Il **percorso di destinazione del File** inserito è la cartella su cui risiede il file originale.
2. Spuntare su "**Richiedi**" per completare l'operazione:

3. Cliccare "**Ok**" al messaggio che notifica la corretta marcatura del file per completare l'operazione:



Il documento è disponibile nella cartella indicata in fase di apposizione della marcatura stessa:

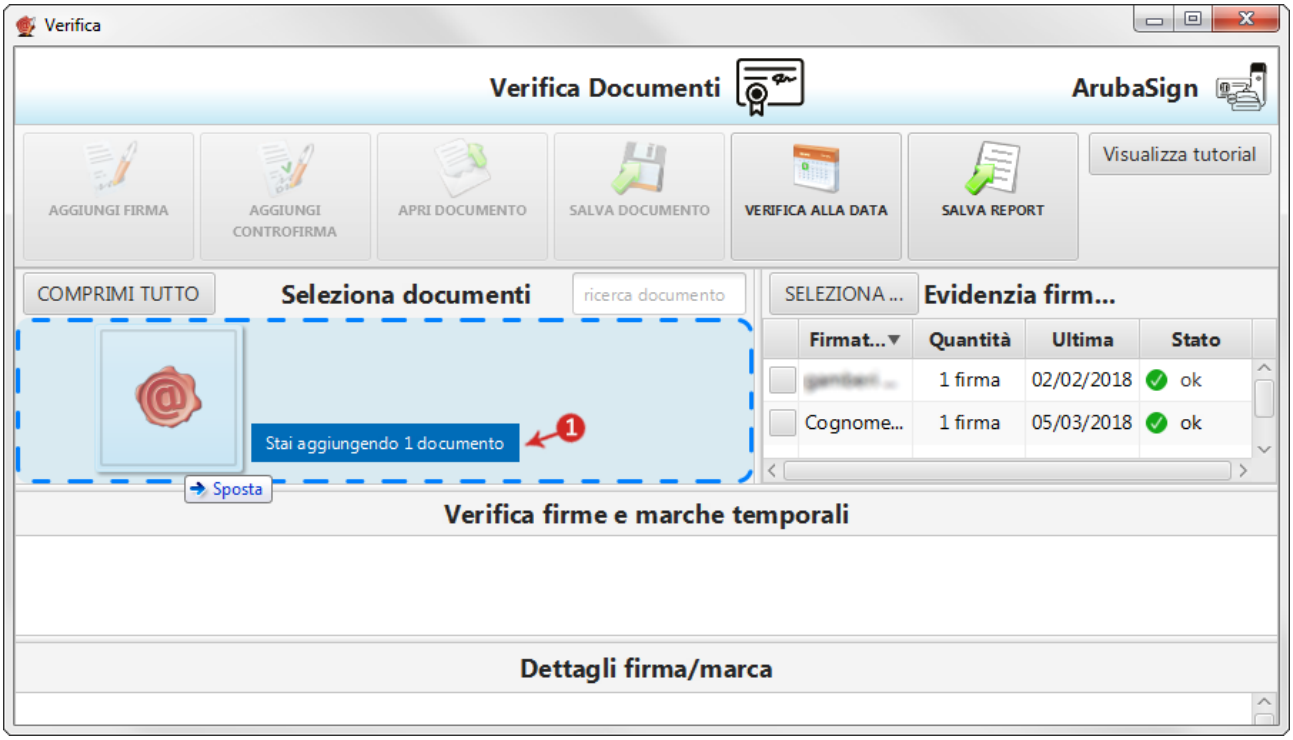


2.10 Verifica di File Firmati (Aruba Sign e Firma Digitale)

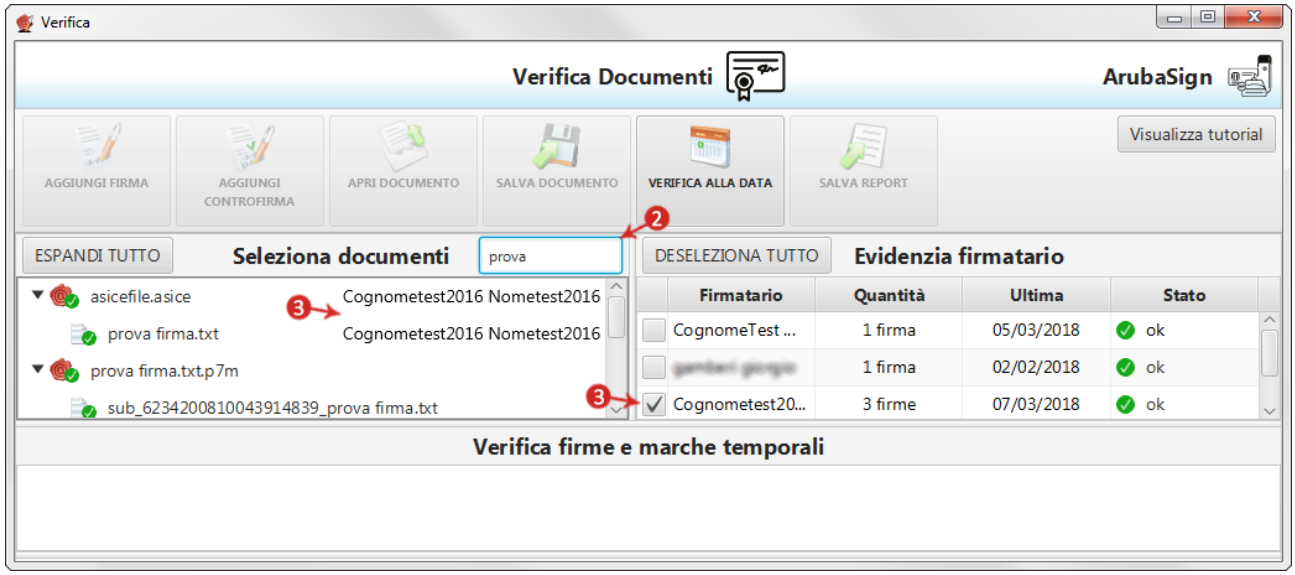
Per verificare uno o più File firmati con Aruba Sign, trascinare il/i documento/i sopra il pulsante "**Verifica**":

Alla schermata visualizzata è possibile:

1. Verificare ulteriori file firmati trascinandoli da locale su "**Seleziona Documenti**":

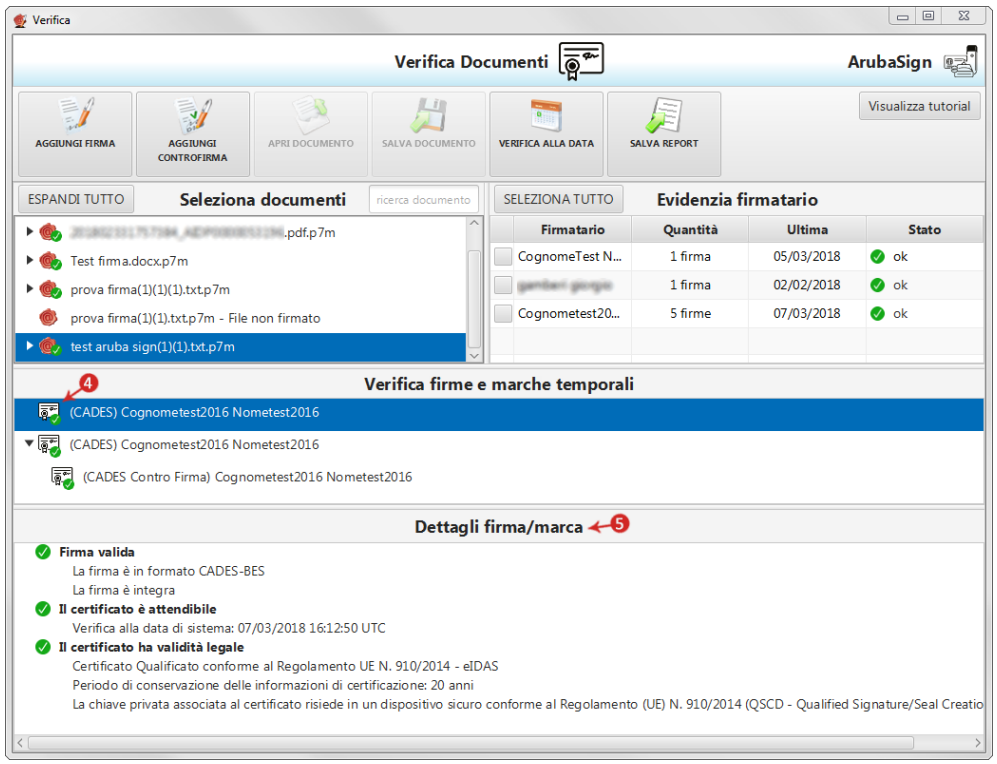


2. Il campo "**Ricerca documento**" consente di ricercare un singolo file tra quelli inseriti su "**Seleziona documenti**";
3. Su "**Evidenzia firmatario**" sono riportati il nome e cognome del/i firmatario/i, il numero di firme che ha apposto, la data dell'ultima apposizione e lo "**Stato**" (esito) della verifica. Per visionare quali sono i documenti firmati da uno specifico firmatario, inserire il flag in corrispondenza del soggetto interessato, il nome appare a fianco dei singoli file che ha firmato presenti nell'area "**Seleziona documenti**":

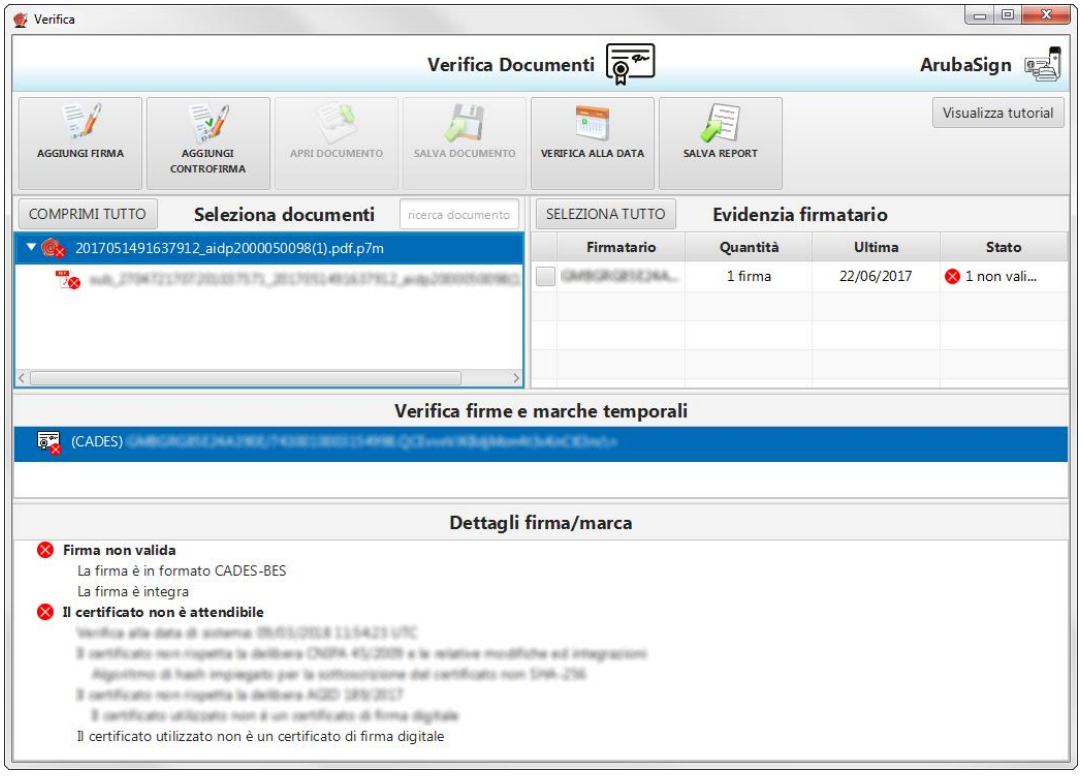


Una volta selezionato/evidenziato un singolo documento:

4. Su "**Verifica firme e marche temporali**" sono visibili le firme presenti all'interno del file;
5. Da "**Dettagli firma/marca**" è possibile verificare la validità della firma apposta, in particolare:
   - **Firma valida**
     Attesta il formato della firma e che il documento non è stato alterato dopo la firma;
   - **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**
     Attesta che il certificato del sottoscrittore è un certificato di Firma Digitale qualificato:



Se la verifica ha esito positivo si visualizza una spunta verde in corrispondenza di tutti i campi. Nel caso in cui si riscontrino una o più anomalie, ad esempio per Certificato scaduto o non attendibile, il sistema indica il messaggio di errore "**Firma KO**", attestante che **sono stati portati a termine tutti i controlli previsti per la verifica della validità della Firma apposta**, **ma qualcuno non è andato a buon fine**, come da immagine esemplificativa sottostante:

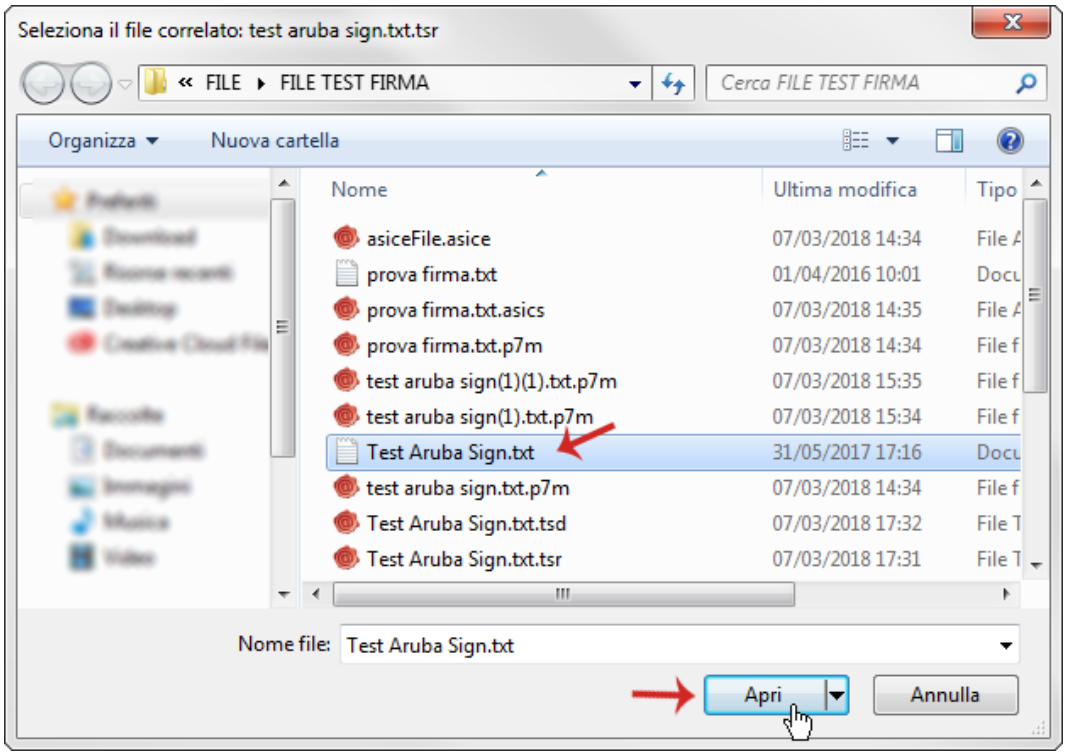


2.11 Verifica di marca temporale in Formato TSR (Aruba Sign e Firma Digitale)

Una marca temporale in formato **TSR è separata dal documento su cui è apposta**. Pertanto, per verifica il file TSR, è indispensabile possedere anche il documento sottoposto a marca temporale, e che ha generato il TSR stesso.

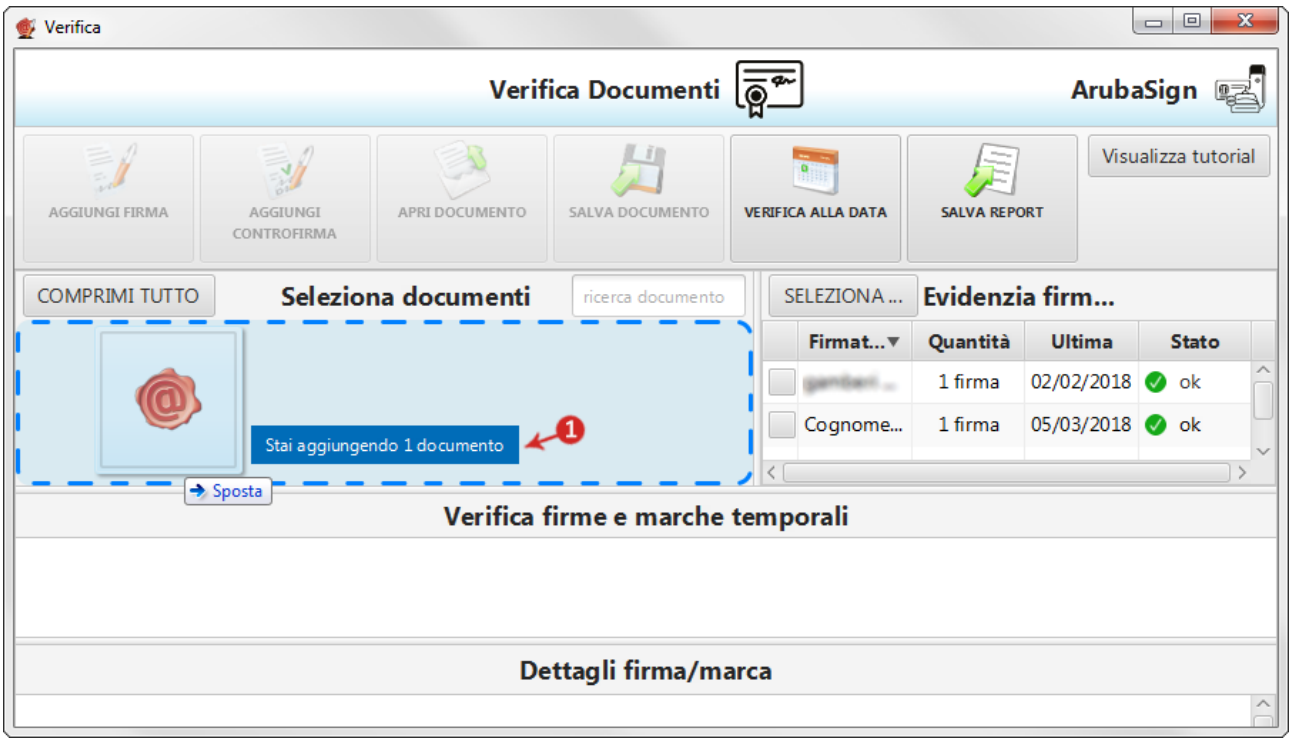
Per procedere trascinare la **Marca Temporale da verificare** sopra il pulsante "**Verifica**":

Il software esegue l'associazione "**Marca Temporale**" → "**File Marcato**" e **chiede di aprire il file associato alla marca**. Selezionare da locale il file associato alla marca stessa, quindi spuntare su "**Apri**":

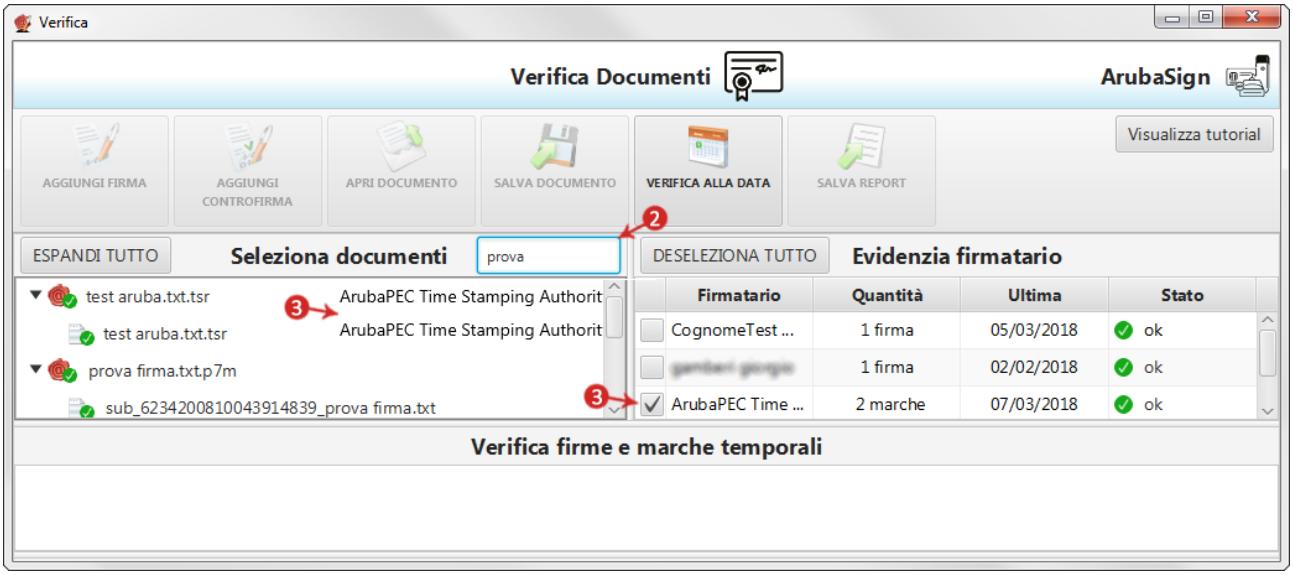


Alla schermata visualizzata è possibile:

1. Verificare ulteriori file firmati trascinandoli da locale su "**Seleziona Documenti**":

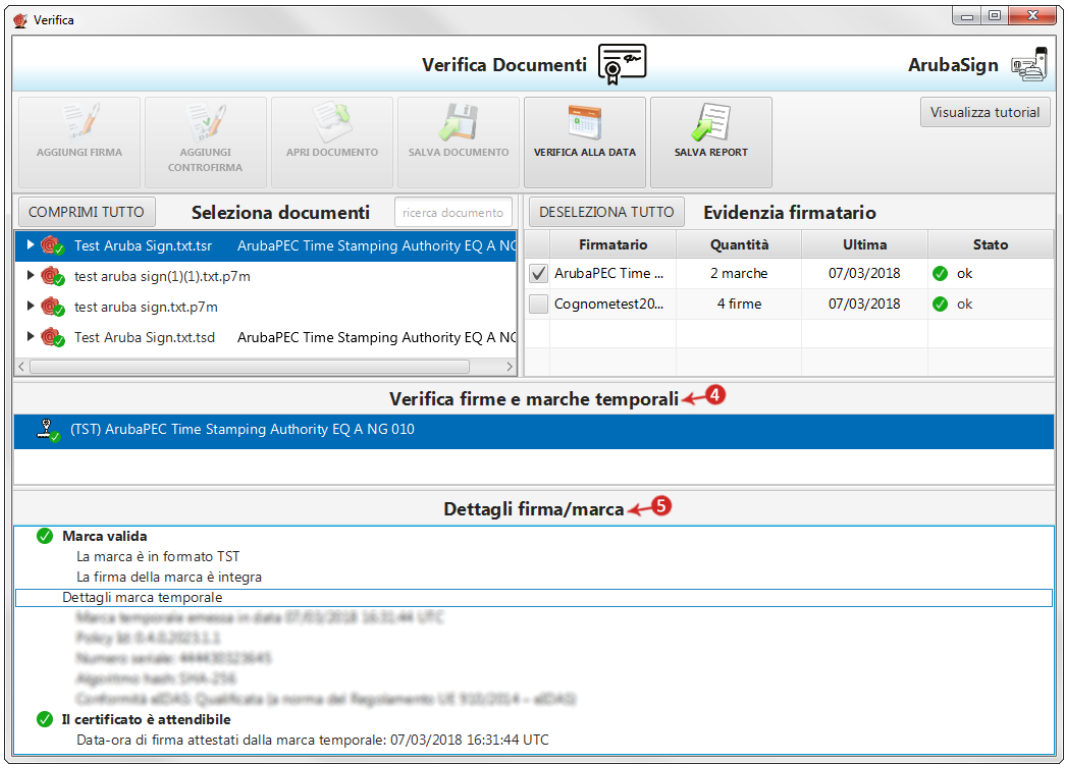


2. Il campo "**Ricerca documento**" consente di ricercare un singolo file tra quelli inseriti su "**Seleziona documenti**";
3. Su "**Evidenzia firmatario**" sono riportati i dettagli della marca apposta e il numero di documenti marcati, la data dell'ultima apposizione e lo "**Stato**" (esito) della verifica. Per visionare quali sono i documenti marcati tra quelli presenti nell'area "**Seleziona documenti**", inserire il flag in corrispondenza della marca stessa, il dettaglio appare a fianco dei singoli file:

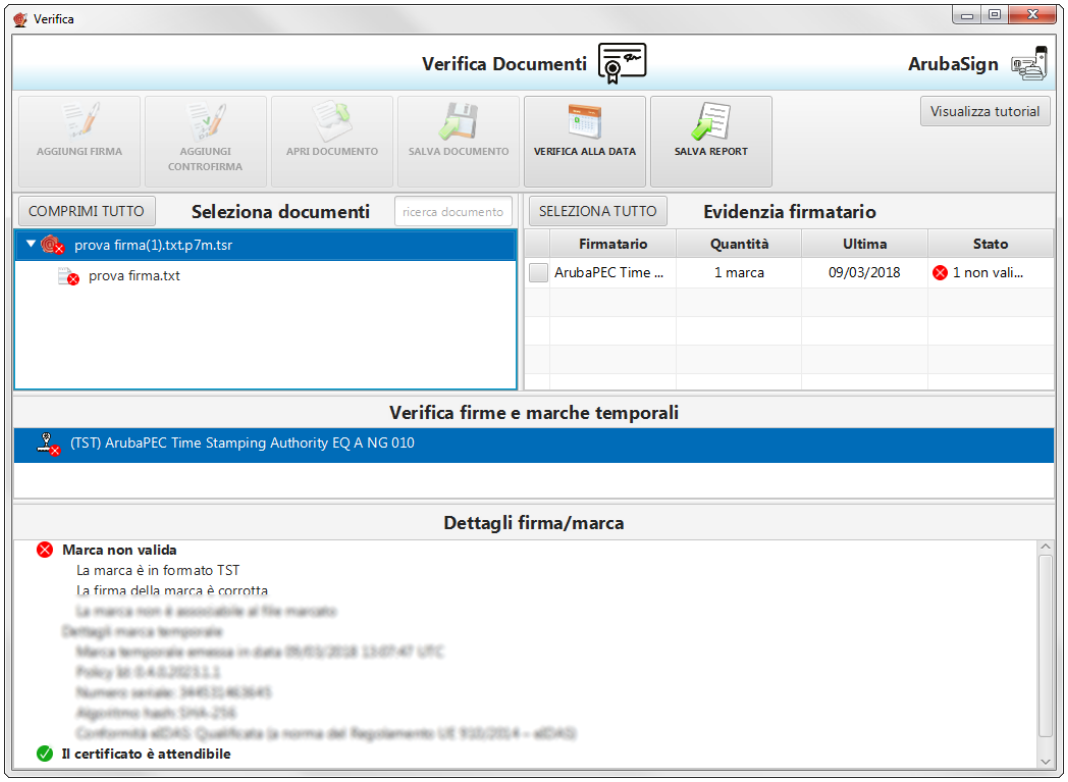


Una volta selezionato/evidenziato un singolo documento:

4. Su "**Verifica firme e marche temporali**" sono visibili le marche presenti all'interno del file;
5. Da "**Dettagli firma/marca**" è possibile verificare la validità della firma apposta, in particolare:
   - **Marca valida**
     Indica che la marca temporale è integra ed è correttamente associata al documento selezionato, nella parte "**Dettagli marca temporale**", sono riportate le specifiche della marca stessa;
   - **Il certificato è attendibile**
     Attesta che la Marca Temporale è rilasciata da un'Autorità di Certificazione inclusa nell'Elenco Pubblico dei Certificatori:



Se la verifica ha esito positivo si visualizza una spunta verde in corrispondenza di tutti i campi. Nel caso in cui si riscontrino una o più anomalie, ad esempio per Certificato scaduto o non attendibile, il sistema indica il messaggio di errore "**Marca KO**", attestante che **sono stati portati a termine tutti i controlli previsti per la verifica della validità della Firma apposta**, **ma qualcuno non è andato a buon fine**, come da immagine esemplificativa sottostante:



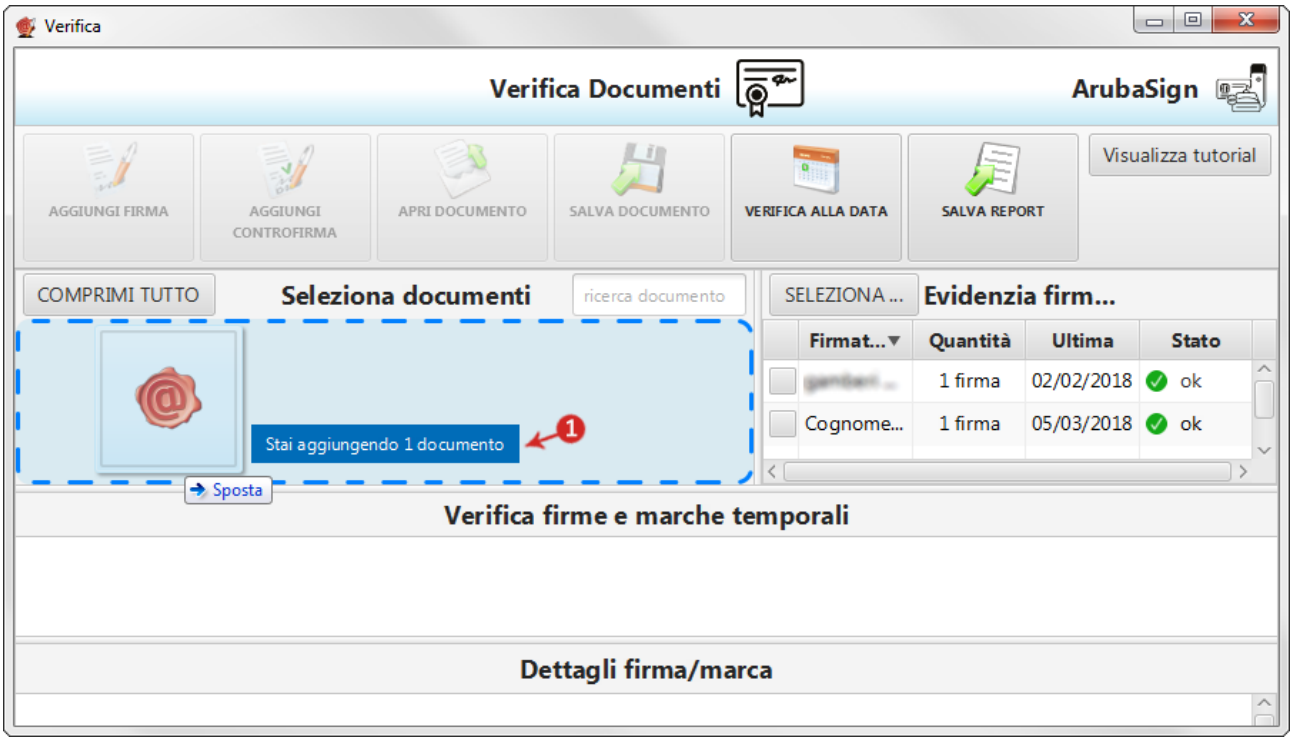
2.12 Verifica di marca temporale in Formato TSD (Aruba Sign e Firma Digitale)

Una marca temporale in formato **TSD** comprende sia **il file sottoposto a marcatura che la marcatura temporale stessa**. Pertanto, per verifica il file **TSD**, non è indispensabile possedere anche il documento sottoposto a marca temporale, e che ha generato il TSD stesso.

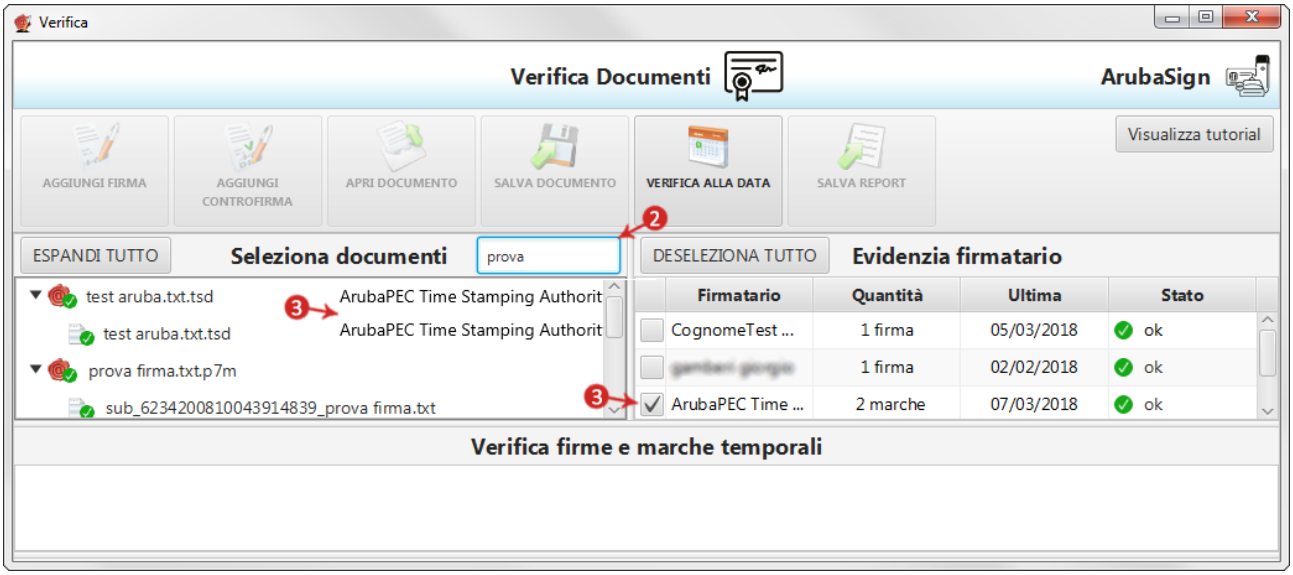
Per procedere trascinare la **Marca Temporale da verificare** sopra il pulsante "**Verifica**":

Alla schermata visualizzata è possibile:

1. Verificare ulteriori file firmati trascinandoli da locale su "**Seleziona Documenti**":

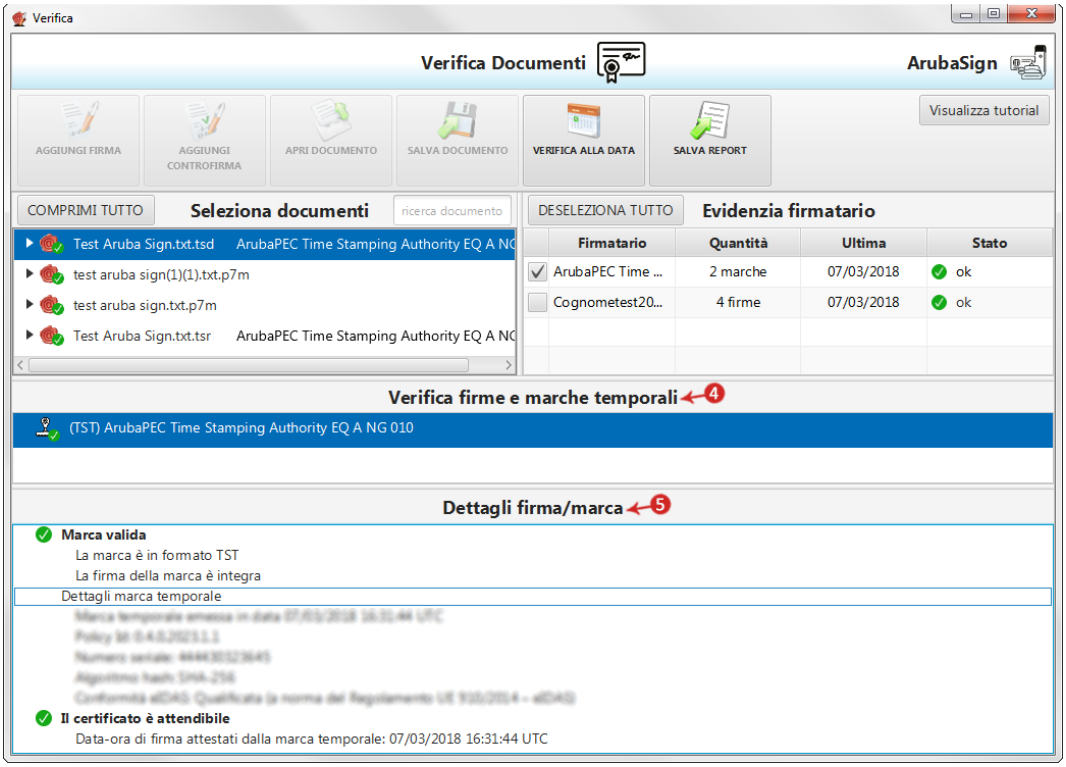


2. Il campo "**Ricerca documento**" consente di ricercare un singolo file tra quelli inseriti su "**Seleziona documenti**";
3. Su "**Evidenzia firmatario**" sono riportati i dettagli della marca apposta e il numero di documenti marcati, la data dell'ultima apposizione e lo "**Stato**" (esito) della verifica. Per visionare quali sono i documenti marcati tra quelli presenti nell'area "**Seleziona documenti**", inserire il flag in corrispondenza della marca stessa, il dettaglio appare a fianco dei singoli file:

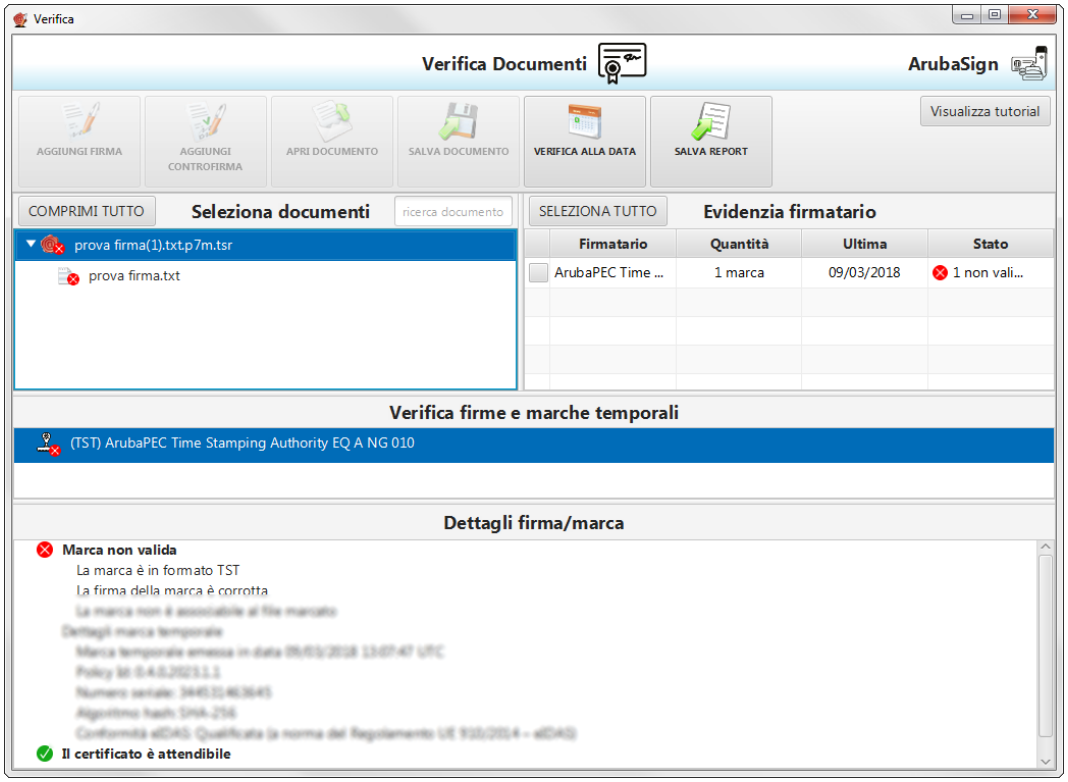


Una volta selezionato/evidenziato un singolo documento:

4. Su "**Verifica firme e marche temporali**" sono visibili le marche presenti all'interno del file;
5. Da "**Dettagli firma/marca**" è possibile verificare la validità della firma apposta, in particolare:
   - **Marca valida**
     Indica che la marca temporale è integra ed è correttamente associata al documento selezionato, nella parte "**Dettagli marca temporale**", sono riportate le specifiche della marca stessa;
   - **Il certificato è attendibile**
     Attesta che la Marca Temporale è rilasciata da un'Autorità di Certificazione inclusa nell'Elenco Pubblico dei Certificatori:



Se la verifica ha esito positivo si visualizza una spunta verde in corrispondenza di tutti i campi. Nel caso in cui si riscontrino una o più anomalie, ad esempio per Certificato scaduto o non attendibile, il sistema indica il messaggio di errore "**Marca KO**", attestante che **sono stati portati a termine tutti i controlli previsti per la verifica della validità della Firma apposta**, **ma qualcuno non è andato a buon fine**, come da immagine esemplificativa sottostante:



3. Principali funzioni barra di menù Aruba Sign (Firma Digitale)

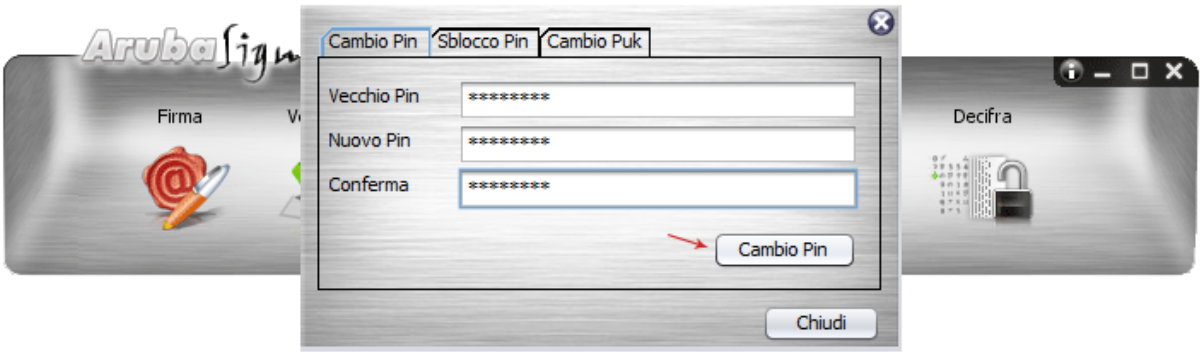
3.1 Menù "Gestione Carta" Aruba Sign – Firma Digitale

3.1.1 Cambio PIN SMART CARD

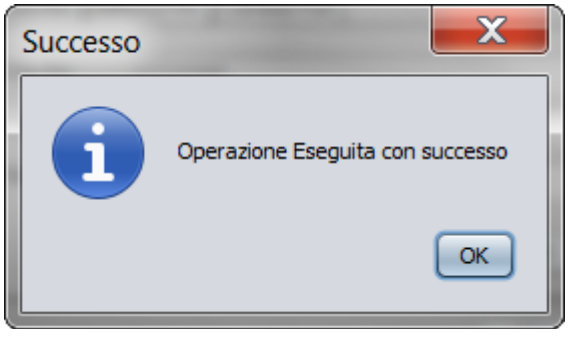
Per cambiare il **codice PIN** della Smart Card, cliccare sul pulsante "**Gestione Carta**" del Software Aruba Sign:

Al Tab "**Cambio PIN**" inserire:

- PIN precedente;
- Impostare e confermare un nuovo codice PIN. **E' obbligatorio l'utilizzo** di soli caratteri numerici (0,1,2,3,4,5,6,7,8 e 9). Non sono ammessi caratteri alfabetici (a,b,A,B, etc..). Ai fini della sicurezza si consiglia l'utilizzo di codici PIN composti almeno da 5 numeri;
- Spuntare su "**Cambio PIN**":



Se l'operazione è eseguita correttamente si visualizza la seguente schermata di conferma:



Di seguito una **esemplificazione degli errori che possono verificarsi**:

1. **ARUBA SIGN - PIN Errato pericolo blocco carta**

Il messaggio di errore indica che alla voce "**Vecchio PIN**" **si è inserito un codice errato**. L'inserimento di **PIN non validi per tre volte consecutive**, può causare il Blocco del PIN e della carta, in caso di smarrimento anche del PUK.

2. **ARUBA SIGN - PIN Bloccato**

Il messaggio di errore **indica che alla voce "Vecchio PIN" si è inserito un codice errato per tre volte consecutive**, **provocando il blocco del PIN stesso**. Per cambiarlo, eseguire la procedura indicata al paragrafo 11.2.

3.1.2 Sblocco PIN SMART CARD

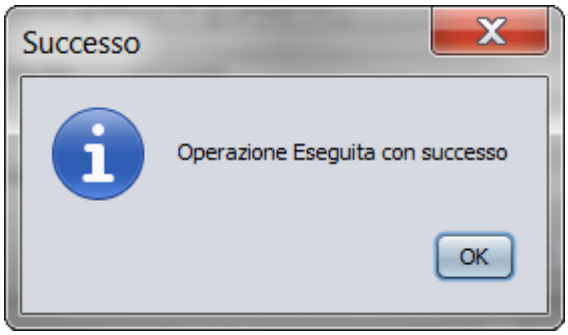
Per sbloccare il **codice PIN** della Smart Card, cliccare sul pulsante "**Gestione Carta**" del Software Aruba Sign:

Al Tab "**Sblocco PIN**" inserire:

- Codice PUK della Smart Card;
- Impostare e confermare un nuovo codice PIN. **E' obbligatorio l'utilizzo** di soli caratteri numerici (0,1,2,3,4,5,6,7,8 e 9). Non sono ammessi caratteri alfabetici (a,b,A,B, etc..). Ai fini della sicurezza si consiglia l'utilizzo di codici PIN composti almeno da 5 numeri;

- Spuntare su "**Sblocca PIN**":

Se l'operazione è eseguita correttamente si visualizza la seguente schermata di conferma:



Di seguito una **esemplificazione degli errori che possono verificarsi**:

1. **ARUBA SIGN - PUK Errato pericolo blocco carta**

Il messaggio di errore indica che alla voce "**PUK**" o "**Vecchio PUK**" **si è inserito un codice errato**. L'inserimento di tre codici PUK consecutivi non validi causa il Blocco definitivo della Smart Card stessa.

2. **ARUBA SIGN - PUK Bloccato**

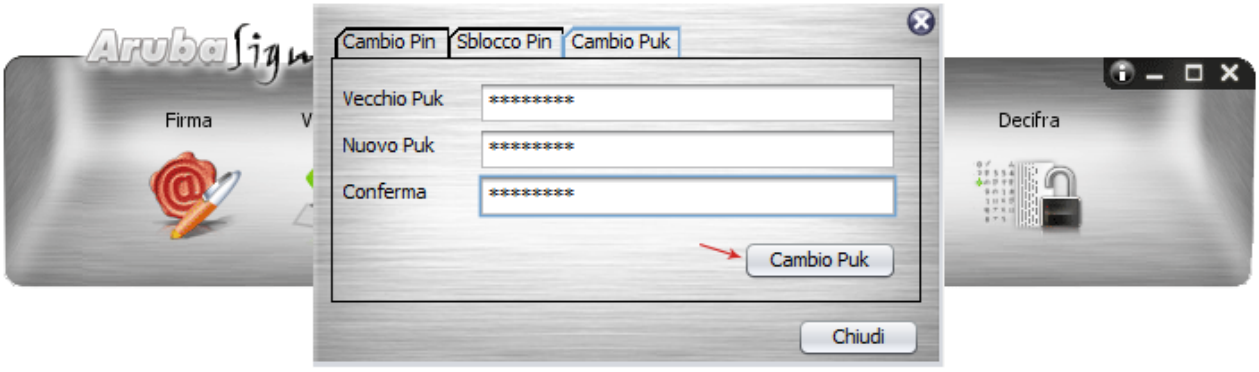
Il messaggio di errore indica che alla voce "**PUK**" o "**Vecchio PUK**" **si è inserito un codice errato per tre volte consecutive**, **provocando il blocco del PUK stesso e la revoca definitiva della Smart Card**. In questo caso chiedere la revoca dei certificati attuali e acquistare una nuova carta.

3.1.3 Cambio PUK SMART CARD

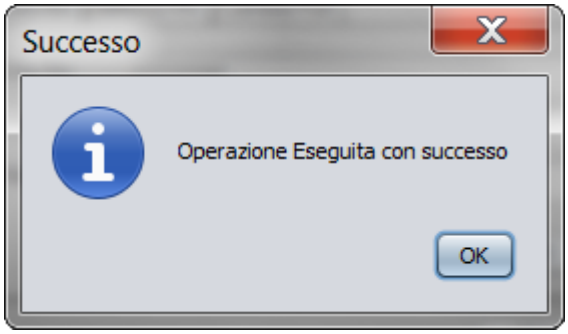
Per cambiare il **codice PUK** della Smart Card, cliccare sul pulsante "**Gestione Carta**" del Software Aruba Sign:

Al Tab "**Cambio PUK**" inserire:

- Vecchio Codice PUK della Smart Card;
- Impostare e confermare un nuovo codice PUK. **E' obbligatorio l'utilizzo** di soli caratteri numerici (0,1,2,3,4,5,6,7,8 e 9). In alcun modo sono ammessi caratteri alfabetici (a,b,A,B, etc..). Ai fini della sicurezza si consiglia l'utilizzo di codici PUK composti almeno da 8 numeri;
- Spuntare su "**Cambio PUK**":



Se l'operazione è eseguita correttamente si visualizza la seguente schermata di conferma:



Di seguito una **esemplificazione degli errori che possono verificarsi**:

1. **ARUBA SIGN - PUK Errato pericolo blocco carta**

Il messaggio di errore indica che alla voce "**PUK**" o "**Vecchio PUK**" **si è inserito un codice errato**. L'inserimento di tre codici PUK consecutivi non validi causa il Blocco definitivo della Smart Card stessa.

2. **ARUBA SIGN - PUK Bloccato**

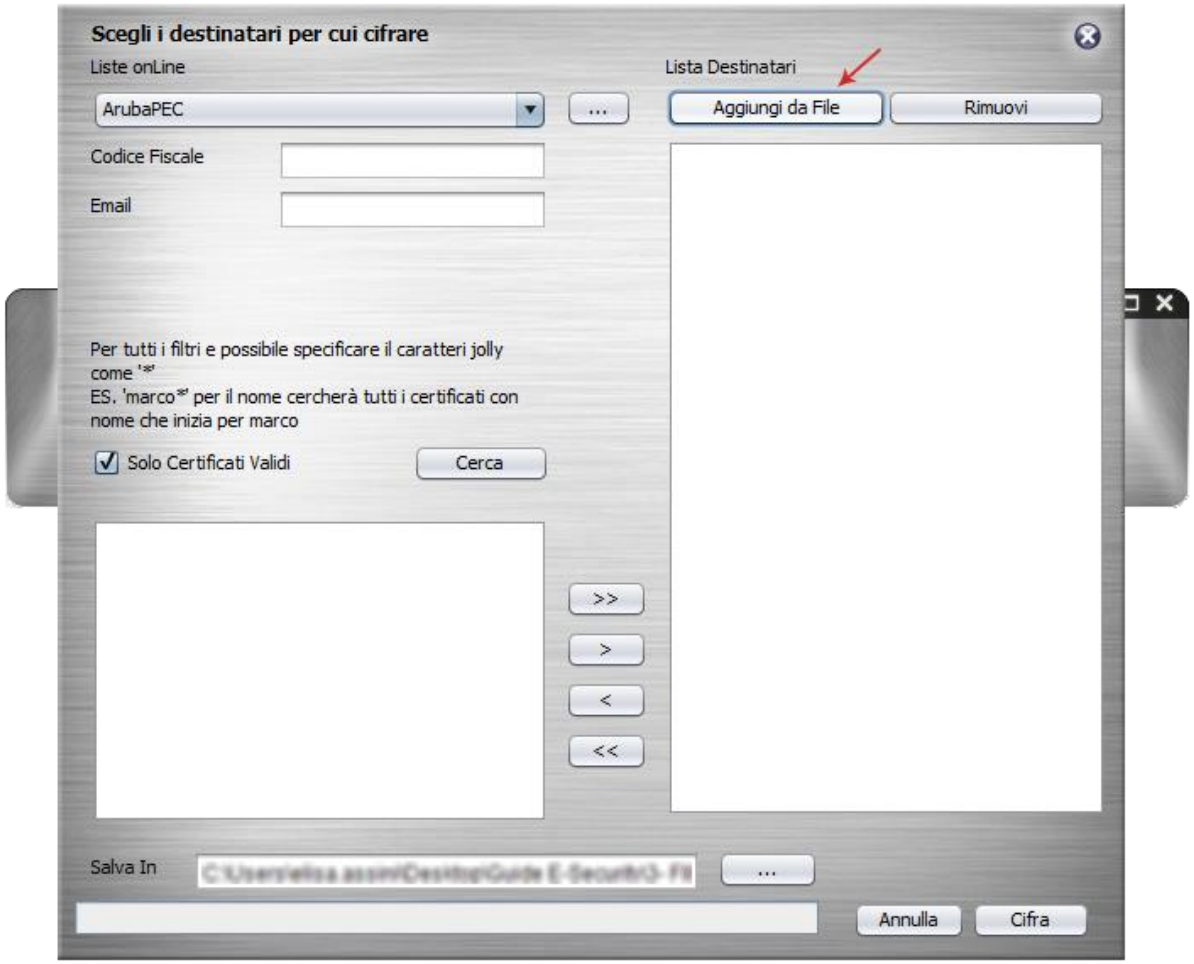
Il messaggio di errore indica che alla voce "**PUK**" o "**Vecchio PUK**" **si è inserito un codice errato per tre volte consecutive**, **provocando il blocco del PUK stesso e la revoca definitiva della Smart Card**. In questo caso chiedere la revoca dei certificati attuali e acquistare una nuova carta.

3.2 Menù "Cifra" e "Decifra" Aruba Sign – Firma Digitale

3.2.1 Cifrare un file con software di Firma Digitale Aruba Sign

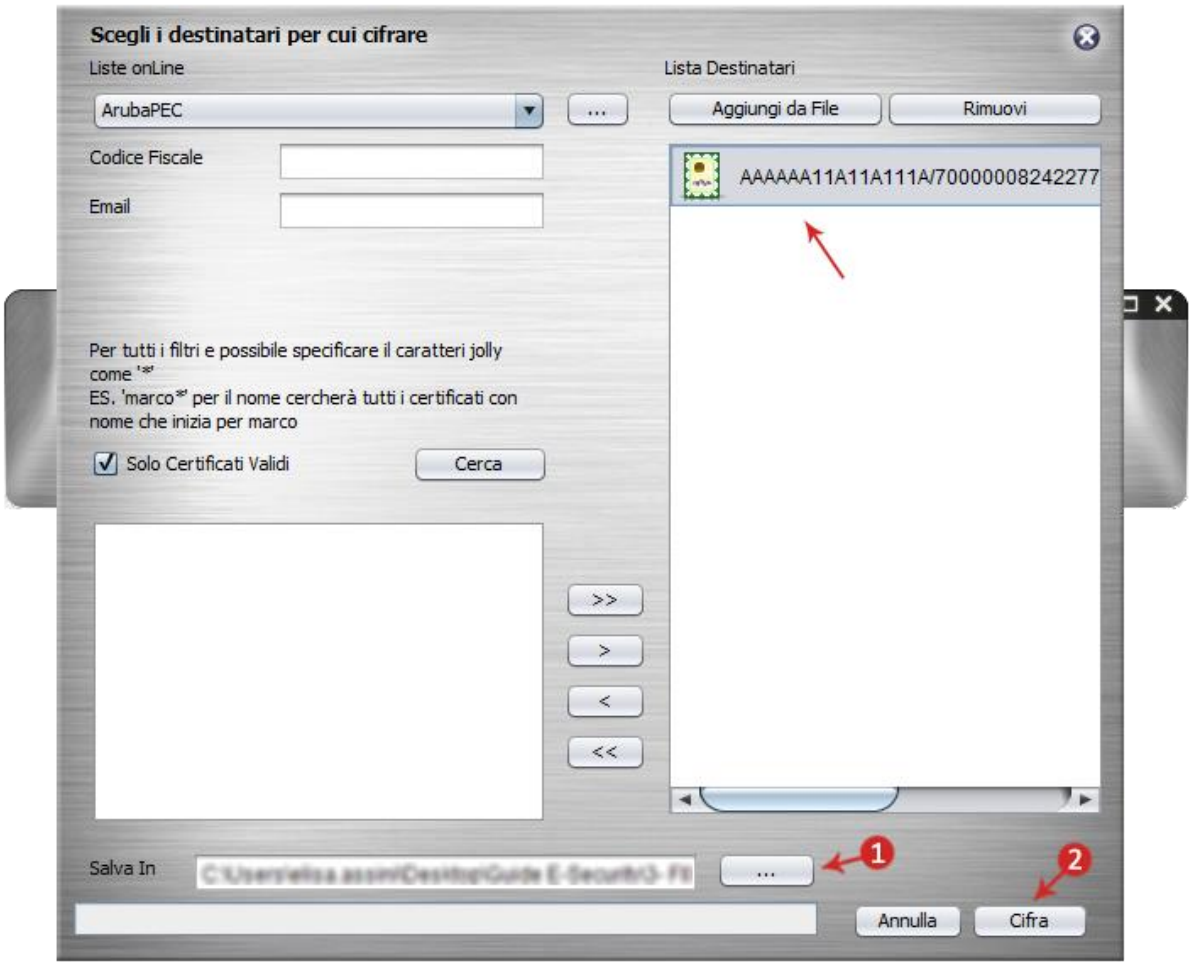
Per cifrare un File con Software di Firma Aruba Sign, esportare in locale il **Certificato di Autenticazione CNS** in formato .cer, quindi trascinare il file che si desidera cifrare sopra il pulsante "**Cifra**":

Alla finestra visualizzata utilizzare il pulsante "**Aggiungi da File**" per caricare il certificato esportato e presente nel proprio PC:

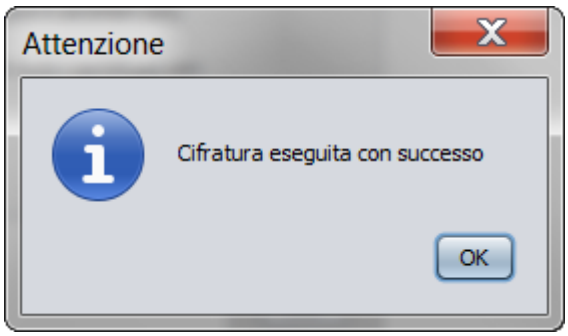


Una volta caricato il certificato, lo stesso è visibile nella finestra sottostante al pulsante "**Aggiungi da File**". Per procedere:

1. Verificare la correttezza del percorso su cui salvare il file cifrato, o selezionare una nuova cartella utilizzando il pulsante indicato in figura;
2. Spuntare su "**Cifra**":



Il programma di cifratura crea un file con estensione **.p7e** che **include il file originale**. **Se l'operazione è eseguita correttamente si visualizza la seguente schermata di conferma** e il documento è visibile nella cartella di destinazione indicata in fase di creazione. Cliccare su "**Ok**":



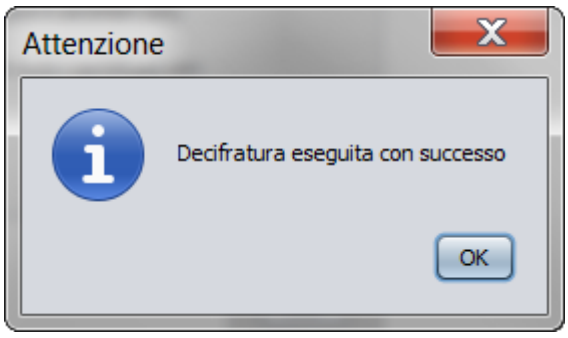
3.2.2 Decifrare un file con software di Firma Digitale Aruba Sign

Per decifrare un File con Software di Firma Digitale Aruba Sign, trascinare il file cifrato (formato **.p7e**) sopra il pulsante **"Decifra"**:

Arubasign verifica che nella **Smart Card sia presente** almeno uno dei **certificati indicati nella fase di cifratura**.
Alla schermata visualizzata:

1. lasciare spuntata l'opzione **"Con Smart Card"**;
2. Inserire il **PIN** della Smart Card stessa;
3. Verificare la correttezza del percorso su cui salvare il file cifrato, o selezionare una nuova cartella utilizzando il pulsante indicato in figura;
4. Spuntare su "**Ok**" per procedere:

Se l'operazione è stata eseguita correttamente si visualizza la seguente schermata di conferma. Cliccare su "**Ok**" per chiuderla:



3.3 Configurazione Proxy http Aruba Sign

Per utilizzare il **Software Aruba Sign in una rete protetta da Proxy** aprire il menù "**Opzioni e Parametri**" di Aruba Sign:

Quindi allo specifico Tab "**Proxy HTTP**" togliere la spunta dalla voce "**Individua proxy in maniera automatica**", impostare i relativi parametri e salvarli. Di seguito un esempio di configurazione:

Proxy Url: 192.168.1.1
Proxy Port: 8080
Proxy User: Nome utente
Proxy Password: Password

Cliccare su "**Salva**" per completare l'operazione.

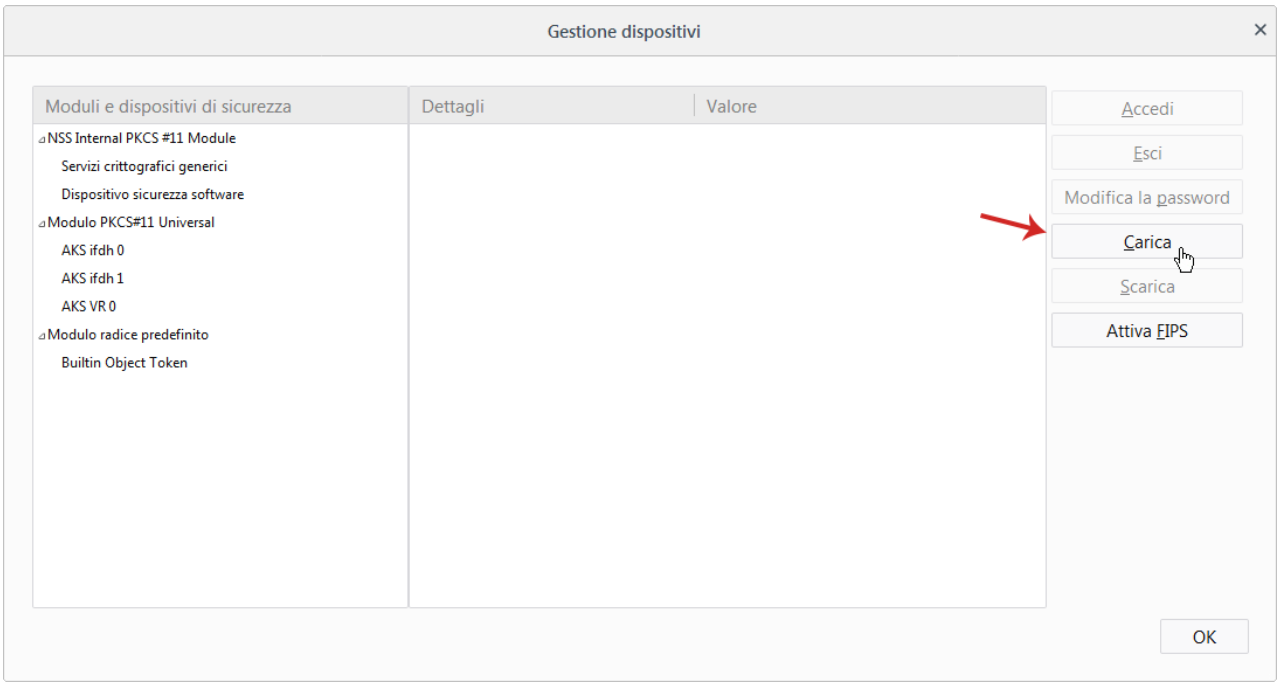
Qualora non siano disponibili i dati relativi a una delle due sezioni HTTP o LDAP ad esempio nel caso in cui la rete non supporti entrambe le configurazioni, procedere solo con la creazione relativa alla tipologia di Proxy supportata.

4. Import Certificato Aruba Sign (PC)

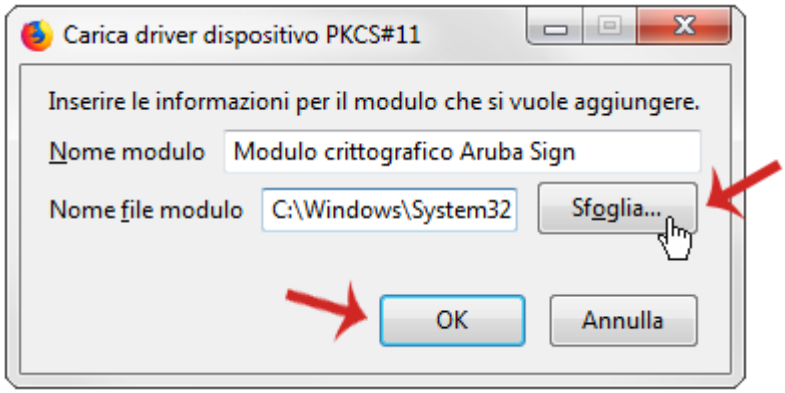
4.1 "Import Certificato" su Mozilla Firefox Firma Digitale (PC)

La funzione "**Import Certificato**" per Aruba Sign è automatica su **Internet Explorer e Google Chrome**. Di seguito le modalità per **eseguire manualmente** l'**Import Certificato su Mozilla Firefox e abilitare l'utilizzo del Browser installato localmente su PC a cui è collegato il dispositivo**. Per procedere:

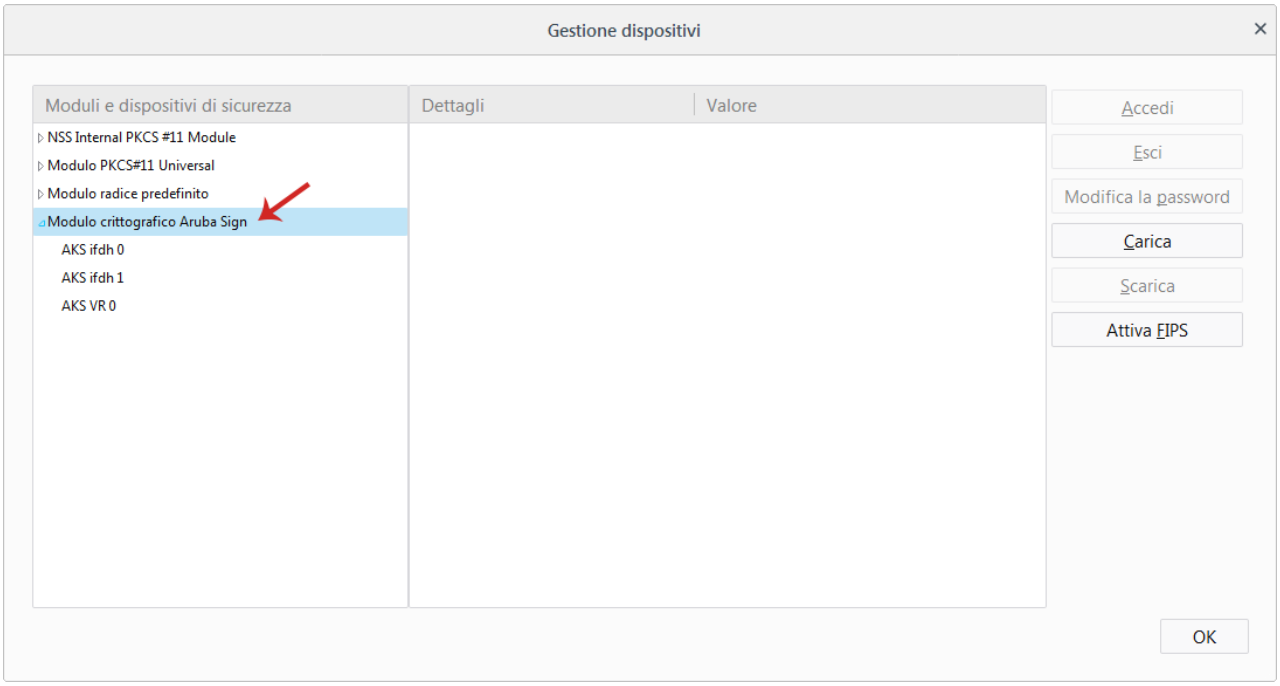
1. Avviare **Mozilla Firefox**;
2. Dall'icona "**Strumenti**" in alto a destra, scegliere "**Opzioni**";
3. Da "**Privacy e sicurezza**" in alto a sinistra, scorrere fino a visualizzare "**Certificati**" in fondo alla pagina, quindi selezionare il tab "**Dispositivi di Sicurezza**";
4. Dal Pannello "**Gestione Dispositivi**", cliccare sul pulsante "**Carica**":



5. Al Tab "**Carica dispositivo PKCS#11**" visualizzato, procedere come di seguito indicato:
   - Su "**Nome modulo**" indicare una stringa descrittiva che identifichi il modulo crittografico che si sta aggiungendo;
   - Utilizzare "**Sfoglia**" per spostarsi all'interno della directory C:\WINDOWS\system32 e selezionare il file **bit4xpki.dll**;
   - Una volta selezionato, verificare che il campo Nome file modulo sia valorizzato con il percorso della libreria;
   - Cliccare su "**Ok**" per proseguire:



6. Verificare che all'interno della finestra "**Gestioni dispositivi**" compaia il nuovo modulo appena aggiunto quindi cliccare su "**Ok**":



Terminata la procedura di import manuale dei certificati è terminata ed è **possibile effettuare l'accesso tramite il certificato CNS**. **Nel caso in cui i certificati di firma e CNS vengano importati all'interno dello Store di Mozilla FireFox** in alcun modo cliccare sul pulsante "**Elimina**". L'azione potrebbe causare l'eliminazione dei certificati CNS e Firma digitale all'interno della Smart Card e l'impossibilità di recuperarli.

4.2 Verifica corretta importazione Certificato Aruba Sign (PC)

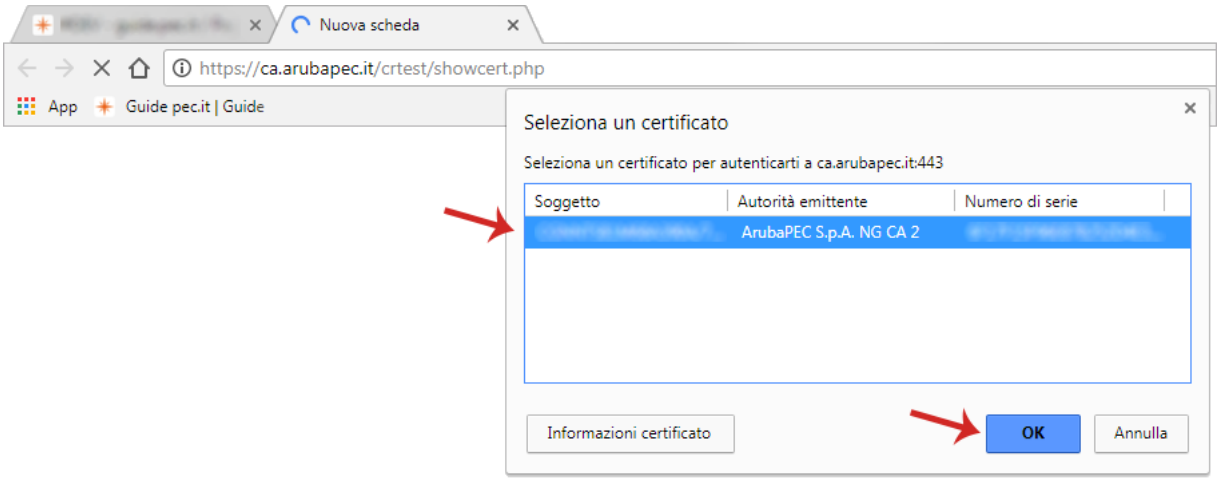
Una volta completata la procedura di "**Import Certificato**", per verificare la corretta installazione del Certificato, procedere come di seguito indicato:

4.2.1 Verifica corretta importazione Certificato Aruba sign su Google Chrome

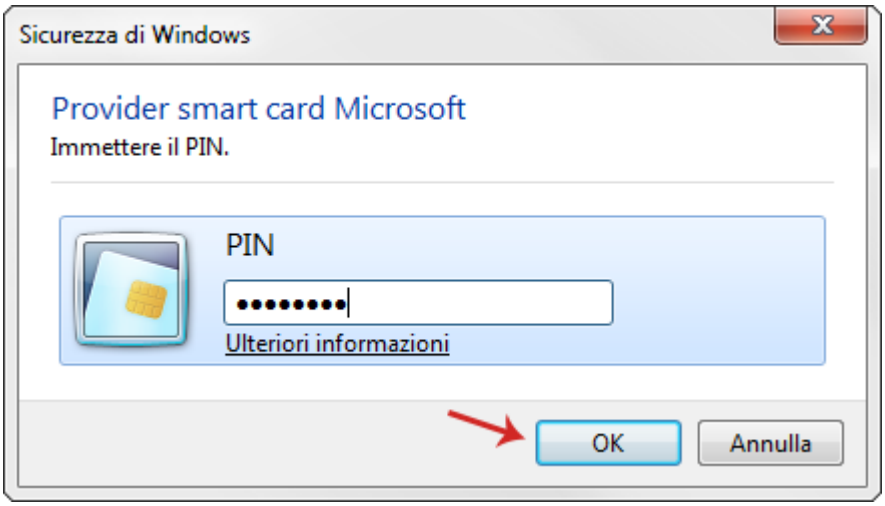
Verificare corretta importazione del Certificato da https://ca.arubapec.it/crtest/showcert.php

Questa procedura consente l'accesso a un sito di test con il proprio certificato CNS. Per procedere:

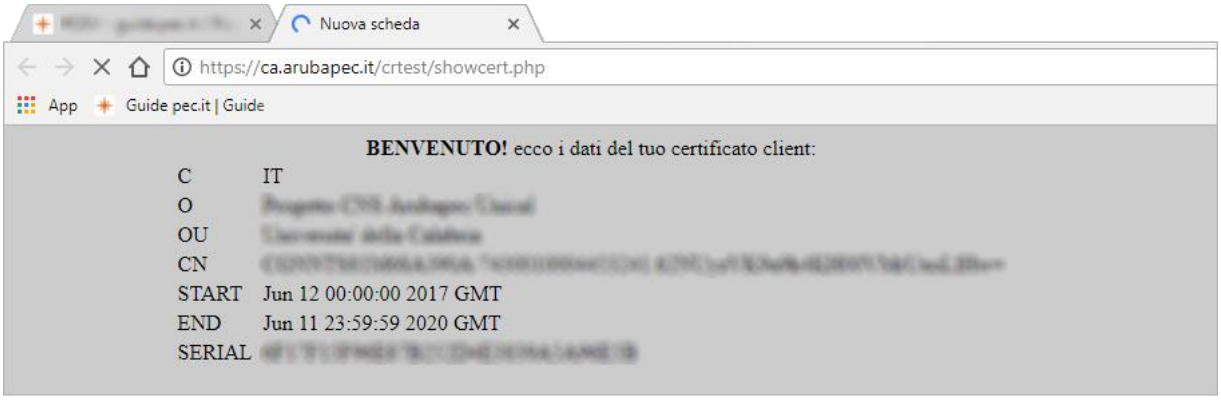
1. Avviare **Google Chrome**;
2. Collegarsi al link https://ca.arubapec.it/crtest/showcert.php;
3. **Selezionare il certificato da utilizzare per l'accesso** e cliccare su "**Ok**":



4. Inserire il PIN della Smart Card e cliccare su "**Ok**":



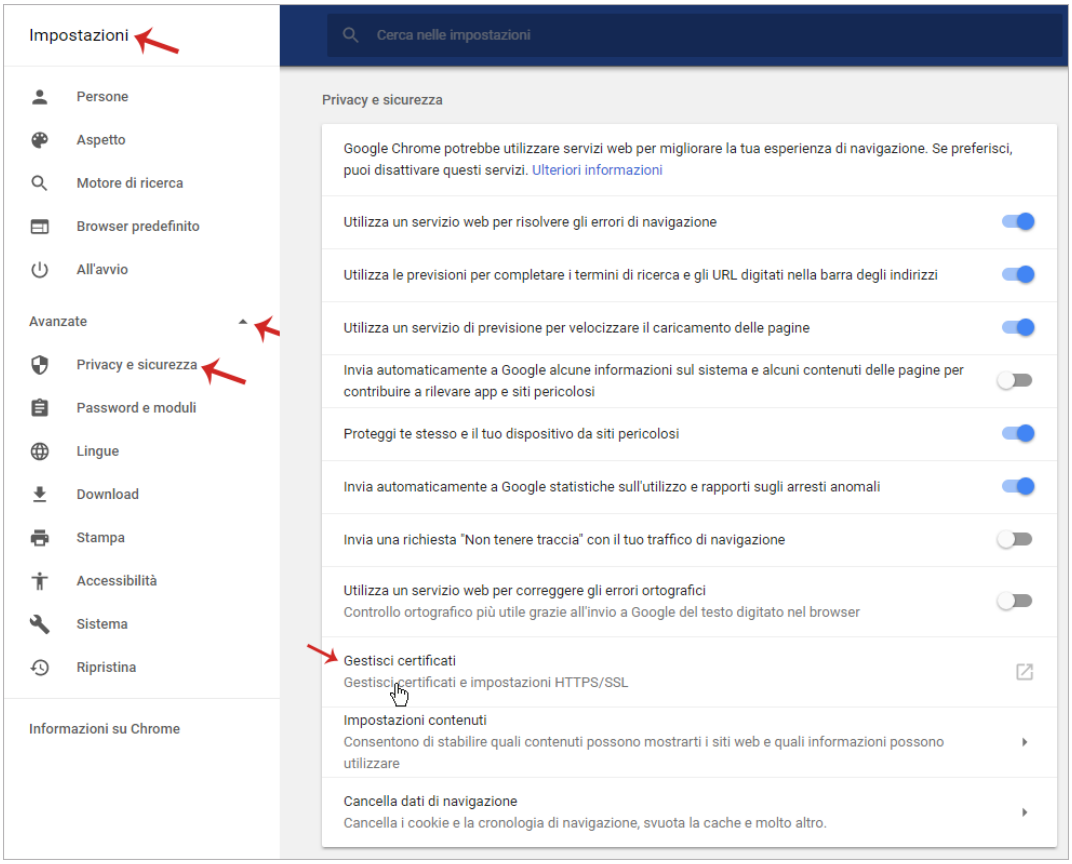
5. Verificare che il Browser mostri la pagina riepilogativa contenente i dati del certificato usato per l'accesso sicuro:



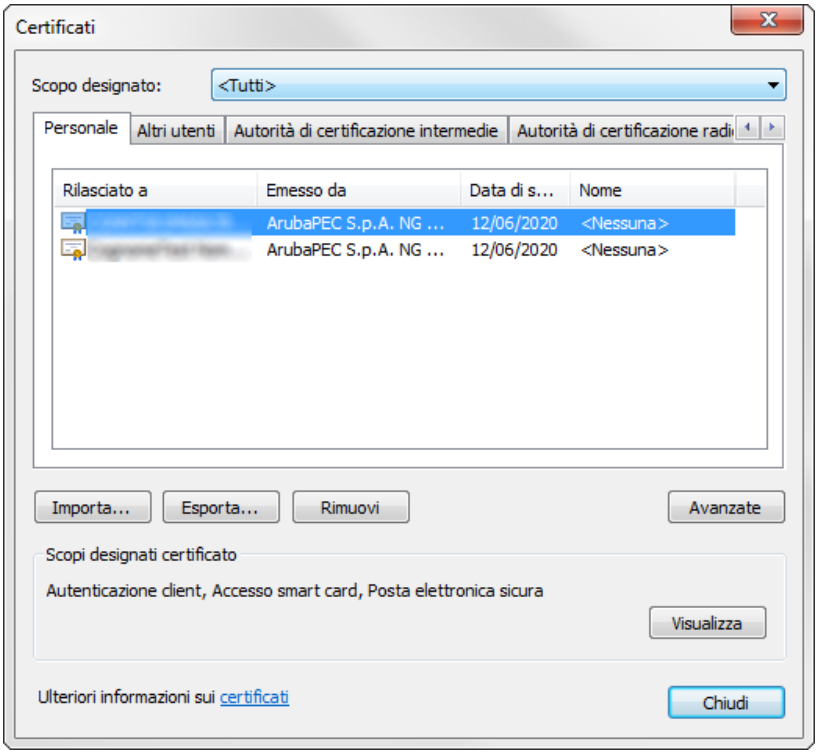
Verificare la corretta importazione del Certificato da "Strumenti" di Google Chrome:

Questa procedura consente di verificare l'effettivo caricamento dei Certificati, e quindi il corretto esito della procedura di "**Import Certificato**". Per procedere:

1. Avviare **Google Chrome**;
2. Selezionare dal menù in alto a destra in alto a destra l'icona "**Opzioni**";
3. Dal menù in alto a destra "**Impostazioni**" selezionare "**Avanzate > Privacy e Sicurezza > Gestisci Certificati**":



4. Col kit di Firma Digitale collegato al PC, deve comparire in elenco il Codice Fiscale relativo al proprio Certificato:

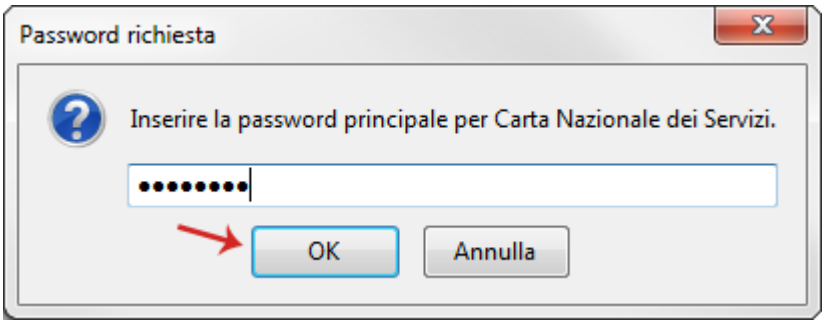


4.2.2 Verifica corretta importazione Certificato Aruba Sign su Mozilla Firefox

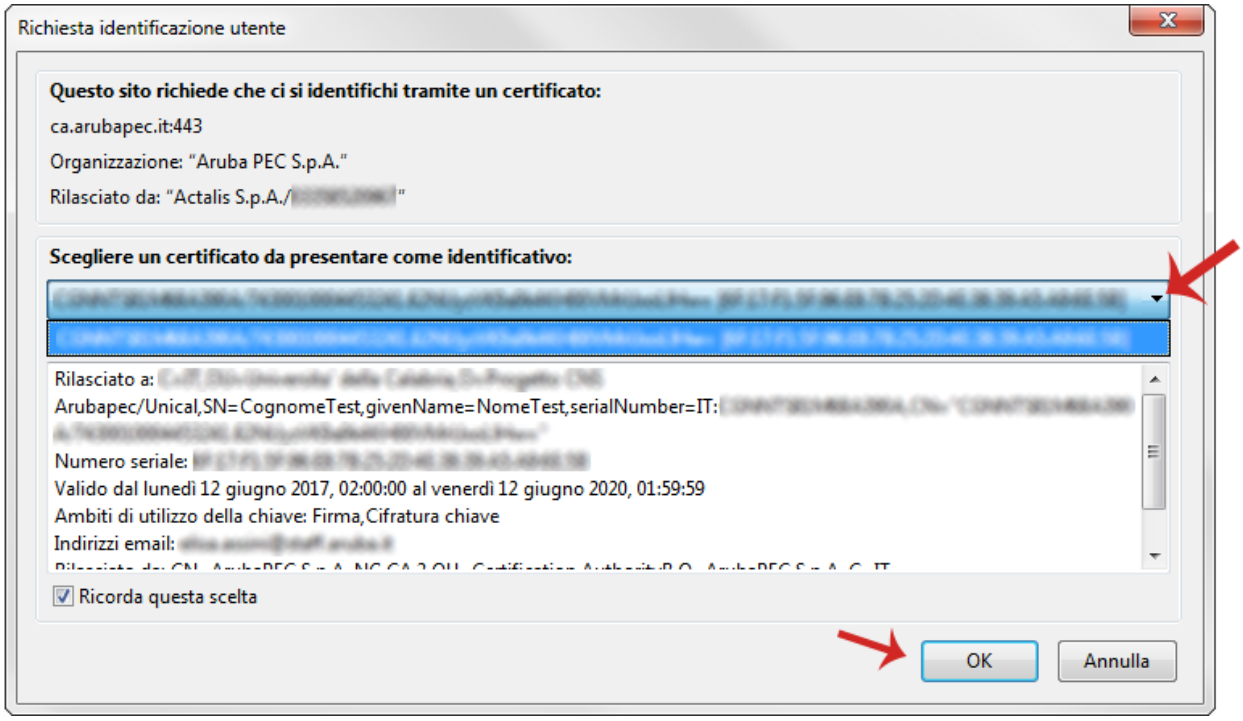
Verificare corretta importazione del Certificato da https://ca.arubapec.it/crtest/showcert.php

Questa procedura consente l'accesso a un sito di test con il proprio certificato CNS. Per procedere:

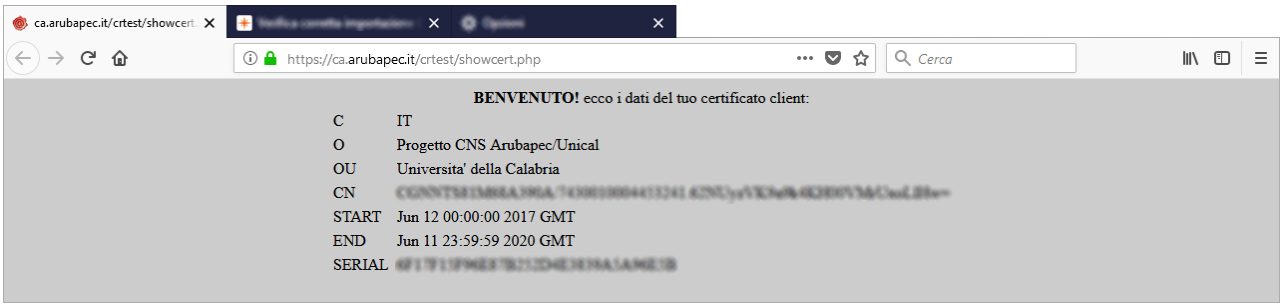
1. Avviare **Mozilla Firefox**;
2. Collegarsi al link https://ca.arubapec.it/crtest/showcert.php;
3. Inserire il PIN della carta e spuntare su "**Ok**":



4. Alla finestra "**Richiesta Identificazione Utente**" selezionare il **certificato da utilizzare per l'accesso** e cliccare su "**Ok**":



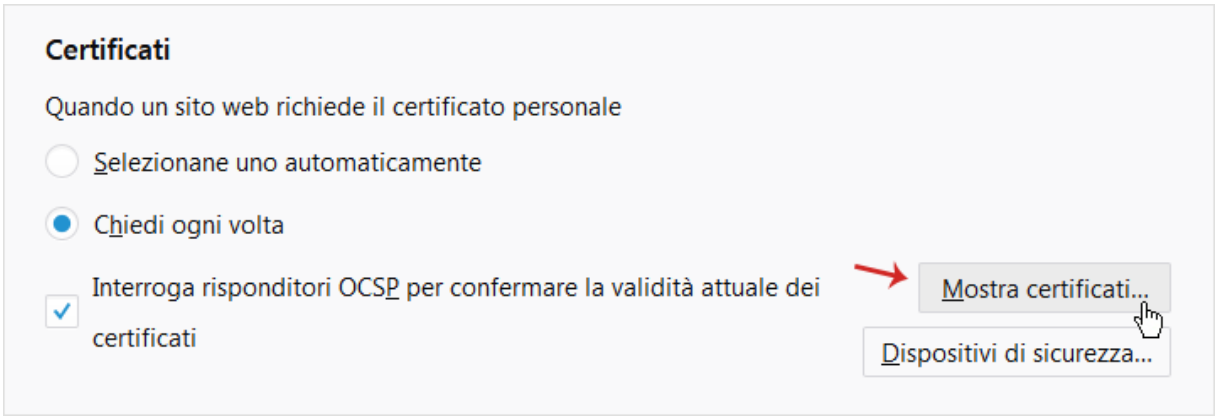
5. Verificare che il Browser mostri la pagina riepilogativa contenente i dati del certificato usato per l'accesso sicuro:



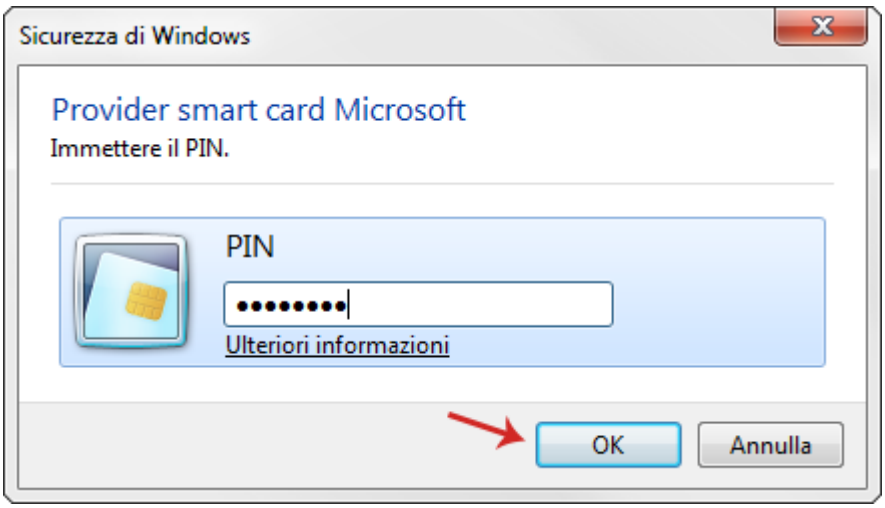
Verificare la corretta importazione del Certificato da "Strumenti" di Mozilla Firefox:

Questa procedura consente di verificare l'effettivo caricamento dei Certificati, e quindi il corretto esito della procedura di "**Import Certificato**". Per procedere:

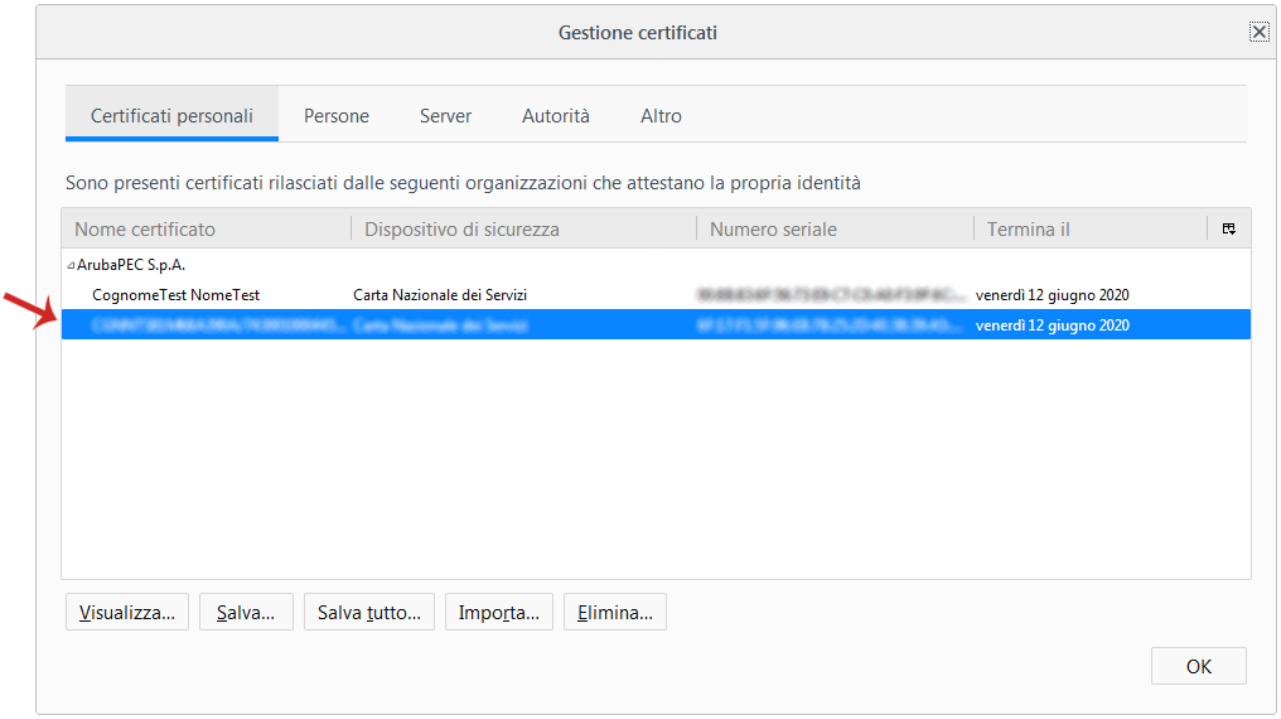
1. Avviare **Mozilla Firefox**;
2. Dall'icona "**Strumenti**" in alto a destra, scegliere "**Opzioni**";
3. Da "**Privacy e sicurezza**" in alto a sinistra, scorrere fino a visualizzare "**Certificati**" in fondo alla pagina, quindi selezionare il tab "**Mostra Certificati**":



4. Inserire il PIN della Smart Card e cliccare su "**Ok**":

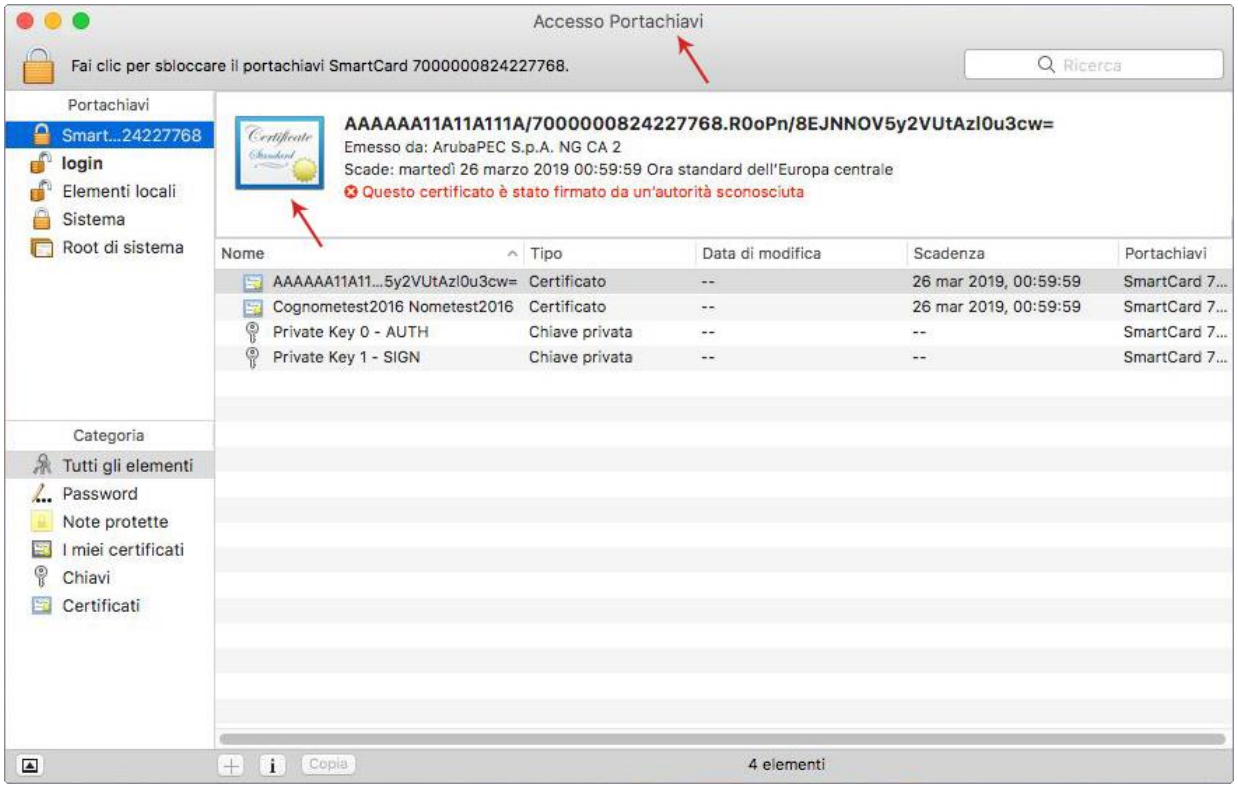


5. Dal Tab "**Certificati Personali**" verificare che siano visibili i certificati installati su Aruba Key:



4.3 "Import Certificato" con Aruba Sign (MAC)

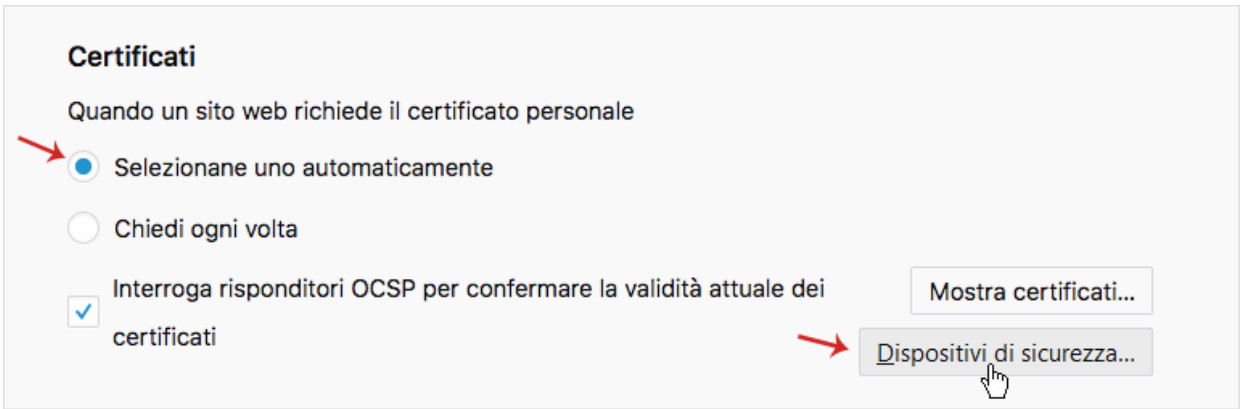
La funzione "**Import Certificato**" su MAC per **Aruba Sign è automatica**. Una volta installato il Software, i certificati sono importati nel "**Portachiavi**" del MAC. Il certificato è visualizzato come da immagine esemplificativa sottostante:



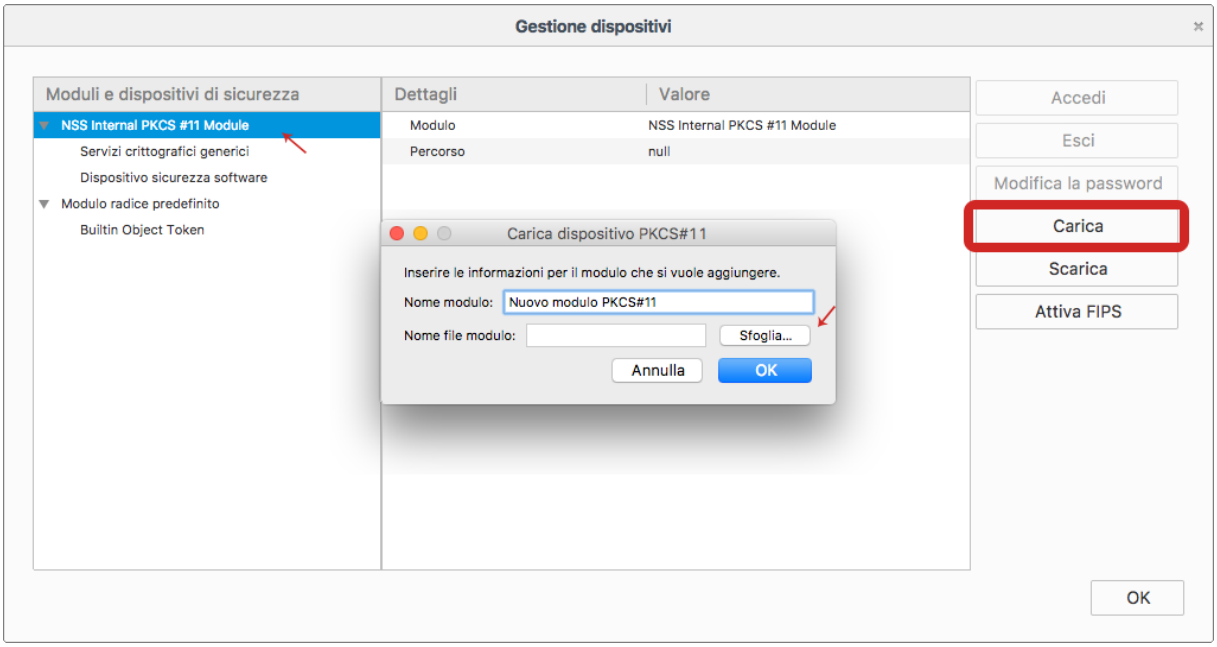
Dalla versione 10.6 alla 10.9 di MAC per poter utilizzare Safari per autenticazioni tramite Smart Card, si rimanda alle guide specifiche del produttore (il Certificato deve essere scaricato con codice fiscale in formato .cer tramite Aruba Sign).

In alternativa è possibile utilizzare Mozilla Firefox per autenticazioni tramite Smart Card. Per procedere:

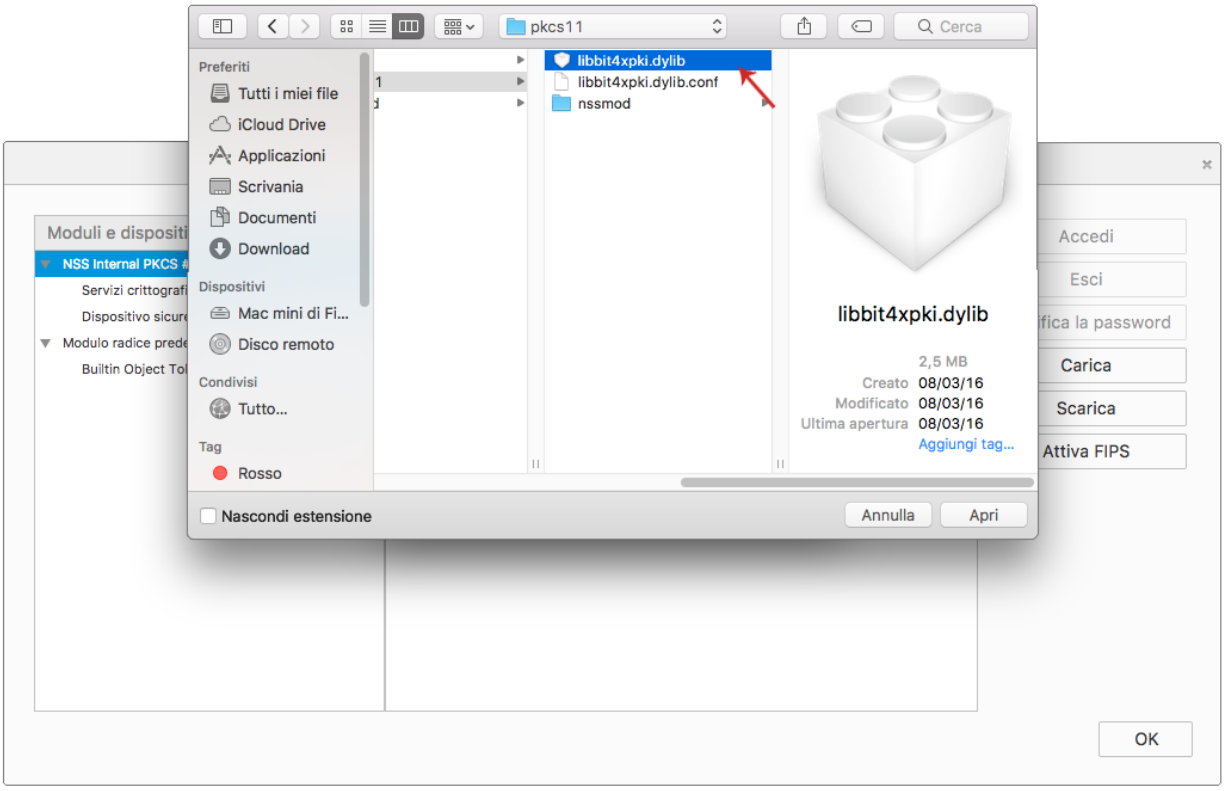
1. Avviare **Mozilla Firefox**;
2. Dall'icona "**Strumenti**" in alto a destra, scegliere "**Preferenze**";
3. Da "**Privacy e sicurezza**" in alto a sinistra, scorrere fino a visualizzare "**Certificati**" in fondo alla pagina;
4. Spuntare l'opzione "**Selezionane uno automaticamente**" quindi "**Dispositivi di Sicurezza**":



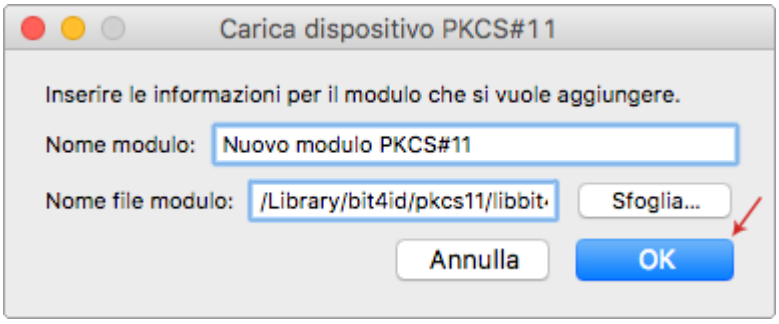
5. Nella finestra "**Gestione dispositivi**" selezionare a sinistra "**NSS Internal PKCS # 11 Module**" quindi cliccare sul pulsante "**Carica**":



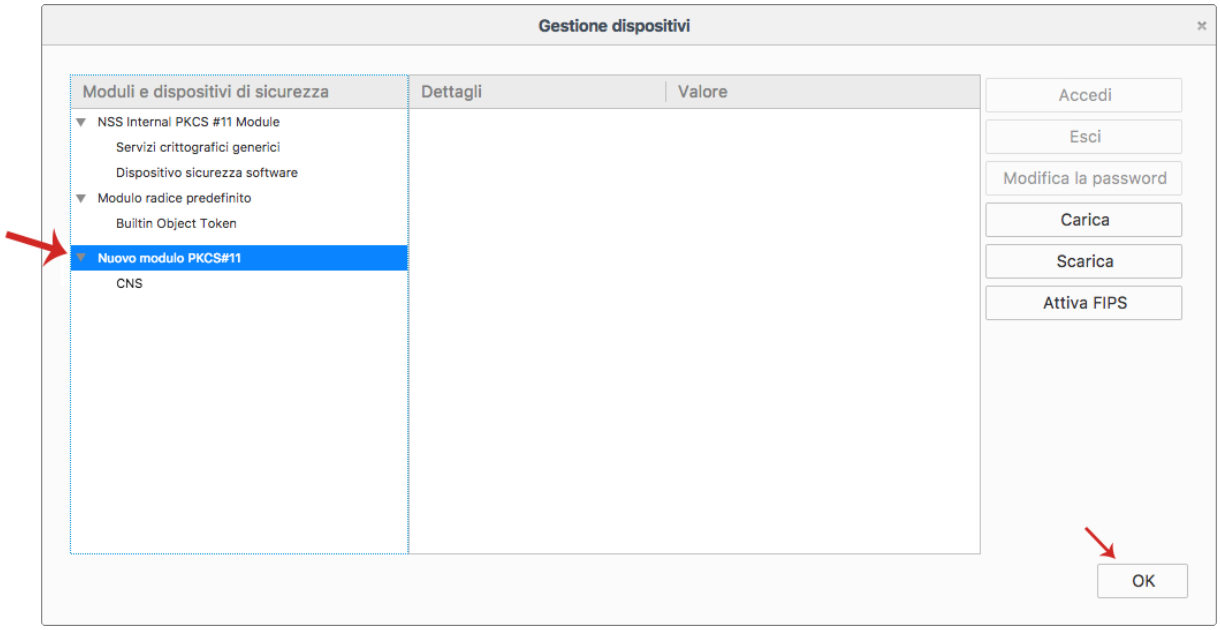
6. Al Tab "**Carica dispositivo PKCS#11**" visualizzato utilizzare "**Sfoglia**" per spostarsi all'interno della directory e selezionare il file **bit4xpki.dylib**:



7. Verificare che il campo Nome file modulo sia valorizzato con il percorso della libreria selezionata utilizzando il tasto "**Sfoglia**" come indicato allo Step precedente e cliccare su "**Ok**" per proseguire:



8. Verificare che all'interno della finestra "**Gestioni dispositivi**" compaia il nuovo modulo appena aggiunto quindi cliccare su "**Ok**":



Mozilla Firefox è pronto per essere utilizzato per autenticazioni tramite Smart Card.

Nel caso in cui i certificati di firma e CNS vengano importati all'interno dello Store di Mozilla FireFox in alcun modo cliccare sul pulsante "**Elimina**". L'azione potrebbe causare l'eliminazione dei certificati CNS e Firma digitale all'interno della Smart Card e l'impossibilità di recuperarli.

5. Utilizzo Aruba Sign e Firma Remota

5.1 Smartphone compatibili con il servizio Firma Remota OTP mobile

Di seguito l'elenco degli smartphone compatibili con il servizio di Firma Remota OTP mobile:

Apple: Sistema operativo IOS 8.0 e successivi;
Android: v2.3 e successive;
Windows Phone: v8.0 e successive;
Blackberry: v10 e successive.

5.2 Attivazione Account Firma Remota e installazione Aruba Sign

I **Kit di Firma Remota** sono composti da:

- **Certificato di Firma digitale che risiede presso un server sicuro di Aruba** (**HSM** "**Hardware Security Module**");
- Dispositivo OTP (One Time Password);
- **Software di Firma e Verifica Aruba Sign**, che permettono al titolare di autenticarsi con le proprie credenziali e di firmare i propri file da qualsiasi postazione connessa a internet.

5.2.1 Attivare un account di Firma Remota

Collegarsi al link https://manage.pec.it/KitFirmaDigitale/SelezionaKit.aspx e selezionare il Kit acquistato spuntando su "**Attiva**" in corrispondenza di uno dei dispositivi sotto indicati:

- **OTP con Display**;
- **OTP USB**;
- **OTP Mobile**:

- Alla schermata "**Inserimento Dati Scratch card**" inserire i dati relativi alla licenza acquistata (Codice Segreto Licenza, Codice Fiscale Titolare del Kit, Seriale Dispositivo in caso di utilizzo di OTP con Display e OTP USB);
- Completare l'attivazione da "**Riepilogo dati cliente e inserimento codice Sicurezza inviato via SMS**", con l'inserimento di un codice di Sicurezza a validità temporanea (20 minuti) ricevuto per SMS al numero di cellulare indicato in fase di ordine del servizio e due password OTP generate con il Token acquistato, quindi scegliere un nome utente e relativa password.

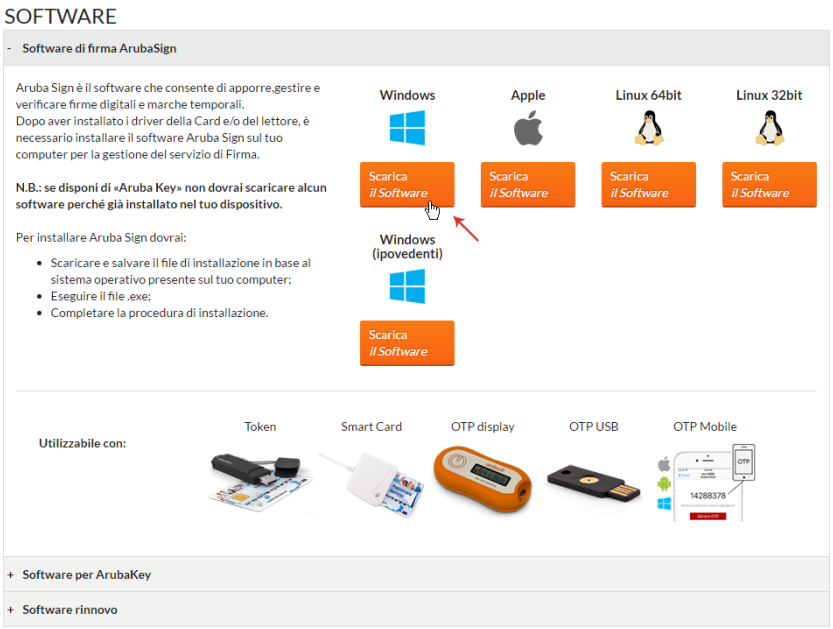
Per le procedure complete di attivazione dei singoli Kit di Firma Digitale e ulteriori approfondimenti si rimanda alle guide dedicate:

- Modalità di attivazione del servizio Firma Remota con OTP con display;
- Modalità di attivazione del servizio Firma Remota con OTP USB;
- Modalità di attivazione del servizio Firma Remota con OTP mobile.

5.2.2 Installazione e avvio Software Aruba Sign

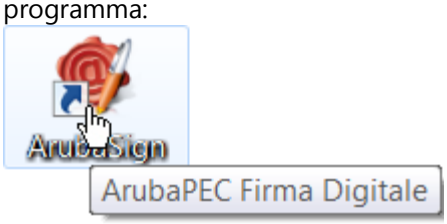
Una volta eseguita l'Attivazione del Kit di Firma Digitale Remota e la creazione del proprio Account, **installare il Software Aruba Sign**:

1. Collegarsi a https://www.pec.it/download-software-driver.aspx;
2. Dal menù a tendina "**Software**" → selezionare "**Software di Firma Aruba Sign**", quindi cliccare sul pulsante "**Scarica il Software**" **corrispondente al sistema operativo utilizzato** (l'esempio di seguito indicato si riferisce a Windows):

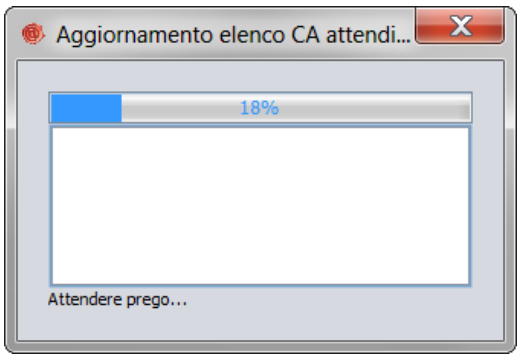


3. **Scaricare ed eseguire su locale il File di installazione**, quindi installare il Software utilizzando la procedura guidata:
   - Selezionare la "**Lingua di Installazione**";
   - Al Tab "**Installazione di Aruba Sign**", cliccare su "**Avanti**";
   - Selezionare la **cartella di destinazione** e cliccare su "**Avanti**";
   - Premere "**Installa**" per continuare l'installazione;
   - Attendere il completamento dell'installazione di Aruba Sign sul computer;
   - Premere "**Fine**" per completare l'installazione.

4. Completo il processo, **sul desktop si visualizza l'icona di Aruba Sign** che permette l'avvio del programma:



5. Il sistema effettua l'aggiornamento automatico del Database dei certificatori, come da immagine esemplificativa sottostante:



6. Completato l'aggiornamento, **si visualizza la schermata principale del Software**:

5.3 Configurazione parametri Firma Remota su Aruba Sign

Per **configurare l'Account di Firma Remota su Aruba Sign**, **avviare il software**, quindi scegliere il menù "**Opzioni e Parametri**":

Selezionare il Tab "**Firma Remota**" e completare il Form come di seguito indicato:

1. I **parametri dell'indirizzo server primario e secondario** vengono **valorizzati automaticamente**, non devono essere modificati;
2. Scrivere il proprio username dell'**Account di Firma Remota** creato in fase di Attivazione del servizio;
3. Cliccare su "**Salva**" per completare l'operazione:

La configurazione è terminata ed è possibile procedere a **firmare documenti digitali** utilizzando la Firma Remota di Aruba, apporre marche temporali, e verificare i file firmati stessi.

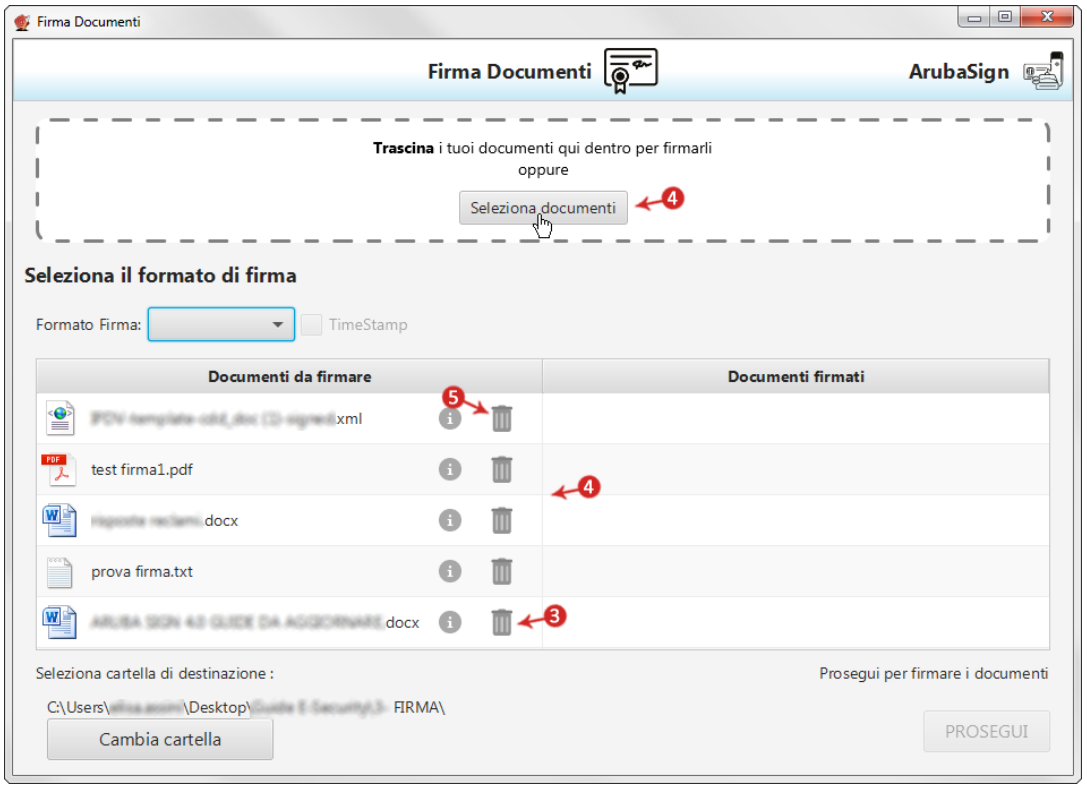
6. Firma e verifica file Aruba Sign - Firma Remota

6.1 Caricamento documenti da firmare e/o cartelle su Aruba Sign

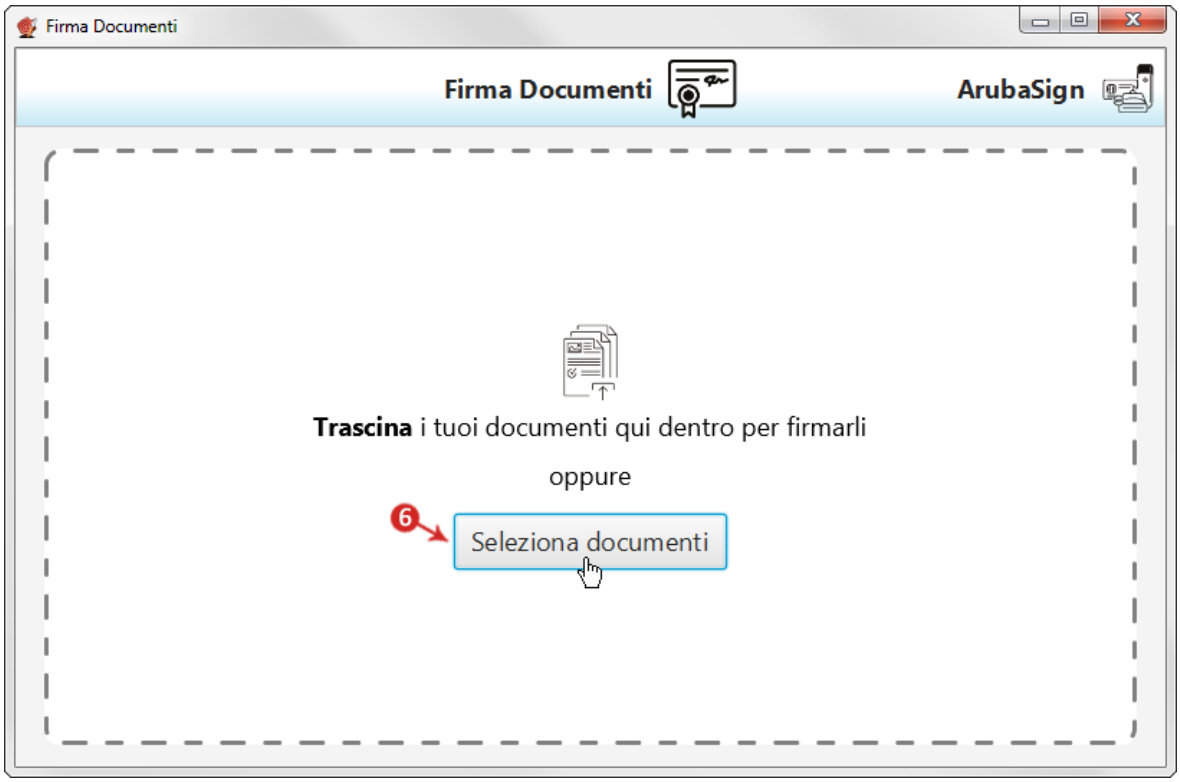
Per **caricare uno o più file su Aruba Sign** e/o una **intera cartella**:

8. Aprire il Software Aruba Sign;
9. Trascinare un qualsiasi documento e/o una cartella (sono accettate tutte le estensioni) sopra l'icona "**Firma**" e attendere che Aruba Sign recuperi le informazioni relative ai certificati contenute nella Smart Card:

10. Alla schermata "**Firma Documenti**", sono visibili i documenti importati in corrispondenza del Tab "**Documenti da firmare**";
11. Per aggiungere ulteriori documenti, cliccare su "**Seleziona Documenti**" e caricare i file desiderati da locale. Gli stessi sono visibili in elenco su "**Documenti da firmare**";
12. I documenti caricati possono essere rimossi in qualsiasi momento cliccando sull'icona "**Cestino**":



13. In alternativa, per uploadare file, cliccare su "**Firma**" dalla barra di menù di ArubaSign. Si visualizza la schermata "**Firma Documenti**", da cui caricare **file** e/o **cartelle** contenenti documenti da firmare cliccando su "**Seleziona Documenti**":



14. Completato il caricamento, si visualizza la schermata indicata agli step 3/4/5 ed è possibile compiere le operazioni descritte ai rispettivi punti.

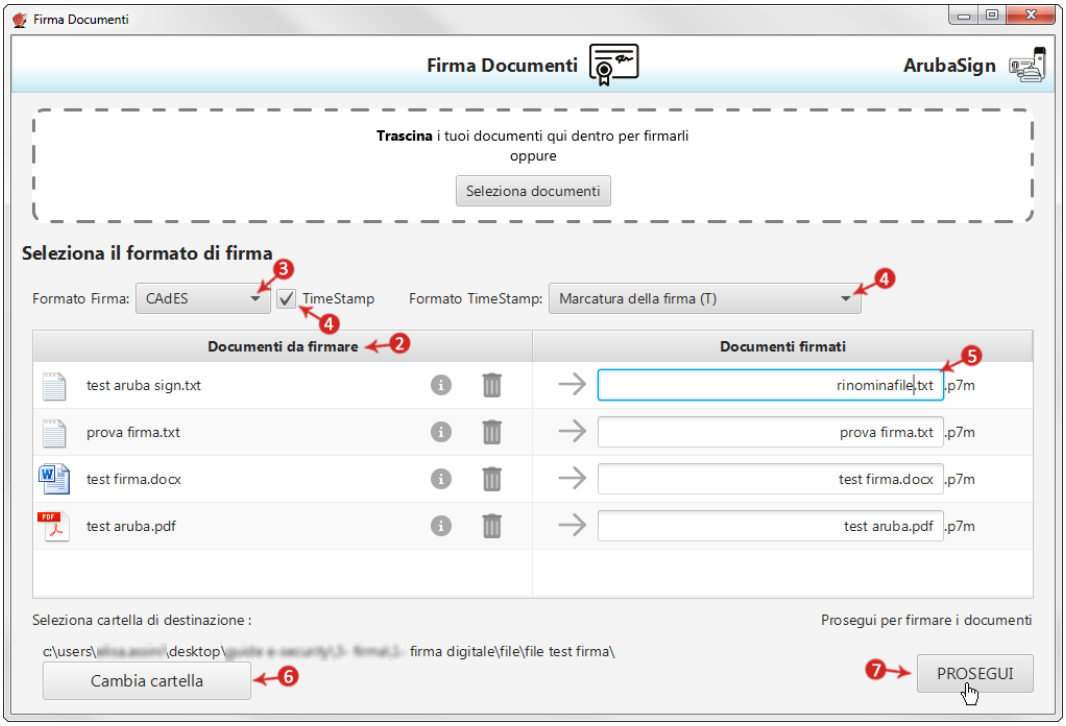
In caso di caricamento di una intera cartella vengono importati tutti i file contenuti nella cartella stessa e quelli eventualmente presenti in sottocartelle. Al momento della Firma, però, il sistema non consente di firmare documenti con identico nome. In questo caso si visualizza un messaggio di errore e la procedura è interrotta.

6.2 "Firma" uno o più file in formato .p7m - Firma Remota

Un **file firmato digitalmente assume estensione .p7m**, che si somma all'estensione del file originario. Ad esempio, un **documento .txt**, al **termine del processo di Firma Digitale** diviene un **documento .txt.p7m** che rappresenta una **busta informatica** (**PKCS#7**). La busta incorpora al suo interno il documento originario, il certificato del sottoscrittore e un hash del documento firmato con il certificato del sottoscrittore. **Un documento sottoscritto digitalmente ha piena validità legale**.

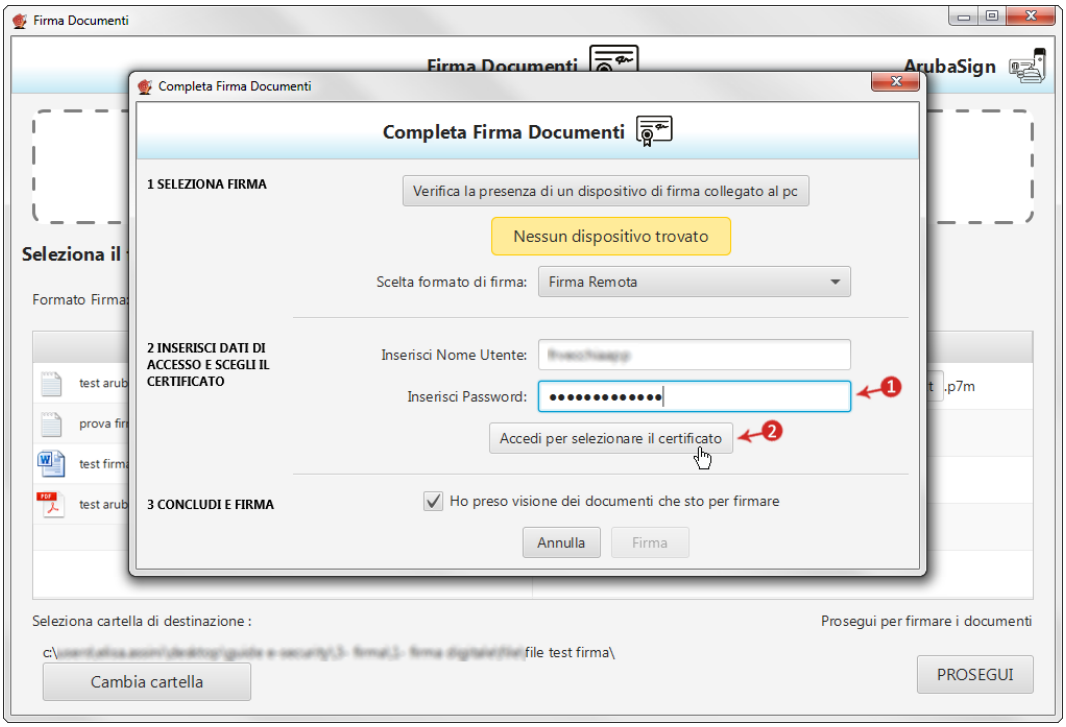
Per **firmare digitalmente uno o più file in formato .p7m** (**Firma CAdES**) e/o una intera cartella **con Aruba Sign e Firma Remota**:

1. **Caricare uno o più documenti e/o una intera cartella**;
2. Il **singolo/i documenti caricati/o** sono visibili all'apposita schermata "**Documenti da firmare**";
3. Dall'apposito menù a tendina "**Formato Firma**" selezionare come tipologia di Firma "**CAdES**" per firmare il file in formato .p7m;
4. Inserire il Flag in corrispondenza della voce "**TimeStamp**" per apporre al file una marcatura temporale nel formato scelto dall'apposito menù a tendina "**Formato TimeStamp**" (lo stesso è visibile solo dopo aver selezionato la voce "**TimeStamp**");
5. Dalla finestra "**Documenti firmati**" rinominare, se desiderato, eventuali file prima di apporre la firma;
6. Da "**Cambia cartella**" verificare che il percorso utilizzato per salvare il/i file firmato/i sia quello desiderato, o selezionarne uno nuovo utilizzando il pulsante indicato;
7. Cliccare su "**Prosegui**" per continuare. Sono firmati tutti i documenti presenti alla finestra "**Documenti da firmare**":

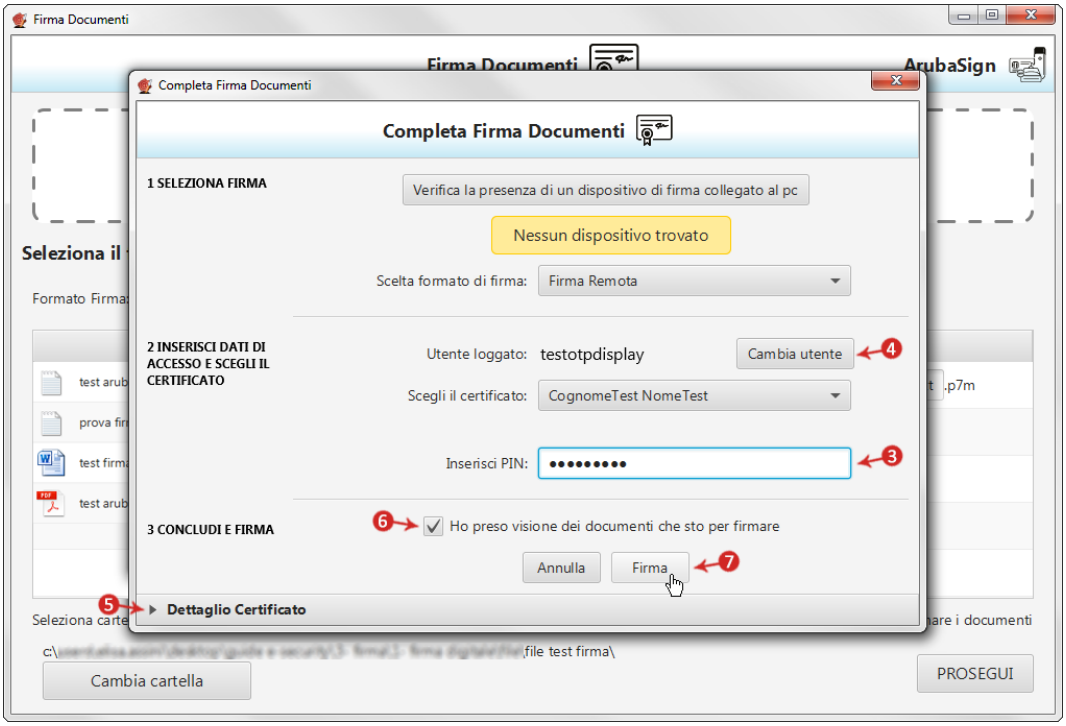


Alla schermata "**Completa Firma Documenti**":

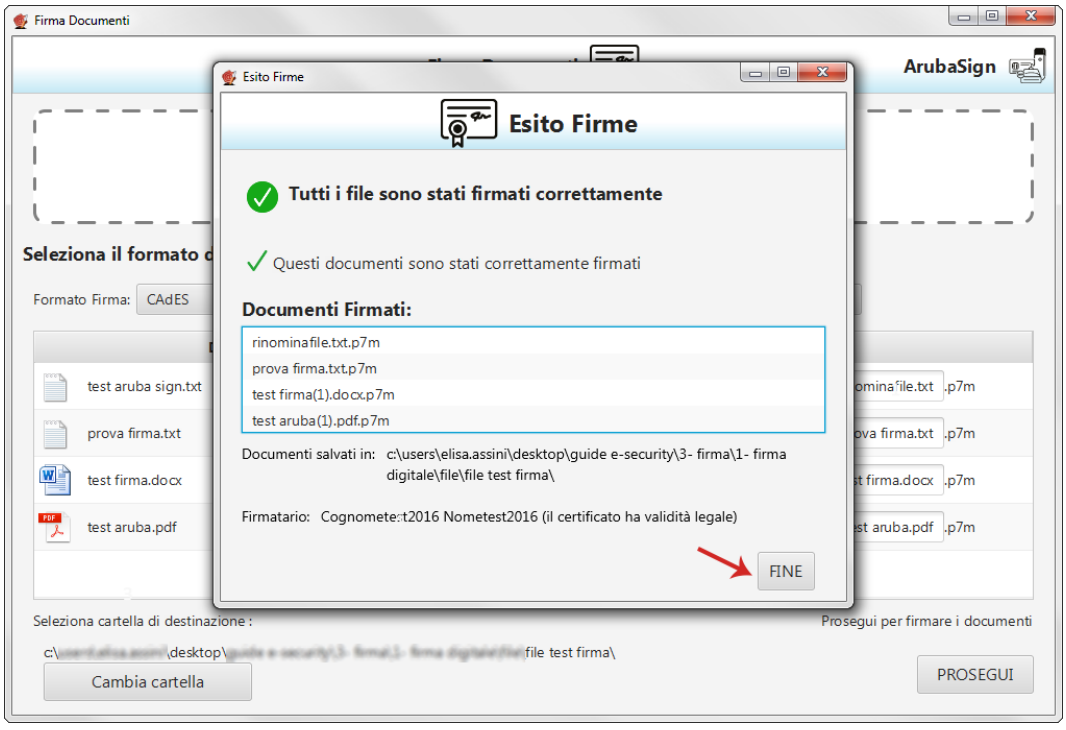
1. Inserire la **password del proprio Account di Firma Remota**;
2. Cliccare su "**Accedi per selezionare il certificato**" per proseguire:



3. Inserire un **codice OTP generato con il proprio dispositivo di Firma Remota**;
4. Cliccando su "**Cambia utente**" è possibile scegliere di firmare con altro Account di Firma Remota configurato;
5. Da "**Dettagli Certificato**" visionare, qualora desiderato, le caratteristiche e la validità del Certificato utilizzato per la Firma;
6. Dichiarare di aver preso visione del documento/i e di essere consapevole della validità ai sensi di legge della Firma apposta;
7. Cliccare su "**Firma**" per concludere il processo:



Al termine dell'operazione si visualizza la seguente schermata che notifica la corretta firma del file. Cliccare su "**FINE**" per chiudere la schermata:



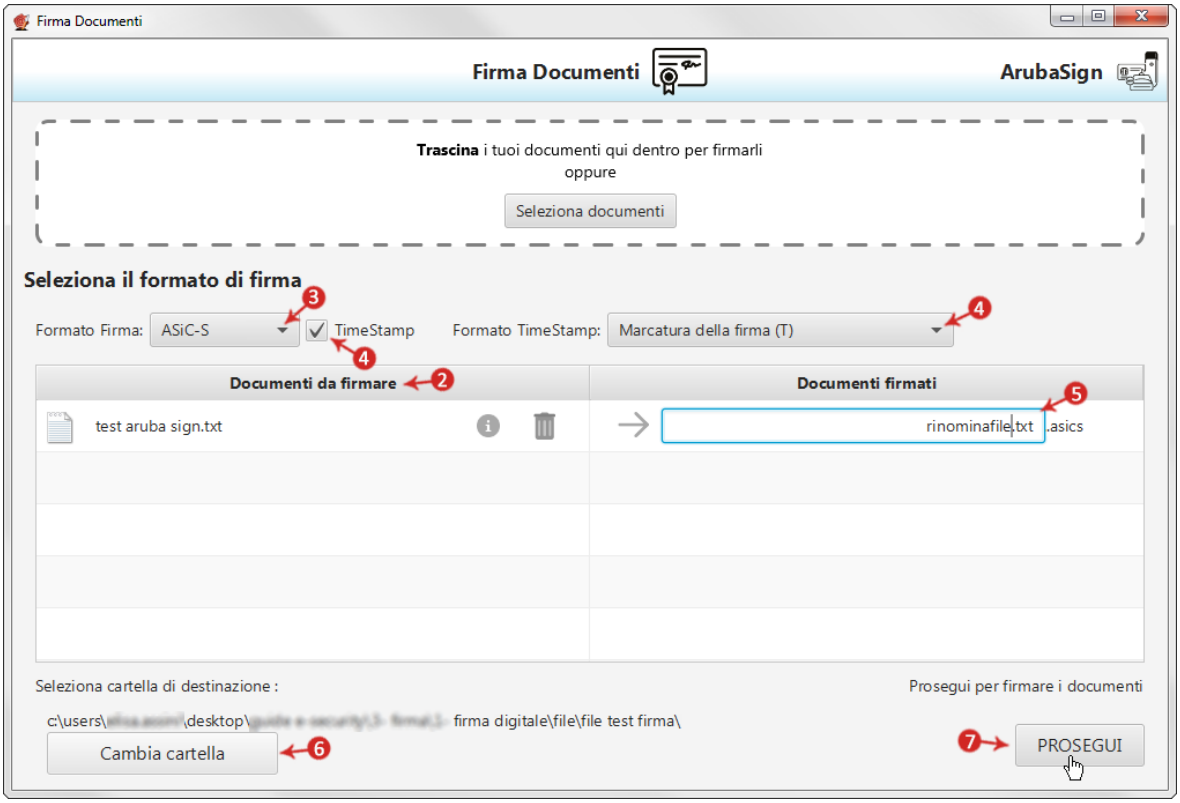
Il documento/i firmato/i sono salvati in formato .p7m nella cartella indicata in fase di Firma.

6.3 Firmare un singolo file in formato ASiC-S - Firma Remota

Il formato di firma **asic-s** (**Associated Signature Containers** "**ASiC simple**") è un **contenitore di dati che raggruppa un file e le relative firme digitali detached e/o marche temporali associate**, utilizzando il formato **.zip**.

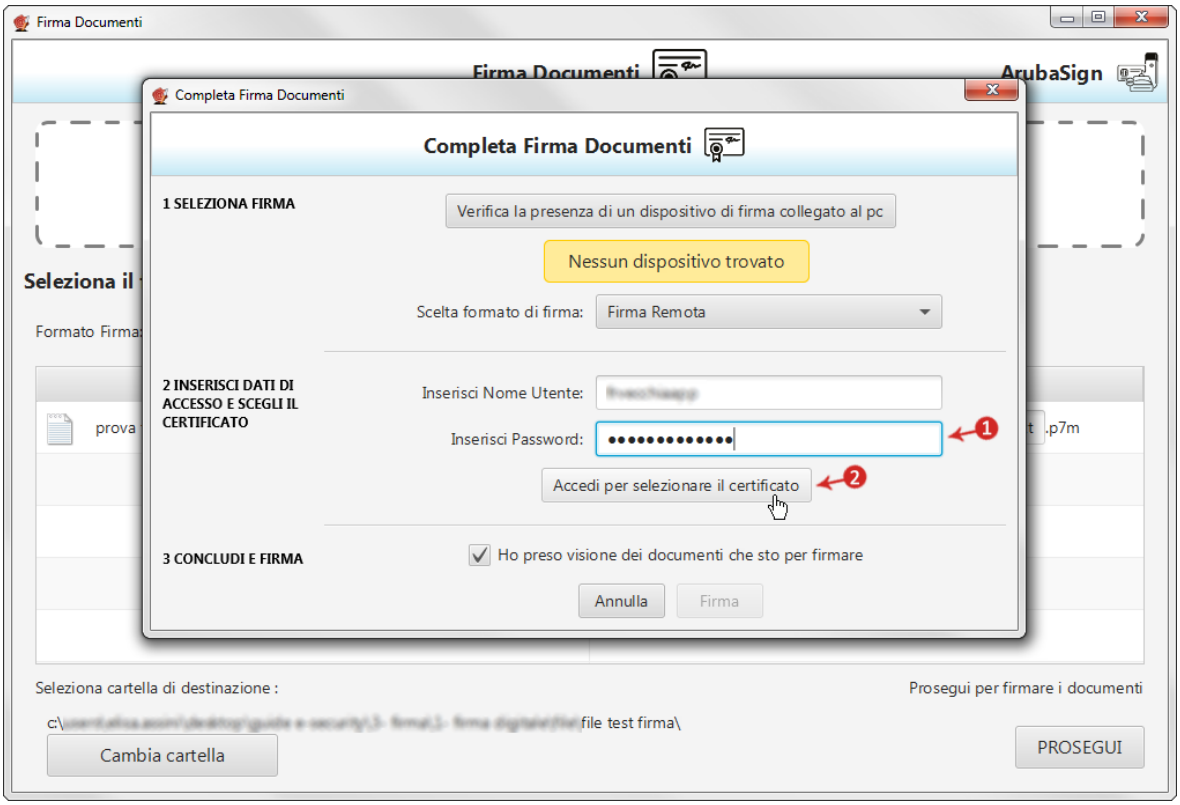
Per **firmare digitalmente un file in formato ASiC-S con Aruba Sign e Firma Remota**:

1. **Caricare il documento**. **Questo formato di Firma è applicabile solo in caso di caricamento su Aruba Sign di un singolo File**, per firmare più file in formato ASiC, selezionare la specifica voce ASiC-E;
2. Il **singolo/i documenti caricati/o** sono visibili all'apposita schermata "**Documenti da firmare**";
3. Dall'apposito menù a tendina "**Formato Firma**" selezionare come tipologia di Firma "**ASiC-S**";
4. Inserire il Flag in corrispondenza della voce "**TimeStamp**" per apporre al file una marcatura temporale nel formato scelto dall'apposito menù a tendina "**Formato TimeStamp**" (lo stesso è visibile solo dopo aver selezionato la voce "**TimeStamp**");
5. Dalla finestra "**Documenti firmati**" rinominare, se desiderato, il file;
6. Da "**Cambia cartella**" verificare che il percorso utilizzato per salvare il file firmato sia quello desiderato, o selezionarne uno nuovo utilizzando il pulsante indicato;
7. Cliccare su "**Prosegui**" per continuare:

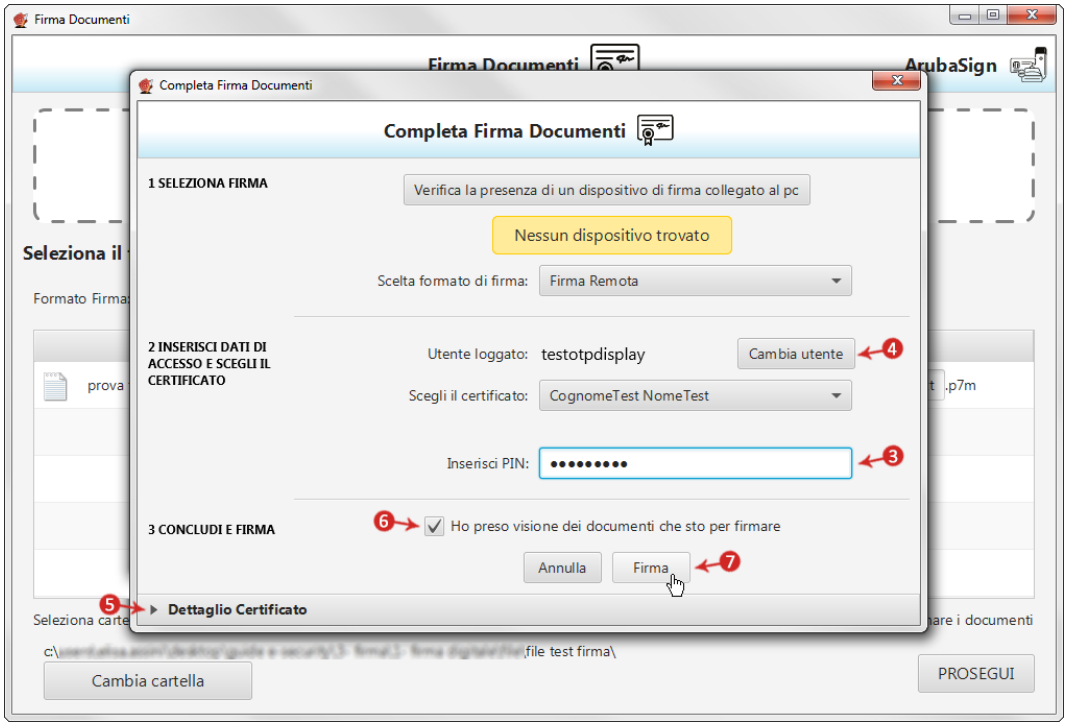


Alla schermata "**Completa Firma Documenti**":

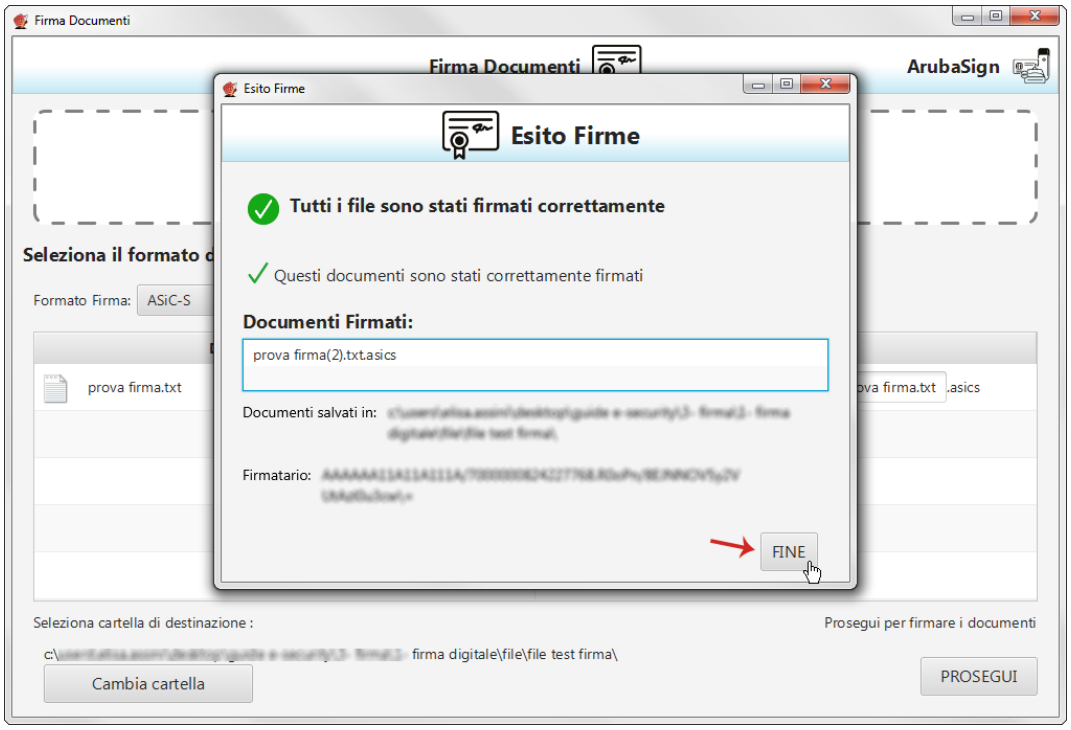
1. Inserire la **password del proprio Account di Firma Remota**;
2. Cliccare su "**Accedi per selezionare il certificato**" per proseguire:



3. Inserire un **codice OTP generato con il proprio dispositivo di Firma Remota**;
4. Cliccando su "**Cambia utente**" è possibile scegliere di firmare con altro Account di Firma Remota configurato;
5. Da "**Dettagli Certificato**" visionare, qualora desiderato, le caratteristiche e la validità del Certificato utilizzato per la Firma;
6. Dichiarare di aver preso visione del documento/i e di essere consapevole della validità ai sensi di legge della Firma apposta;
7. Cliccare su "**Firma**" per concludere il processo:



Al termine dell'operazione si visualizza la seguente schermata che notifica la corretta firma del file. Cliccare su "**FINE**" per chiudere la schermata:



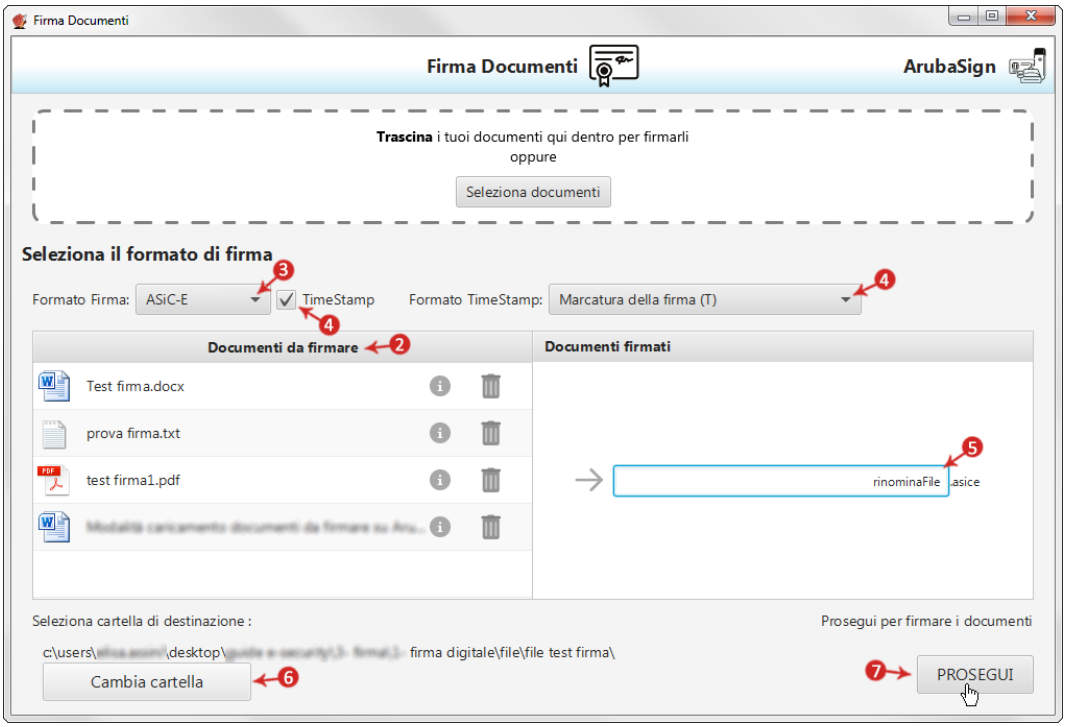
Il documento firmato in **formato ASiC-S** è salvato nella cartella indicata in fase di Firma.

6.4 "Firma" di più file in formato ASiC-E - Firma Remota

Il formato di firma ASiC-E (**Associated Signature Containers** "**ASiC simple**") è un **contenitore di dati che raggruppa più file e le relative firme digitali detached e/o marche temporali associate**, utilizzando il formato **.zip**.

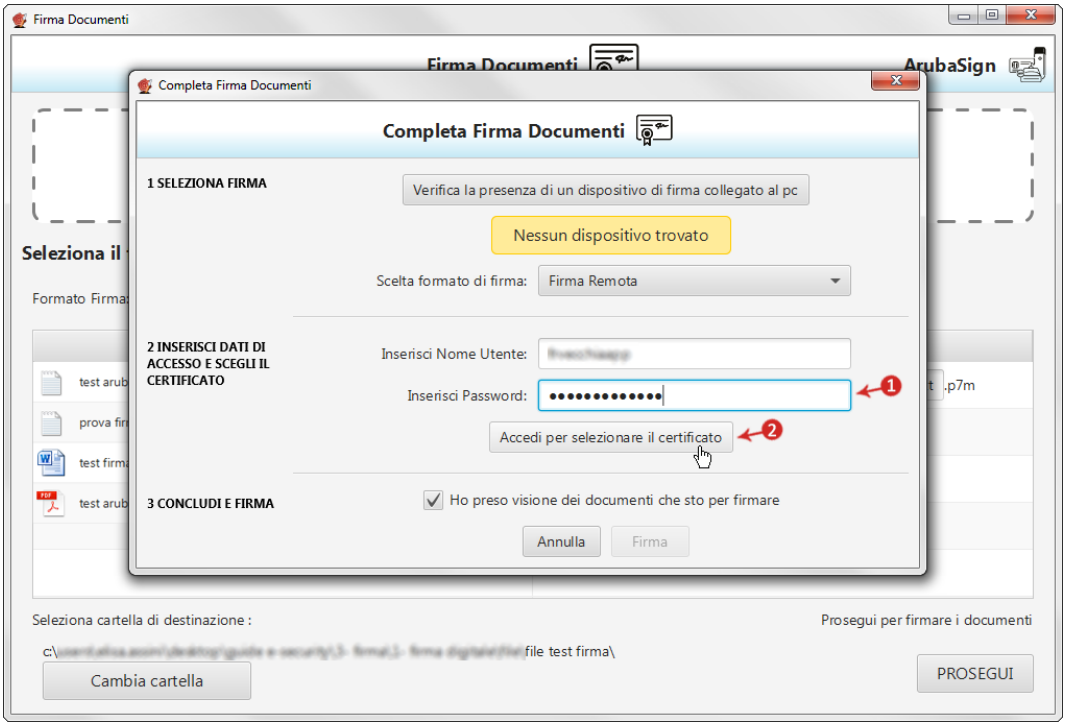
Per **firmare digitalmente più file in formato ASiC-E con Aruba Sign e Firma Remota**:

1. **Caricare i documenti e/o una intera cartella**. **Questo formato di Firma è applicabile solo in caso di caricamento su Aruba Sign di più documenti**, per firmare un solo file in formato ASiC, selezionare dall'apposito menù a tendina "**Formato Firma**" ASiC-S;
2. I **documenti caricati** sono visibili all'apposita schermata "**Documenti da firmare**";
3. Dall'apposito menù a tendina "**Formato Firma**" selezionare come tipologia di Firma "**ASiC-E**";
4. Inserire il Flag in corrispondenza della voce "**TimeStamp**" per apporre ai file una marcatura temporale nel formato scelto dall'apposito menù a tendina "**Formato TimeStamp**" (lo stesso è visibile solo dopo aver selezionato la voce "**TimeStamp**");
5. Dalla finestra "**Documenti firmati**" rinominare, se desiderato, il contenitore dei file;
6. Da "**Cambia cartella**" verificare che il percorso utilizzato per salvare i file firmati sia quello desiderato, o selezionarne uno nuovo utilizzando il pulsante indicato;
7. Cliccare su "**Prosegui**" per continuare. Sono firmati tutti i documenti presenti alla finestra "**Documenti da firmare**":

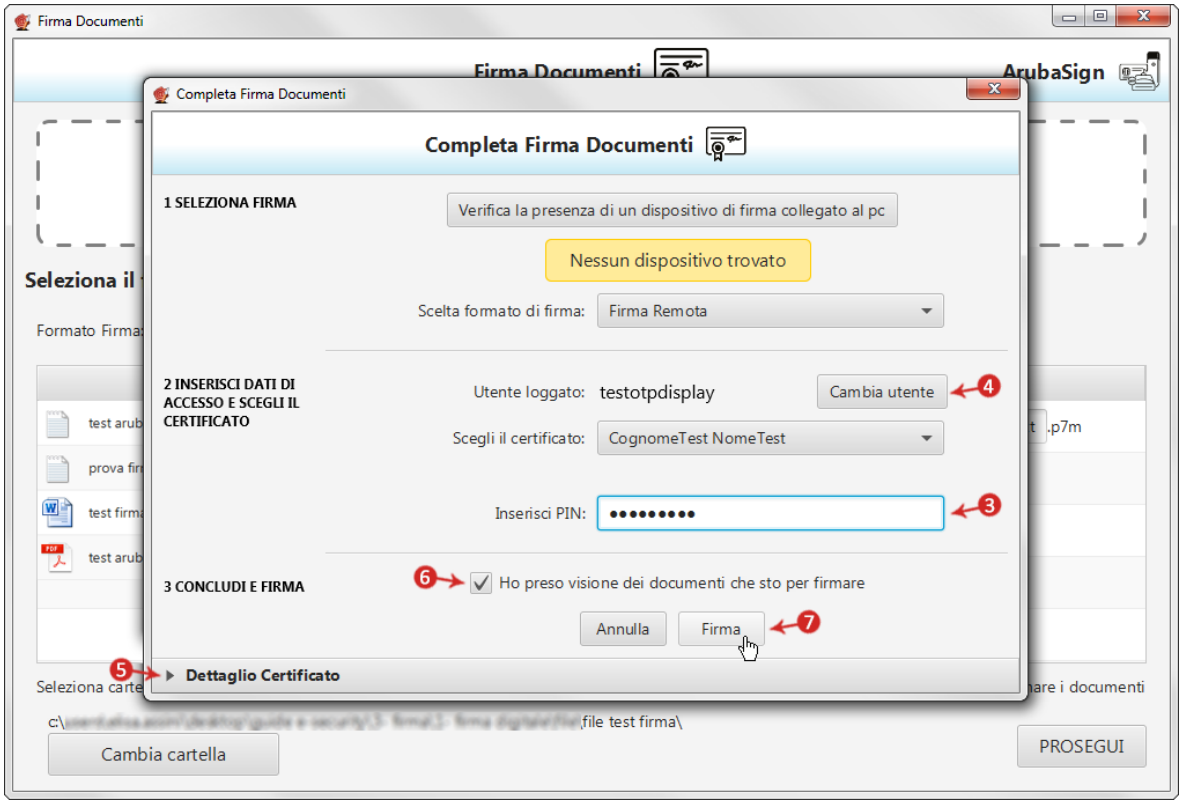


Alla schermata "**Completa Firma Documenti**":

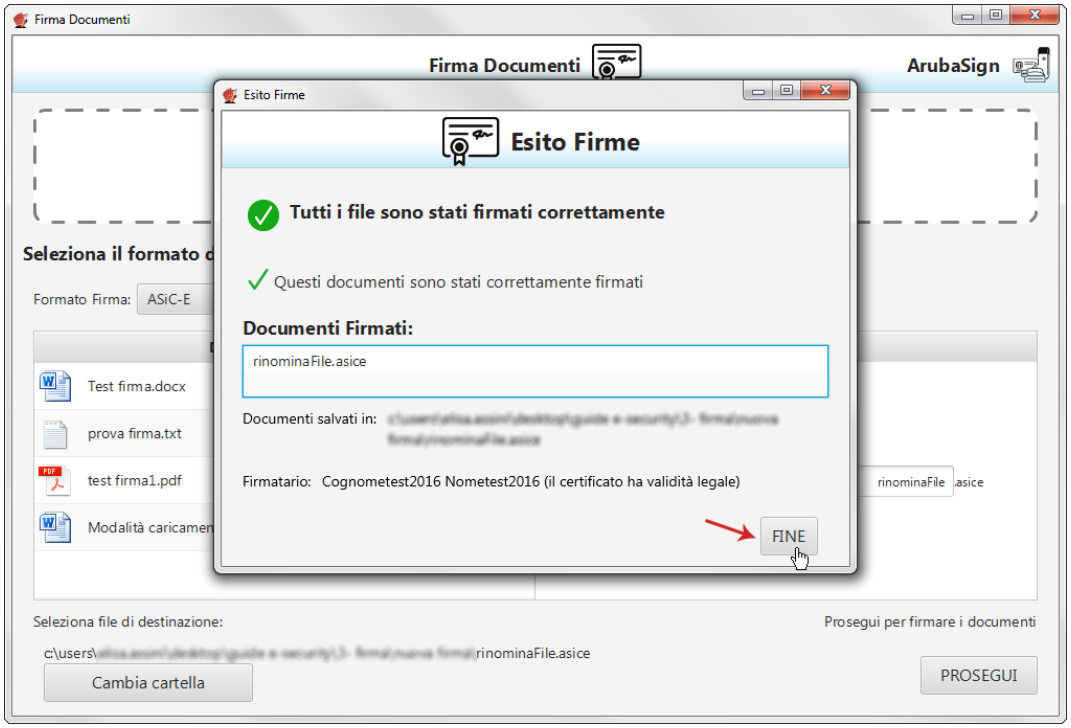
1. Inserire la **password del proprio Account di Firma Remota**;
2. Cliccare su "**Accedi per selezionare il certificato**" per proseguire:



3. Inserire un **codice OTP generato con il proprio dispositivo di Firma Remota**;
4. Cliccando su "**Cambia utente**" è possibile scegliere di firmare con altro Account di Firma Remota configurato;
5. Da "**Dettagli Certificato**" visionare, qualora desiderato, le caratteristiche e la validità del Certificato utilizzato per la Firma;
6. Dichiarare di aver preso visione del documento/i e di essere consapevole della validità ai sensi di legge della Firma apposta;
7. Cliccare su "**Firma**" per concludere il processo:



Al termine dell'operazione si visualizza la seguente schermata che notifica la corretta firma dei file. Cliccare su "**FINE**" per chiudere la schermata:



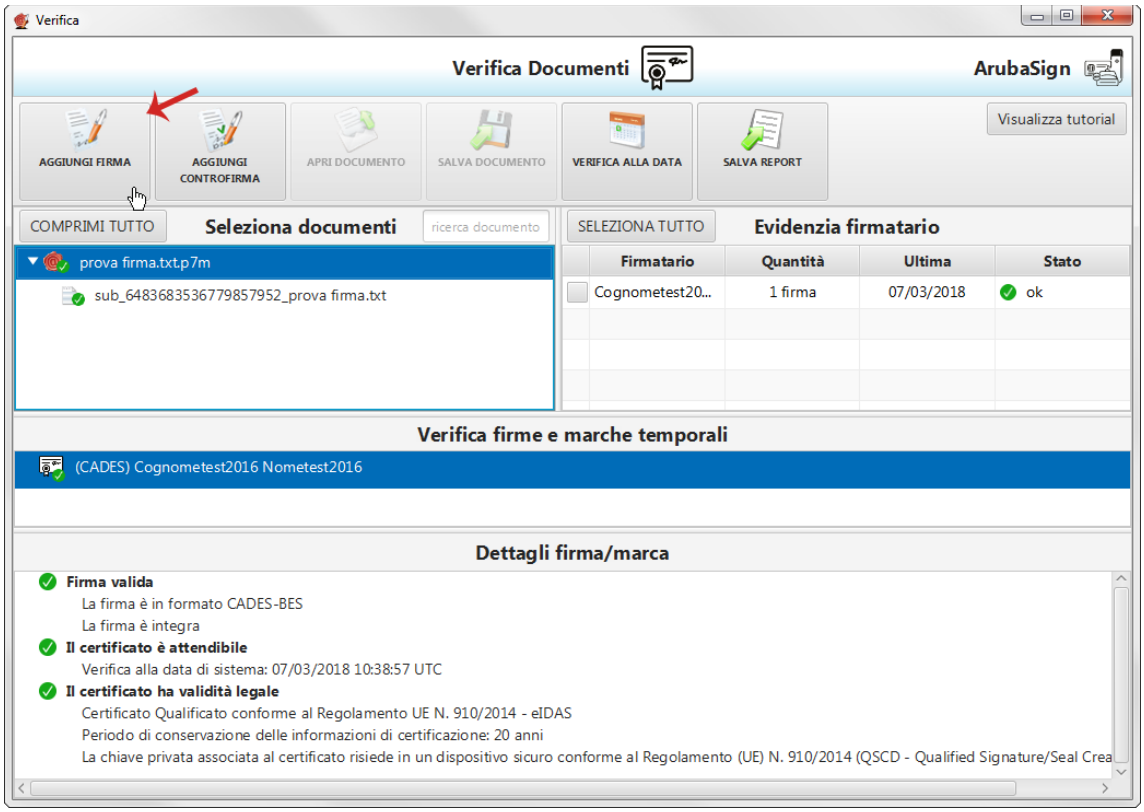
Il contenitore di documenti in **formato ASiC-E** è salvato nella cartella indicata in fase di Firma. In fase di verifica del contenitore è possibile visionare il dettaglio delle Firme apposte a ogni singolo documento.

6.5 Apposizione "Firma Parallela" - Firma Remota

La funzione "**Firma Parallela**" è accessibile trascinando sopra il pulsante di verifica del Software Aruba Sign **uno o più file già firmati in formato .p7m (CAdES) o .PDF (PAdES)**. E' aggiunta allo stesso livello e allo stesso contenuto di una firma preesistente e viene di norma utilizzata per aggiungere firme ad un documento già firmato in formato .p7m in quei flussi documentali che ne prevedono l'utilizzo.

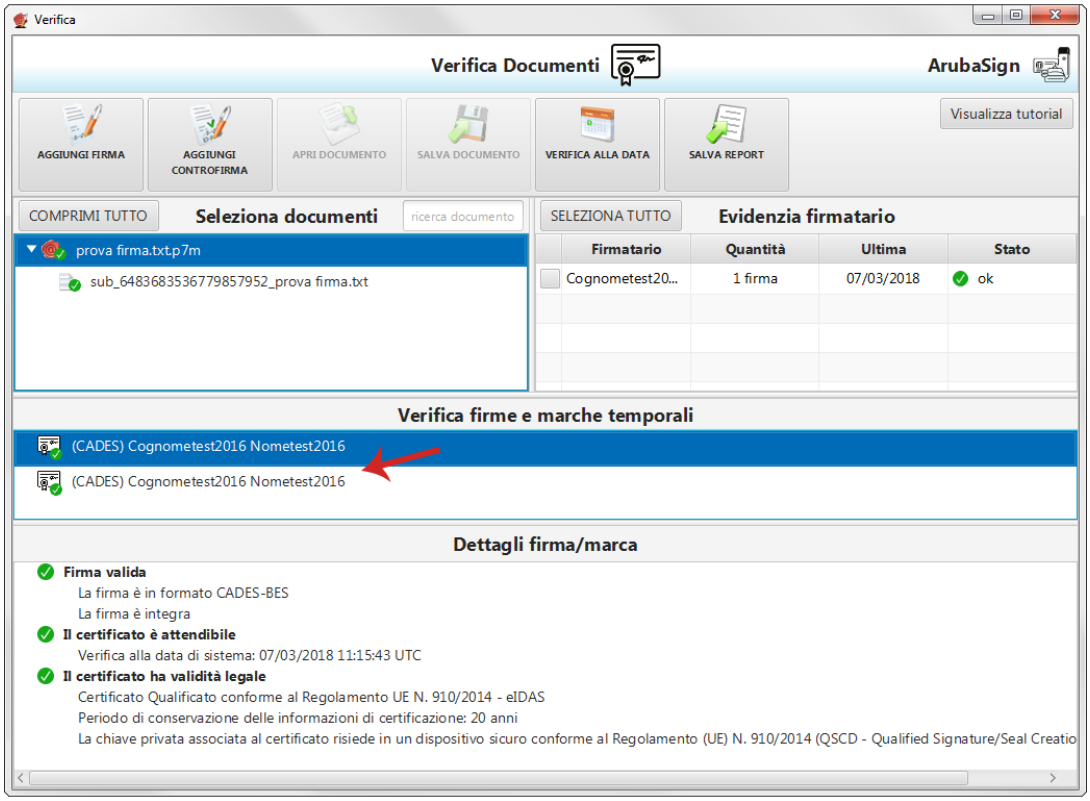
Per crearla **trascinare un file .p7m (CAdES)** o **.PDF (PAdES)**, sopra il menù "**Verifica**" di **Aruba Sign**:

Da "**Verifica documenti**" selezionare il documento (anche in caso di caricamento di un solo file) su cui apporre la **Firma Parallela** poi cliccare su "**Aggiungi Firma**":



Firmare digitalmente il file. **Il sistema non consente di selezionare il formato della Firma.** In caso di File **.p7m** la "**Firma Parallela**" è apposta in tale formato; per i file .PDF è possibile apporre una Firma Grafica o Invisibile. **La nuova firma è apposta allo stesso livello di quella preesistente**. **Il sistema** sovrascrive il documento già esistente e salvato nella cartella indicata in fase di Firma del documento stesso.

Trascinando il file sul pulsante "Verifica" è possibile visionare la presenza della Firma Parallela, come da immagine esemplificativa sottostante:

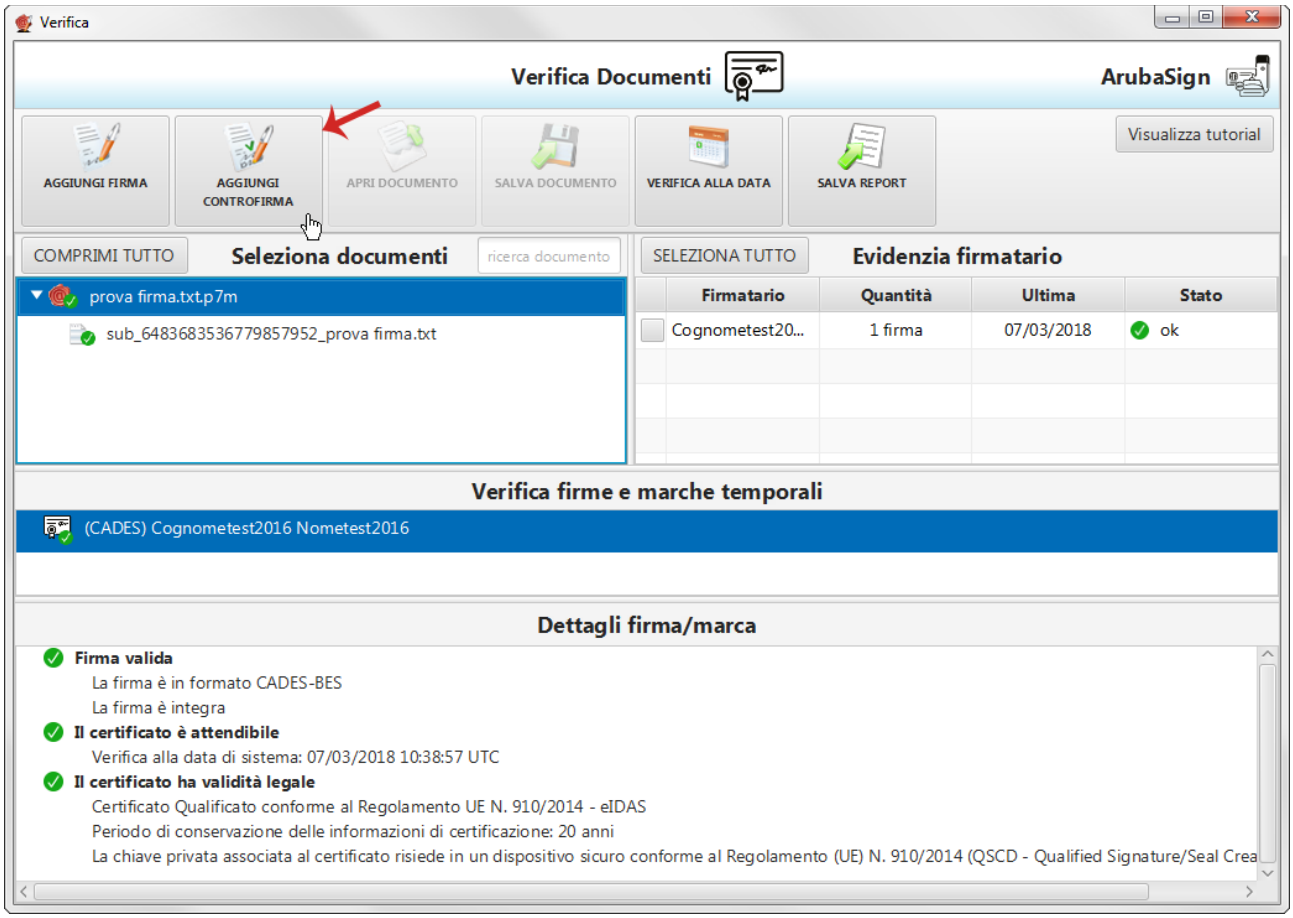


6.6 Apposizione "Controfirma" - Firma Remota

La funzione "**Controfirma**" è accessibile trascinando sopra il pulsante di verifica del Software Aruba Sign **uno o più file già firmati in formato .p7m**. E' apposta a un livello sottostante di una firma preesistente e sottoscrive quest'ultima. E' più annidata rispetto alla firma a cui si riferisce (aspetto evidenziato da una rappresentazione ad albero delle firme stesse).

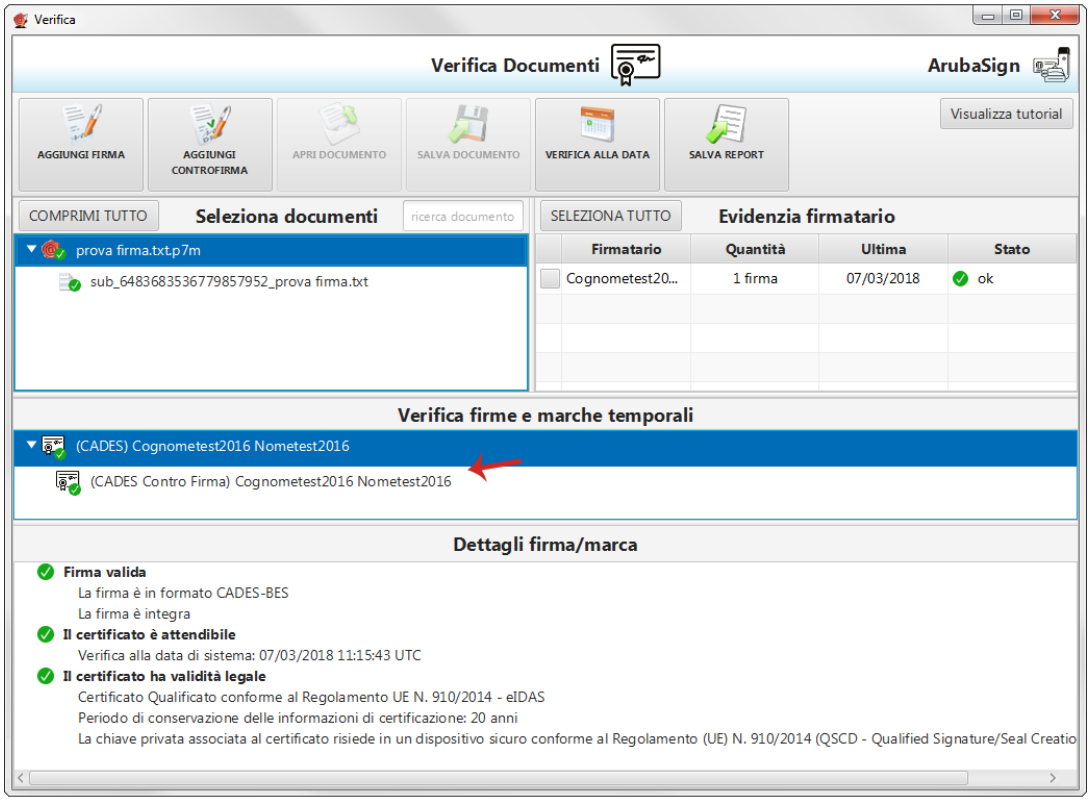
Per crearla **trascinare un file .p7m (CAdES)**, sopra il menù "**Verifica**" di **Aruba Sign**:

Da "**Verifica documenti**" selezionare il documento (anche in caso di caricamento di un solo file) su cui apporre la **Controfirma** poi cliccare su "**Aggiungi Controfirma**":



Firmare digitalmente il file in formato .p7m. **La nuova Firma è apposta a un livello sottostante della firma preesistente**. Il sistema sovrascrive il documento già esistente e salvato nella cartella indicata in fase di Firma del documento stesso.

Trascinando il file sul pulsante "Verifica" è possibile visionare la presenza della Controfirma, come da immagine esemplificativa sottostante:

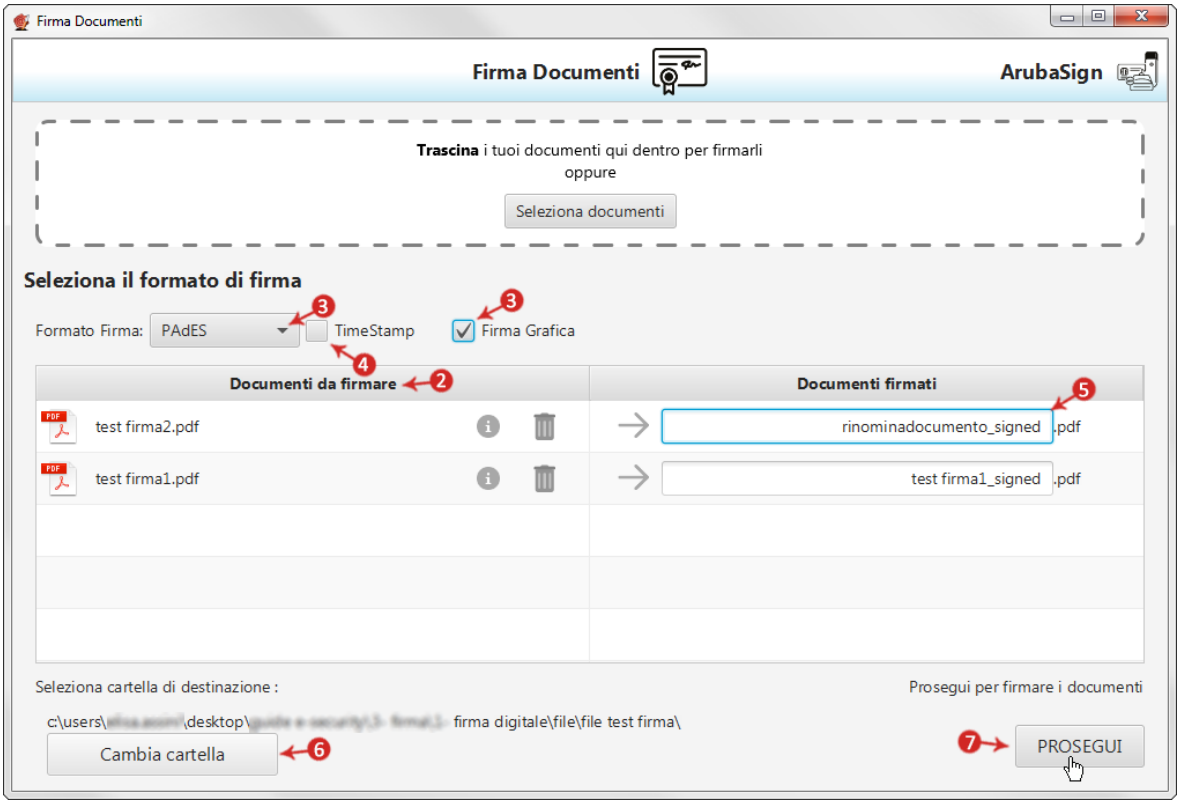


6.7 Apposizione Firma PDF - Grafica (Firma Remota)

Il Formato di Firma PAdES è applicabile ai soli file già convertiti in formato .PDF ed **è visibile solo se nel menù "Firma Documenti" di Aruba Sign sono caricati esclusivamente file con questa estensione**. Se sono caricati più file con estensioni diverse tra loro, la firma **PAdES** non risulta tra i formati selezionabili da menù "**Firma**".

La Firma PAdES - Firma Grafica permette di scegliere la posizione e la dimensione del campo che ospita la Firma Digitale. Per **firmare digitalmente uno o più file in formato .PDF in formato PAdES - Firma Grafica** e/o una intera cartella **con Aruba Sign e Firma Remota**:

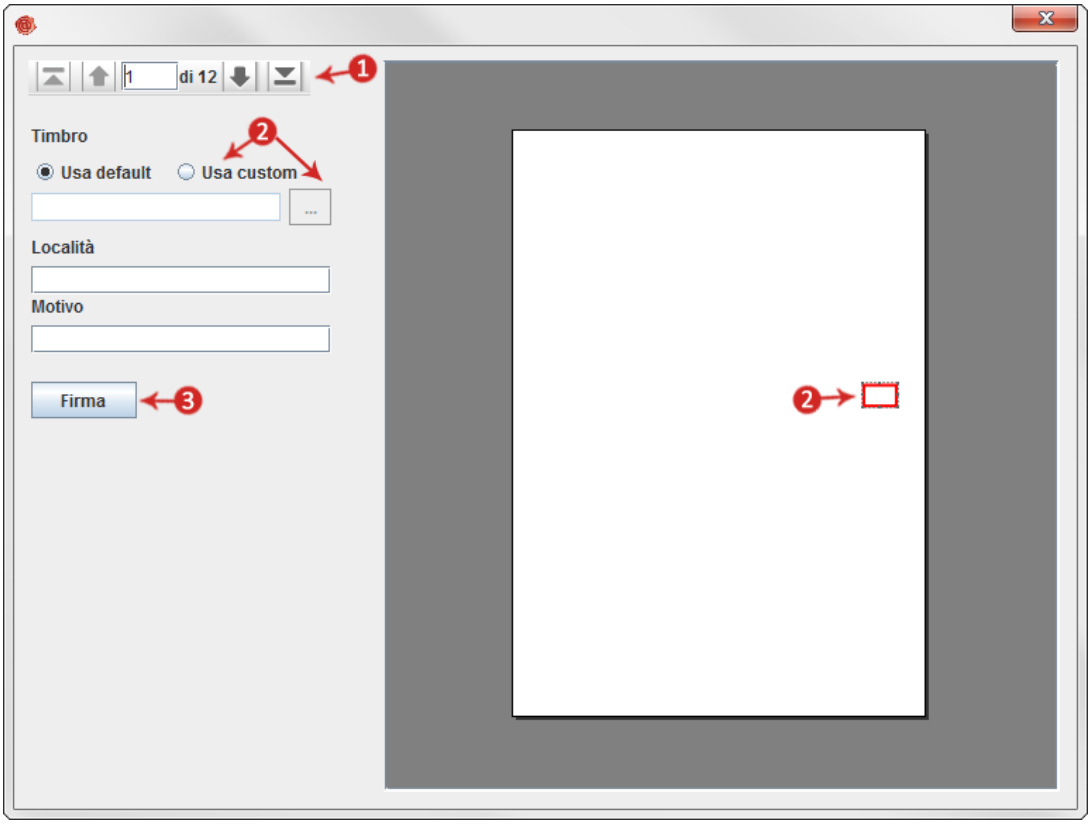
1. **Caricare uno o più documenti e/o una intera cartella**;
2. Il **singolo/i documenti caricati/o** sono visibili all'apposita schermata "**Documenti da firmare**";
3. Dall'apposito menù a tendina "**Formato Firma**" selezionare come tipologia di Firma "**PAdES**" per firmare il file in formato .PDF e lasciare il Flag su "**Firma Grafica**";
4. Inserire il Flag in corrispondenza della voce "**TimeStamp**" per apporre al file una marcatura temporale nel formato scelto dall'apposito menù a tendina "**Formato TimeStamp**" (lo stesso è visibile solo dopo aver selezionato la voce "**TimeStamp**");
5. Dalla finestra "**Documenti firmati**" rinominare, se desiderato, eventuali file prima di apporre la firma;
6. Da "**Cambia cartella**" verificare che il percorso utilizzato per salvare il/i file firmato/i sia quello desiderato, o selezionarne uno nuovo utilizzando il pulsante indicato;
7. Cliccare su "**Prosegui**" per continuare. Sono firmati tutti i documenti presenti alla finestra "**Documenti da firmare**":



Alla schermata "**Firma PDF**":

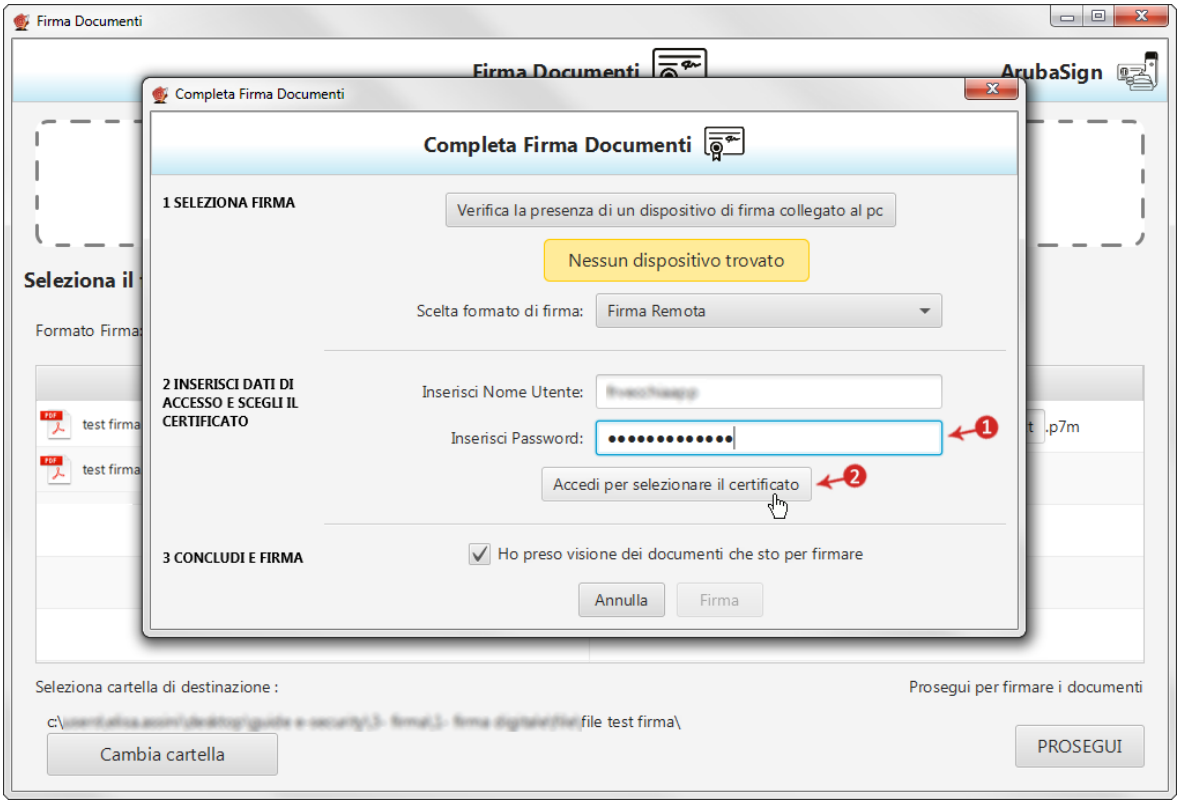
1. Indicare, dal menù in alto, il numero di pagina dove far comparire il timbro;

2. Definire, attraverso la finestra di anteprima, la **posizione** e la **dimensione del campo** che ospiterà la Firma Digitale. Al campo "**Timbro**", è possibile caricare da locale, spuntando "**Usa custom**" e utilizzando l'apposito pulsante indicato in figura, una img in formato .gif/.jpg/.png da sostituire a quella presente di default per il timbro. L'immagine caricata è ridimensionata in scala rispetto alle dimensione dell'area selezionata;
3. Cliccare su "**Firma**" per procedere:

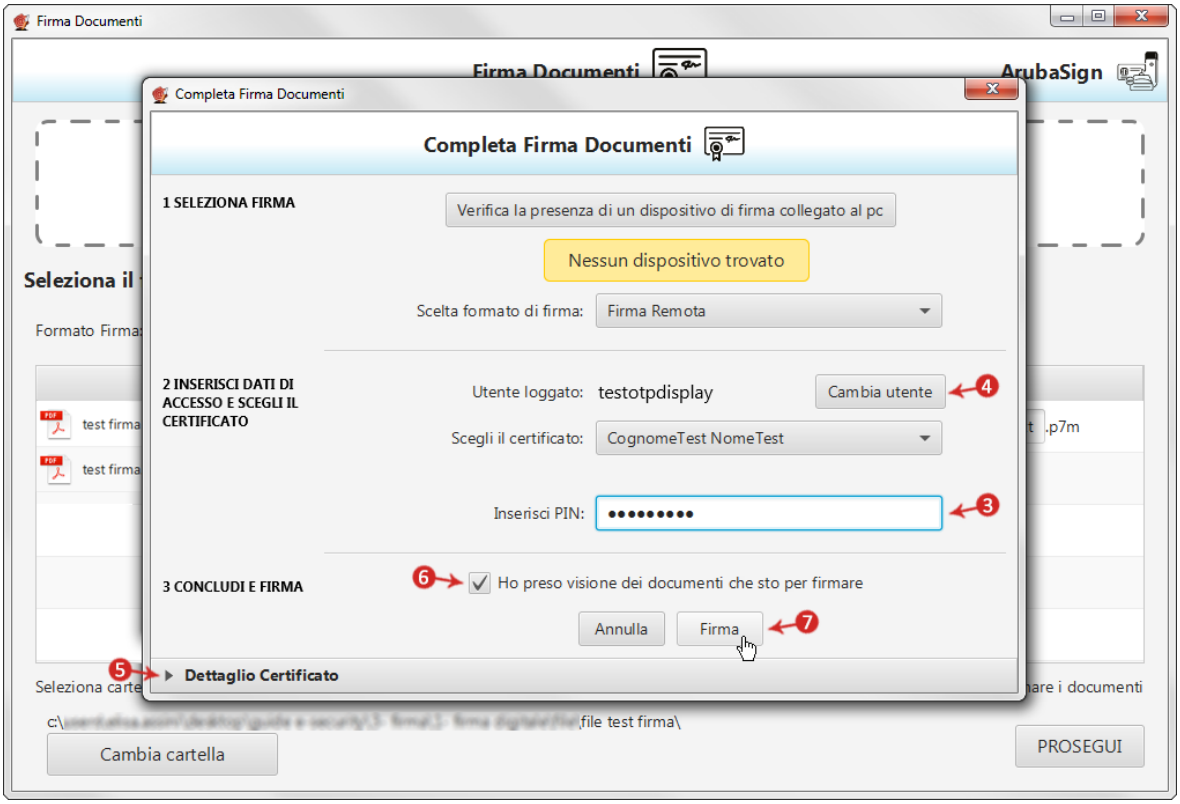


Alla schermata "**Completa Firma Documenti**":

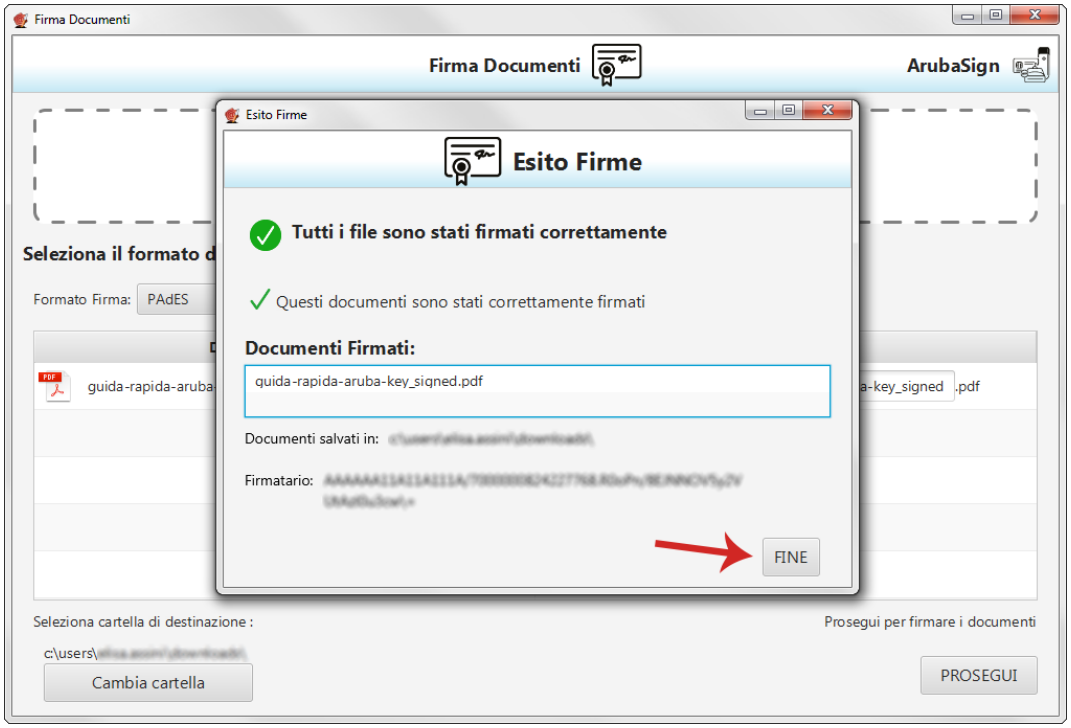
1. Inserire la **password del proprio Account di Firma Remota**;
2. Cliccare su "**Accedi per selezionare il certificato**" per proseguire:



3. Inserire un **codice OTP generato con il proprio dispositivo di Firma Remota**;
4. Cliccando su "**Cambia utente**" è possibile scegliere di firmare con altro Account di Firma Remota configurato;
5. Da "**Dettagli Certificato**" visionare, qualora desiderato, le caratteristiche e la validità del Certificato utilizzato per la Firma;
6. Dichiarare di aver preso visione del documento/i e di essere consapevole della validità ai sensi di legge della Firma apposta;
7. Cliccare su "**Firma**" per concludere il processo:



Al termine dell'operazione si visualizza la seguente schermata che notifica la corretta firma del file. Cliccare su "**FINE**" per chiudere la schermata:



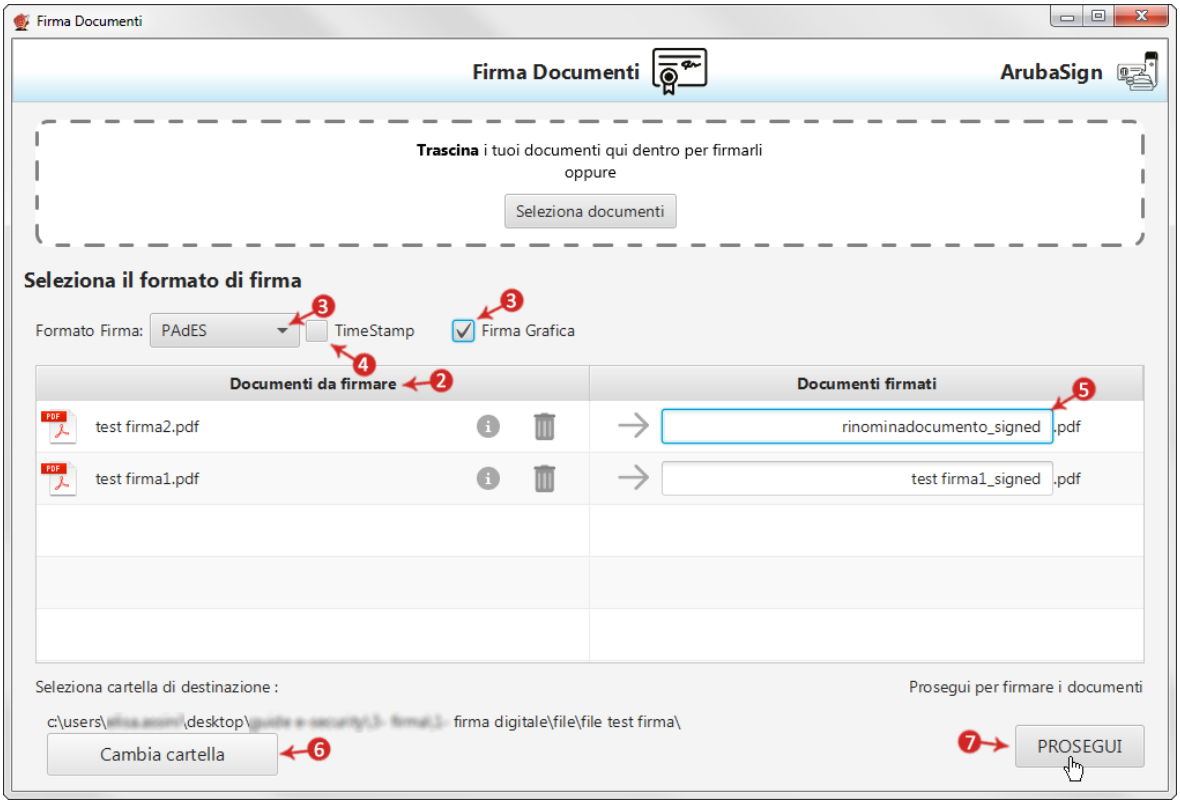
Il documento firmato viene salvato nella cartella indicata durante il processo, aggiungendo al **nome originale l'estensione** "**signed.pdf**".

6.8 Apposizione Firma PDF - Invisibile (Firma Remota)

Il Formato di Firma PAdES è applicabile ai soli file già convertiti in formato .PDF, ed **è visibile solo se nel menù "Firma Documenti" di Aruba Sign sono caricati esclusivamente file con questa estensione**. Se sono caricati più file con estensioni diverse tra loro, la firma **PAdES** non risulta tra i formati selezionabili da menù "**Firma**".

La Firma PAdES - Firma Invisibile consente di evitare l'inserimento dell'"**appearance**" (**campo firma visibile**) all'interno delle pagine del documento firmato. Per **firmare digitalmente uno o più file in formato .PDF in formato PAdES - Firma Invisibile** e/o una intera cartella **con Aruba Sign e Firma Remota**:

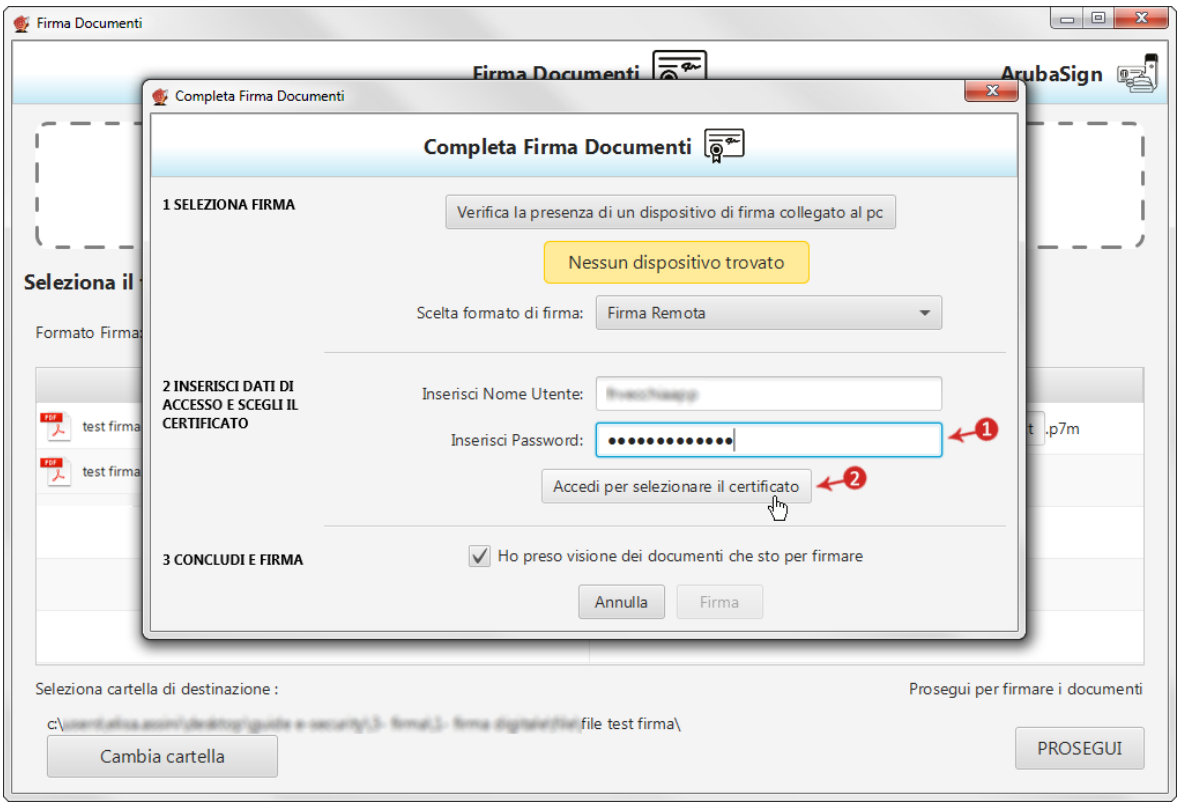
1. **Caricare uno o più documenti e/o una intera cartella**;
2. Il **singolo/i documenti caricati/o** sono visibili all'apposita schermata "**Documenti da firmare**";
3. Dall'apposito menù a tendina "**Formato Firma**" selezionare come tipologia di Firma "**PAdES**" per firmare il file in formato .PDF e lasciare il Flag su "**Firma Grafica**";
4. Inserire il Flag in corrispondenza della voce "**TimeStamp**" per apporre al file una marcatura temporale nel formato scelto dall'apposito menù a tendina "**Formato TimeStamp**" (lo stesso è visibile solo dopo aver selezionato la voce "**TimeStamp**");
5. Dalla finestra "**Documenti firmati**" rinominare, se desiderato, eventuali file prima di apporre la firma;
6. Da "**Cambia cartella**" verificare che il percorso utilizzato per salvare il/i file firmato/i sia quello desiderato, o selezionarne uno nuovo utilizzando il pulsante indicato;
7. Cliccare su "**Prosegui**" per continuare. Sono firmati tutti i documenti presenti alla finestra "**Documenti da firmare**":



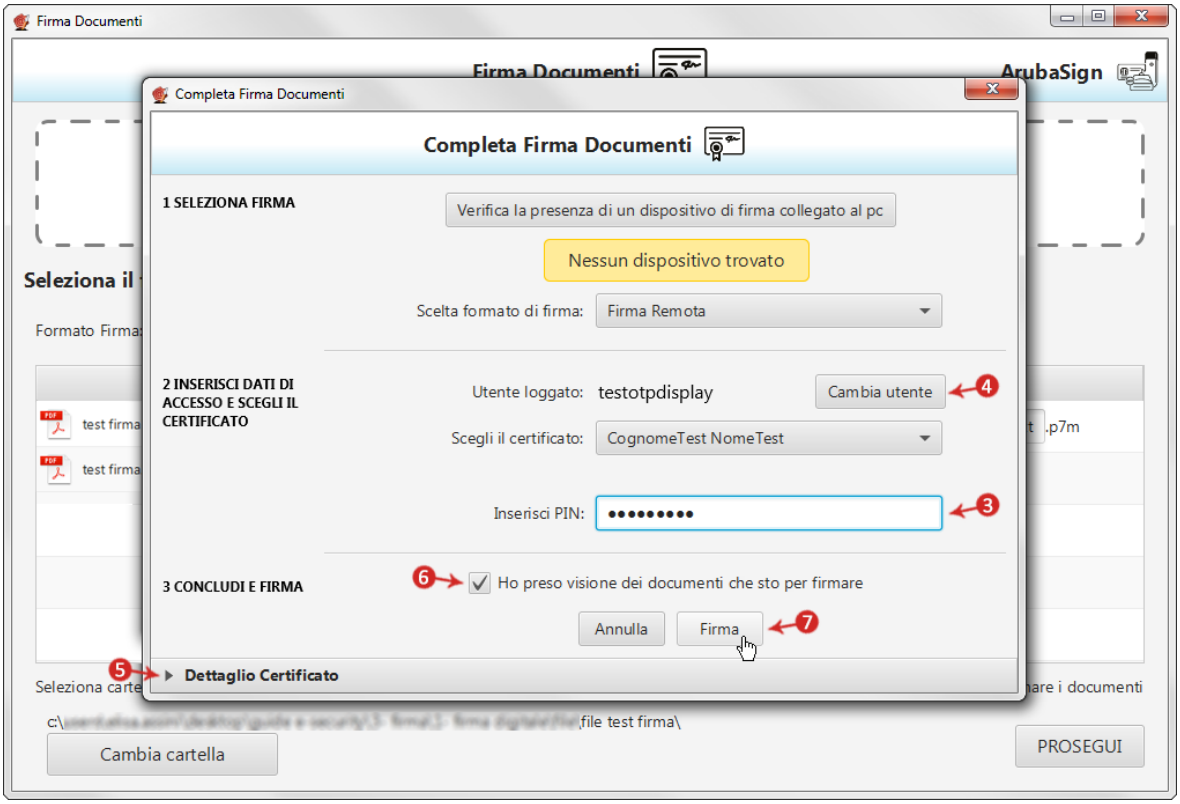
Alla schermata "**Completa Firma Documenti**":

1. Inserire la **password del proprio Account di Firma Remota**;

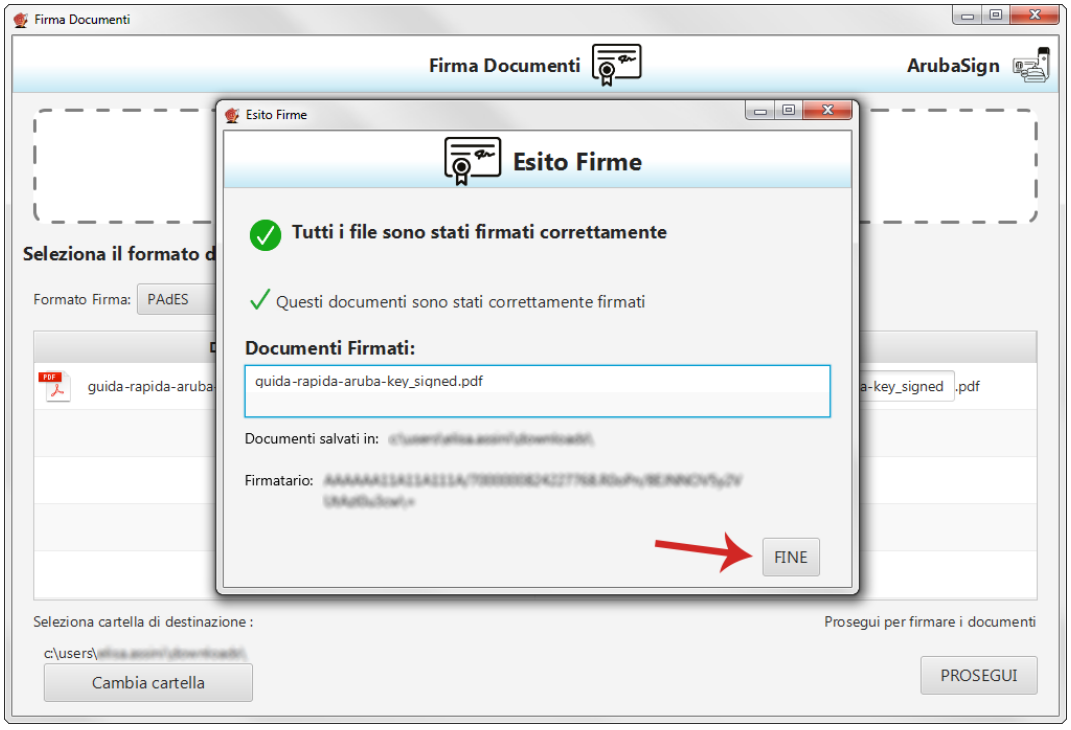
2. Cliccare su "**Accedi per selezionare il certificato**" per proseguire:



3. Inserire un **codice OTP generato con il proprio dispositivo di Firma Remota**;
4. Cliccando su "**Cambia utente**" è possibile scegliere di firmare con altro Account di Firma Remota configurato;
5. Da "**Dettagli Certificato**" visionare, qualora desiderato, le caratteristiche e la validità del Certificato utilizzato per la Firma;
6. Dichiarare di aver preso visione del documento/i e di essere consapevole della validità ai sensi di legge della Firma apposta;
7. Cliccare su "**Firma**" per concludere il processo:



Al termine dell'operazione si visualizza la seguente schermata che notifica la corretta firma del file. Cliccare su "**FINE**" per chiudere la schermata:



Il documento firmato viene salvato nella cartella indicata durante il processo, aggiungendo al **nome originale l'estensione** "**signed.pdf**".

6.9 Apposizione di Marche Temporali - Firma Remota

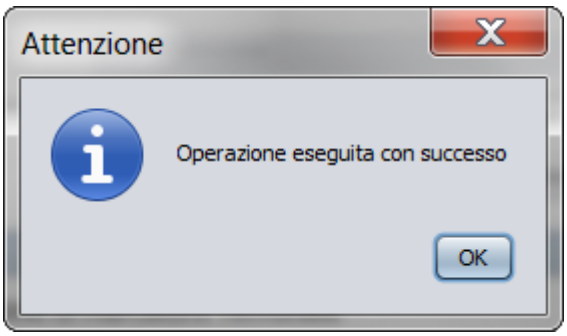
Per apporre una marca temporale è sufficiente trascinare il file sopra il pulsante "**Timestamp**":

Alla pagina visualizzata:

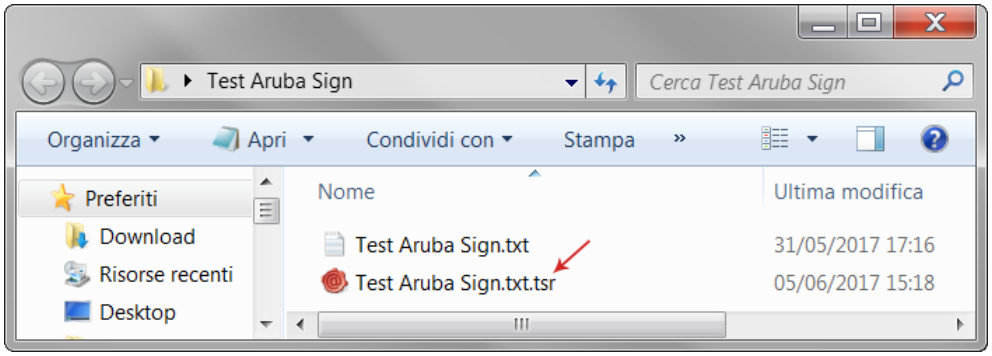
1. **Selezionare il formato di salvataggio della marca temporale. E' possibile scegliere tra**:
   - **TSR**: Il File creato contiene solo l'impronta del file, non tutto il file, e **la marca temporale in formato TSR è separata dal documento**. Pertanto, per verifica il file TSR, è indispensabile possedere anche il documento sottoposto a marca temporale, e che ha generato il TSR stesso. Se si appone una marca temporale in formato TSR e si desidera inviarla a un destinatario, è necessario inviare anche il documento di origine.
   - **TSD**: Il File creato comprende sia **il file sottoposto a marcatura che la marcatura temporale stessa**. Se si appone una marca temporale in formato TSD e si desidera inviarla a un destinatario, non è necessario inviare anche il documento di origine.
   - **Gli altri dati (password e cartella di destinazione del file) sono indicati automaticamente del sistema**:
     - La **password** è preimpostata a seguito della configurazione dell'Account di marcatura Temporale;
     - Il **percorso di destinazione del File** inserito è la cartella su cui risiede il file originale.

2. Spuntare su "**Richiedi**" per completare l'operazione:

3. Cliccare "**Ok**" al messaggio che notifica la corretta marcatura del file per completare l'operazione:



Il documento è disponibile nella cartella indicata in fase di apposizione della marcatura stessa:

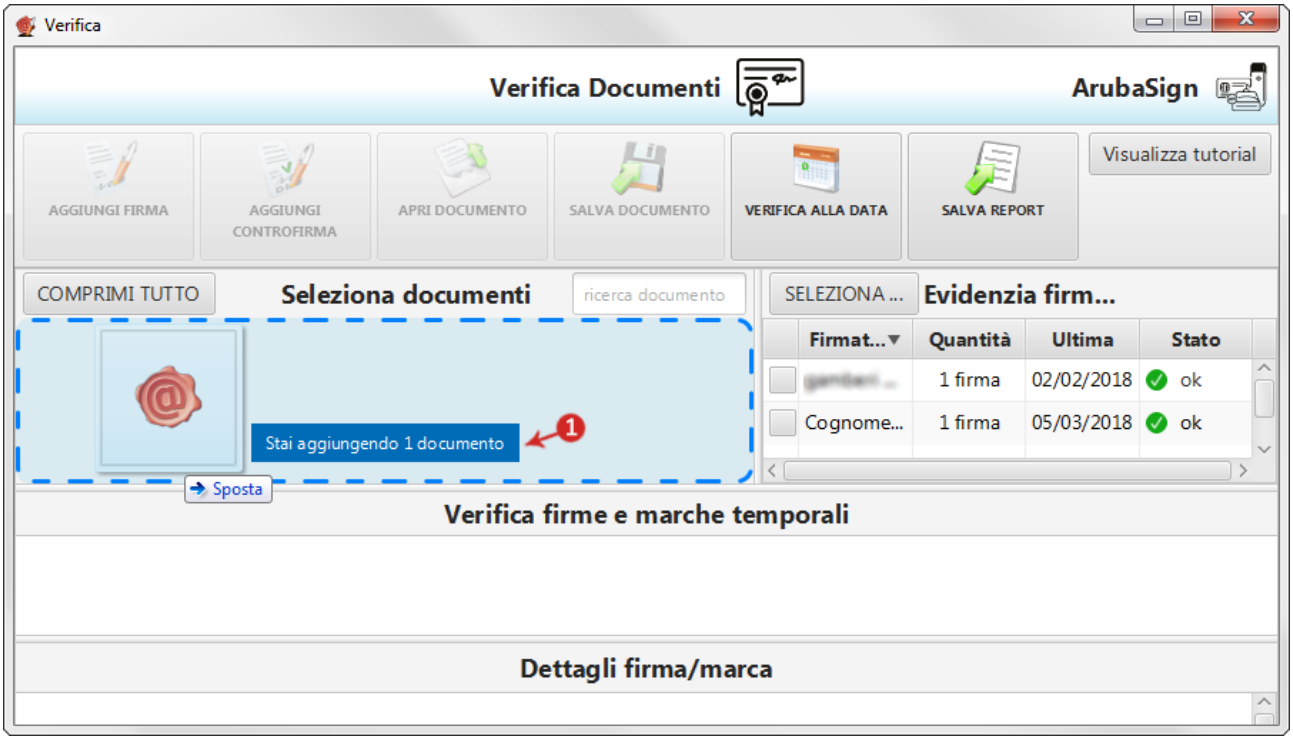


6.10 Verifica di File Firmati (Aruba Sign e Firma Remota)

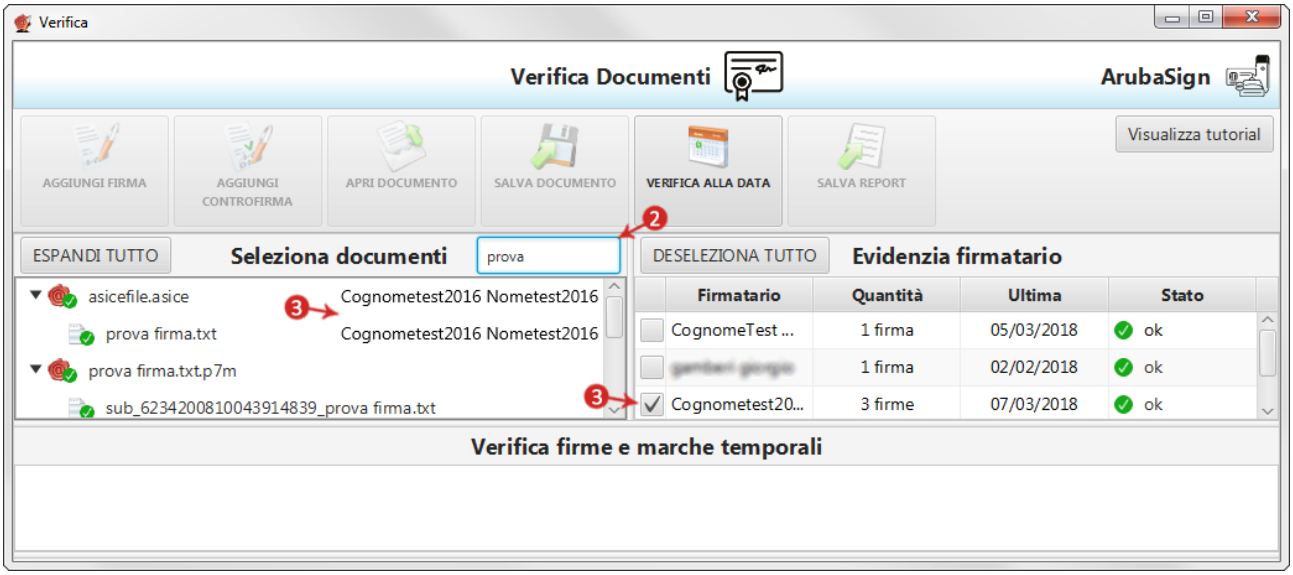
Per verificare uno o più File firmati con Aruba Sign, trascinare il/i documento/i sopra il pulsante "**Verifica**":

Alla schermata visualizzata è possibile:

1. Verificare ulteriori file firmati trascinandoli da locale su "**Seleziona Documenti**":

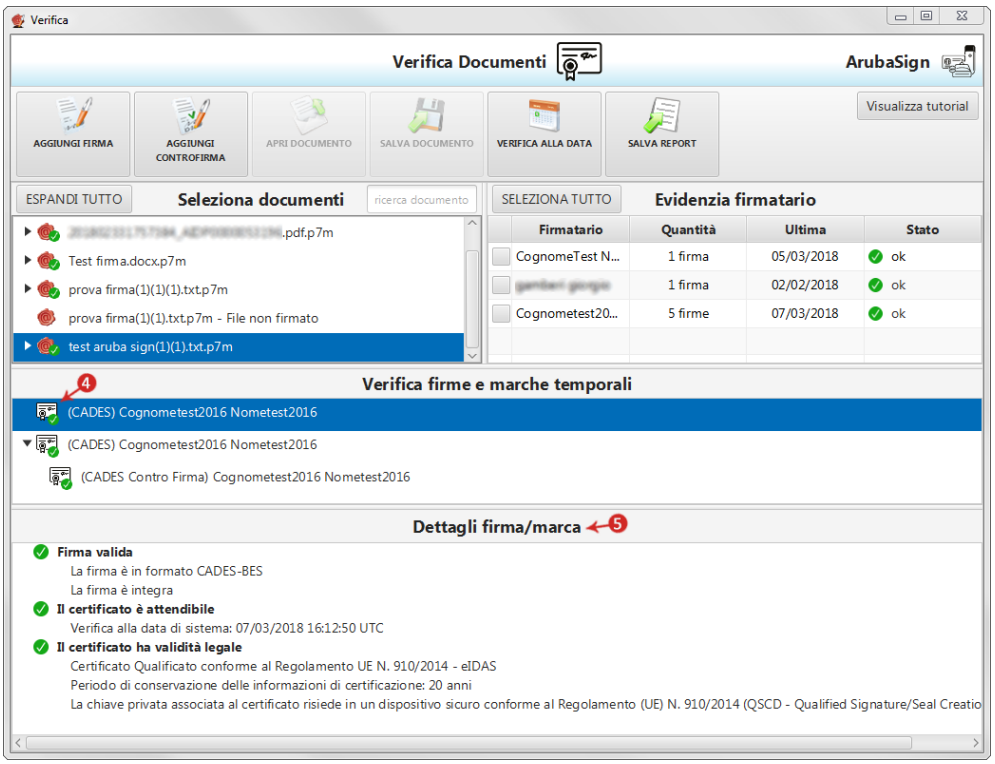


2. Il campo "**Ricerca documento**" consente di ricercare un singolo file tra quelli inseriti su "**Seleziona documenti**";
3. Su "**Evidenzia firmatario**" sono riportati il nome e cognome del/i firmatario/i, il numero di firme che ha apposto, la data dell'ultima apposizione e lo "**Stato**" (esito) della verifica. Per visionare quali sono i documenti firmati da uno specifico firmatario, inserire il flag in corrispondenza del soggetto interessato, il nome appare a fianco dei singoli file che ha firmato presenti nell'area "**Seleziona documenti**":

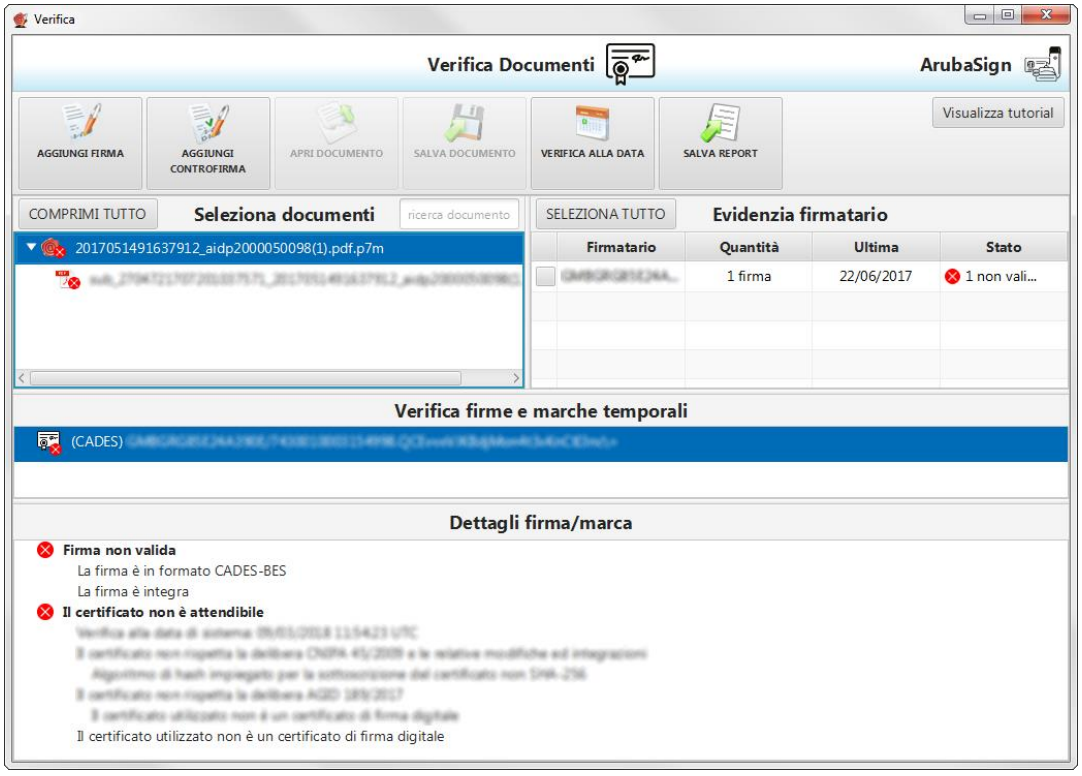


Una volta selezionato/evidenziato un singolo documento:

4. Su "**Verifica firme e marche temporali**" sono visibili le firme presenti all'interno del file;
5. Da "**Dettagli firma/marca**" è possibile verificare la validità della firma apposta, in particolare:
   - **Firma valida**
     Attesta il formato della firma e che il documento non è stato alterato dopo la firma;
   - **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**
     Attesta che il certificato del sottoscrittore è un certificato di Firma Digitale qualificato:



Se la verifica ha esito positivo si visualizza una spunta verde in corrispondenza di tutti i campi. Nel caso in cui si riscontrino una o più anomalie, ad esempio per Certificato scaduto o non attendibile, il sistema indica il messaggio di errore "**Firma KO**", attestante che **sono stati portati a termine tutti i controlli previsti per la verifica della validità della Firma apposta**, **ma qualcuno non è andato a buon fine**, come da immagine esemplificativa sottostante:

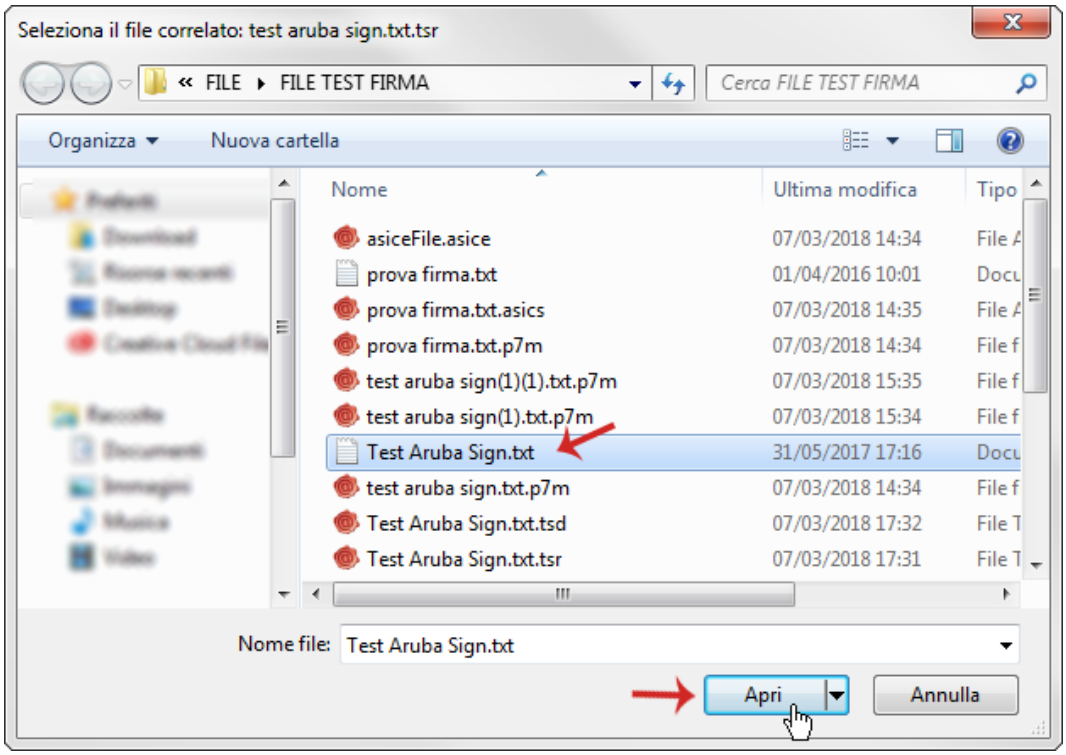


6.11 Verifica di marca temporale in Formato TSR (Aruba Sign e Firma Remota)

Una marca temporale in formato **TSR è separata dal documento su cui è apposta**. Pertanto, per verifica il file TSR, è indispensabile possedere anche il documento sottoposto a marca temporale, e che ha generato il TSR stesso.

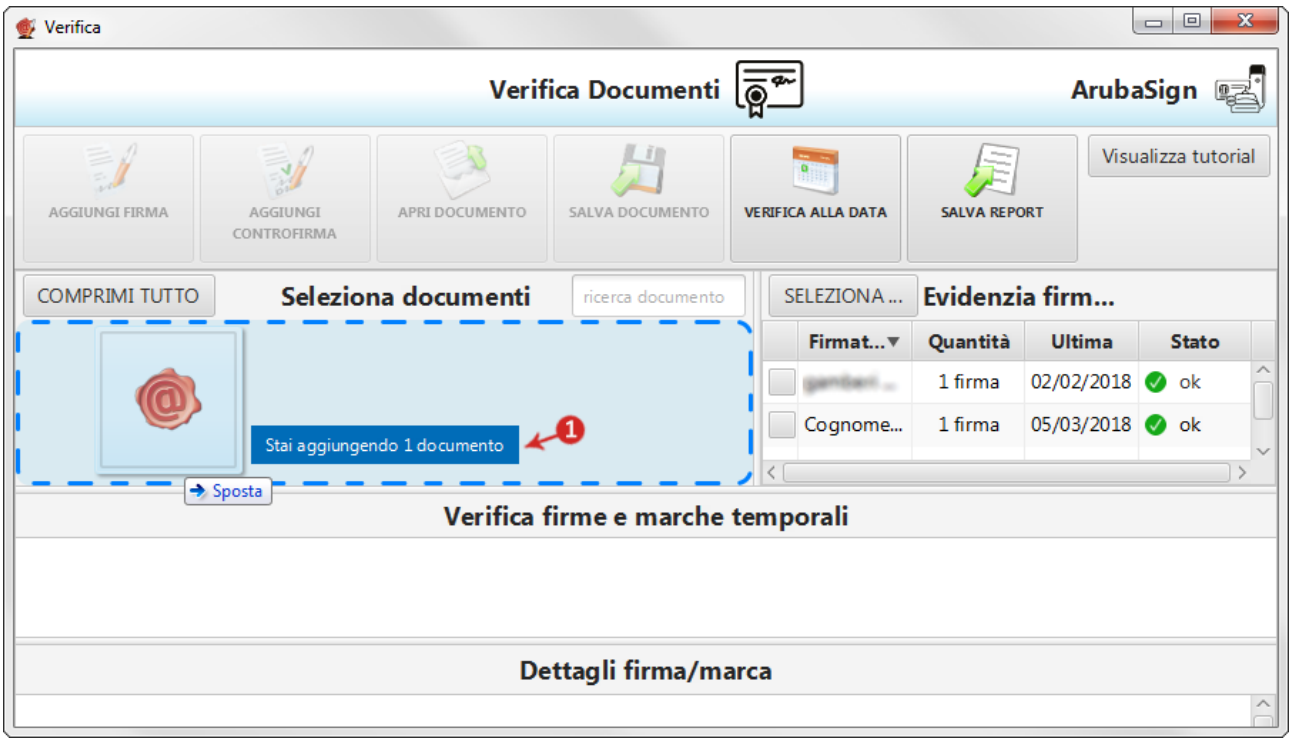
Per procedere trascinare la **Marca Temporale da verificare** sopra il pulsante "**Verifica**":

Il software esegue l'associazione "**Marca Temporale**" → "**File Marcato**" e **chiede di aprire il file associato alla marca**. Selezionare da locale il file associato alla marca stessa, quindi spuntare su "**Apri**":

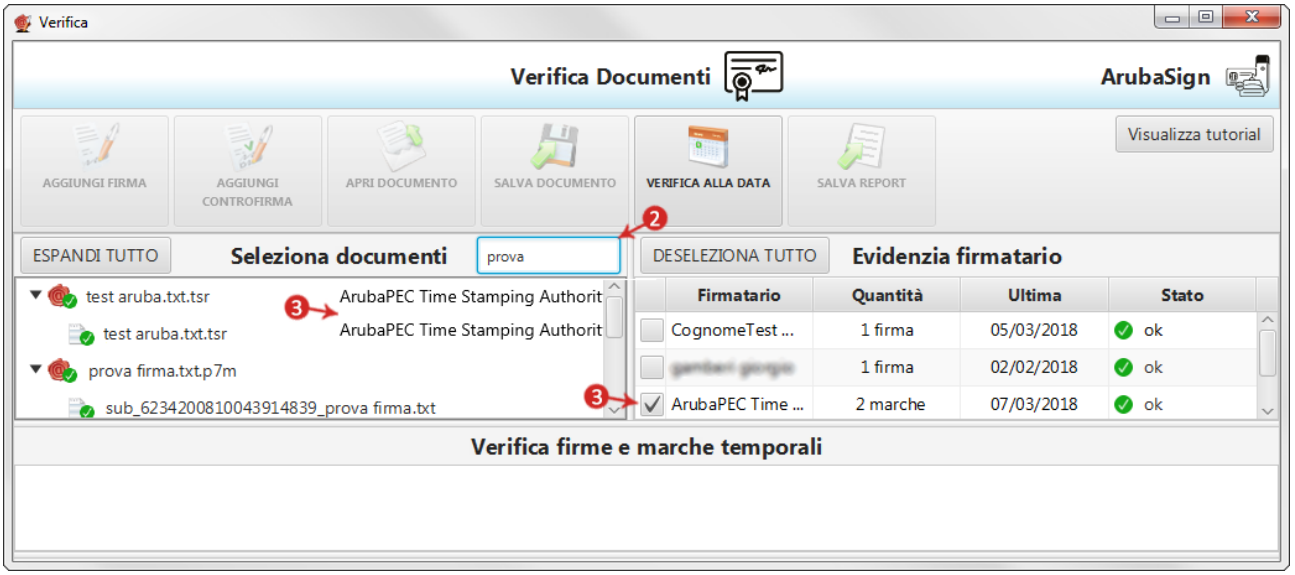


Alla schermata visualizzata è possibile:

1. Verificare ulteriori file firmati trascinandoli da locale su "**Seleziona Documenti**":

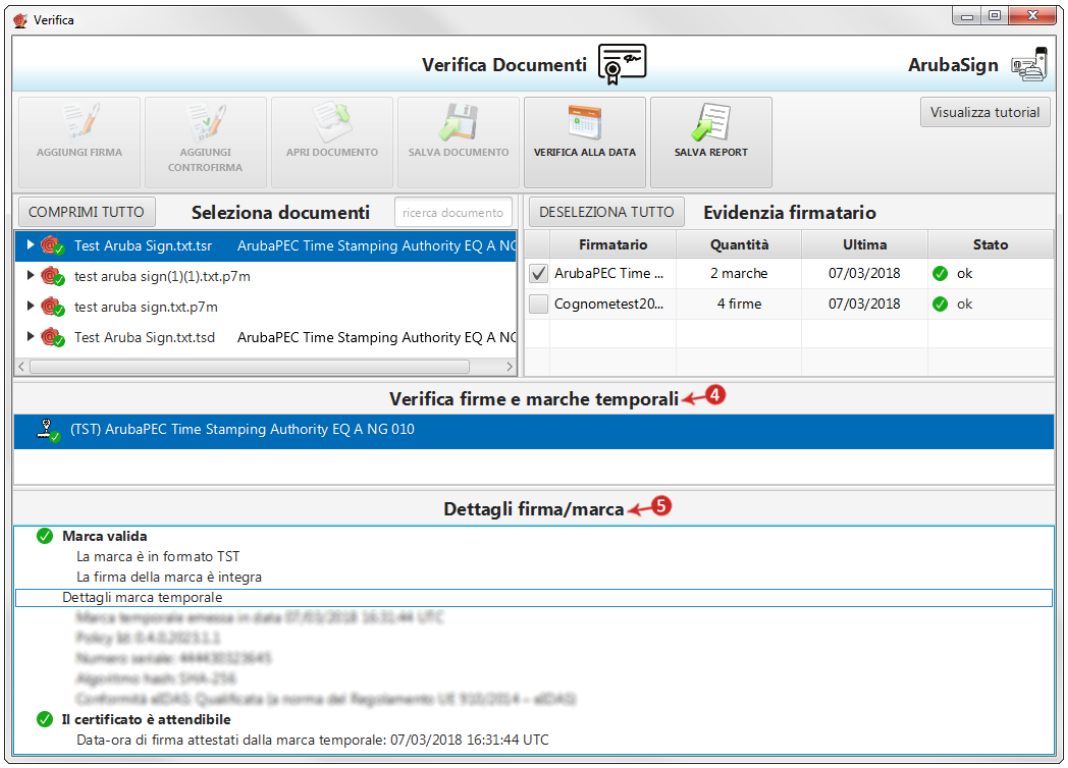


2. Il campo "**Ricerca documento**" consente di ricercare un singolo file tra quelli inseriti su "**Seleziona documenti**";
3. Su "**Evidenzia firmatario**" sono riportati i dettagli della marca apposta e il numero di documenti marcati, la data dell'ultima apposizione e lo "**Stato**" (esito) della verifica. Per visionare quali sono i documenti marcati tra quelli presenti nell'area "**Seleziona documenti**", inserire il flag in corrispondenza della marca stessa, il dettaglio appare a fianco dei singoli file:

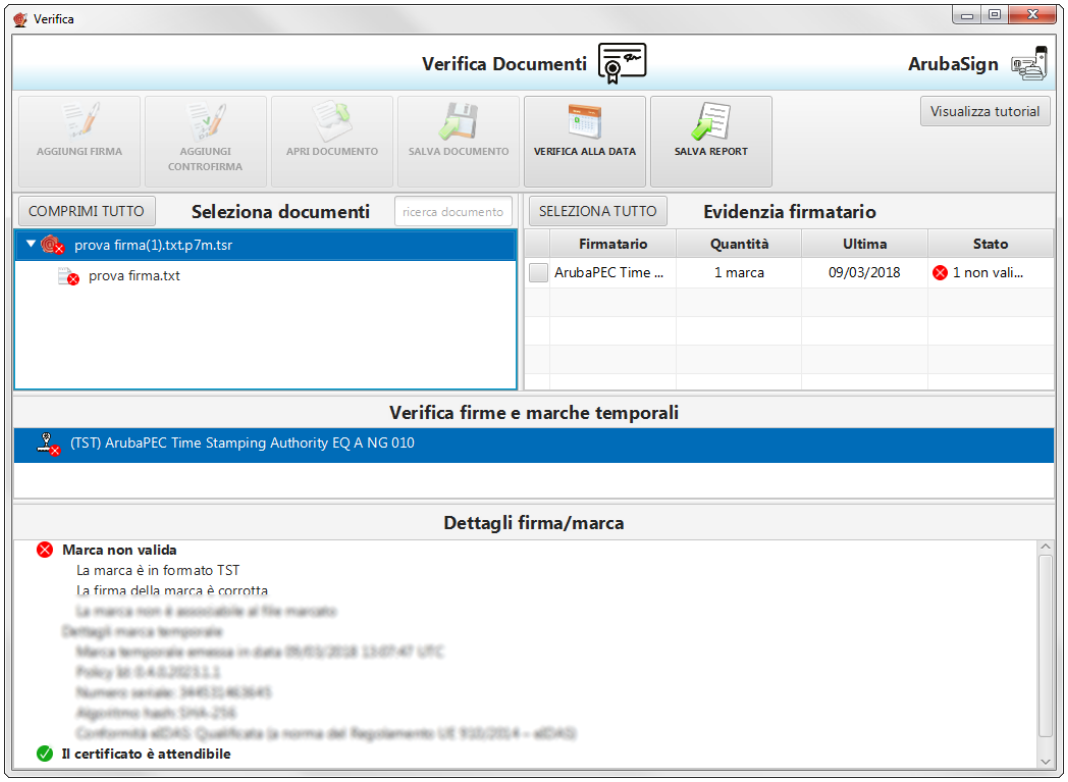


Una volta selezionato/evidenziato un singolo documento:

4. Su "**Verifica firme e marche temporali**" sono visibili le marche presenti all'interno del file;
5. Da "**Dettagli firma/marca**" è possibile verificare la validità della firma apposta, in particolare:
   - **Marca valida**
     Indica che la marca temporale è integra ed è correttamente associata al documento selezionato, nella parte "**Dettagli marca temporale**", sono riportate le specifiche della marca stessa;
   - **Il certificato è attendibile**
     Attesta che la Marca Temporale è rilasciata da un'Autorità di Certificazione inclusa nell'Elenco Pubblico dei Certificatori:



Se la verifica ha esito positivo si visualizza una spunta verde in corrispondenza di tutti i campi. Nel caso in cui si riscontrino una o più anomalie, ad esempio per Certificato scaduto o non attendibile, il sistema indica il messaggio di errore "**Marca KO**", attestante che **sono stati portati a termine tutti i controlli previsti per la verifica della validità della Firma apposta**, **ma qualcuno non è andato a buon fine**, come da immagine esemplificativa sottostante:



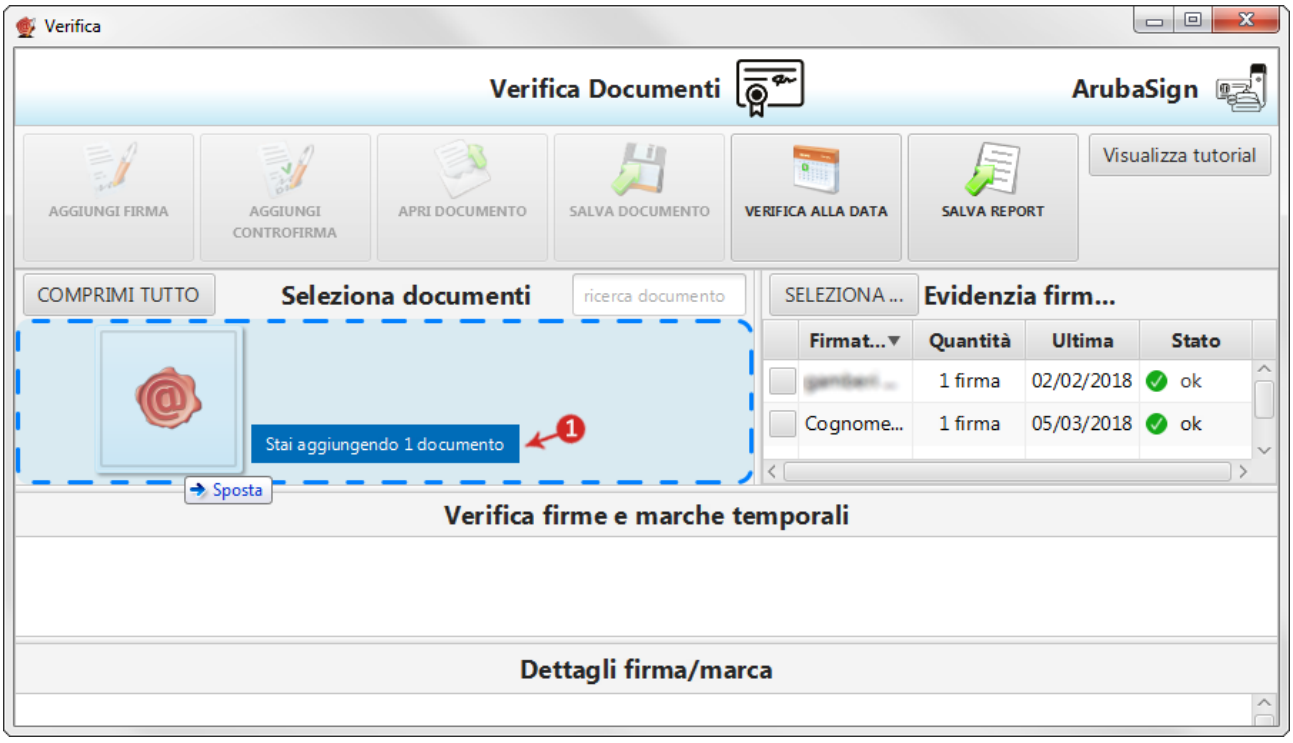
6.12 Verifica di marca temporale in Formato TSD (Aruba Sign e Firma Remota)

Una marca temporale in formato **TSD** comprende sia **il file sottoposto a marcatura che la marcatura temporale stessa**. Pertanto, per verifica il file **TSD**, non è indispensabile possedere anche il documento sottoposto a marca temporale, e che ha generato il TSD stesso.

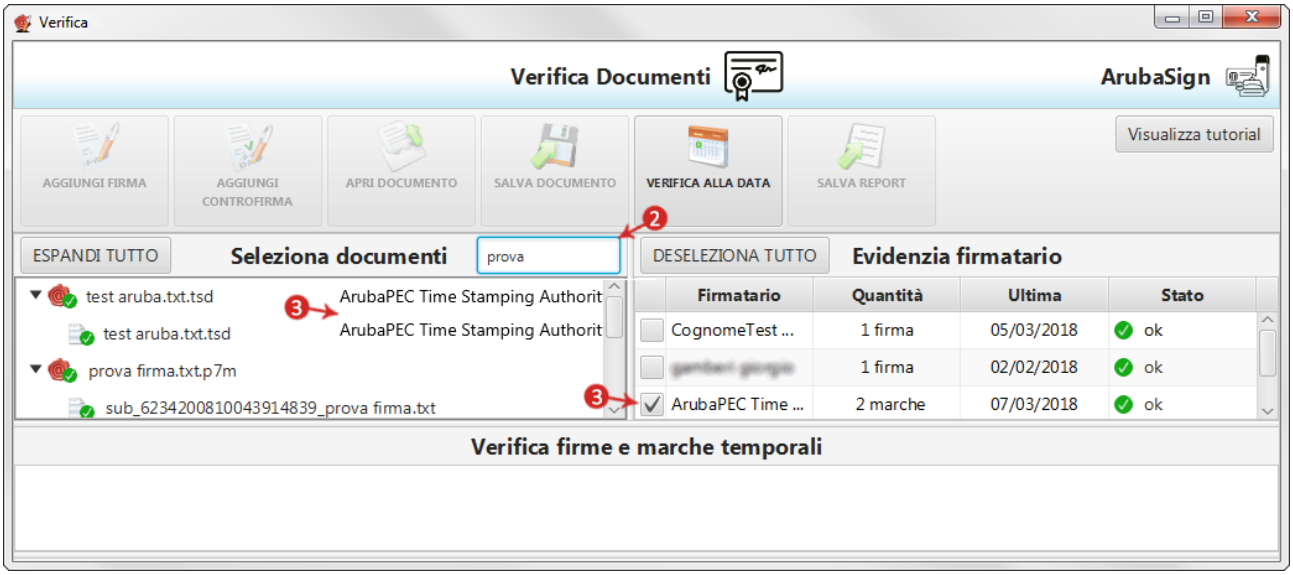
Per procedere trascinare la **Marca Temporale da verificare** sopra il pulsante "**Verifica**":

Alla schermata visualizzata è possibile:

1. Verificare ulteriori file firmati trascinandoli da locale su "**Seleziona Documenti**":

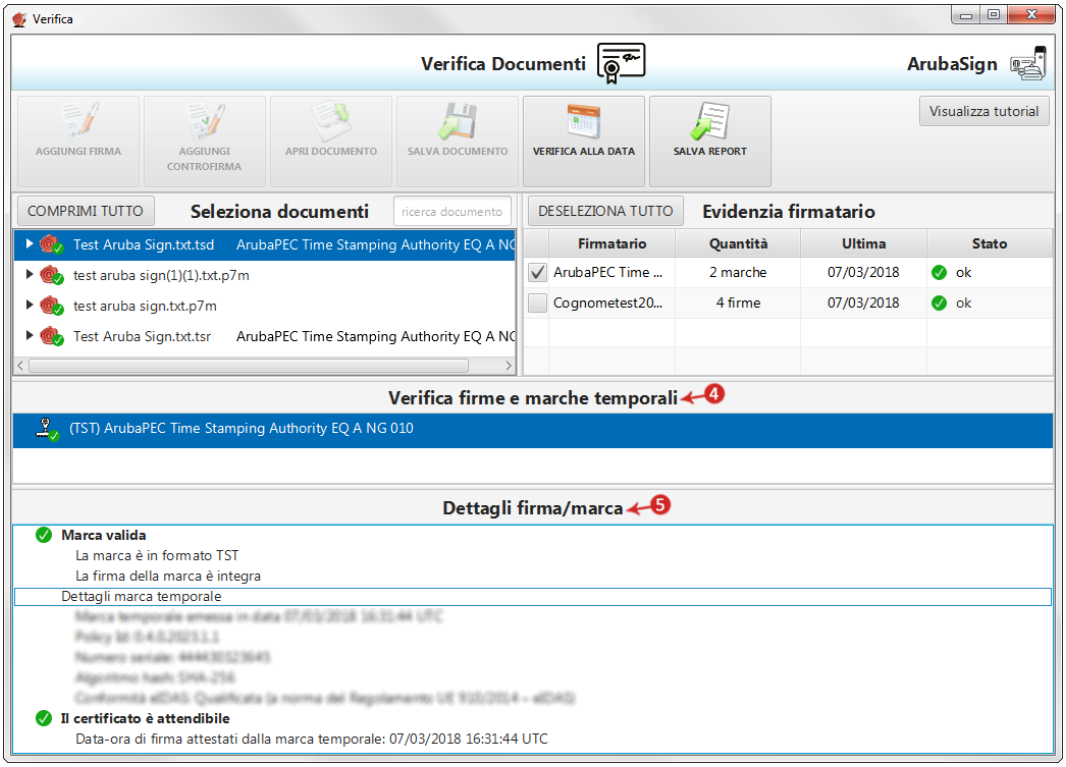


2. Il campo "**Ricerca documento**" consente di ricercare un singolo file tra quelli inseriti su "**Seleziona documenti**";
3. Su "**Evidenzia firmatario**" sono riportati i dettagli della marca apposta e il numero di documenti marcati, la data dell'ultima apposizione e lo "**Stato**" (esito) della verifica. Per visionare quali sono i documenti marcati tra quelli presenti nell'area "**Seleziona documenti**", inserire il flag in corrispondenza della marca stessa, il dettaglio appare a fianco dei singoli file:

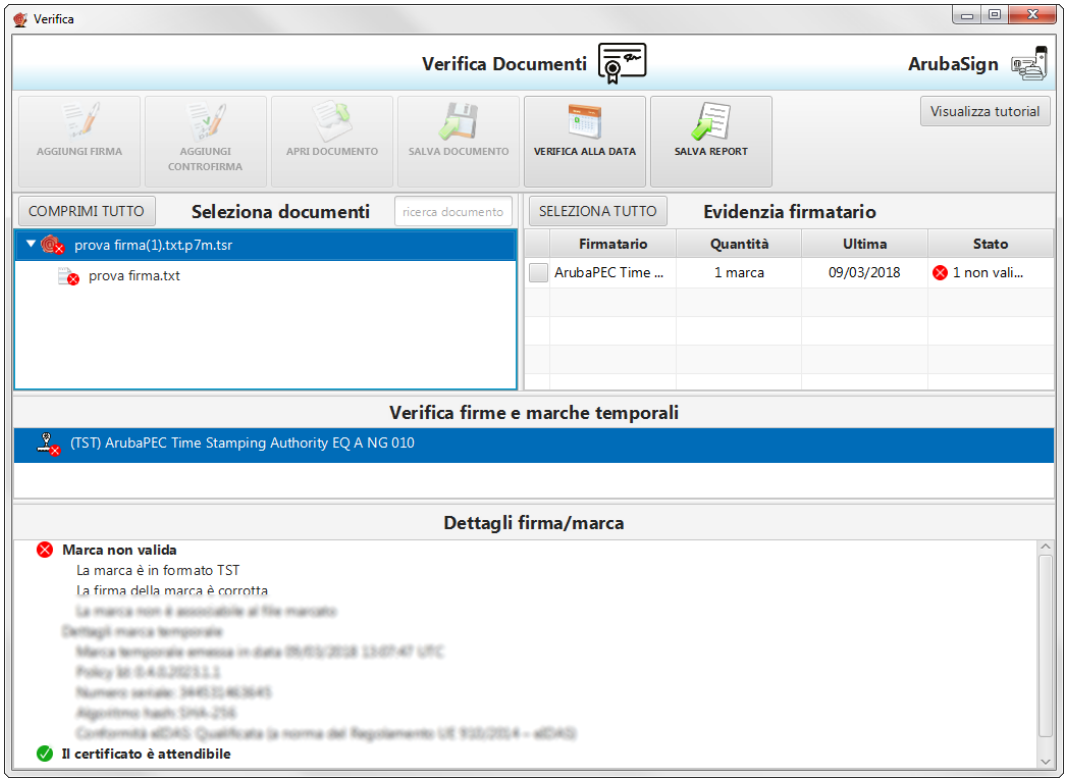


Una volta selezionato/evidenziato un singolo documento:

4. Su "**Verifica firme e marche temporali**" sono visibili le marche presenti all'interno del file;
5. Da "**Dettagli firma/marca**" è possibile verificare la validità della firma apposta, in particolare:
   - **Marca valida**
     Indica che la marca temporale è integra ed è correttamente associata al documento selezionato, nella parte "**Dettagli marca temporale**", sono riportate le specifiche della marca stessa;
   - **Il certificato è attendibile**
     Attesta che la Marca Temporale è rilasciata da un'Autorità di Certificazione inclusa nell'Elenco Pubblico dei Certificatori:



Se la verifica ha esito positivo si visualizza una spunta verde in corrispondenza di tutti i campi. Nel caso in cui si riscontrino una o più anomalie, ad esempio per Certificato scaduto o non attendibile, il sistema indica il messaggio di errore "**Marca KO**", attestante che **sono stati portati a termine tutti i controlli previsti per la verifica della validità della Firma apposta**, **ma qualcuno non è andato a buon fine**, come da immagine esemplificativa sottostante:



6.13 Generare PIN OTP con Dispositivi di Firma Remota

6.13.1 Generare una password OTP con OTP Display

Per generare un PIN OTP con l'**OTP con Display**, tenere premuto il **pulsante rosso del proprio OTP con display**, rilasciarlo e attendere che il **codice sia visualizzato sul display**, come da immagine esemplificativa sottostante:

Nel caso in cui si utilizzi Dispositivi OTP a evento, cioè Display c100, (con seriale che inizia per uno), generare PIN OTP solo ed esclusivamente in caso di effettivo utilizzo degli stessi per apporre Firma Remota a documenti. Qualora si generi tramite il proprio Token un tot numero di PIN OTP senza utilizzarli, **il Certificato di Firma Remota va fuori sincronizzazione e la procedura di Firma** di un documento non va a buon fine. **Per ovviare il problema** e sbloccare il dispositivo, effettuare la sincronizzazione della Firma, come indicato al paragrafo successivo di questa stessa guida rapida.

6.13.2 Generare una password OTP con OTP USB

Per generare un PIN con l'**OTP USB** inserire il Token in una porta USB. Attendere l'installazione dei driver del dispositivo che risulta conclusa nel momento **in cui si illumina il led al centro del Token stesso**, come da immagine esemplificativa sottostante:

A questo punto eseguire contemporaneamente le operazioni sotto indicate:

- Posizionare il cursore del mouse sopra il riquadro Password OTP;
- Sfiorare con il dito il led luminoso del Token OTP USB collegato alla presa USB del pc

Generare PIN OTP solo ed esclusivamente in caso di effettivo utilizzo degli stessi per apporre Firma Remota a documenti. Qualora si generi tramite il proprio Token un tot numero di PIN OTP senza utilizzarli, **il Certificato di Firma Remota va fuori sincronizzazione e la procedura di Firma** di un documento non va a buon fine. **Per ovviare il problema** e sbloccare il dispositivo, effettuare la sincronizzazione della Firma, come indicato al paragrafo successivo di questa stessa guida rapida.

6.13.3 Generare una password OTP con OTP Mobile

Per generare un PIN con l'**OTP Mobile**, scaricare **l'applicazione Aruba Mobile OTP** sul proprio smartphone, quindi **per generare una Password OTP**, aprire l'applicazione stessa e cliccare sull'account di Firma Remota configurato:

Il **PIN OTP**, di **validità temporale momentanea**, **si visualizza in automatico**, come da immagine esemplificativa sottostante:

Nel caso in cui si utilizzi **la versione della App OTP mobile precedente a settembre 2016**, **generare PIN OTP solo ed esclusivamente in caso di effettivo utilizzo degli stessi per apporre Firma Remota a documenti**. Qualora si generi tramite il proprio Token un tot numero di PIN OTP senza utilizzarli, **il Certificato di Firma Remota va fuori sincronizzazione e la procedura di Firma** di un documento non va a buon fine. **Per ovviare il problema** e sbloccare il dispositivo, effettuare la sincronizzazione della Firma, come indicato al paragrafo successivo di questa stessa guida rapida.

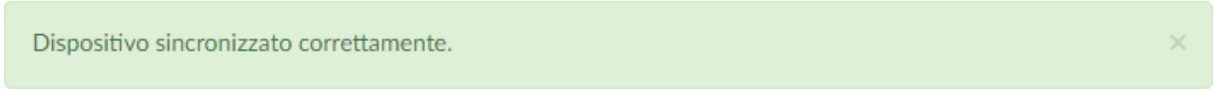
7. Sincronizzazione Dispositivo Firma Remota

Per eseguire la sincronizzazione del Dispositivo di Firma Remota in proprio possesso, autenticarsi al Pannello di "**Gestione Firma Remota**" collegandosi al link https://selfcare.firma-remota.it/asmonitor/panel/login e inserendo Username di Firma Remota e relativa password, quindi:

1. Dal menù in alto selezionare la specifica voce "**Gestione Dispositivi**":

2. Al Form "**Gestione**", da "**Sincronizzazione dispositivo**" (secondo in basso) inserire Codice Utente indicato nella scratch card ricevuta a seguito dell'ordine del servizio;
3. Due codici OTP consecutivi generati con il Token posseduto (In caso di utilizzo di dispositivi che generano password OTP temporali, è richiesto l'inserimento di un solo codice OTP);
4. Spuntare su "**Sincronizza dispositivo**" per completare la procedura:

Si visualizza la seguente schermata di conferma:



8. Configurazione Proxy http (Firma Remota)

Per utilizzare il **Software Aruba Sign in una rete protetta da Proxy** aprire il menù "**Opzioni e Parametri**" di Aruba Sign:

Quindi allo specifico Tab "**Proxy HTTP**" togliere la spunta dalla voce "**Individua proxy in maniera automatica**", impostare i relativi parametri e salvarli. Di seguito un esempio di configurazione:

Proxy Url: 192.168.1.1
Proxy Port: 8080
Proxy User: Nome utente
Proxy Password: Password

Cliccare su "**Salva**" per completare l'operazione.

Qualora non siano disponibili i dati relativi a una delle due sezioni HTTP o LDAP ad esempio nel caso in cui la rete non supporti entrambe le configurazioni, procedere solo con la creazione relativa alla tipologia di Proxy supportata.

Per ulteriori approfondimenti si consiglia di visionare le guide online:

- Aruba Sign e Firma Digitale;
- Aruba Sign e Firma Remota.