

Firma Digitale

Software Aruba Sign

Sommario

1	Prerequisiti hardware e software	4
2	Utilizzo Aruba Sign e Firma Remota	4
2.1	Attivazione Account Firma Remota e installazione Aruba Sign.....	4
2.2	Configurazione parametri Firma Remota su Aruba Sign	5
3	Firma e verifica file Aruba Sign - Firma Remota	6
3.1	Firma uno o più file in formato .p7m - Firma Remota.....	9
3.2	Firmare un singolo file in formato ASiC-S - Firma Remota	12
3.3	Firma di più file in formato ASiC-E - Firma Remota.....	14
3.4	Apposizione Firma Parallela - Firma Remota.....	16
3.5	Apposizione Controfirma - Firma Remota.....	18
3.6	Apposizione Firma PDF - Grafica Firma Remota.....	20
3.7	Apposizione Firma PDF - Invisibile Firma Remota	22
3.8	Apposizione di Marche Temporali - Firma Remota	24
	Verifica Marche Temporali Residue	26
3.9	Verifica di file Firmati Aruba Sign e Firma Remota.....	27
3.10	Verifica Marche Temporali in formato TSR Aruba Sign e Firma Remota.....	31
3.11	Verifica Marche Temporali in formato TSD Aruba Sign e Firma Remota	33
3.12	Generare PIN OTP con Dispositivi di Firma Remota	35
	Generare una password OTP con OTP Display	35
	Generare una password OTP con OTP Mobile	36
4	Sincronizzazione dispositivo Firma Remota	37
5	Configurazione Proxy http Firma Remota	37
6	Installazione e avvio del software – Firma Digitale	39
6.1	Installare i driver dei lettori di Firma Digitale	39
6.2	Installare i driver Smart Card.....	40
6.3	Installare il software Aruba Sign.....	41
7	Firma e verifica file Aruba Sign - Firma Digitale	42
7.1	Caricare documenti da firmare e/o cartelle su Aruba Sign	42
7.2	Firmare uno o più file in formato .p7m - Firma Digitale.....	43
7.3	Firmare un singolo file in formato ASiC-S - Firma Digitale	45
7.4	Firmare più file in formato ASiC-E - Firma Digitale.....	46
7.5	Apposizione Firma Parallela - Firma Digitale	48
7.6	Apposizione Controfirma - Firma Digitale	49
7.7	Apposizione Firma PDF - Grafica - Firma Digitale	51
7.8	Firmare un PDF con firma invisibile - Firma Digitale	53
7.9	Apposizione di Marche Temporali - Firma Digitale	55
7.10	Verifica di file firmati - Firma Digitale	56
7.11	Verifica di Marca Temporale in formato TSR - Firma Digitale	58
7.12	Verifica di Marca Temporale in formato TSD - Firma Digitale	60
8.1	Gestione PIN/PUK.....	62
8.2	Cifra e Decifra un file Aruba Sign Windows.....	64
8.3	Configurazione Proxy http Aruba Sign.....	67
9	Import e verifica certificato Firma Digitale	68
9.1	Import certificato	68

9.2	Verifica certificati	70
9.3	Import Certificato con Aruba Sign Mac	75
9.4	Import Certificato su Mozilla Firefox - Aruba Sign Mac.....	76

1 Prerequisiti hardware e software

La postazione in cui viene collegato il software Aruba Sign deve possedere i seguenti prerequisiti:

Software

Sistemi Operativi:

- Windows 8 32/64bit e successivi;
- Mac OS 10.15 e successivi;
- Linux Ubuntu 20.04 LTS e versioni LTS successive.

Per Windows è richiesta versione Internet Explorer 11.

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
- possibilità di poter instaurare connessioni HTTP, HTTPS e LDAP

2 Utilizzo Aruba Sign e Firma Remota

2.1 Attivazione Account Firma Remota e installazione Aruba Sign

La Firma Remota è composta 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.

4

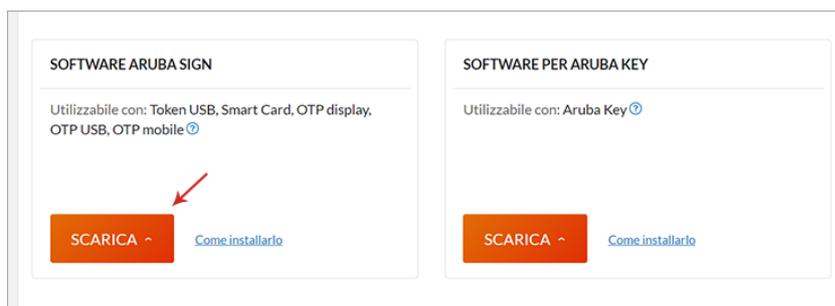
Attivare un account di Firma Remota

Per l'attivazione della Firma Remota con Scratch Card o senza Scratch Card, consultare la guida dedicata di [attivazione Firma Remota](#).

Installazione e avvio software Aruba Sign

Una volta eseguita l'attivazione della Firma Remota e la creazione del proprio account, installare il software Aruba Sign:

- collegarsi nella sezione [download-software-driver](#);
- dal menu a tendina **Software per firmare** → selezionare **Software Aruba Sign**, quindi cliccare su **Scarica** per continuare (l'esempio di seguito indicato si riferisce a Windows):



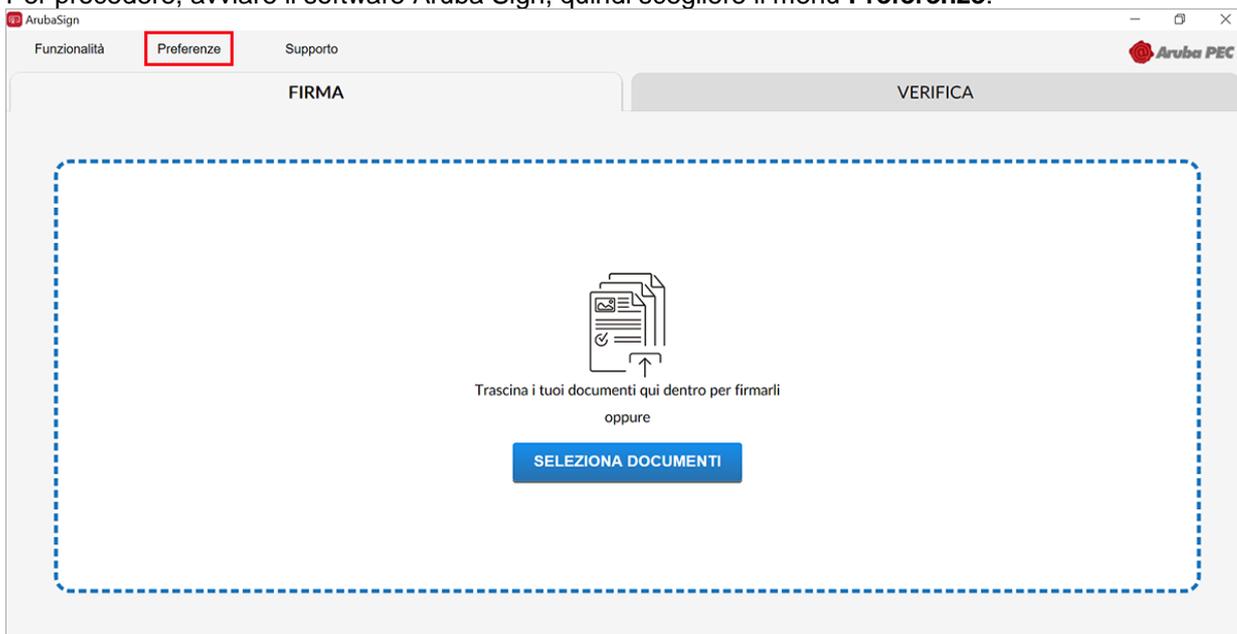
Scaricare ed eseguire su locale il file di installazione, quindi **installare il software** utilizzando la procedura guidata:

- 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.

2.2 Configurazione parametri Firma Remota su Aruba Sign

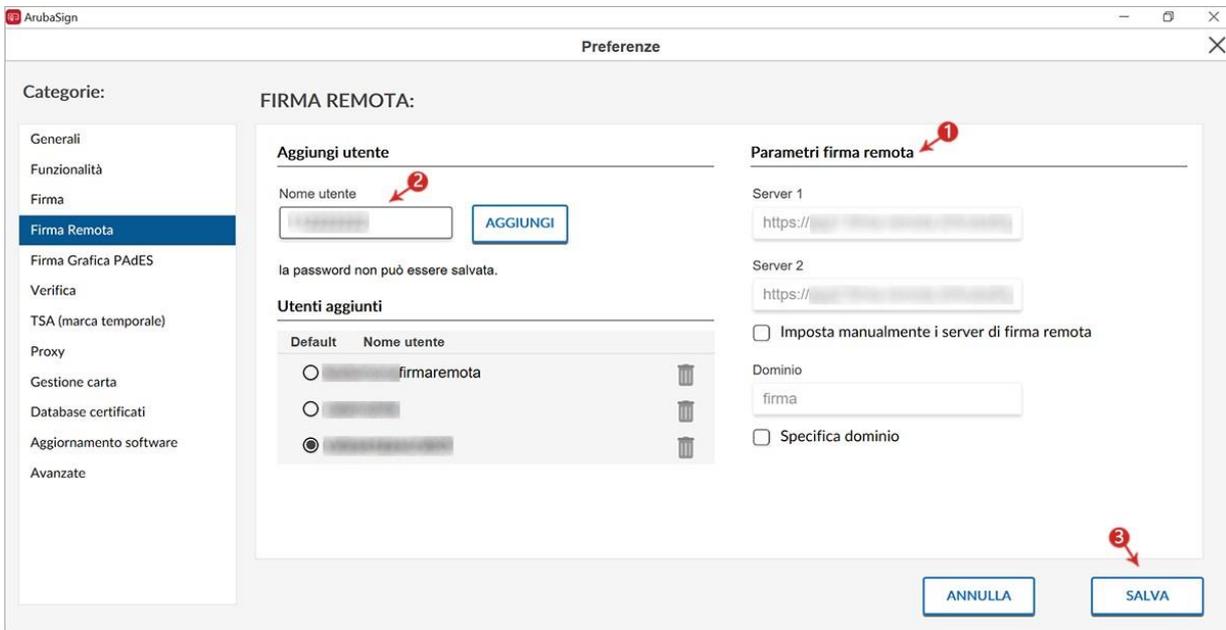
Una volta eseguita l'attivazione della Firma Digitale Remota, procedere all'installazione gratuita del software di firma Aruba Sign, è possibile la configurazione del proprio account (nome utente), per firmare documenti digitali, apporre marche temporali, e verificare i file firmati stessi. In caso di mancata configurazione è necessario inserire ad ogni utilizzo il nome utente e relativa password.

Per procedere, avviare il software Aruba Sign, quindi scegliere il menu **Preferenze**:



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

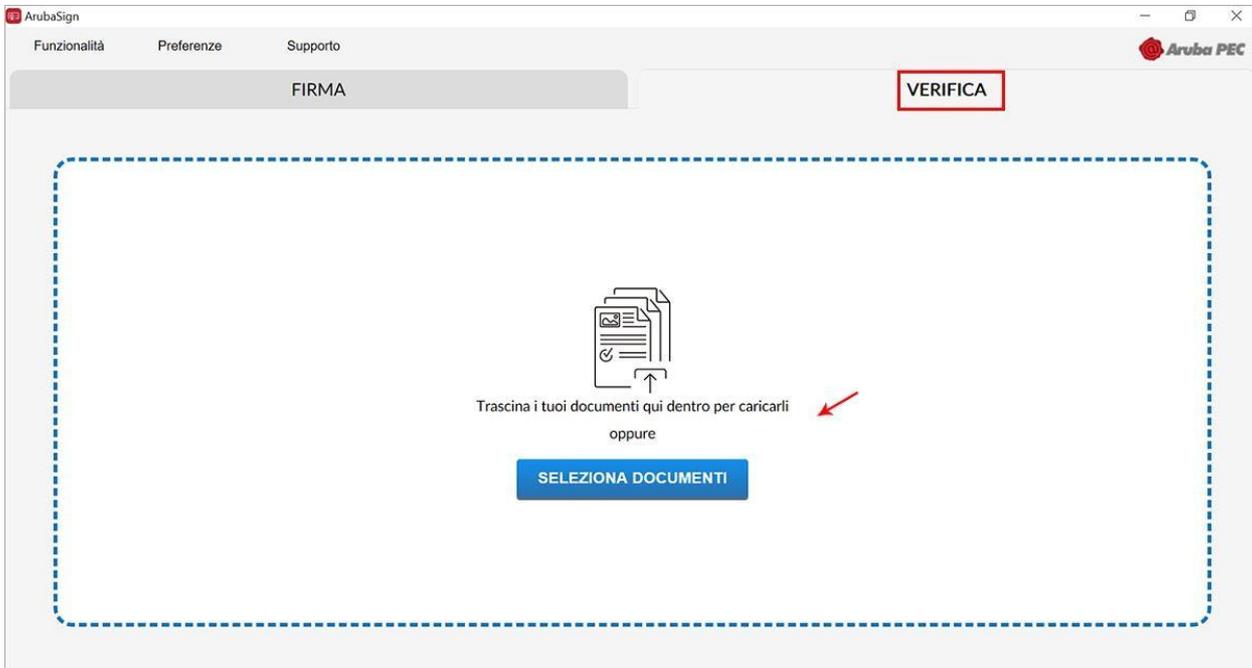
1. in caso di **soluzioni personalizzate**, inserire manualmente i parametri dell'indirizzo server primario e secondario, inserendo il flag nella checkbox apposita o lasciare quelli valorizzati automaticamente dal sistema;
2. scrivere il **Nome Utente Firma Remota** creato in fase di attivazione del servizio. Nel caso in cui il dominio sia "firma", cioè per soluzioni non personalizzate, è sufficiente inserire solo il nome utente, omettendo la specifica dominio;
3. cliccare su **Salva** per completare l'operazione:



3 Firma e verifica file Aruba Sign - Firma Remota

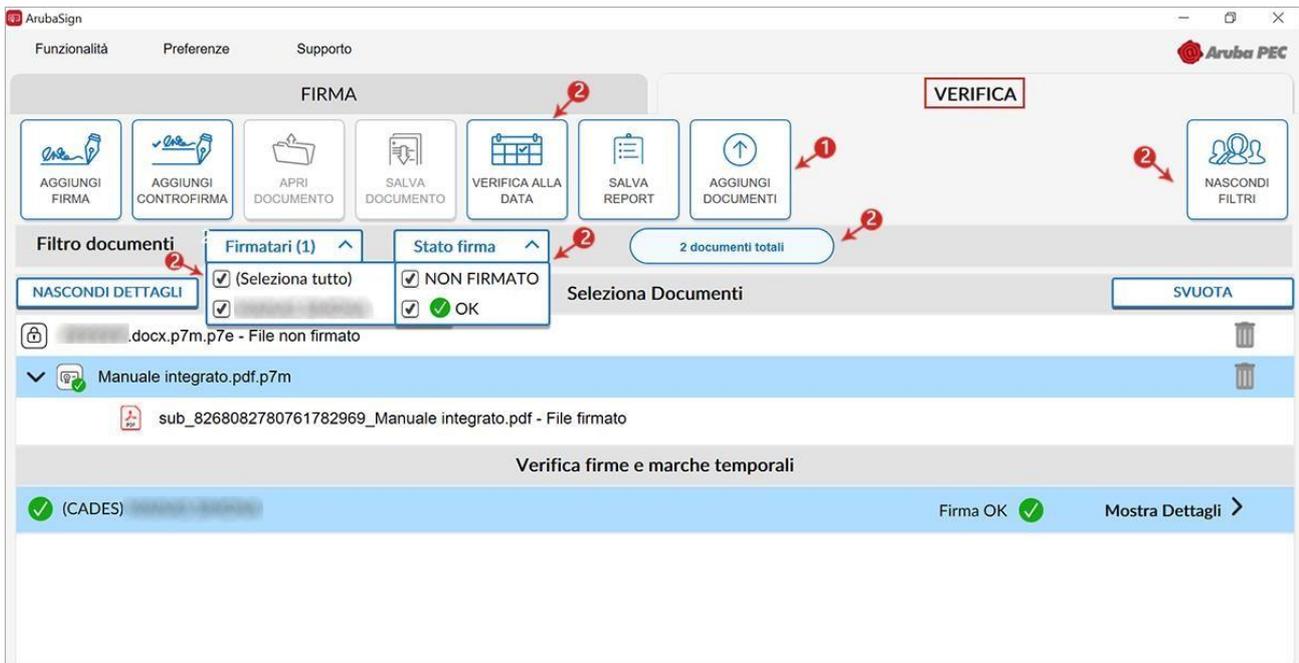
La verifica dei file firmati permette di verificare la validità legale del certificato.

Per verificare uno o più file firmati con Aruba Sign, selezionare il documento nella scheda **Verifica**:



Alla schermata visualizzata è possibile:

1. verificare ulteriori file firmati trascinandoli da locale o su **Aggiungi Documento**;
2. da **Mostra/Nascondi Filtri** 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":



7

3. **Verifica firme e marche temporali** sono visibili le firme presenti all'interno del file:

- **Firma valida**

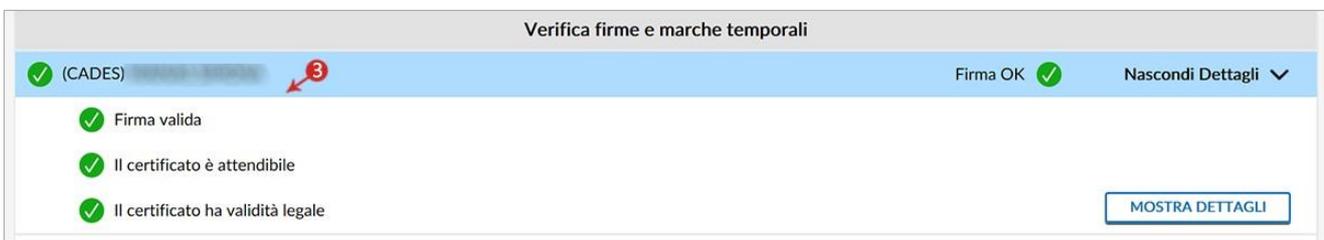
Attesta il formato della firma e che il documento non è stato alterato dopo la firma;

- **Il certificato è attendibile**

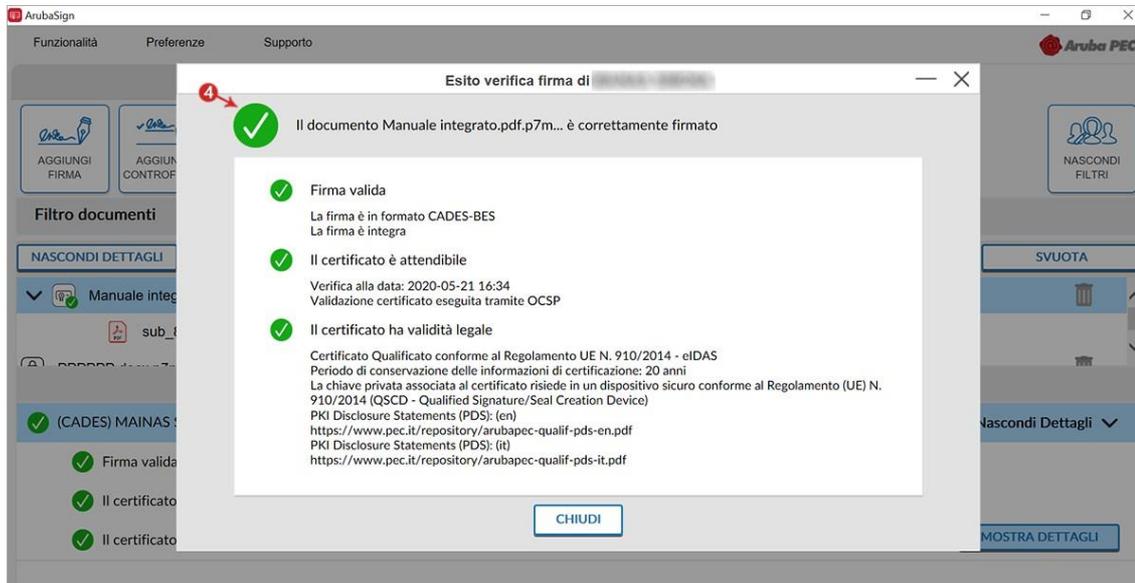
Il messaggio indica che il certificato del sottoscrittore è garantito da una Autorità di Certificazione inclusa nell'Elenco Pubblico dei Certificatori e che non risulta scaduto alla data della Verifica;

- **Il certificato ha validità legale**

Attesta che il certificato del sottoscrittore è un certificato di Firma Digitale qualificato:



Da **Mostra Dettagli** è possibile verificare la validità della firma apposta:



In caso di necessità è possibile attivare un'opzione che consente di verificare uno o più File Firmati con certificati non emessi da una Certification Authority.

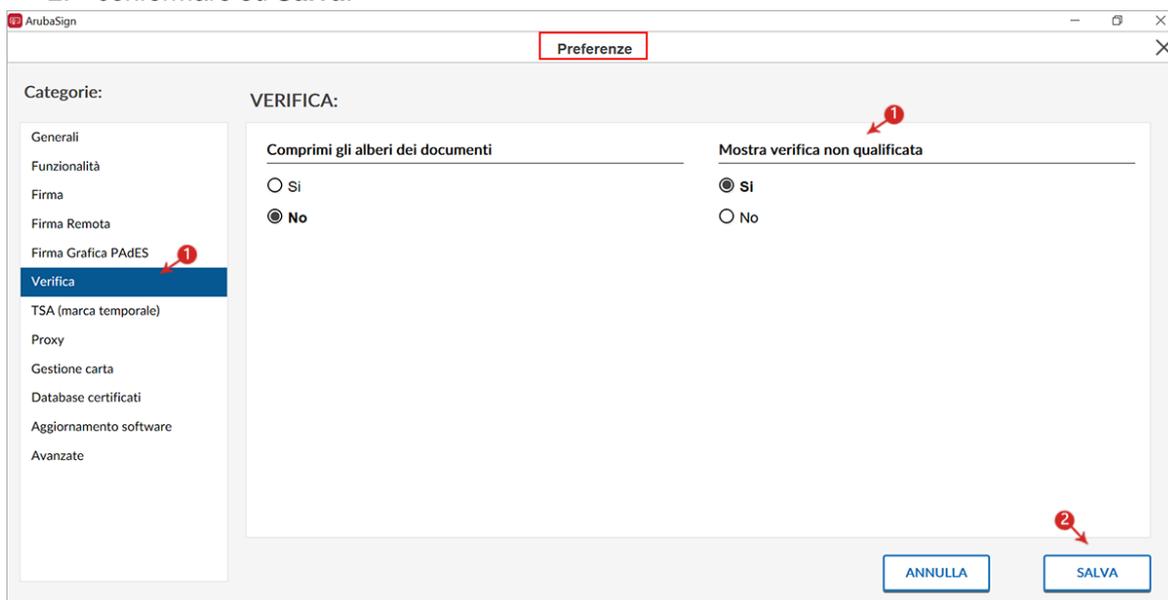
La verifica della Firma opposta può essere:

- **Non qualificata:** la firma è considerata valida se è integra e il certificato valido. Non è richiesto che sia emesso da una Certification authority di firma digitale.
- **Qualificata:** la firma apposta a un file è considerata valida se è integra, il certificato valido e rilasciato da una Certification Authority qualificata nel rispetto della normativa vigente circa la firma digitale qualificata.

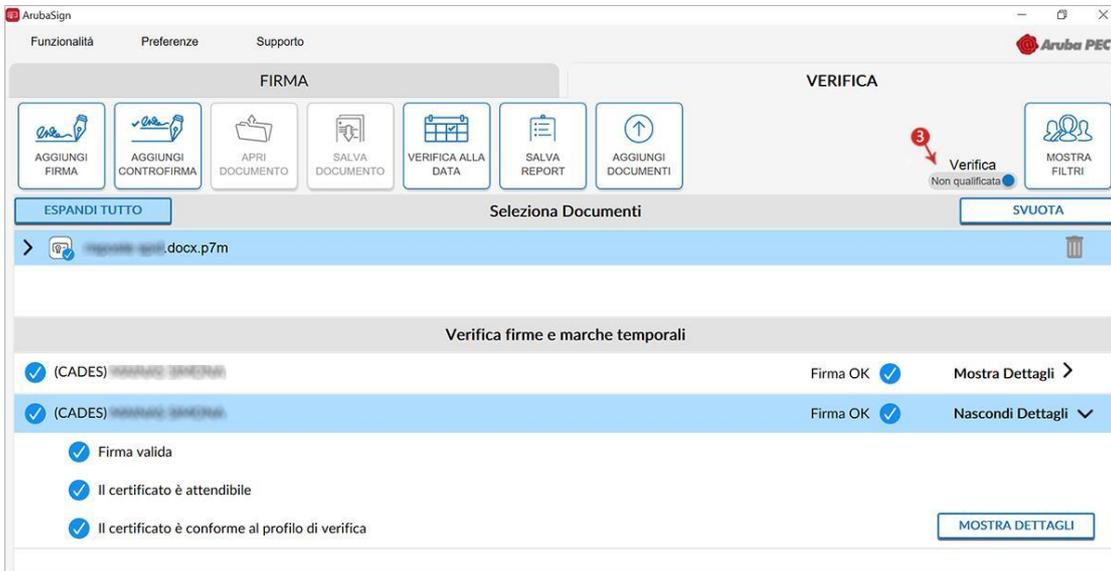
8

Per attivare l'opzione, accedere su **Preferenze** di Aruba Sign:

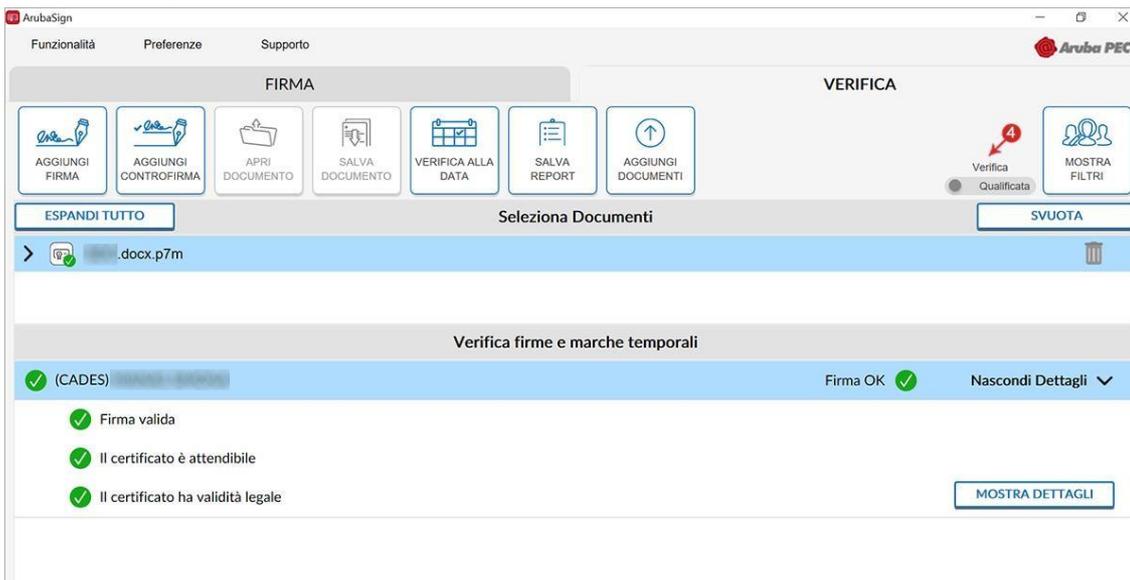
1. su **Verifica** abilitare **Mostra verifica non qualificata**;
2. confermare su **Salva**:



3. L'opzione di verifica **Non qualificata** è attiva:



4. Se l'opzione non viene attivata, la verifica è **Qualificata**:

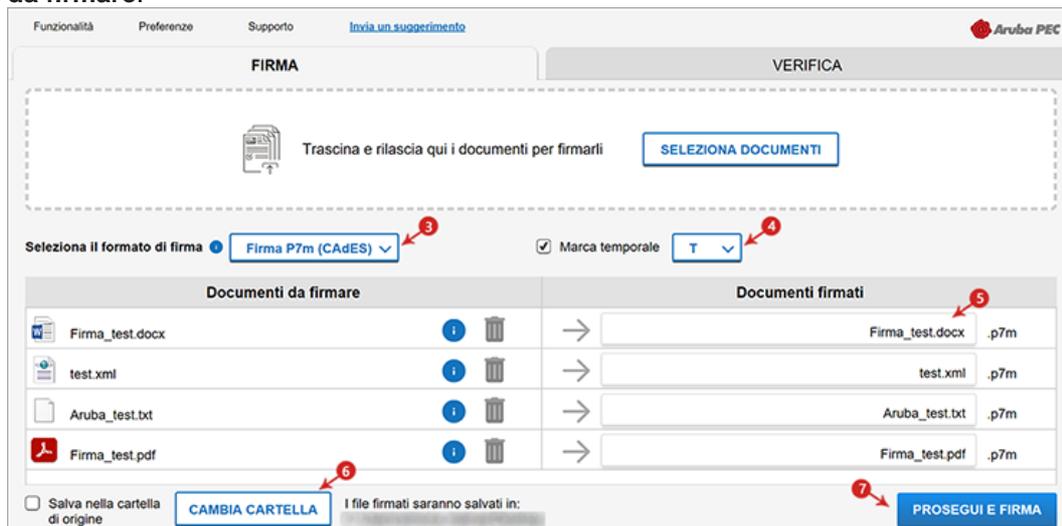


3.1 Firma uno o più file in formato .p7m - Firma Remota

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 Digitale Remota:

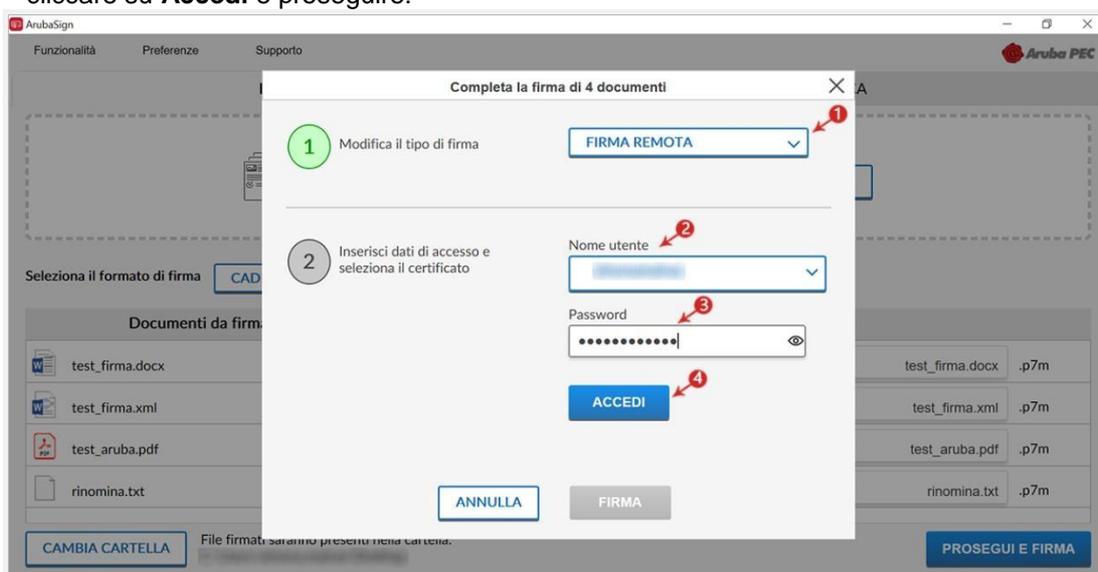
1. trascinare o selezionare uno o più documenti e/o una intera cartella;
2. il singolo/i documenti caricati/o sono visibili all'apposita schermata **Documenti da firmare**;
3. dall'apposito menu a tendina **Seleziona il formato firma** selezionare come tipologia di Firma CADES per firmare il file in formato .p7m;
4. se in possesso di marche temporali, oltre alla firma, è possibile apporre al file una marcatura temporale. Inserire il flag in corrispondenza della voce **Marca Temporale** nel formato scelto dall'apposito menu a tendina;
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 **Proseguì e Firma** per continuare. Sono firmati tutti i documenti presenti alla finestra **Documenti da firmare**;



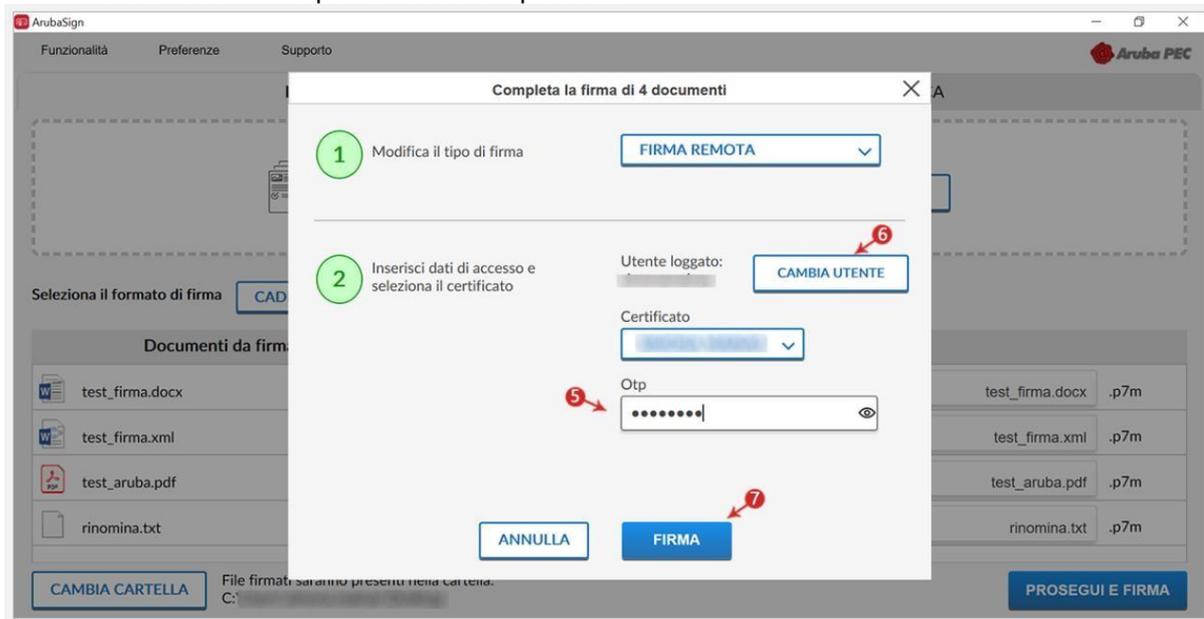
10

Alla schermata Completa la firma di 4 documenti:

1. selezionare o modificare il **tipo di firma**;
2. inserire i dati di accesso **Nome e utente** del proprio account di Firma Digitale Remota;
3. inserire la **Password** del proprio account di Firma Digitale Remota;
4. cliccare su **Accedi** e proseguire:

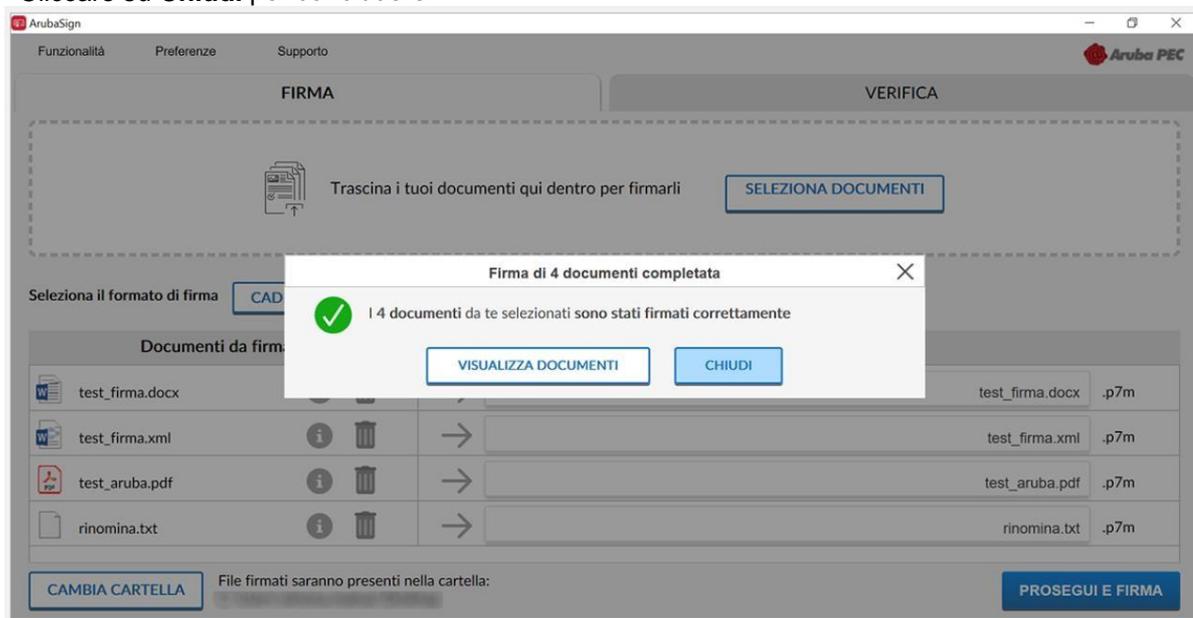


5. inserire un **codice OTP** generato con il proprio dispositivo di Firma Digitale Remota;
6. cliccando su **Cambia Utente** è possibile scegliere di firmare con altro account di Firma Digitale Remota configurato;
7. cliccare su **Firma** per concludere il processo:



Al termine dell'operazione si visualizza la seguente schermata che notifica la corretta firma del file.

Cliccare su **Chiudi** per concludere:



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

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

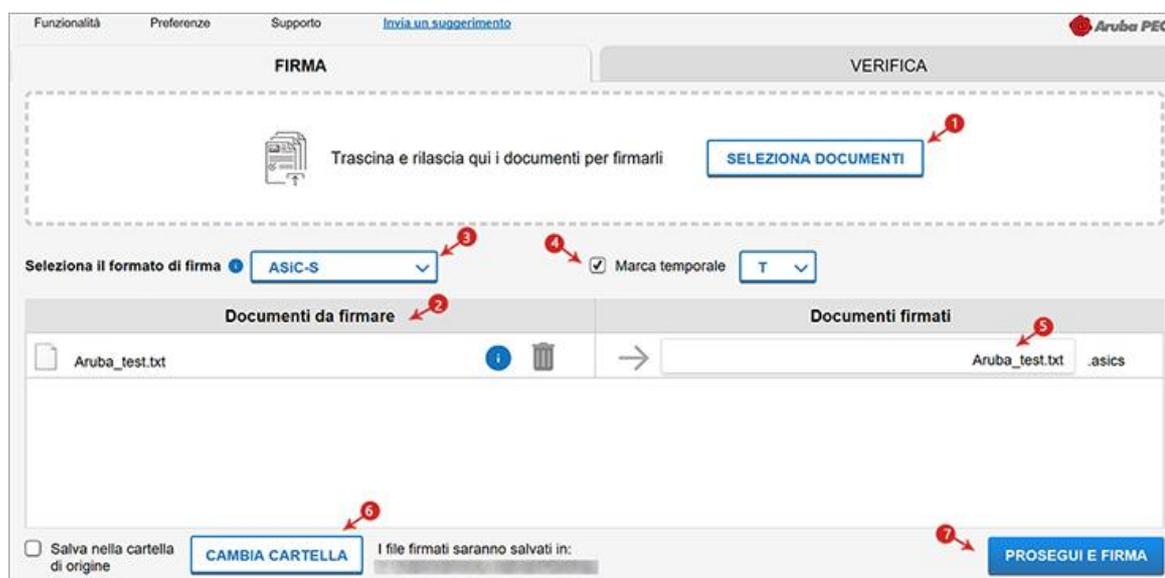
Il formato di firma **ASiC-S** (Associated Signature Containers ASiC simple) è un contenitore di dati che raggruppa un file e le relative firme digitali distaccate e/o marche temporali associate, utilizzando il **formato .zip**.

Per firmare digitalmente un file in formato ASiC-S:

1. caricare il documento;

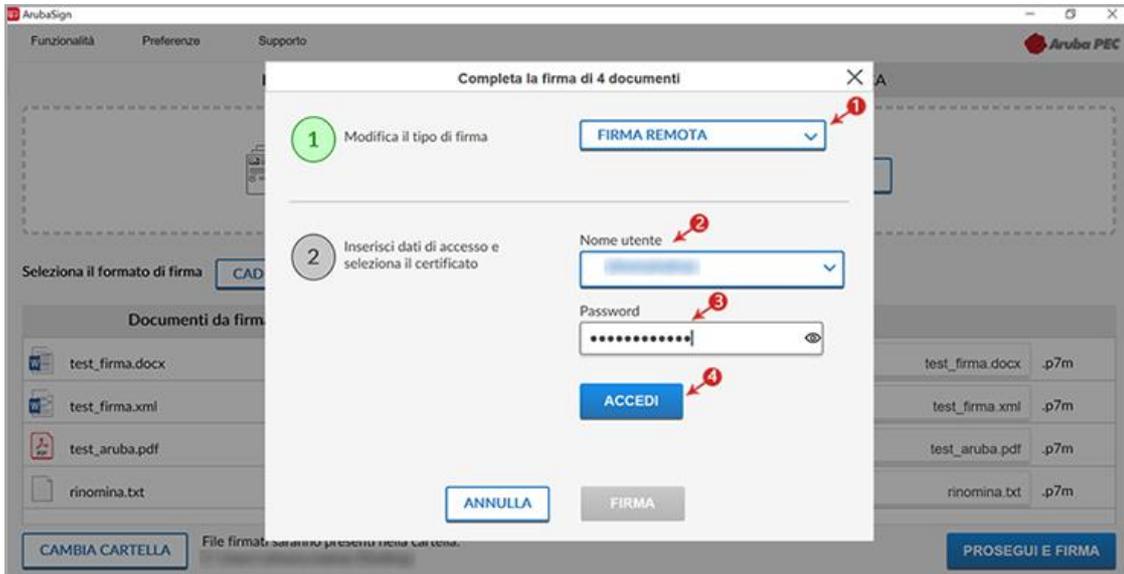
Questo formato di firma è **applicabile solo in caso di caricamento** su Aruba Sign di un **singolo file**, per firmare più file in formato ASiC, selezionare la specifica voce ASiC-E.

2. il singolo/i documenti caricati/o sono visibili nella schermata **Documenti da firmare**;
3. dall'apposito menu a tendina **Seleziona il formato firma** selezionare come tipologia di firma **ASiC-S**;
4. se in possesso di marche temporali, oltre alla firma, è possibile apporre al file una marcatura temporale. Inserire il flag in corrispondenza della voce **Marca temporale** nel formato scelto dall'apposito menu a tendina;
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 e Firma** per continuare:

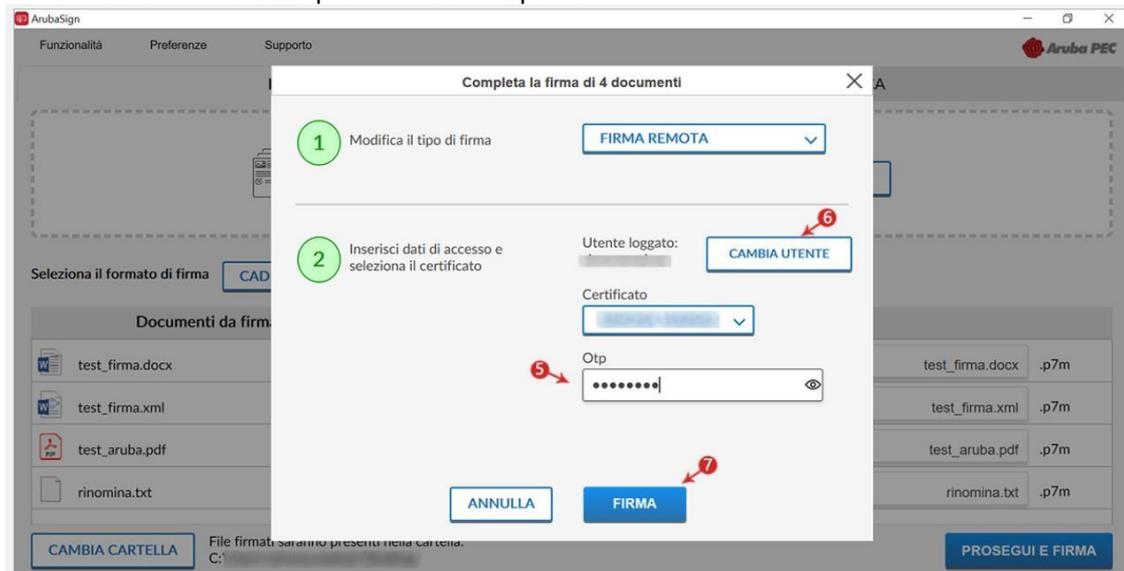


Alla schermata Completa la firma di 4 documenti:

1. selezionare o modificare il **tipo di firma**;
2. inserire i dati di accesso **Nome e utente** del proprio account di Firma Digitale Remota;
3. inserire la **Password** del proprio account di Firma Digitale Remota;
4. cliccare su **Accedi** e proseguire:



5. inserire un **codice OTP** generato con il proprio dispositivo di Firma Digitale Remota;
6. cliccando su **Cambia Utente** è possibile scegliere di firmare con altro account di Firma Digitale Remota configurato;
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 **Chiudi** per concludere:

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



3.3 Firma di più file in formato ASiC-E - Firma Remota

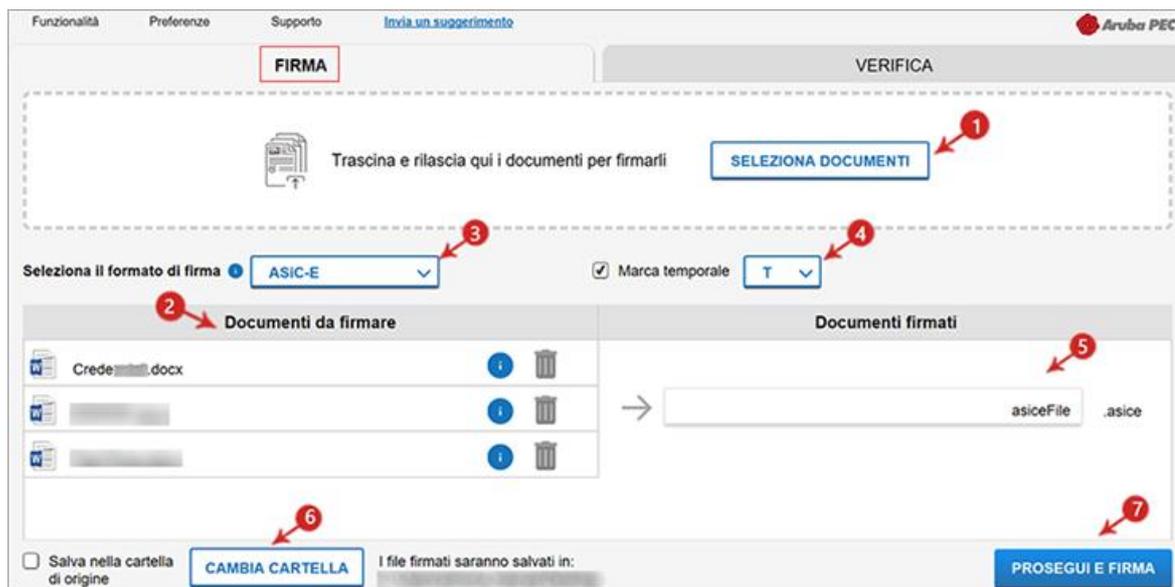
Il formato di firma **ASiC-E** (Associated Signature Containers ASiC simple) è un contenitore di dati che raggruppa più file e le relative firme digitali detached e/o marche temporali associate, utilizzando il **formato .zip**.

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 menu a tendina Formato Firma ASiC-S.

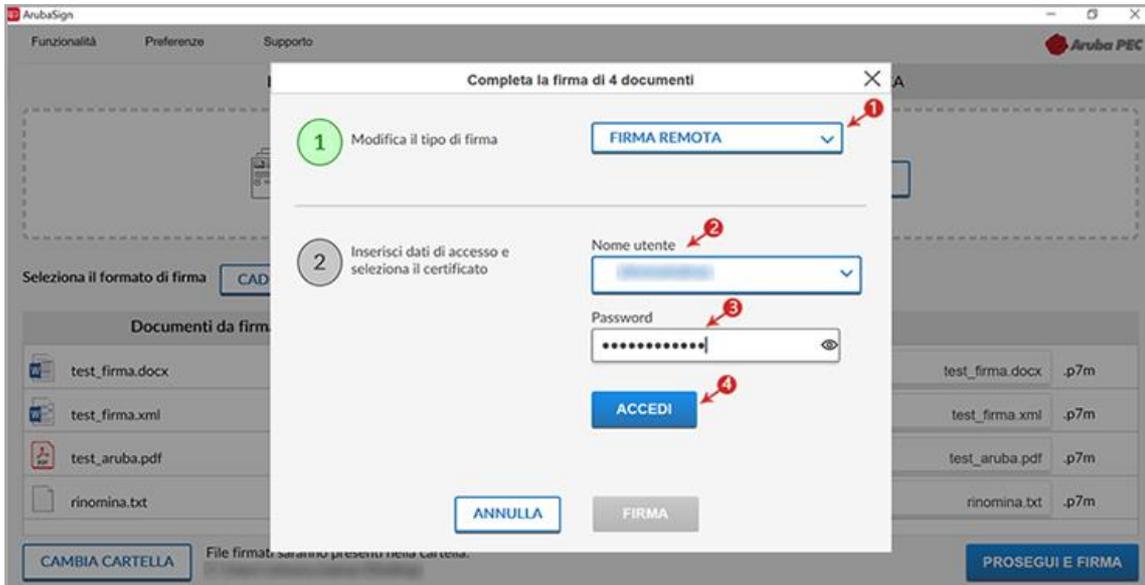
2. i documenti caricati sono visibili all'apposita schermata **Documenti da firmare**;
3. dall'apposito menu a tendina **Seleziona il formato firma** selezionare come tipologia di Firma **ASiC-E**;
4. se in possesso di marche temporali, oltre alla firma, è possibile apporre al file una marcatura temporale. Inserire il flag in corrispondenza della voce **Marca temporale** nel formato scelto dall'apposito menu a tendina;
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 e Firma** per continuare. Sono firmati tutti i documenti presenti alla finestra **Documenti da firmare**:



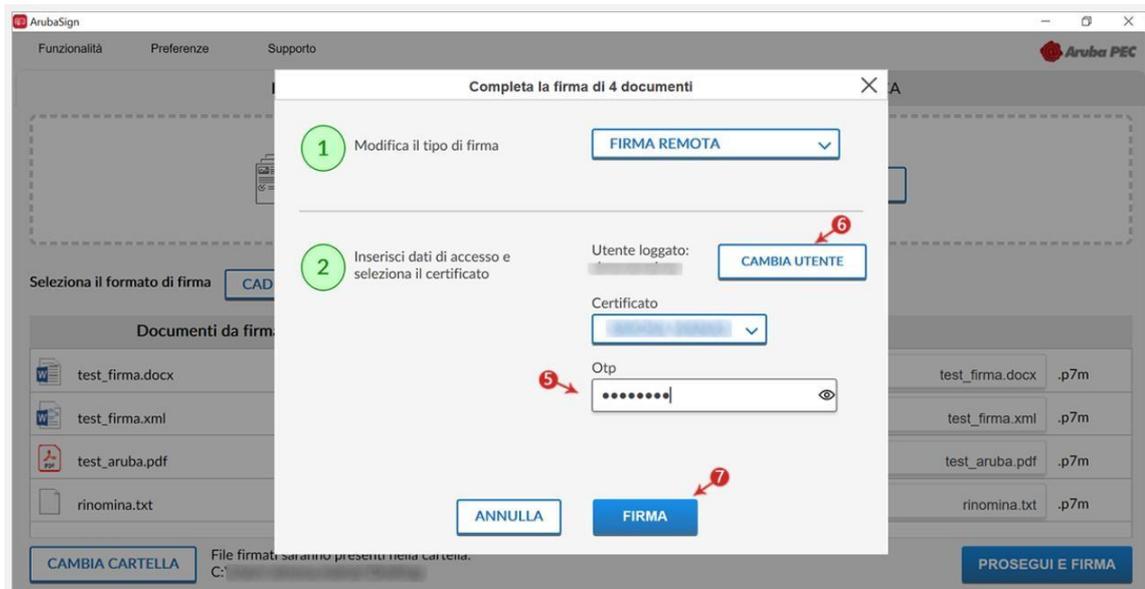
14

Alla schermata Completa la firma documenti:

1. selezionare o modificare il **tipo di firma**;
2. inserire i dati di accesso **Nome e utente** del proprio account di Firma Remota;
3. inserire la **Password** del proprio account di Firma Remota;
4. cliccare su **Accedi** e proseguire:



5. inserire il **codice OTP** generato con il dispositivo di Firma Remota;
6. cliccando su **Cambia Utente** è possibile scegliere di firmare con altro account di Firma Remota configurato;
7. cliccare su **Firma** per concludere il processo:



15

Al termine dell'operazione si visualizza la seguente schermata che notifica la corretta firma dei file. Cliccare su Chiudi per concludere:

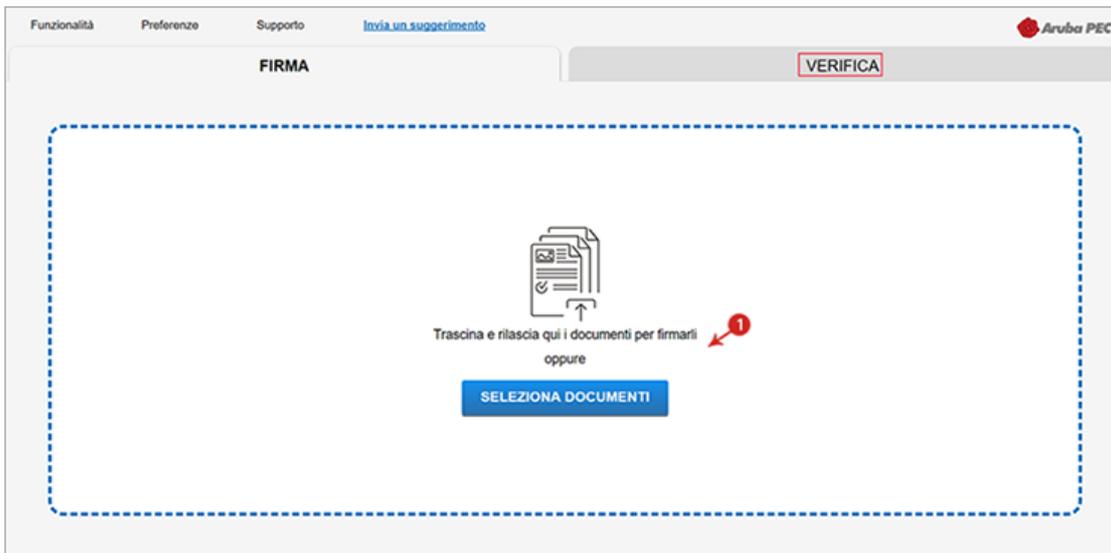


Il contenitore di documenti in **formato ASiC-E** è salvato nella cartella indicata in fase di Firma. In fase di verifica del contenitore è possibile visionare il dettaglio delle Firme apposte a ogni singolo documento.

3.4 Apposizione Firma Parallela - Firma Remota

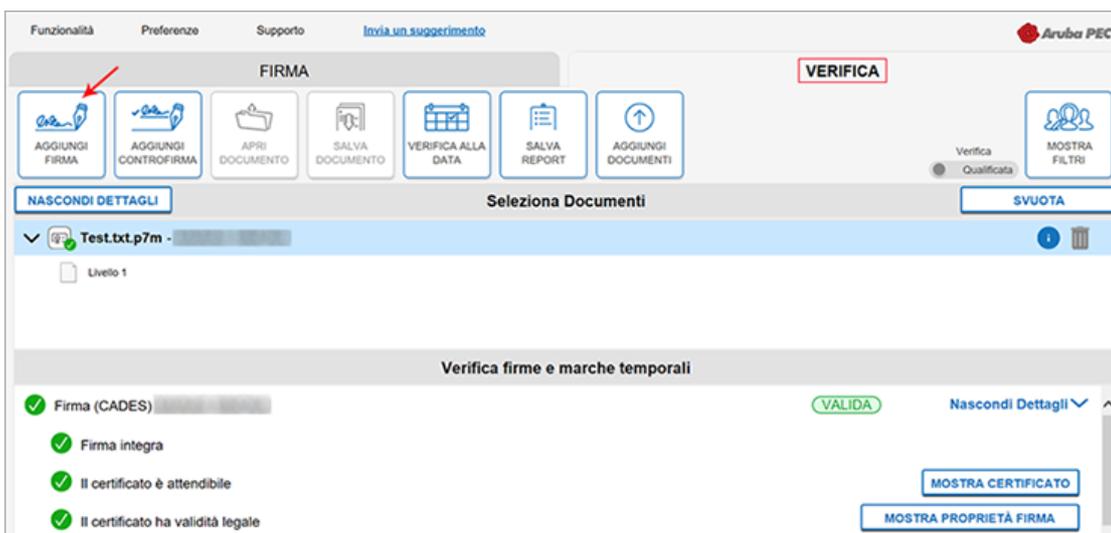
La funzione **Firma Parallela** è accessibile trascinando o selezionando il documento all'interno della scheda **Verifica** del software Aruba Sign uno o più file già firmati in **formato .p7m (CADES) o .PDF (PADES)**. È aggiunta allo stesso livello e allo stesso contenuto di una firma preesistente e 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 selezionare o trascinare un file .p7m (CADES) o .PDF (PADES), su **Verifica** di Aruba Sign:



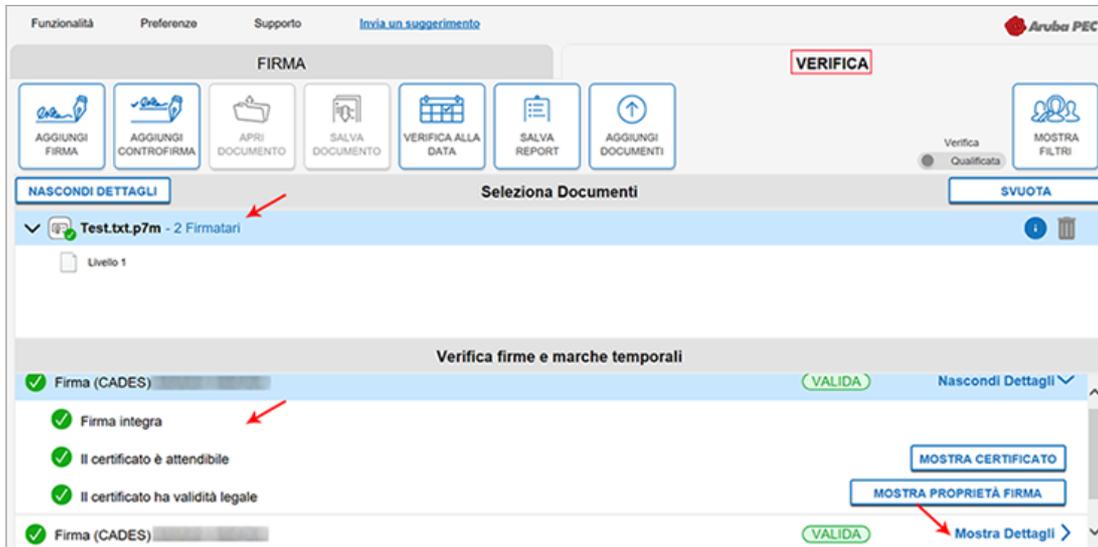
16

Selezionato il documento (anche in caso di caricamento di un solo file) su cui apporre la Firma Parallela poi cliccare su **Aggiungi Firma**:

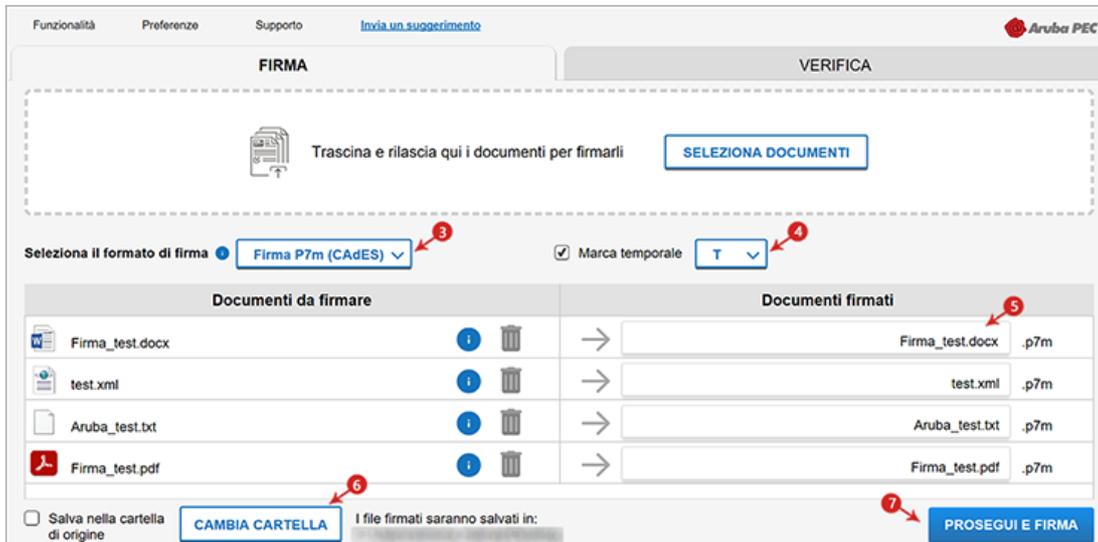


Firmare digitalmente il file. **Il sistema non consente di selezionare il formato della Firma.** In caso di File .p7m la Firma Parallela è apposta in tale formato, per i file .PDF è possibile apporre una Firma Grafica o Invisibile. La nuova firma è apposta allo stesso livello di quella preesistente.

È possibile visionare la presenza della Firma Parallela e i dettagli su **Mostra Dettagli** come da immagine esemplificativa sottostante:



E infine su **Mostra Dettagli** l'esito di verifica:



Affinché il documento informatico sottoscritto con Firma Digitale, produca gli effetti di legge di cui all'articolo 21, comma 2, del Codice dell'Amministrazione Digitale, il documento da firmare non deve contenere macroistruzioni o codici eseguibili tali da attivare funzionalità che possano modificare gli atti, i fatti o i dati nello stesso rappresentati. (Art. 3, comma 3 del DPCM 13 Gennaio 2004). È unicamente responsabilità dell'utente firmatario accertarsi che tale condizione sia soddisfatta. Ad esempio i file con estensione HTM o HTML sono documenti scritti in HTML che è il linguaggio di marcatura per creare pagine web. Tali file, visualizzabili tramite qualsiasi Web Browser, possono contenere sia del codice interpretato (JavaScript, VBScript) che codice eseguibile (Applet Java, ActiveX ecc...) i quali ne forniscono una forte connotazione dinamica.

3.5 Apposizione Controfirma - Firma Remota

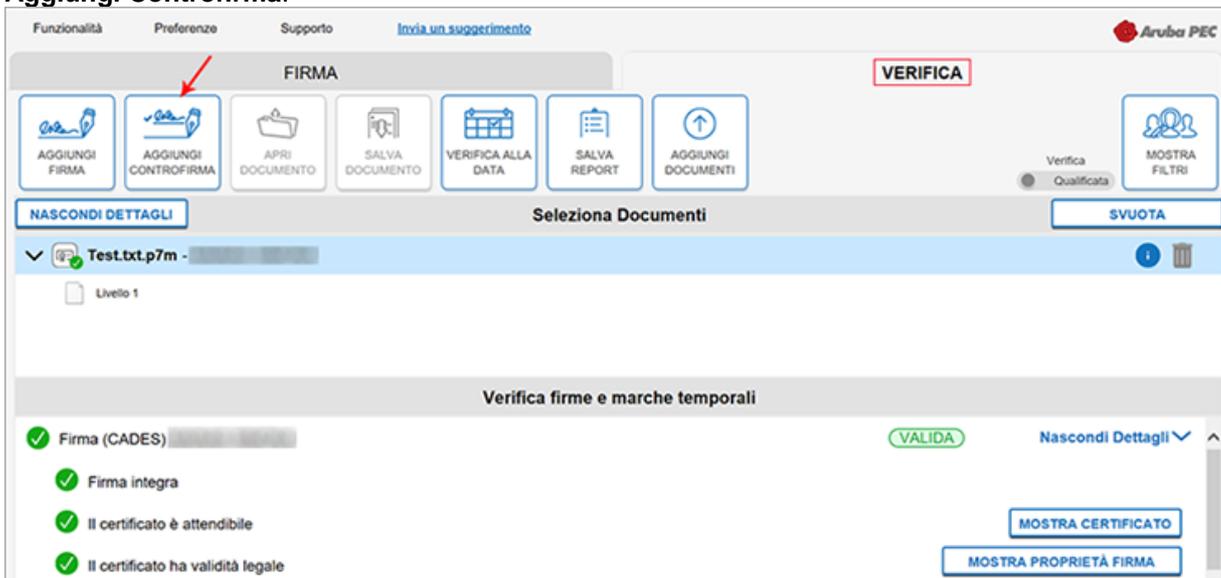
La funzione **Controfirma** è accessibile trascinando o selezionando il documento all'interno della scheda **Verifica** del software Aruba Sign **uno o più file già firmati in formato .p7m**. È apposta a un livello sottostante di una firma preesistente e sottoscrive quest'ultima. È più annidata rispetto alla firma a cui si riferisce (aspetto evidenziato da una rappresentazione ad albero delle firme stesse).

Per crearla selezionare o trascinare un file .p7m (CADES), sopra il menu **Verifica** di Aruba Sign:



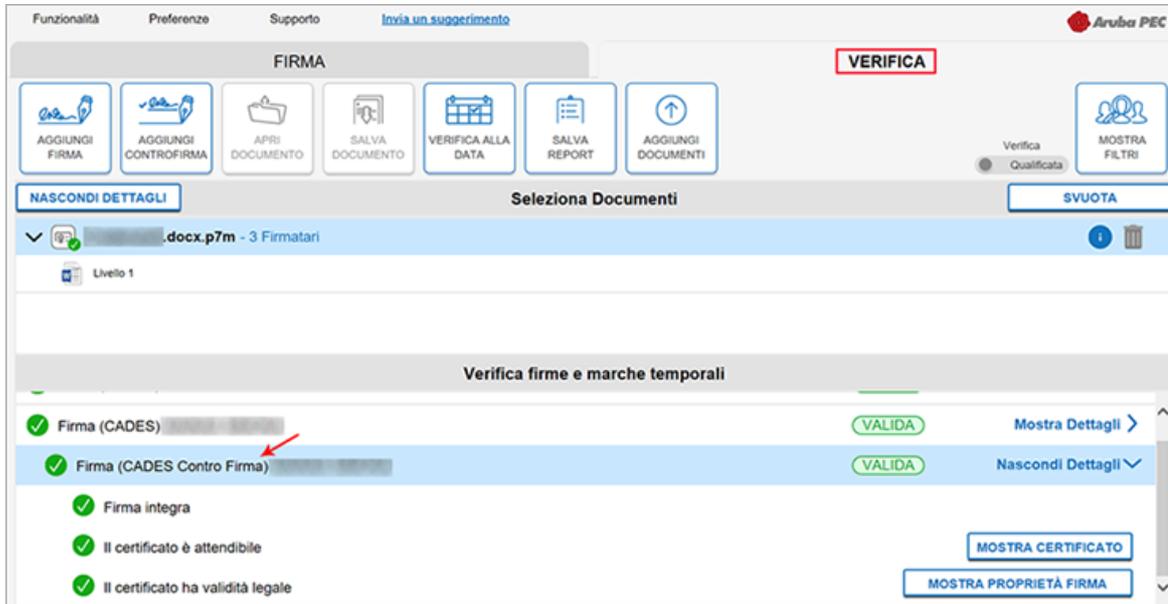
18

Selezionare il documento (anche in caso di caricamento di un solo file) su cui apporre la controfirma cliccare su **Aggiungi Controfirma**:

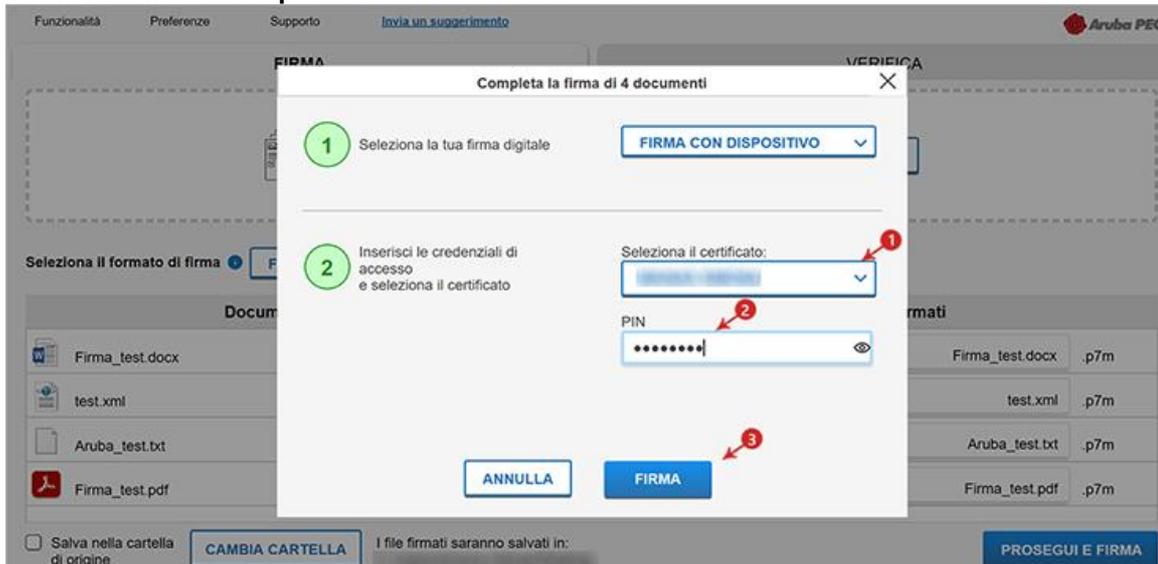


Firmare digitalmente il file in formato .p7m. La nuova **Firma** è apposta a un livello sottostante della firma preesistente.

E' possibile visionare la presenza della Controfirma, come da immagine esemplificativa sottostante:



E infine su **Mostra Proprietà Firma** l'esito di verifica firma:



Affinché il documento informatico sottoscritto con Firma Digitale, produca gli effetti di legge di cui all'articolo 21, comma 2, del Codice dell'Amministrazione Digitale, il documento da firmare non deve contenere macroistruzioni o codici eseguibili tali da attivare funzionalità che possano modificare gli atti, i fatti o i dati nello stesso rappresentati. (Art. 3, comma 3 del DPCM 13 Gennaio 2004). È unicamente responsabilità dell'utente firmatario accertarsi che tale condizione sia soddisfatta. Ad esempio i file con estensione HTM o HTML sono documenti scritti in HTML che è il linguaggio di marcatura per creare pagine web. Tali file, visualizzabili tramite qualsiasi Web Browser, possono contenere sia del codice interpretato (JavaScript, VBScript) che codice eseguibile (Applet Java, ActiveX ecc...) i quali ne forniscono una forte connotazione dinamica.

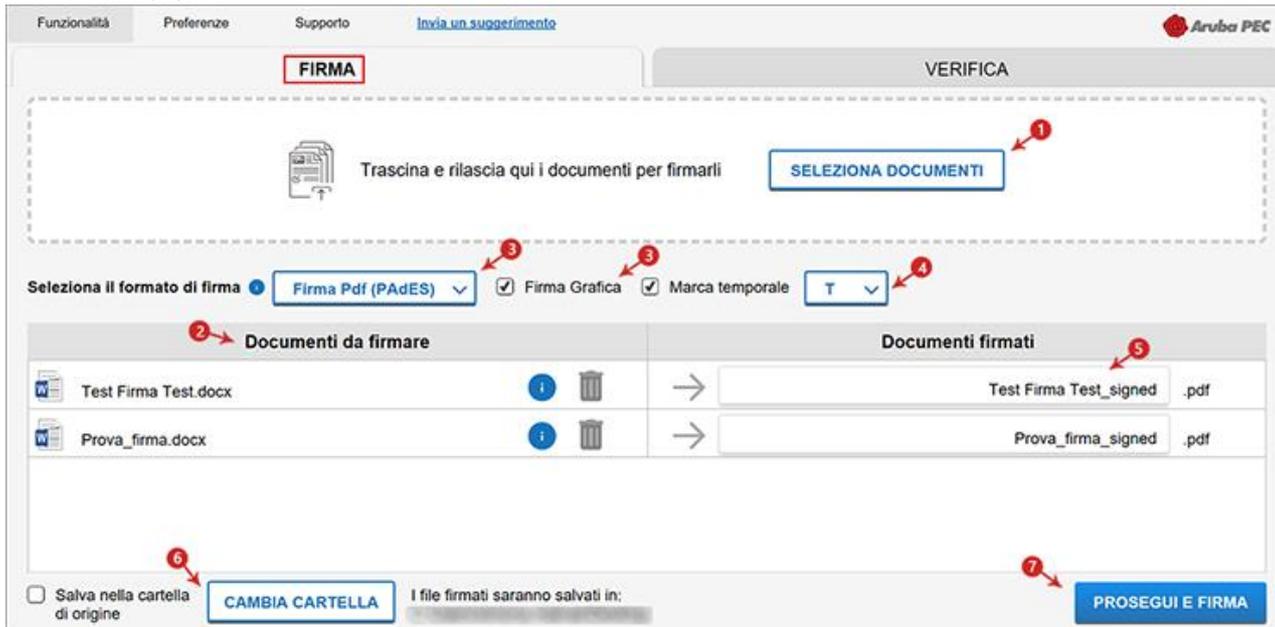
3.6 Apposizione Firma PDF - Grafica Firma Remota

Il formato di firma **PAdES** è applicabile ai soli file **.PDF**, **.doc**, **.docx**, **.xls**, **.xlsx** (supporto a MS Word w MS Excel versione 2007 o superiore).

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:

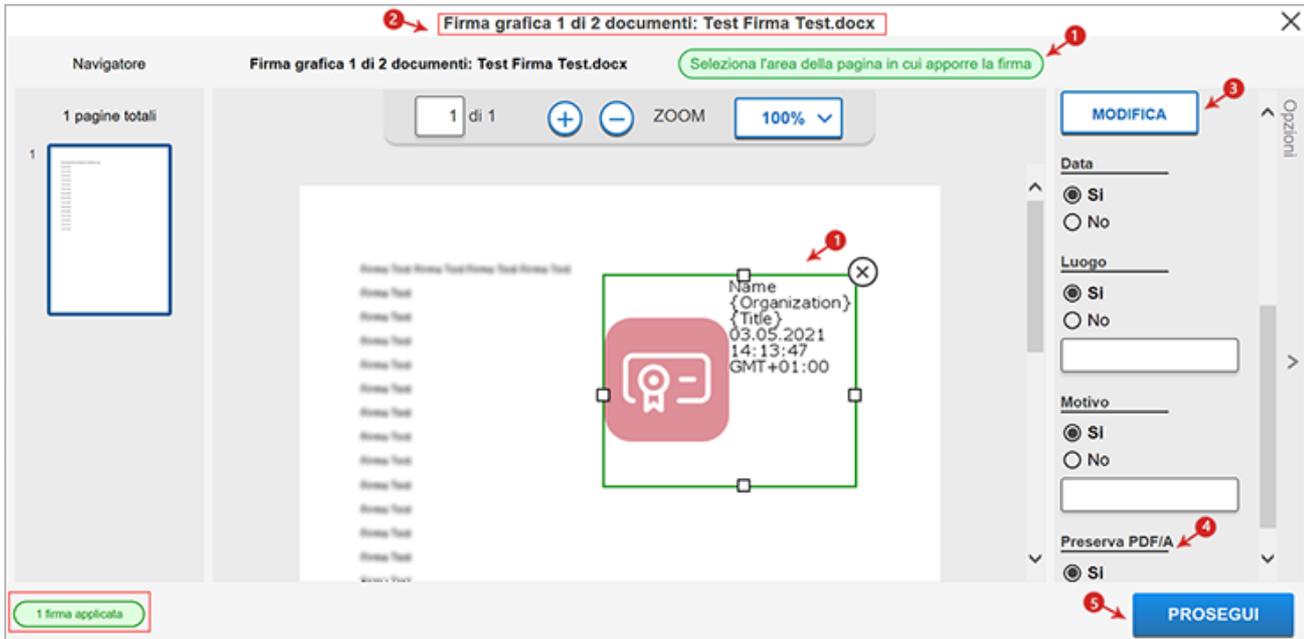
1. trascinare o selezionare uno o più documenti e/o una intera;
2. il singolo/i documenti caricati/o sono visibili all'apposita schermata **Documenti da firmare**;
3. dall'apposito menu a tendina **Seleziona il formato di firma** selezionare come tipologia di firma **PAdES** per firmare il file in formato **.PDF** e lasciare il flag su **Firma Grafica**;
4. se in possesso di marche temporali, oltre alla firma, è possibile apporre al file una marcatura temporale. Inserire il flag in corrispondenza della voce **Marca Temporale** nel formato scelto dall'apposito menu a tendina;
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 e Firma** per continuare. Sono firmati tutti i documenti presenti alla finestra Documenti da firmare:



20

Alla schermata successiva:

1. definire la posizione e la dimensione del campo che ospiterà la Firma Digitale;
2. è possibile visualizzare tutti i documenti o solo quelli firmati;
3. attraverso la finestra **Opzioni sulla destra**, è possibile caricare da locale, attraverso il tasto **Modifica**, 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 dimensioni dell'area selezionata;
4. abilitando la funzione **Preserva PDF/A** la firma grafica è apposta preservando il formato stesso;
5. cliccare su **Prosegui** per procedere:



Alla schermata Completa la firma del documento:

1. selezionare o modificare il tipo di firma;
2. inserire i dati di accesso **Nome e utente** del proprio account di Firma Digitale Remota;
3. inserire la **Password** del proprio account di Firma Digitale Remota;
4. cliccare su **Prosegui**:



5. inserire un **codice OTP** generato con il proprio dispositivo di Firma Digitale Remota;
6. cliccando su **Cambia Utente** è possibile scegliere di firmare con altro account di Firma Digitale Remota configurato;
7. Cliccare su **Firma** per concludere il processo:



Completa la firma di 2 documenti

1 Seleziona la tua firma digitale FIRMA REMOTA

2 Inserisci le credenziali della tua firma remota

Utente: CAMBIA UTENTE

Certificato ...

OTP

ANNULLA FIRMA

Al termine dell'operazione si visualizza la seguente schermata che notifica la corretta firma del file. Cliccare su Chiudi per concludere:



Firma completata

✓ I 2 documenti selezionati sono stati firmati.

APRI CARTELLA CHIUDI

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

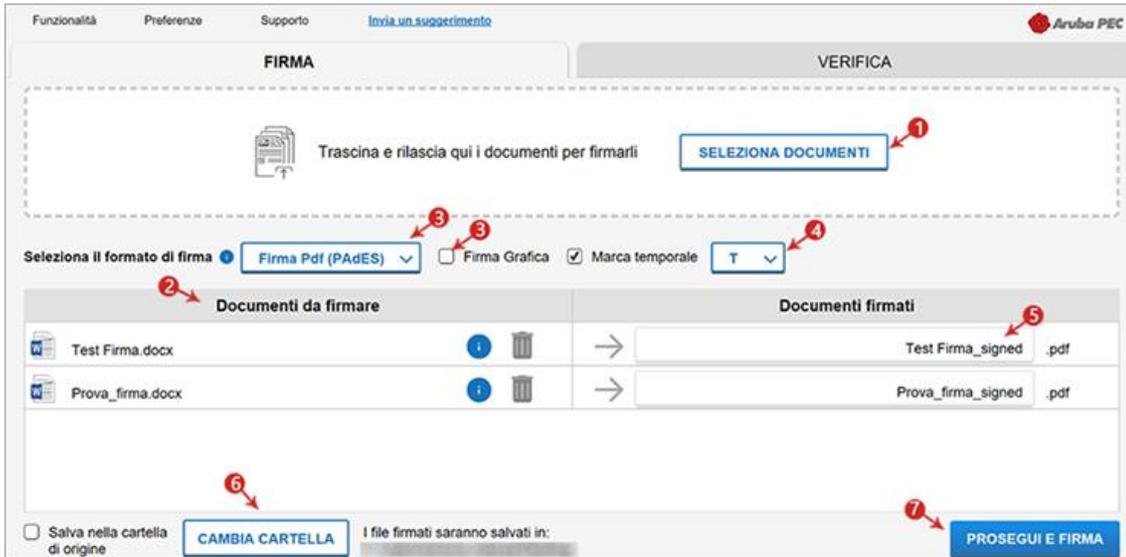
3.7 Apposizione Firma PDF - Invisibile Firma Remota

Il formato di firma **PAdES** è applicabile ai soli file **.PDF, .doc, .docx, .xls, .xlsx** (supporto a MS Word w MS Excel versione 2007 o superiore).

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. trascinare o selezionare uno o più documenti e/o una intera cartella;
2. il singolo/i documenti caricati/o sono visibili all'apposita schermata **Documenti da firmare**;

- dall'apposito menu a tendina **Seleziona il formato** firma selezionare come tipologia di firma **PAdES** per firmare il file in formato .PDF e rimuovere il flag su **Firma Grafica**;
- se in possesso di marche temporali, oltre alla firma, è possibile apporre al file una marcatura temporale. Inserire il flag in corrispondenza della voce **Marca Temporale** nel formato scelto nel menu a tendina;
- dalla finestra **Documenti firmati** rinominare, se desiderato, eventuali file prima di apporre la firma;
- 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;
- clickare su **Proseguì e Firma** per continuare. Sono firmati tutti i documenti presenti alla finestra **Documenti da firmare**:

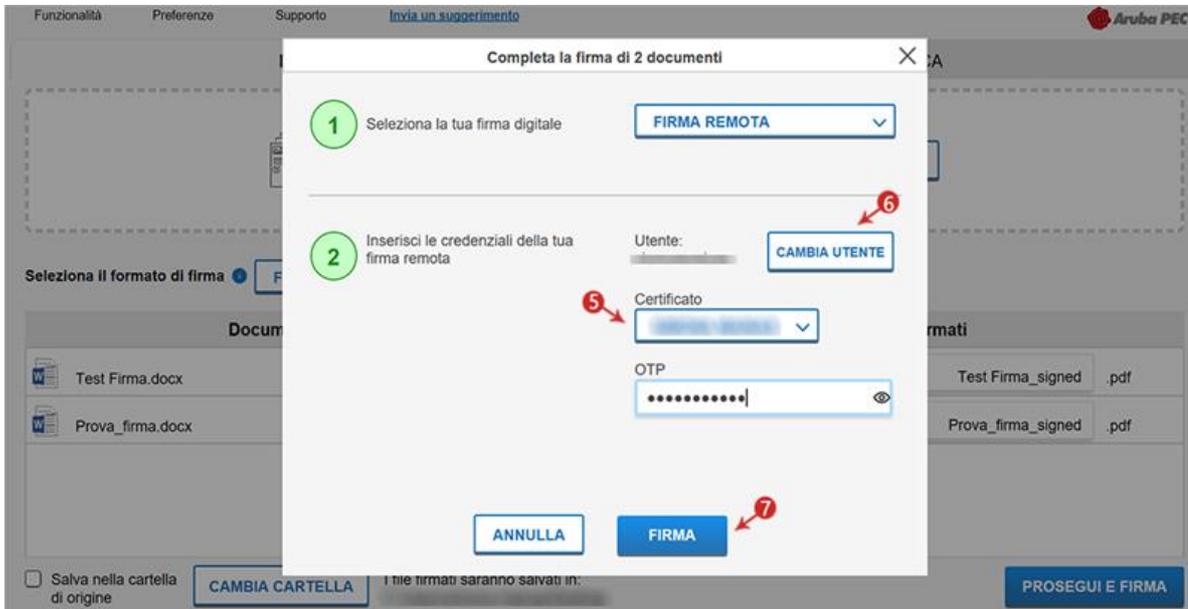


Alla schermata Completa la firma documenti:

- selezionare o modificare il tipo di firma;
- inserire i dati di accesso **Nome utente** del proprio account di Firma Digitale Remota;
- inserire la **Password** del proprio account di Firma Digitale Remota;
- clickare su **Proseguì**:



5. inserire un **codice OTP** generato con il proprio dispositivo di Firma Remota;
6. cliccando su **Cambia Utente** è possibile scegliere di firmare con altro account di Firma Remota configurato;
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 **Chiudi** per concludere:



24

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

3.8 Apposizione di Marche Temporali - Firma Remota

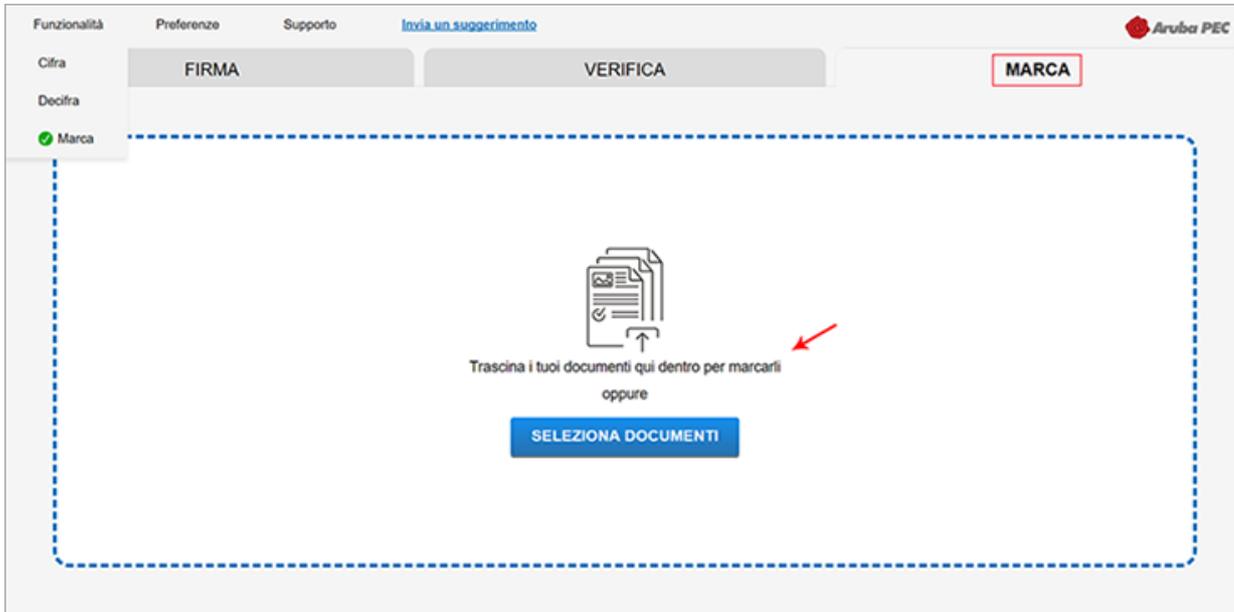
La Marca Temporale permette di:

- **associare data e ora certe e legalmente valide a un documento informatico**, attestando il preciso momento temporale in cui il documento è stato creato, trasmesso o archiviato;
- **garantire la validità nel tempo del documento firmato digitalmente su cui è apposta**, poiché fa sì che la Firma Digitale risulti sempre e comunque valida anche nel caso in cui il relativo Certificato risulti scaduto, sospeso o revocato, purché la Marca sia stata apposta in un momento precedente alla scadenza, revoca o sospensione del Certificato di Firma stesso.

In caso di prima marcatura di un documento con il software Aruba Sign, procedere prima alla configurazione di un proprio account.

Apposizione di Marche Temporali con Aruba Sign

Per apporre una Marca Temporale accedere su **Funzionalità** e poi su **Marca**, se non precedentemente configurato verrà popolato sulla destra la scheda, quindi trascinare o selezionare il file che si desidera cifrare:



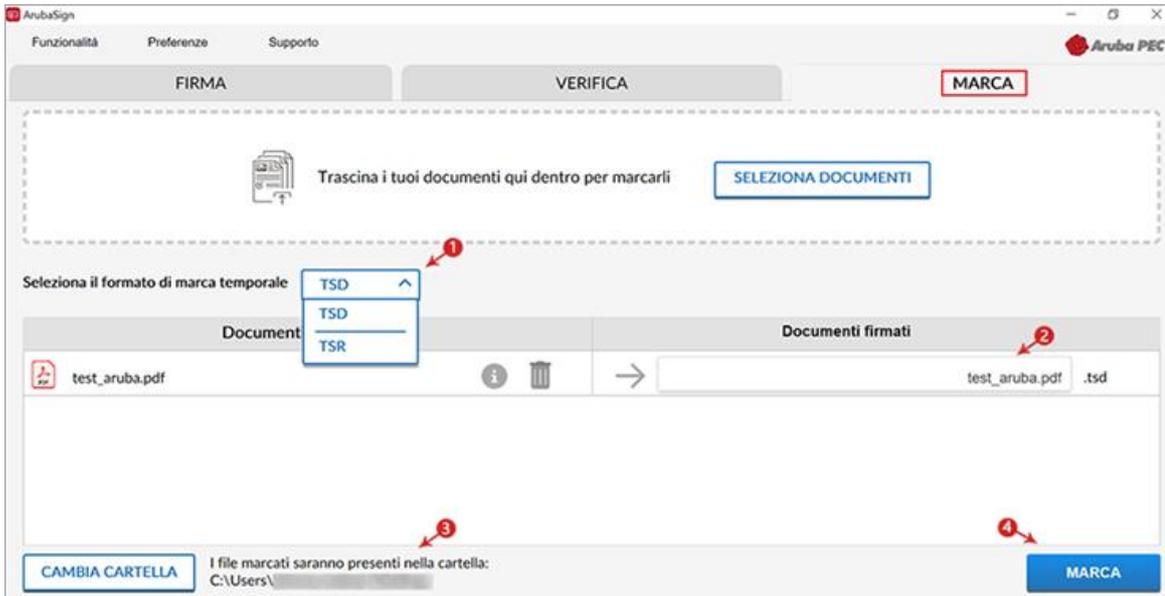
Alla pagina visualizzata:

1. selezionare il formato di salvataggio della marca temporale. È 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 verificare 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 dal 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.

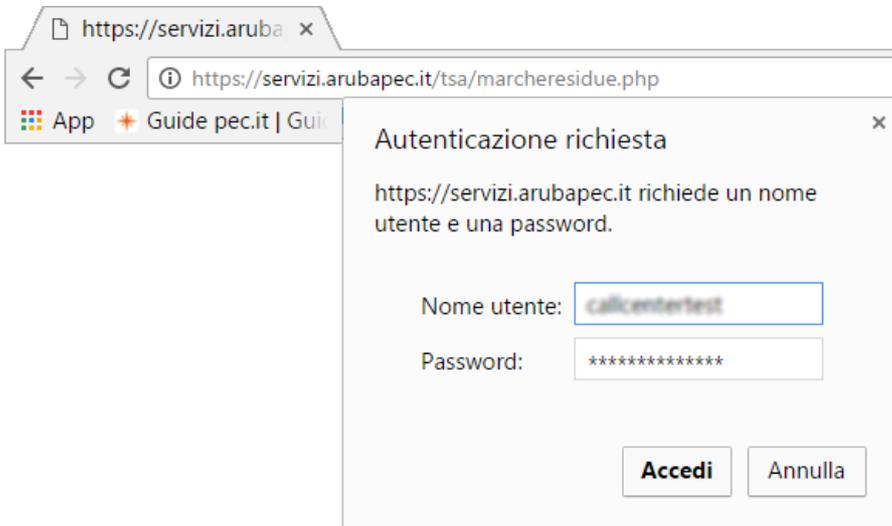
2. dalla finestra **Documenti firmati** rinominare, se desiderato, eventuali file prima di apporre la firma;
3. il documento è disponibile nella cartella indicata in fase di apposizione della marcatura stessa;
4. cliccare **Marca** al messaggio che notifica la corretta marcatura del file per completare l'operazione:



Verifica Marche Temporal Residue

Aruba Sign non indica il numero di marche di volta in volta utilizzate. Qualora si voglia verificare le marche residue:

1. accedere a <https://servizi.arubapec.it/tsa/marcheresidue.php>;
2. al form visualizzato inserire le credenziali del proprio Account di marca temporale, quindi spuntare su **Ok**:



3. si accede alla pagina da cui visualizzare le marche residue:



L'apposizione della Marca Temporale a un documento firmato digitalmente o meno, con Aruba Sign, può avvenire solo ed esclusivamente a seguito [dell'acquisto](#) di un lotto di marche temporali e alla configurazione di un proprio account.

3.9 Verifica di file Firmati Aruba Sign e Firma Remota

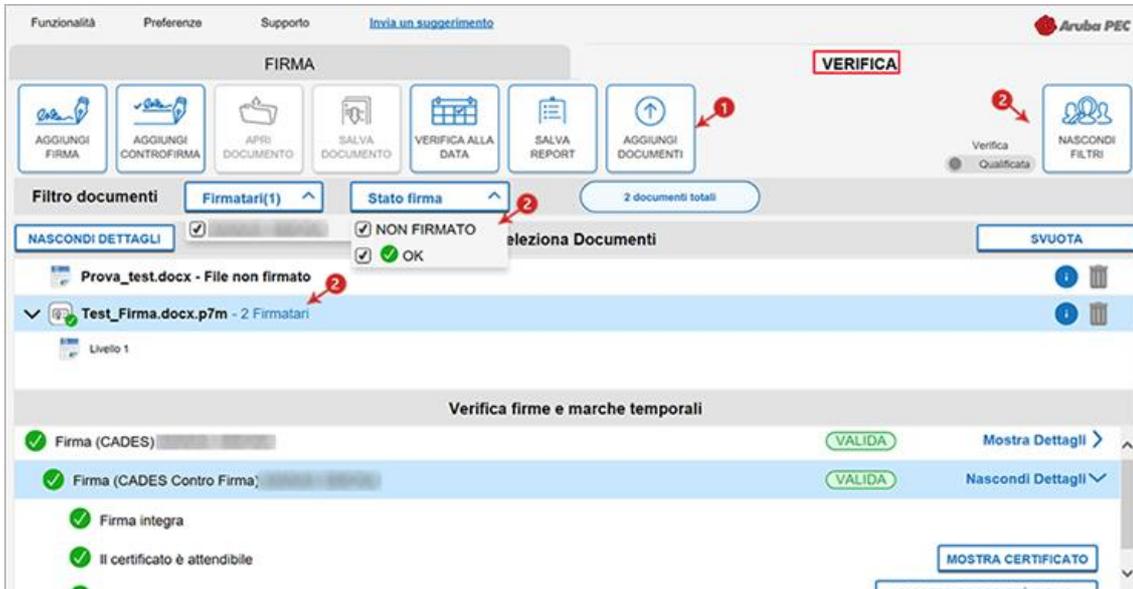
La Verifica dei File firmati permette di verificare la **validità legale del certificato**.

Per verificare uno o più file firmati con Aruba Sign, selezionare il documento nella scheda **Verifica**:



Alla schermata visualizzata è possibile:

1. verificare ulteriori file firmati trascinandoli da locale o su **Aggiungi Documento**;
2. da **Mostra/Nascondi Filtri** 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:



3. verifica firme e marche temporali sono visibili le firme presenti all'interno del file:

- **Firma valida**

Attesta il formato della firma e che il documento non è stato alterato dopo la firma;

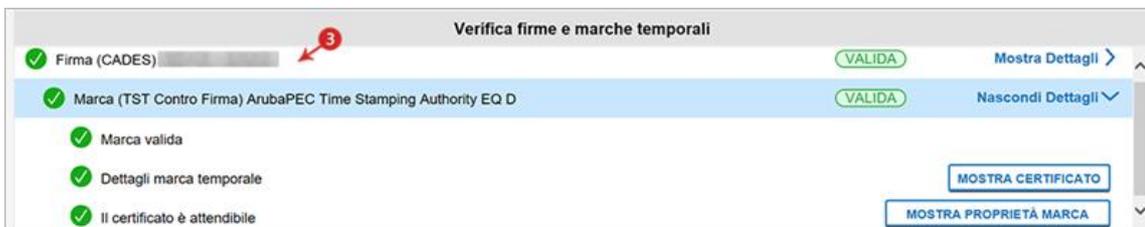
- **Il certificato è attendibile**

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**

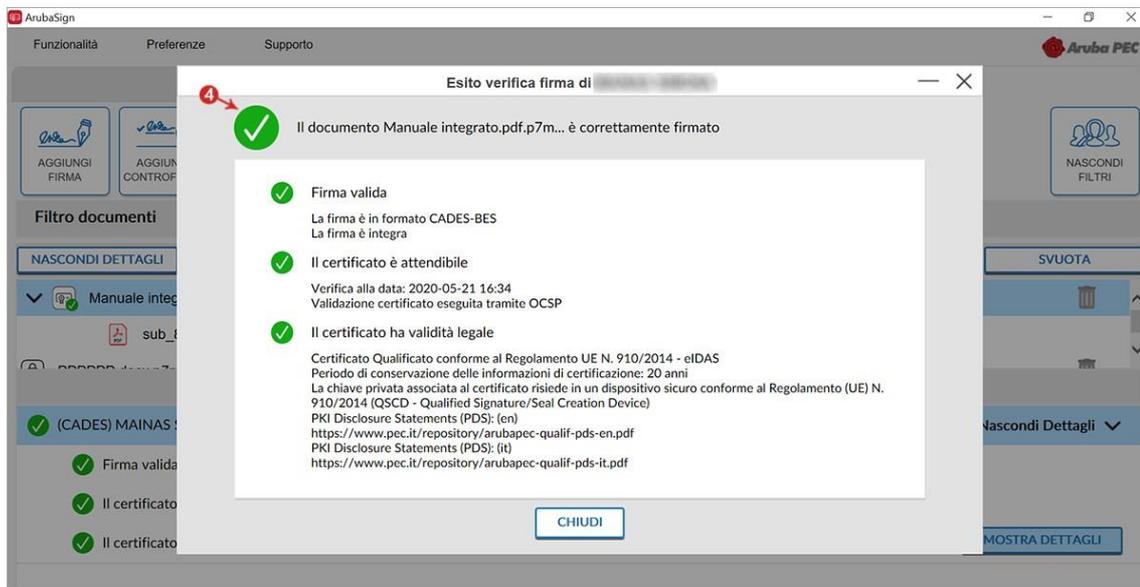
Attesta che il certificato del sottoscrittore è un certificato di Firma Digitale qualificato:

28



4. da **Mostra Dettagli** è possibile verificare la validità della firma apposta.

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.



In caso di necessità è possibile attivare un'opzione che consente di verificare uno o più File Firmati con certificati non emessi da una Certification Authority. La verifica della Firma apposta può essere:

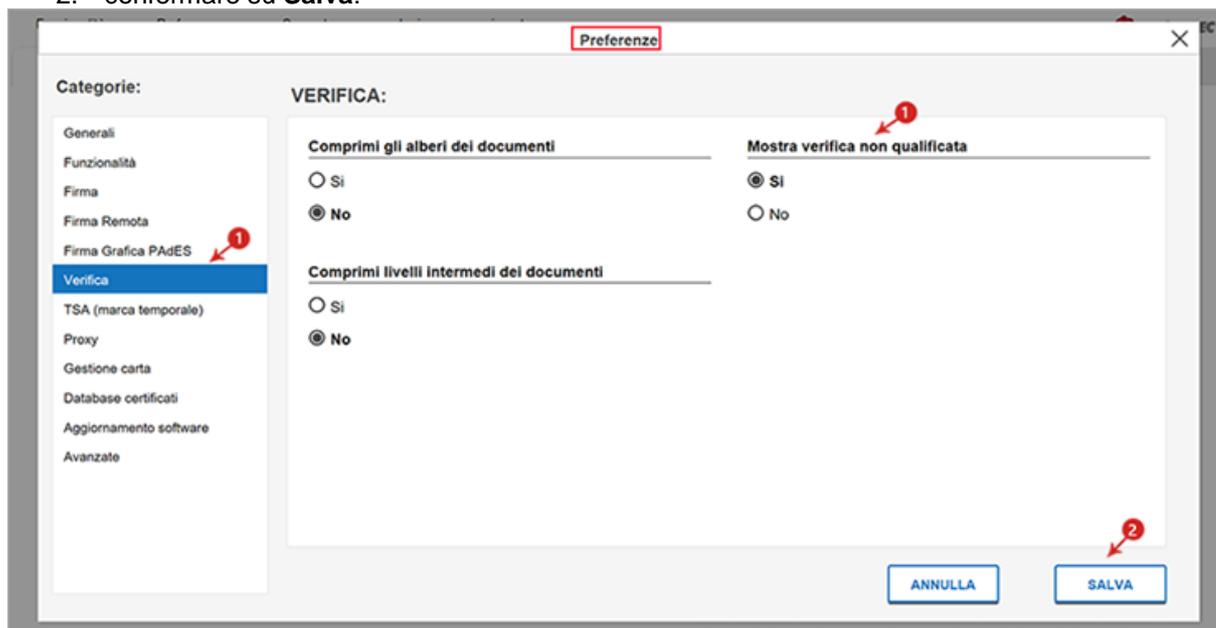
- **Non qualificata:** la firma è considerata valida se è integra e il certificato valido. Non è richiesto che sia emesso da una Certification authority di firma digitale.
- **Qualificata:** la firma apposta a un file è considerata valida se è integra, il certificato valido e rilasciato da una Certification Authority qualificata nel rispetto della normativa vigente circa la firma digitale qualificata.

La Firma **Non Qualificata** non ha la **stessa validità legale della firma Qualificata**.

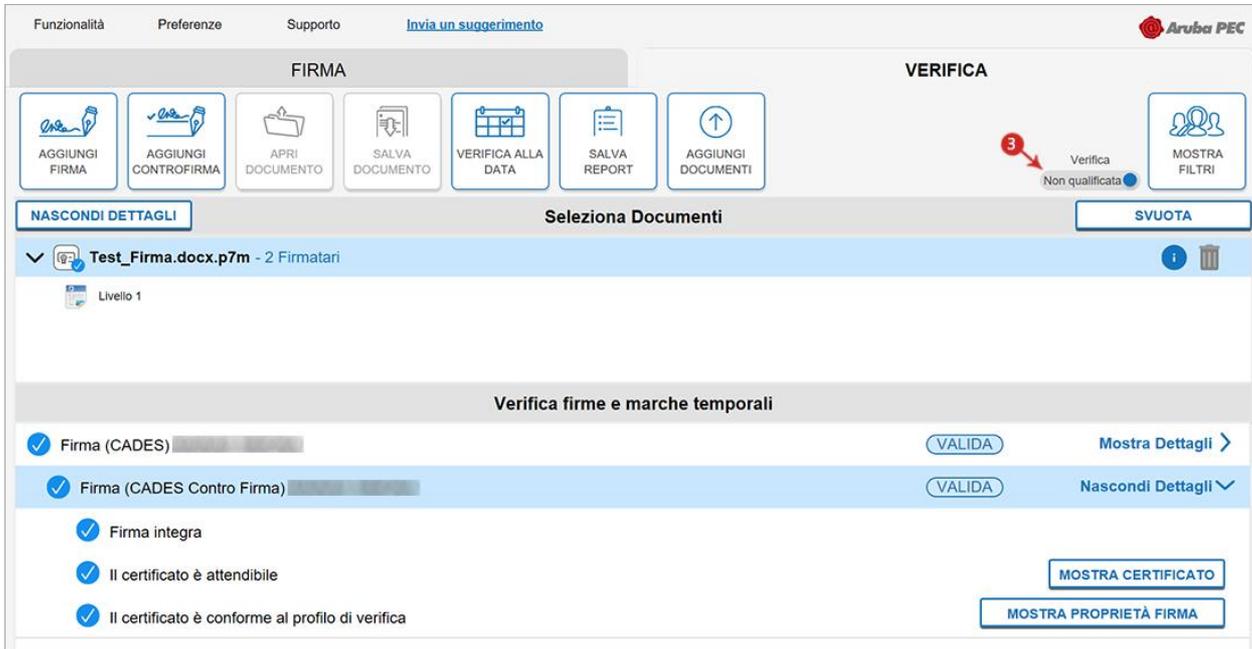
29

Per attivare l'opzione, accedere su **Preferenze** di Aruba Sign:

1. su **Verifica** abilitare **Mostra verifica non qualificata**;
2. confermare su **Salva**:

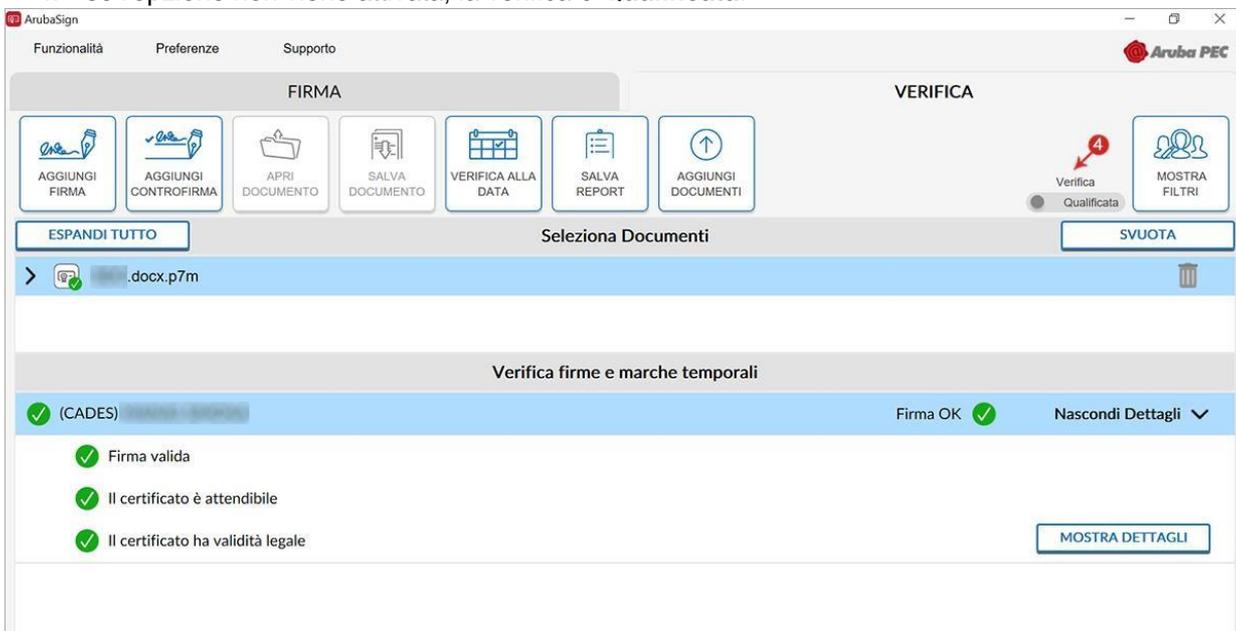


3. l'opzione di verifica **Non qualificata** è attiva:



The screenshot shows the ArubaSign interface with the 'VERIFICA' tab active. In the top right, the 'Verifica' radio button is selected, and the 'Non qualificata' option is highlighted with a red circle and the number '3'. Below, the document 'Test_Firma.docx.p7m' is selected. Under 'Verifica firme e marche temporali', the 'Firma (CADES)' and 'Firma (CADES Contro Firma)' options are checked, and the 'VALIDA' buttons are visible. At the bottom right, there are buttons for 'MOSTRA CERTIFICATO' and 'MOSTRA PROPRIETÀ FIRMA'.

4. se l'opzione non viene attivata, la verifica è **Qualificata**:

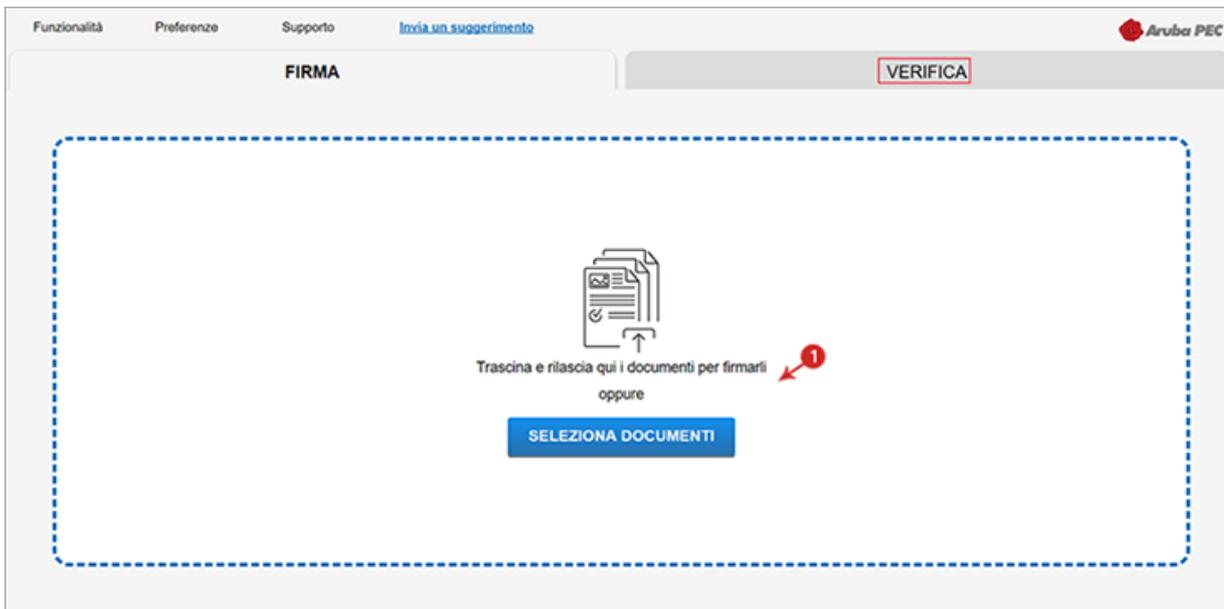


The screenshot shows the ArubaSign interface with the 'VERIFICA' tab active. In the top right, the 'Verifica' radio button is selected, and the 'Qualificata' option is highlighted with a red circle and the number '4'. Below, the document '.docx.p7m' is selected. Under 'Verifica firme e marche temporali', the '(CADES)' option is checked, and the status 'Firma OK' with a green checkmark is displayed. At the bottom right, there is a button for 'MOSTRA DETTAGLI'.

L'orario di marcatura e Firma Digitale si riferisce all'orario UTC (Tempo Coordinato Universale) riferimento da cui sono calcolati tutti gli altri fusi orari del mondo e indicato per essere sempre lo stesso in ogni parte del mondo. In Italia, nel periodo estivo (ora legale), l'orario è 2 ore avanti rispetto alla UTC (Tempo Coordinato Universale), in inverno (ora solare) l'orario è avanti di un'ora sulla UTC.

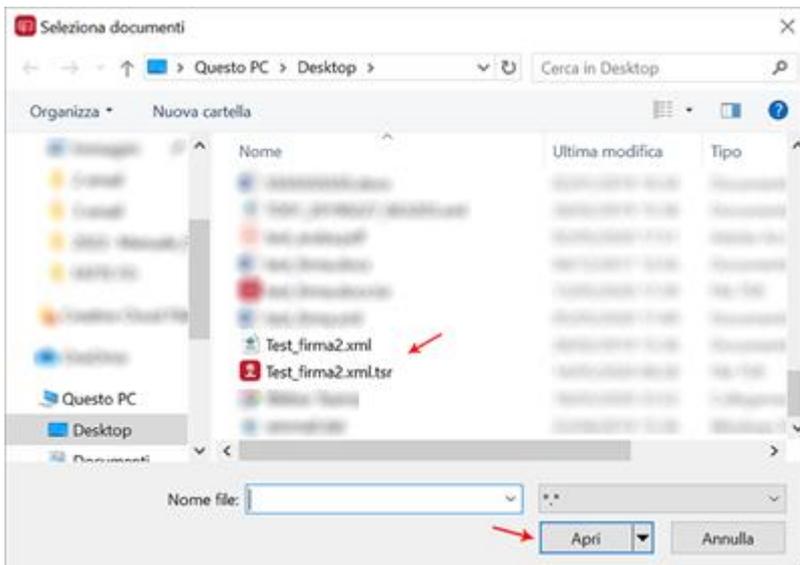
3.10 Verifica Marche Temporali in formato TSR Aruba Sign e Firma Remota

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 verificare uno o più File marcati in formato TSR con Aruba Sign, trascinare o selezionare il documento all'interno della scheda **Verifica**:



Selezionare da locale il file originario e il file associato alla marca stessa, quindi cliccare su **Apri**:

31



Alla schermata visualizzata è possibile:

1. visualizzare il file marcato;

2. su **Verifica firme e marche temporali** sono visibili le marche presenti all'interno del file;

- **Marca valida**

Indica che la marca temporale è integra ed è correttamente associata al documento selezionato;

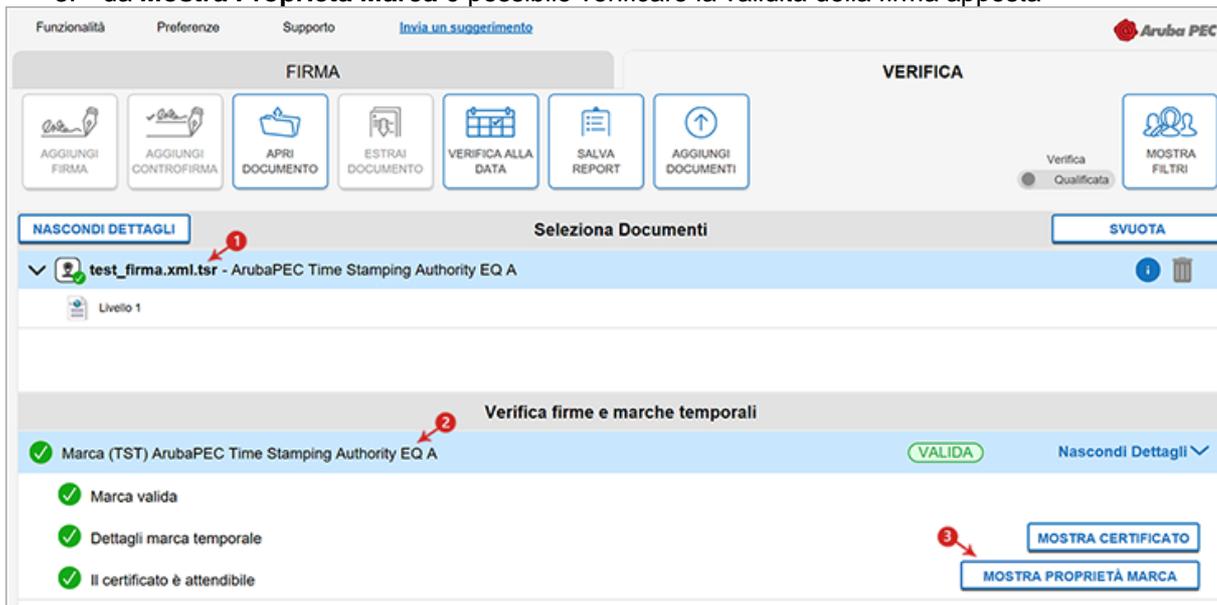
- **Dettagli marca temporale**

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.

3. da **Mostra Proprietà Marca** è possibile verificare la validità della firma apposta




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.

L'orario di marcatura e Firma Digitale si riferisce all'orario UTC (Tempo Coordinato Universale) riferimento da cui sono calcolati tutti gli altri fusi orari del mondo e indicato per essere sempre lo stesso in ogni parte del mondo. In Italia, nel periodo estivo (ora legale), l'orario è 2 ore avanti rispetto alla UTC (Tempo Coordinato Universale), in inverno (ora solare) l'orario è avanti di un'ora sulla UTC.

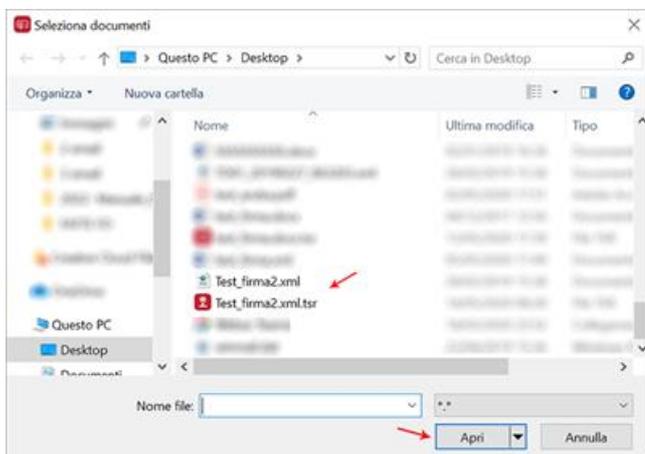
3.11 Verifica Marche Temporali in formato TSD Aruba Sign e Firma Remota

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

Per verificare uno o più File marcati in formato TSD con Aruba Sign, trascinare o selezionare il documento all'interno della scheda **Verifica**:



Selezionare da locale il file associato alla marca stessa, quindi cliccare su **Apri**:



Alla schermata visualizzata è possibile:

1. visualizzare il file marcato;
2. su **Verifica firme e marche temporali** sono visibili le marche presenti all'interno del file;
 - **Marca valida**

Indica che la marca temporale è integra ed è correttamente associata al documento selezionato;

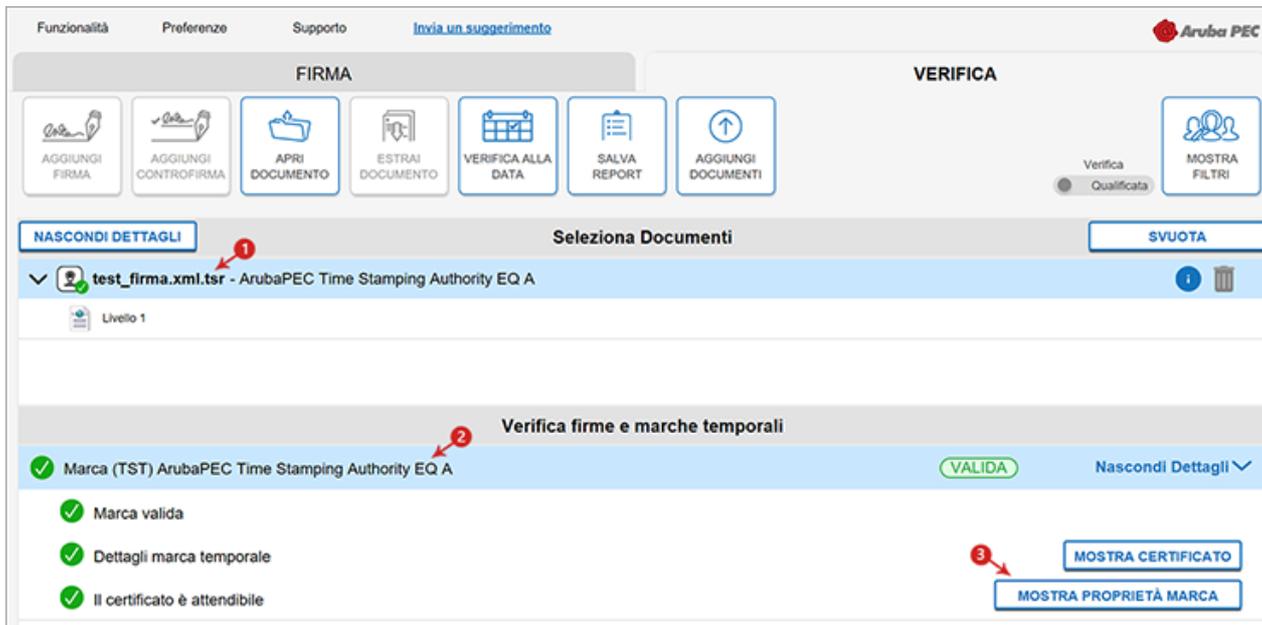
- **Dettagli marca temporale**

Sono riportate le specifiche della marca stessa;

- **Il certificato è attendibile**

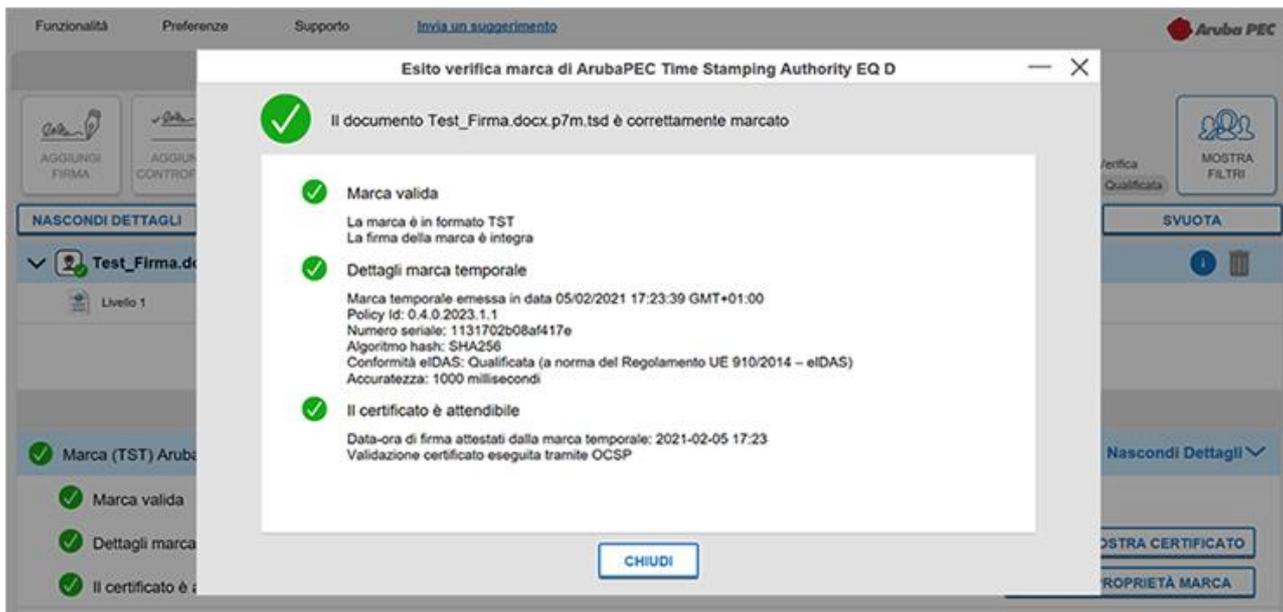
Attesta che la Marca Temporale è rilasciata da un'Autorità di Certificazione inclusa nell'Elenco Pubblico dei Certificatori.

3. da **Mostra Proprietà Marca** è possibile verificare la validità della firma apposta:



The screenshot shows the 'VERIFICA' section of the Aruba PEC interface. At the top, there are navigation tabs: 'Funzionalità', 'Preferenze', 'Supporto', and 'Invia un suggerimento'. Below these are two main sections: 'FIRMA' and 'VERIFICA'. The 'VERIFICA' section contains several icons for actions like 'AGGIUNGI FIRMA', 'AGGIUNGI CONTROFIRMA', 'APRI DOCUMENTO', 'ESTRAI DOCUMENTO', 'VERIFICA ALLA DATA', 'SALVA REPORT', and 'AGGIUNGI DOCUMENTI'. A 'Verifica Qualificata' button is also present. Below the navigation is a 'Seleziona Documenti' section with a 'NASCONDI DETTAGLI' button and a 'SVUOTA' button. A document 'test_firma.xml.tsr - ArubaPEC Time Stamping Authority EQ A' is selected. Below this is a 'Verifica firme e marche temporali' section. It shows a green checkmark and the text 'Marca (TST) ArubaPEC Time Stamping Authority EQ A' with a 'VALIDA' button. Below this are three items: 'Marca valida', 'Dettagli marca temporale', and 'Il certificato è attendibile'. At the bottom right, there are buttons for 'MOSTRA CERTIFICATO' and 'MOSTRA PROPRIETÀ MARCA'. Red arrows point to the 'NASCONDI DETTAGLI' button (1), the 'Verifica firme e marche temporali' section (2), and the 'MOSTRA PROPRIETÀ MARCA' button (3).

34



The screenshot shows a detailed verification result dialog box titled 'Esito verifica marca di ArubaPEC Time Stamping Authority EQ D'. The dialog box contains a green checkmark and the text 'Il documento Test_Firma.docx.p7m.tsd è correttamente marcato'. Below this are three items: 'Marca valida', 'Dettagli marca temporale', and 'Il certificato è attendibile'. The 'Dettagli marca temporale' section provides the following information: 'Marca temporale emessa in data 05/02/2021 17:23:39 GMT+01:00', 'Policy id: 0.4.0.2023.1.1', 'Numero seriale: 1131702b08af417e', 'Algoritmo hash: SHA256', 'Conformità eIDAS: Qualificata (a norma del Regolamento UE 910/2014 - eIDAS)', and 'Accuratezza: 1000 millisecondi'. The 'Il certificato è attendibile' section provides the following information: 'Data-ora di firma attestati dalla marca temporale: 2021-02-05 17:23' and 'Validazione certificato eseguita tramite OCSP'. A 'CHIUDI' button is at the bottom of the dialog box.

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.

L'orario di marcatura e Firma Digitale si riferisce all'orario UTC (Tempo Coordinato Universale) riferimento da cui sono calcolati tutti gli altri fusi orari del mondo e indicato per essere sempre lo stesso in ogni parte del mondo. In Italia, nel periodo estivo (ora legale), l'orario è 2 ore avanti rispetto alla UTC (Tempo Coordinato Universale), in inverno (ora solare) l'orario è avanti di un'ora sulla UTC.

3.12 Generare PIN OTP con Dispositivi di Firma Remota

Generare una password OTP con OTP Display

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

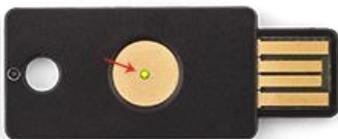


Nel caso in cui si utilizzi un dispositivo OTP a evento, cioè un **Display c100**, (con seriale che inizia per uno), generare PIN OTP solo ed esclusivamente in caso di effettivo utilizzo degli stessi per apporre Firma Remota a documenti. Qualora si generi **tramite il proprio Token** un tot numero di 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.

35

Generare una password OTP con OTP USB

Per generare un PIN con il dispositivo 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:



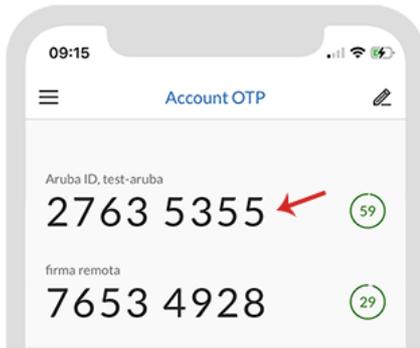
A questo punto eseguire contemporaneamente le operazioni sotto indicate:

- 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.

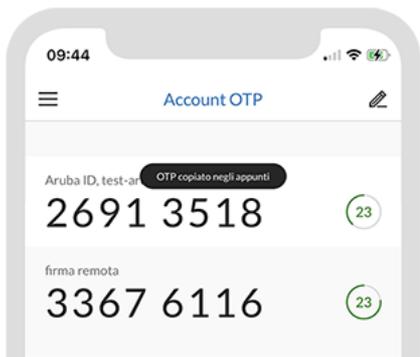
Generare PIN OTP solo ed esclusivamente in caso di effettivo utilizzo degli stessi per apporre Firma Remota a documenti. Qualora si generi tramite il proprio Token un tot numero di PIN OTP senza utilizzarli, il Certificato di Firma Remota va fuori sincronizzazione e la procedura di Firma di un documento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

Generare una password OTP con OTP Mobile

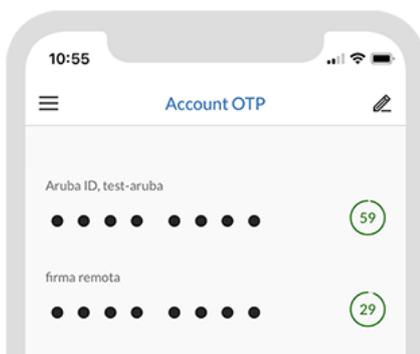
L'app Aruba OTP genera in automatico codici OTP. Per visionarli, aprire l'applicazione. I codici OTP sono generati in automatico e immediatamente visibili. Sopra il codice è presente il nome dell'account di riferimento:



Cliccando sul **codice è possibile copiarlo**. Si potrà poi incollarlo su un'altra app che lo richiede.



Se sul menu **Impostazioni** è stata attivata l'opzione **Nascondi OTP**, i codici generati non sono visibili ma sarà possibile ugualmente copiarli negli appunti:



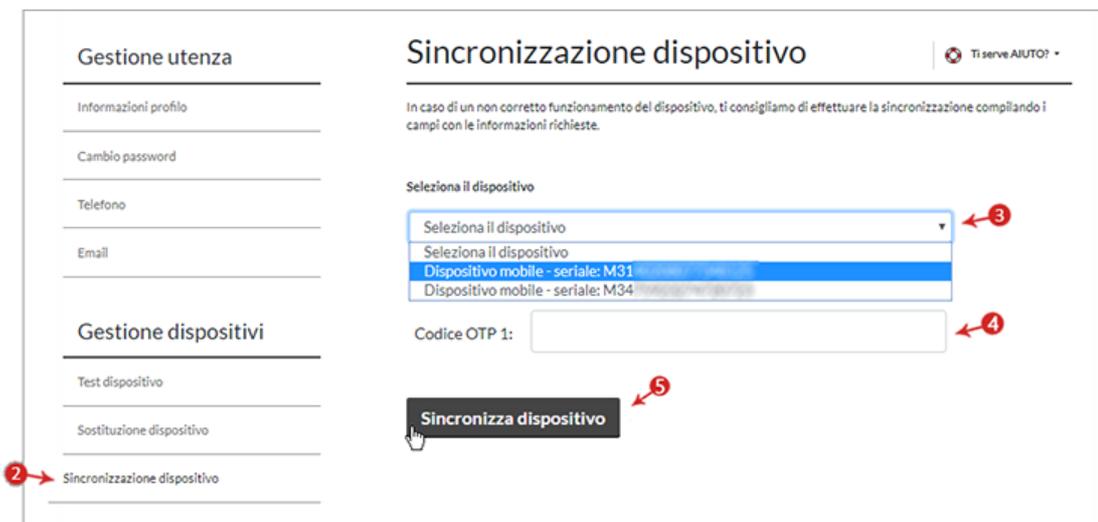
Se si utilizza una versione dell'app Aruba OTP mobile precedente a settembre 2016, occorre generare codici OTP esclusivamente in caso di effettivo utilizzo degli stessi per apporre Firma Remota a documenti. Qualora venga generato un certo numero di codici OTP senza che vengano utilizzati, infatti, il 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, è necessario effettuare la sincronizzazione della Firma.

4 Sincronizzazione dispositivo Firma Remota

Se si genera con un dispositivo di Firma Remota (fisico o mobile) **un certo numero di PIN OTP senza utilizzarli**, o in caso di mal funzionamento del token, il certificato di firma va fuori sincronizzazione e nonostante l'inserimento di PIN OTP corretti, si visualizza una schermata di errore al termine della firma di un documento.

Per sbloccare il dispositivo, **sincronizzare la firma** seguendo la procedura di seguito indicata:

1. accedere al [selfcare Firma Remota](#);
2. dal menu di sinistra selezionare **Gestione dispositivi > Sincronizzazione dispositivo**;
3. su **Seleziona il dispositivo** selezionare il dispositivo da sincronizzare dall'apposito menu a tendina;
4. digitare dei codici OTP generati con il dispositivo da sincronizzare:
 - in caso di **dispositivo OTP a tempo**: OTP con display c200, cioè con seriale che inizia per due, producono PIN temporali che hanno validità 30 o 60 secondi;
 - per **dispositivi OTP a evento**: OTP con display c100, cioè con seriale che inizia per uno e token OTP USB, producono One Time Password non ripetibili.
 - in caso di **dispositivo OTP mobile**;
5. cliccare su **Sincronizza dispositivo** per completare la procedura:



Si visualizza una schermata di conferma.

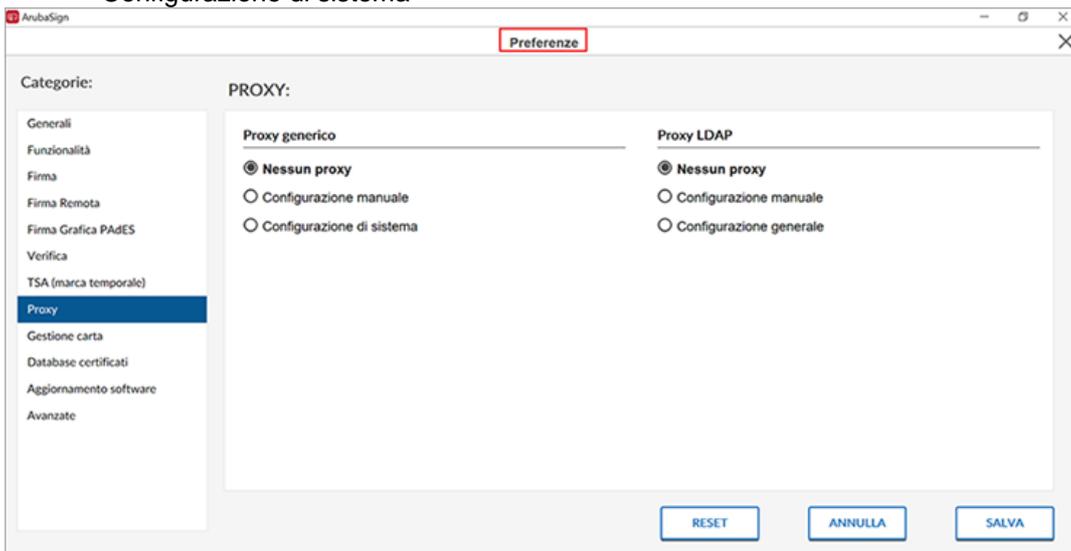
5 Configurazione Proxy http Firma Remota

La configurazione dei **parametri Proxy HTTP**, tramite l'utilizzo del software Aruba Sign, permette di svolgere le operazioni di verifica di un file firmato, aggiornamento, controllo, stato di revoca e richiesta di Marche Temporal qualora la postazione si trovi dietro Proxy HTTP. Per procedere, aprire il menu **Preferenze** di Aruba Sign:



Quindi allo specifico Tab Proxy è possibile scegliere:

- Nessun Proxy
- Configurazione Manuale
- Configurazione di sistema



Se si sceglie la **Configurazione manuale** impostare i relativi parametri e salvarli. Di seguito un esempio di configurazione:

Proxy generico <input type="radio"/> Nessun proxy <input checked="" type="radio"/> Configurazione manuale <input type="radio"/> Configurazione di sistema Tipo <input checked="" type="radio"/> HTTP <input type="radio"/> SOCKS4 <input type="radio"/> SOCKS5 <input type="radio"/> NTLM	Host <input type="text" value="192.168.1.1"/> Porta <input type="text" value="8080"/> Credenziali d'accesso Username <input type="text" value="Nome utente"/> Password <input type="password" value="••••••••"/>
---	---

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.

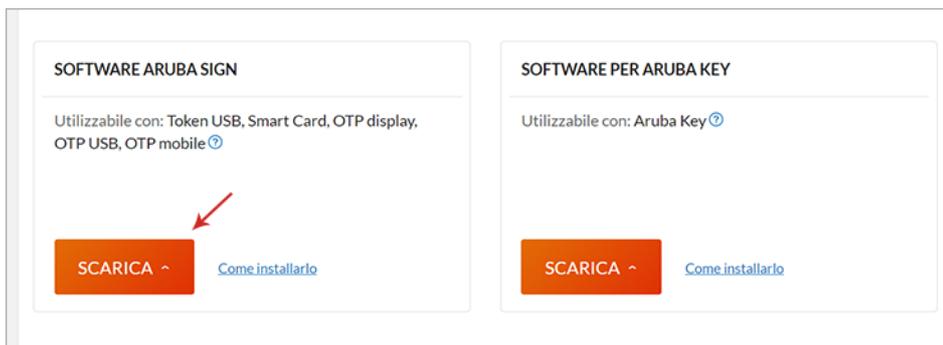
6 Installazione e avvio del software – Firma Digitale

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.

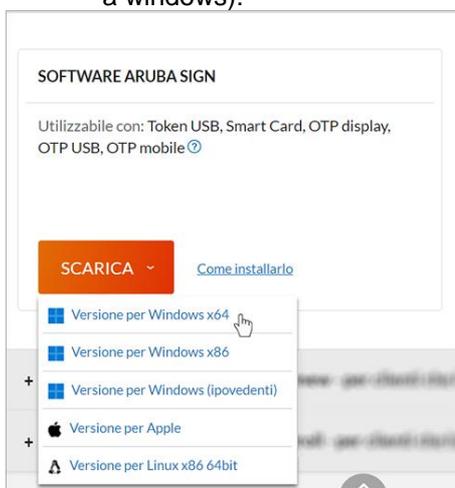
6.1 Installare i driver dei lettori di Firma Digitale

Per scaricare i driver è sufficiente collegarsi alla sezione download da [qui](#), quindi dal form dedicato Driver Lettori:

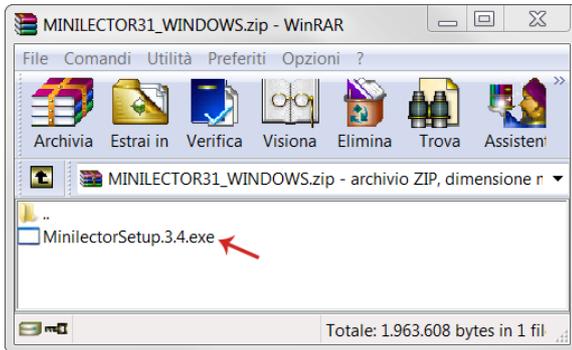
- scegliere l'opzione Firma Digitale e aprire il menu a tendina **Software per firmare > Software Aruba Sign**. Cliccare su **Scarica per continuare**.



- dal menu a tendina che si apre scegliere il sistema operativo utilizzato (l'esempio di seguito indicato si riferisce a windows):



- dalla cartella creata a seguito dell'installazione, decomprimere ed eseguire il file **.exe**:



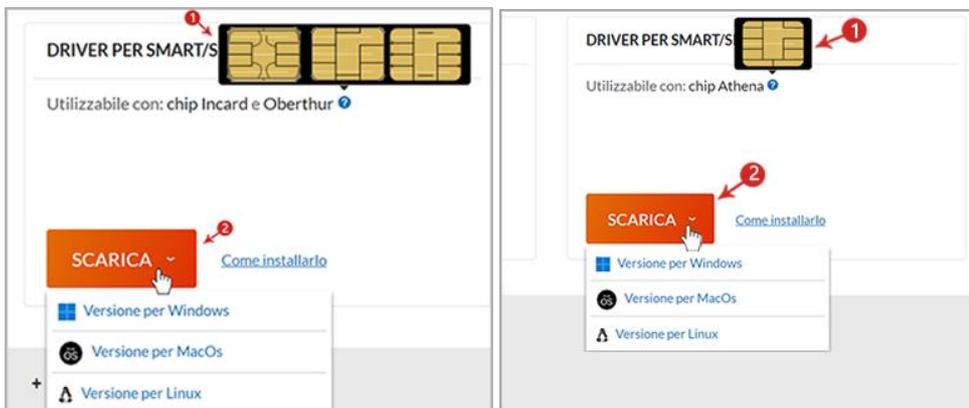
- completare la procedura di installazione, seguendo i passaggi indicati dal sistema.

6.2 Installare i driver Smart Card

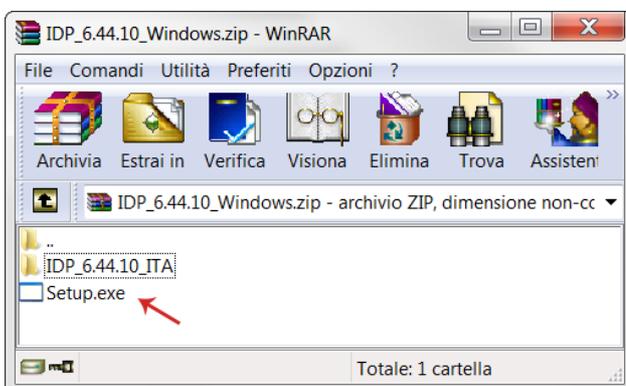
La **Smart Card** ha le dimensioni di una **comune carta di credito con microchip** (o eventualmente quelle di una SIM telefonica) e consente di firmare documenti digitali e di accedere in modo sicuro ai siti web. Per il corretto funzionamento devono essere installati nel computer i relativi driver, scaricabili dalla sezione download da [qui](#), al form Driver Smart Card/SIM Card e differenti a seconda del tipo di Smart Card posseduta.

Le tipologie di Smart Card distribuite da Aruba sono **Incard**, **Oberthur** e **Athena**. Per procedere:

1. confrontare l'immagine del chip della carta posseduta con quelle indicate nelle sezioni dedicate del sito pec.it, visionabili dall'apposito simbolo "?";
2. scaricare e salvare i relativi driver cliccando su **Scarica** in base al sistema operativo presente sul proprio computer:



dalla cartella creata a seguito dell'installazione, decomprimere ed eseguire il **file .exe**:



completare la procedura di installazione, seguendo i passaggi indicati dal sistema.

6.3 Installare il software Aruba Sign

1. collegarsi per effettuare download gratuito è eseguibile dalla pagina raggiungibile a [questo link](#);
2. procedere, scegliere l'opzione Firma Digitale e aprire il menu a tendina **Software per firmare** > **Software Aruba Sign**. Cliccare su **Scarica** per continuare;
3. Scaricare ed eseguire su locale il File di installazione, quindi installare il Software utilizzando la procedura guidata e dal menu a tendina che si apre scegliere il sistema operativo utilizzato;
4. Salvare ed eseguire il file cliccando due volte sull'icona visibile nella cartella prescelta per il download. Alla fine dell'installazione compare il seguente messaggio. Cliccare su **Fine** per concludere:



5. sul **desktop** si visualizza l'**icona di Aruba Sign** che permette l'avvio del programma;
6. completata l'installazione, si visualizza la schermata principale del software:

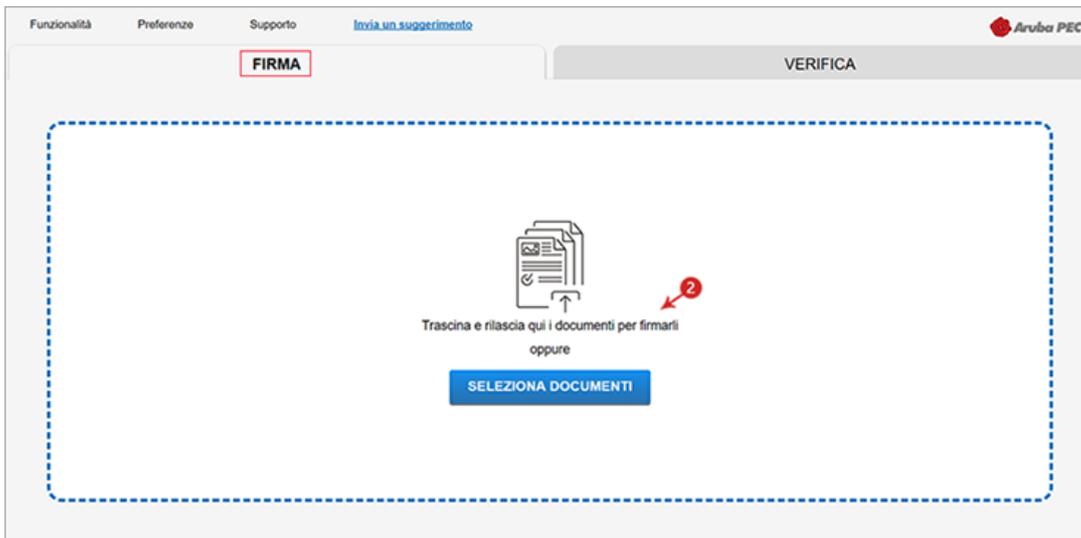


7 Firma e verifica file Aruba Sign - Firma Digitale

7.1 Caricare documenti da firmare e/o cartelle su Aruba Sign

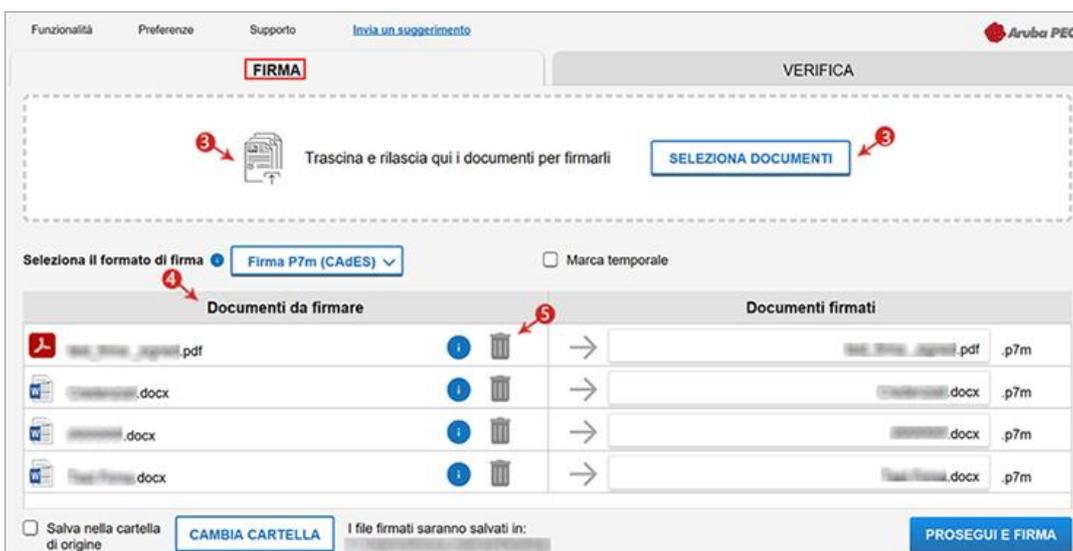
Per caricare uno o più file su Aruba Sign e/o una intera cartella:

1. avviare il software Aruba Sign;
2. nella scheda **Firma** è possibile trascinare un documento e/o cartella o selezionare un documento da caricare cliccando sul pulsante un documento da **Seleziona Documenti** (sono accettate tutte le estensioni):



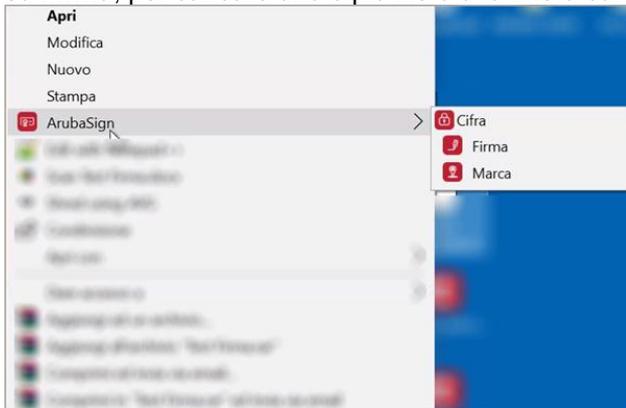
42

3. per aggiungere ulteriori documenti cliccare su **Seleziona Documenti** e caricare i file desiderati da locale o trascinarli nello spazio apposito;
4. i documenti importati sono visibili sotto **Documenti da firmare**;
5. i documenti caricati possono essere rimossi in qualsiasi momento cliccando sull'icona **Cestino**:



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.

In alternativa, è possibile cliccare con il tasto destro del mouse **sull'icona Aruba Sign** presente nel desktop e cliccare su **Firma**, per caricare uno o più file o una intera cartella:



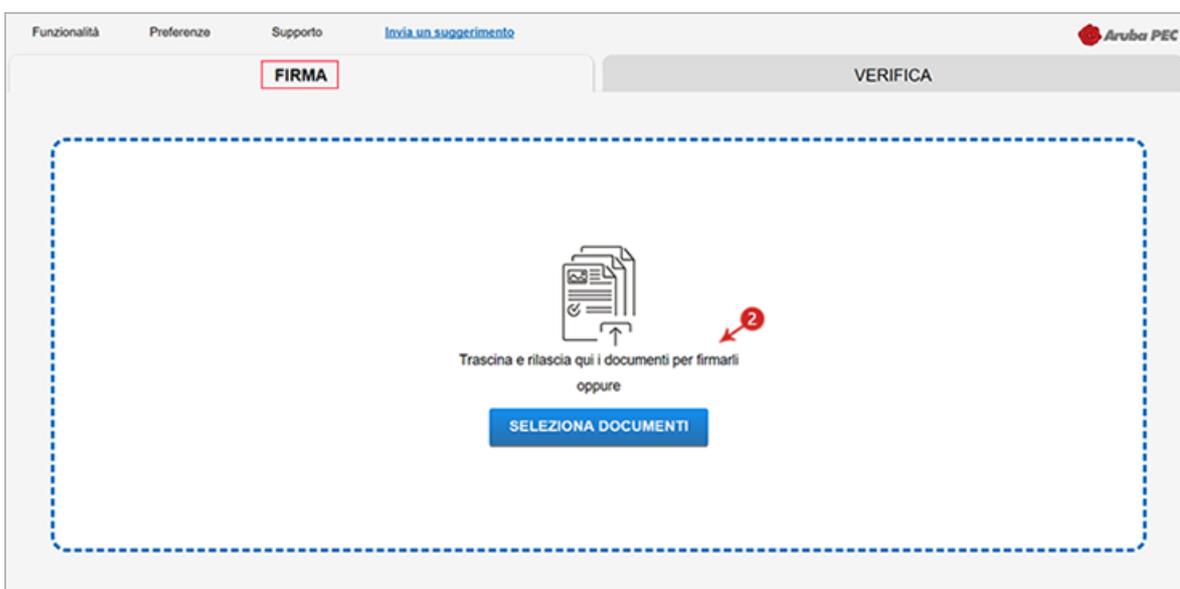
7.2 Firmare uno o più file in formato .p7m - Firma Digitale

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.

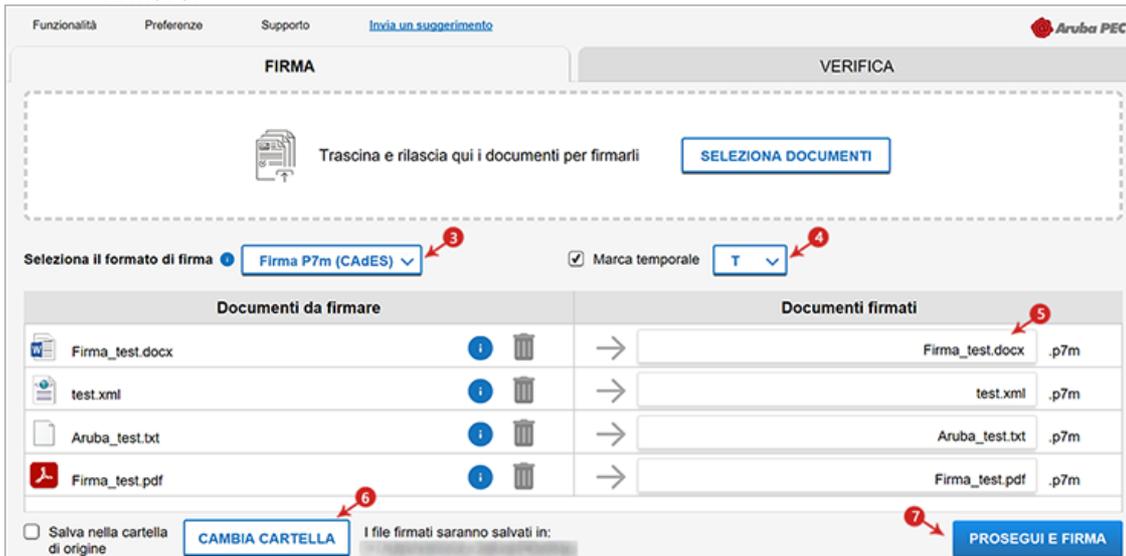
43

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

1. aprire il software Aruba Sign;
2. nella scheda **Firma** è possibile trascinare un documento e/o cartella o selezionare un documento da **Seleziona Documenti** (sono accettate tutte le estensioni):



3. dall'apposito menu a tendina **Seleziona il formato** di firma selezionare come tipologia di **Firma p7m CAeS**;
4. inserire il flag in corrispondenza della voce **Marca Temporale** per apporre al file una marcatura. Per i livelli di firma **T** e **LT** che possono essere abbinati al formato .p7m cliccare [qui](#);
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 **Proseguì per continuare**. Sono firmati tutti i documenti presenti alla finestra **Documenti da firmare**:



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. cliccare su **Firma** per concludere il procedere:



dell'operazione si visualizza la seguente schermata che notifica la corretta firma del file. Cliccare su **Chiudi**:



I documenti firmati sono salvati in formato .p7m nella cartella indicata in fase di firma.

7.3 Firmare 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 distaccate e/o marche temporali associate, utilizzando il **formato .zip**.

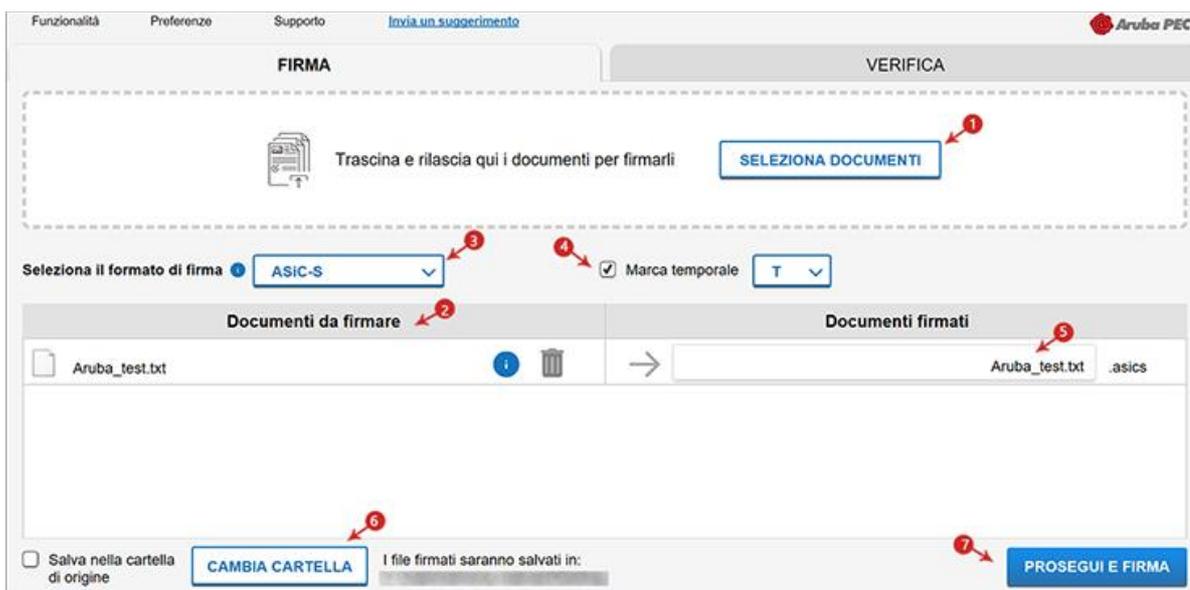
Per firmare digitalmente un file in formato ASiC-S con Aruba Sign:

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 menu a tendina **Seleziona il formato di firma** selezionare come tipologia di Firma ASiC-S;
4. se in possesso di marche temporali, oltre alla firma, è possibile apporre al file una marcatura temporale. Inserire il flag in corrispondenza della voce **Marca Temporale** nel formato scelto dall'apposito menu a tendina;
5. dalla finestra **documenti da 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 e Firma** per continuare:

45



Alla schermata **Completa la firma di 1 documento**:

1. assicurarsi che sia selezionato il **Certificato** per la firma digitale (in formato **Cognome - Nome**);
2. inserire il **PIN** di protezione della Smart Card;
3. cliccare su **Firma** per concludere il processo:



al termine dell'operazione si visualizza la corretta firma del file.

Su **Visualizza Documenti** sono visibili i documenti firmati e salvati in formato .p7m, cliccare su **Chiudi**:



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

7.4 Firmare più file in formato ASiC-E - Firma Digitale

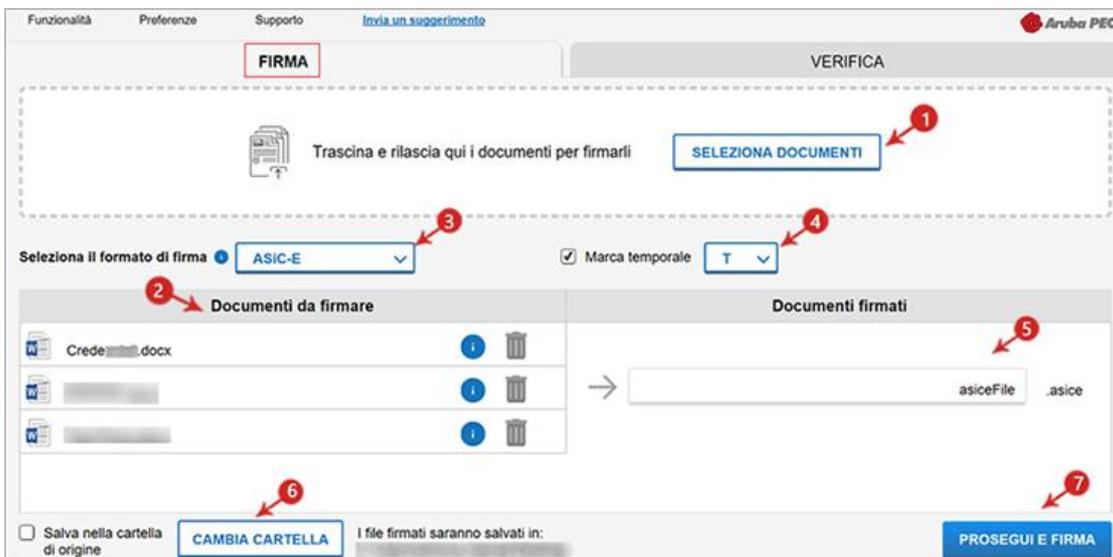
Il formato di firma **ASiC-E** (Associated Signature Containers ASiC extended) è un contenitore di dati che raggruppa più file e le relative firme digitali distaccate e/o marche temporali associate, utilizzando il **formato .zip**.

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 menu a tendina **Seleziona il formato di firma ASiC-S**.

2. i documenti caricati sono visibili all'apposita schermata **Documenti da firmare**;
3. dall'apposito menu a tendina **Seleziona il formato di firma** selezionare come tipologia di Firma ASiC-E;
4. se in possesso di marche temporali, oltre alla firma, è possibile apporre al file una marcatura temporale. Inserire il flag in corrispondenza della voce **Marca temporale** nel formato scelto dall'apposito menu a tendina Marca Temporale;
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 e Firma** per continuare. Sono firmati tutti i documenti presenti alla finestra Documenti da firmare:



47

Alla schermata Completa la firma di 3 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;
3. cliccare su **Firma** per concludere il processo:



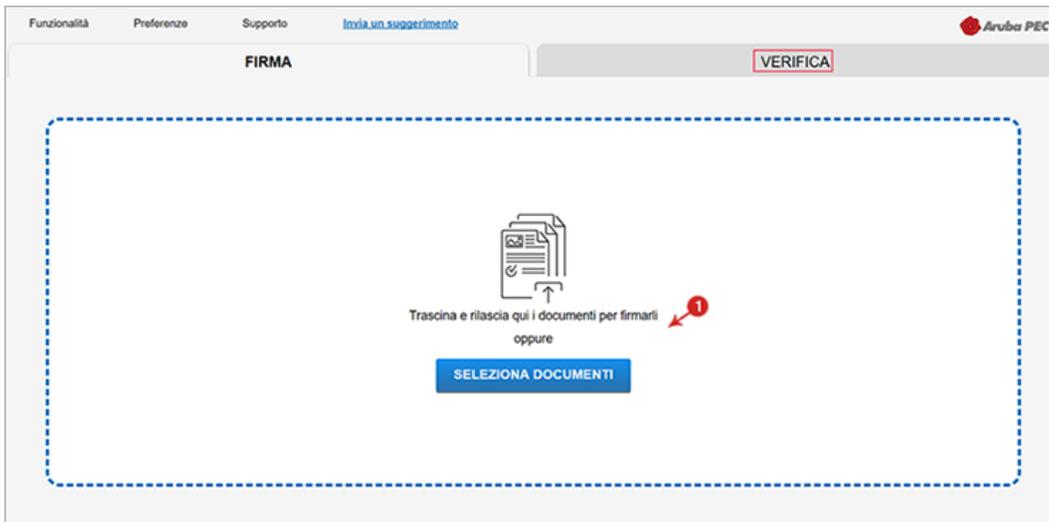
Su **Visualizza Documenti** sono visibili i documenti firmati e salvati in formato .p7m, cliccare su **Chiudi** per terminare:



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.

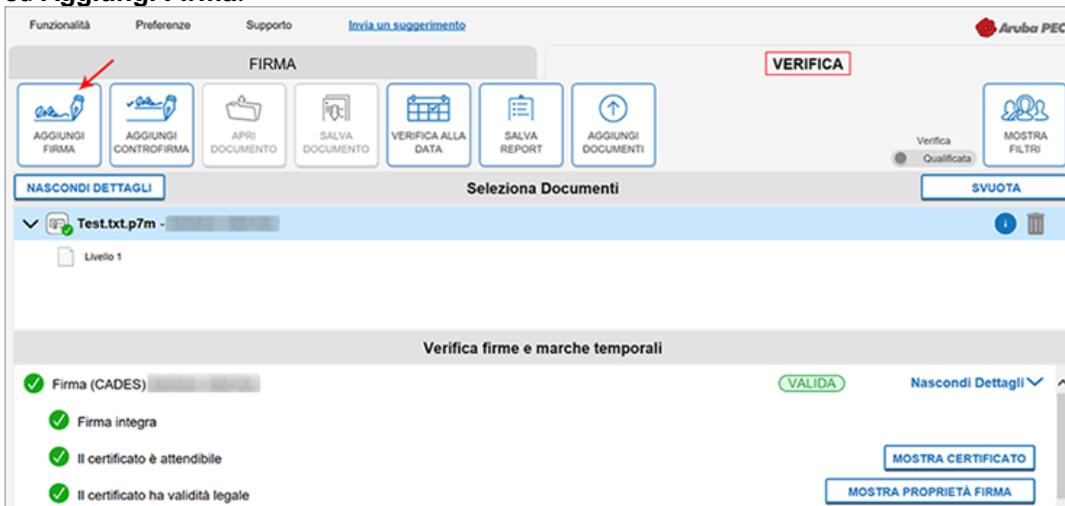
7.5 Apposizione Firma Parallela - Firma Digitale

La funzione **Firma Parallela** è accessibile trascinando o selezionando il documento all'interno della scheda **Verifica** del software Aruba Sign uno o più file già firmati in formato **.p7m (CADES)** o **.PDF (PAdES)**. È 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:



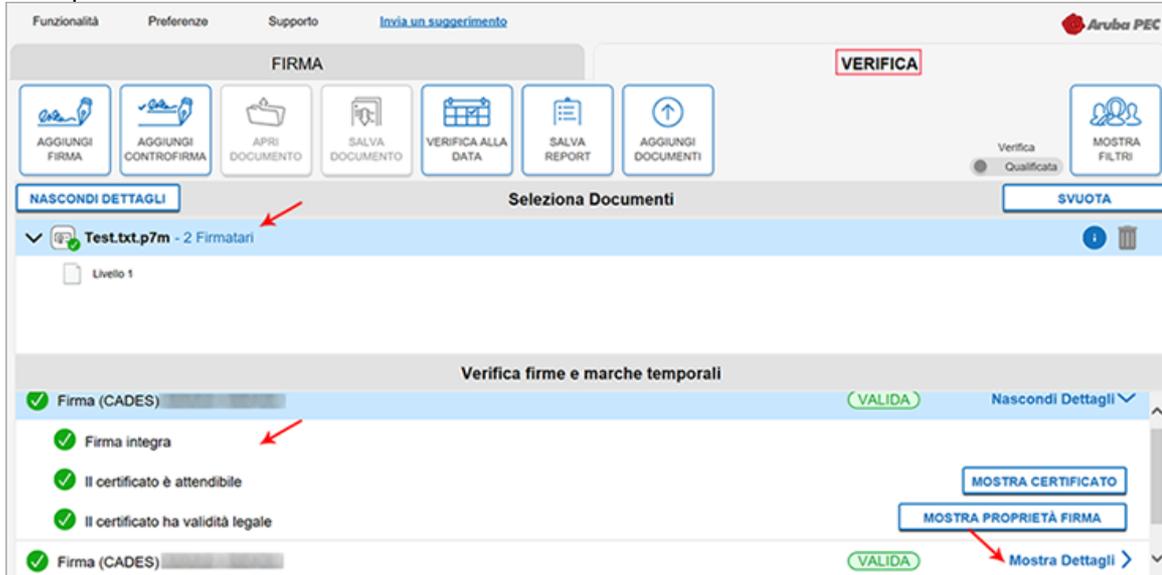
48

Selezionato il documento (anche in caso di caricamento di un solo file) su cui apporre la Firma Parallela poi cliccare su **Aggiungi Firma**:

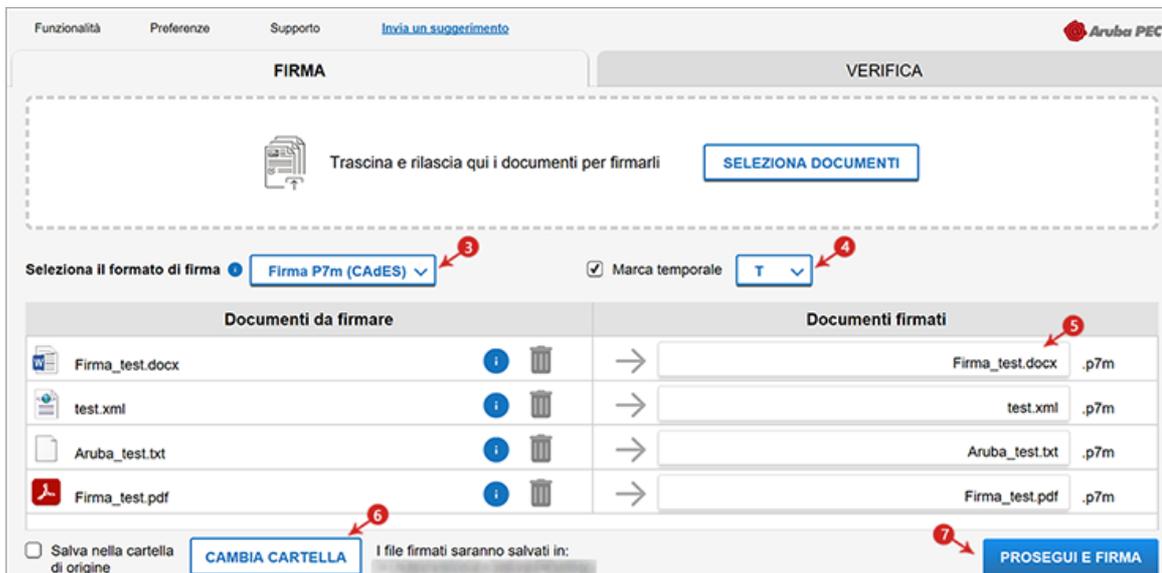


Firmare digitalmente il file. Il sistema non consente di selezionare il formato della Firma. In caso di File .p7m la Firma Parallela è apposta in tale formato, per i file .PDF è possibile apporre una Firma Grafica o Invisibile. **La nuova firma è apposta allo stesso livello di quella preesistente.**

È possibile visionare la presenza della Firma Parallela e i dettagli su **Mostra Certificato** come da immagine esemplificativa sottostante:



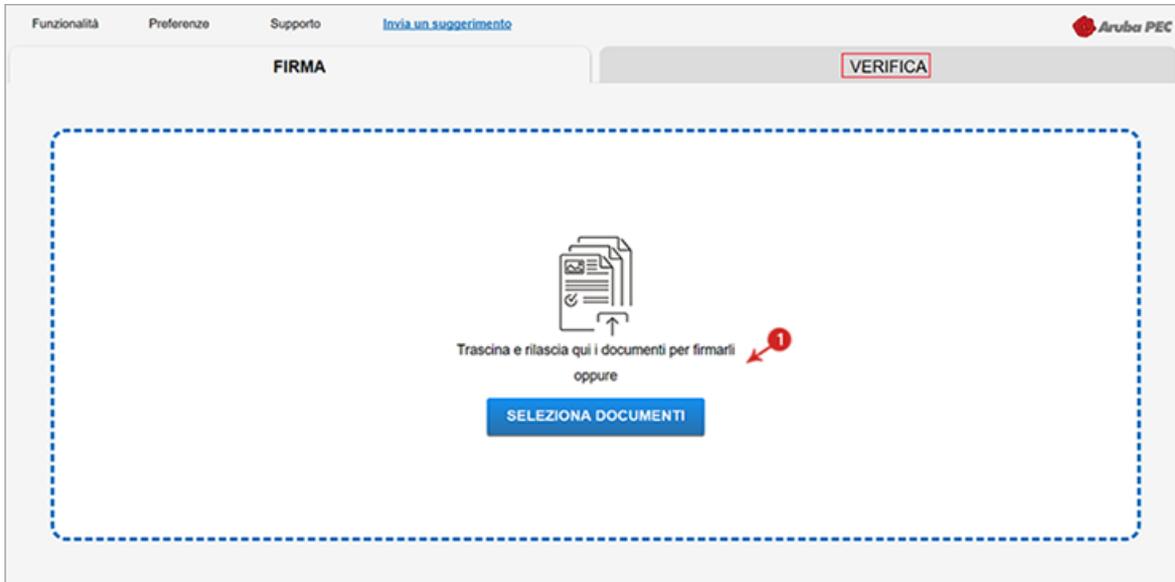
E infine su **Mostra Proprietà Firma** l'esito di verifica:



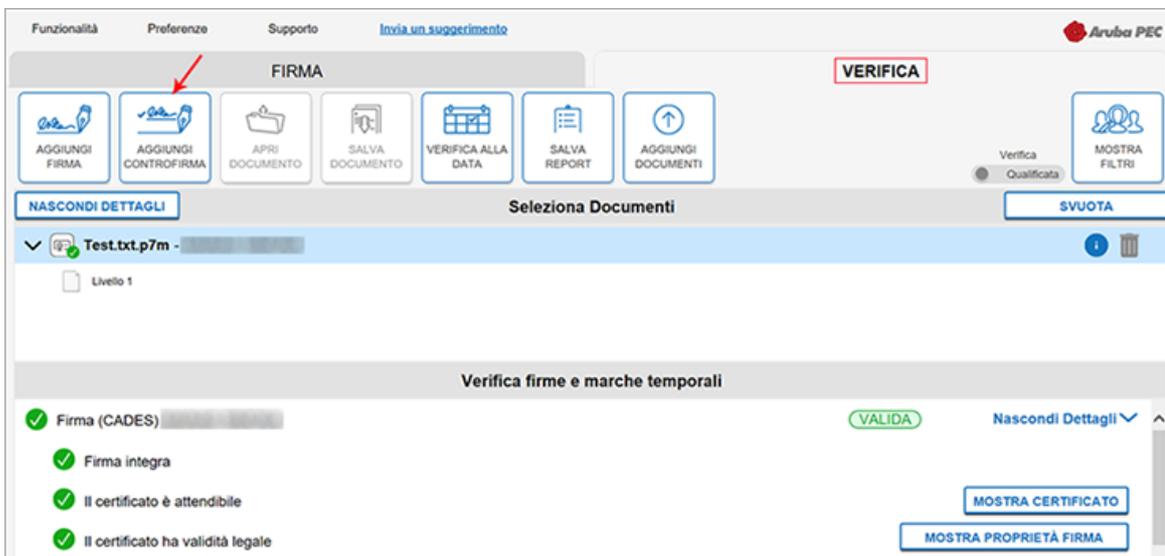
7.6 Apposizione Controfirma - Firma Digitale

La funzione **Controfirma** è accessibile trascinando o selezionando il documento all'interno della scheda **Verifica** del software Aruba Sign uno o più file già firmati in formato .p7m. È apposta a un livello sottostante di una firma preesistente e sottoscrive quest'ultima. **È più annidata rispetto alla firma a cui si riferisce** (aspetto evidenziato da una rappresentazione ad albero delle firme stesse).

Per crearla **selezionare o trascinare un file .p7m (CADES)**, su **Verifica**:



Selezionato il documento (anche in caso di caricamento di un solo file) su cui apporre la Controfirma cliccare su **Aggiungi Controfirma**:

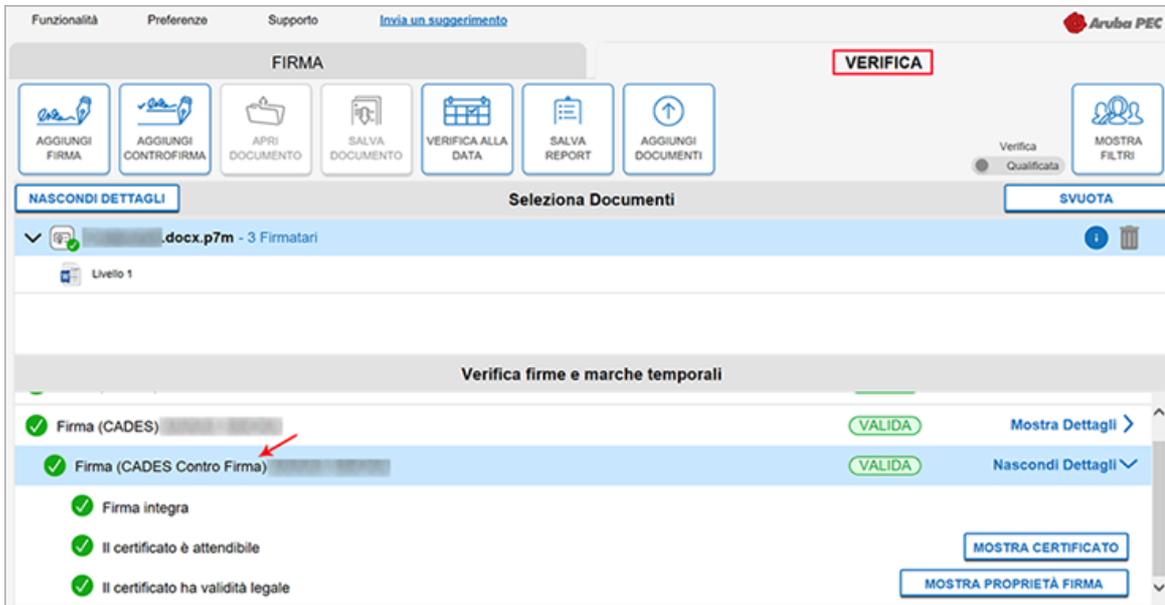


50

Firmare digitalmente il file in formato .p7m.

La nuova firma è apposta a un livello sottostante della firma preesistente.

È possibile visionare la presenza della Controfirma, come da immagine esemplificativa sottostante:



E infine su **Mostra Proprietà Firma** l'esito di verifica firma:



7.7 Apposizione Firma PDF - Grafica - Firma Digitale

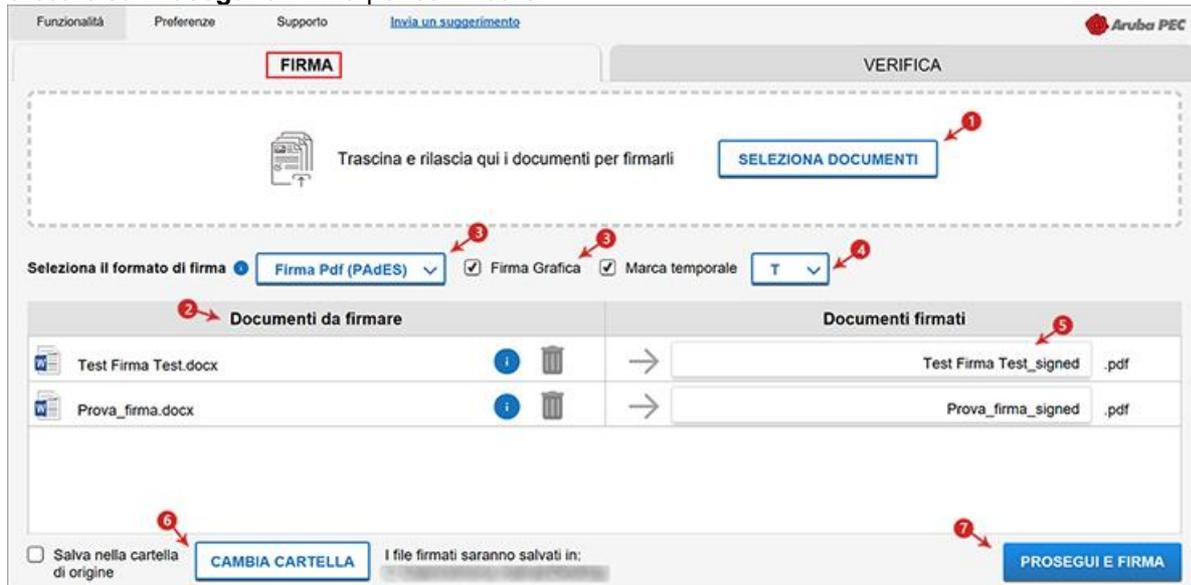
Il formato di **firma PAdES** è applicabile ai soli file **.PDF, .doc, .docx, .xls, .xlsx** (supporto a MS Word w MS Excel versione 2007 o superiore).

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:

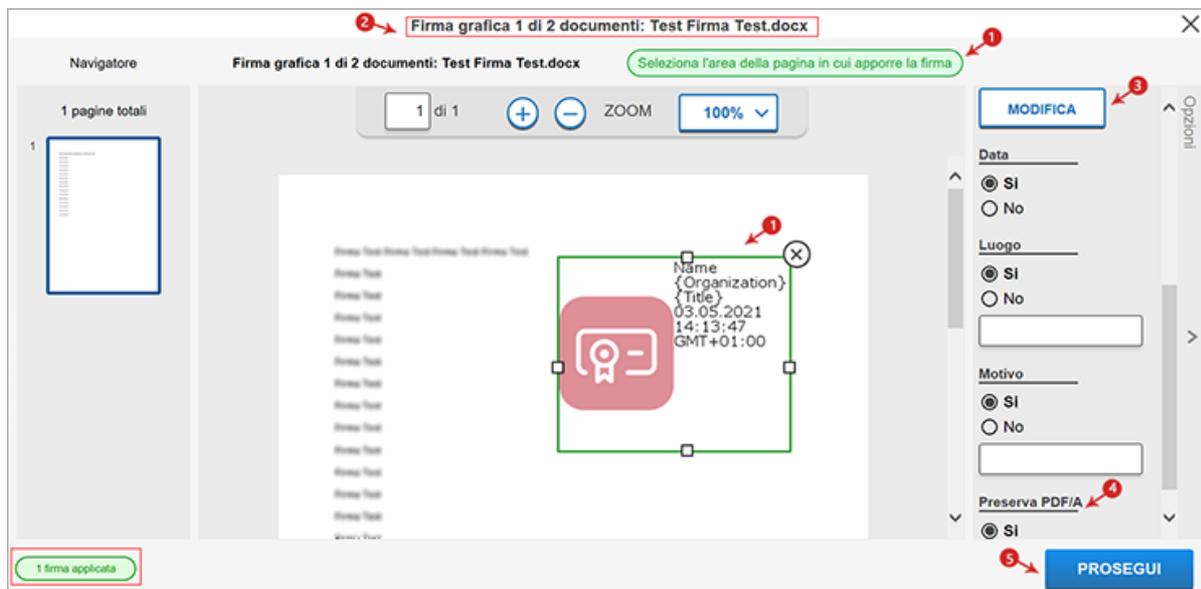
1. trascinare o selezionare uno o più documenti e/o una intera cartella;
2. il singolo/i documenti caricati/o sono visibili all'apposita schermata **Documenti da firmare**;

3. dall'apposito menu a tendina **Seleziona il formato di firma** selezionare come tipologia di **firma PAdES** per **firmare il file in formato .PDF e lasciare il Flag su Firma Grafica**;
4. se in possesso di marche temporali, oltre alla firma, è possibile apporre al file una marcatura temporale. Inserire il flag in corrispondenza della voce **Marca Temporale**;
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 **Proseguì e Firma** per continuare:



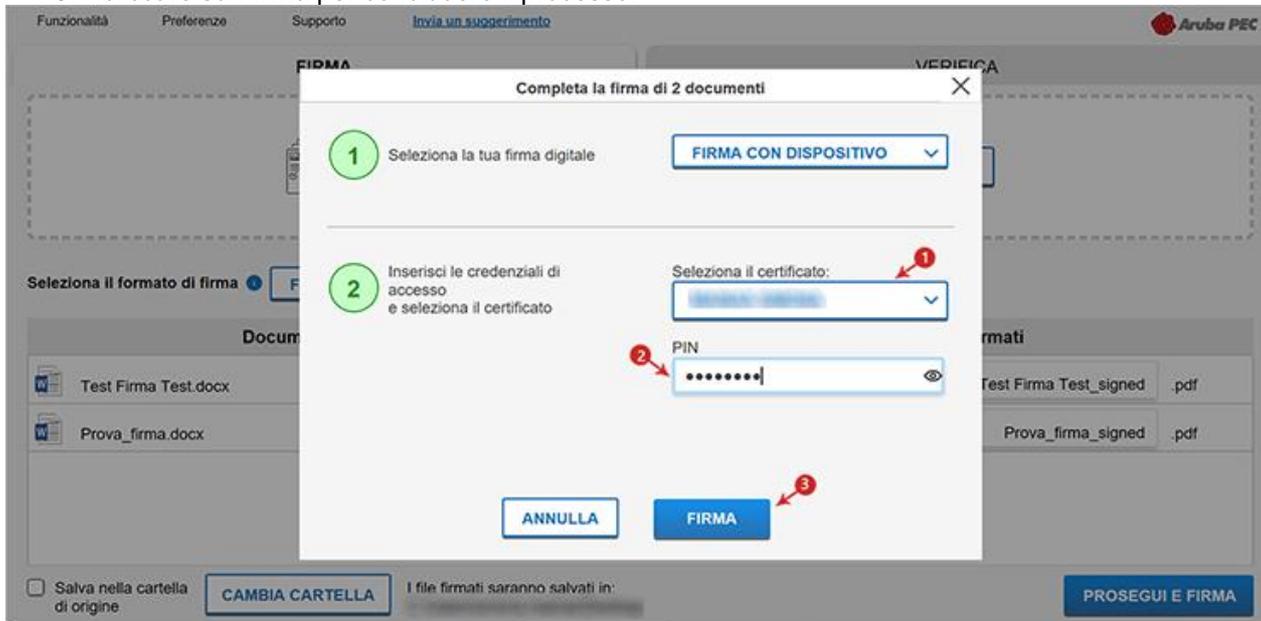
Alla schermata successiva:

1. definire la posizione e la dimensione del campo che ospiterà la Firma Digitale;
2. è possibile visualizzare tutti i documenti o solo quelli firmati;
3. attraverso la finestra **Opzioni** sulla destra, è possibile caricare da locale, attraverso il tasto **Modifica**, 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 dimensioni dell'area selezionata;
4. **abilitando la funzione Preserva PDF/A** la firma grafica è apposta preservando il formato stesso;
5. cliccare su **Proseguì** per procedere:



Alla schermata Completa la firma di 2 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
3. cliccare su **Firma** per concludere il processo:



Su **Visualizza Documenti** sono visibili i documenti firmati e salvati in formato .p7m, cliccare su **Chiudi**:



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

7.8 Firmare un PDF con firma invisibile - Firma Digitale

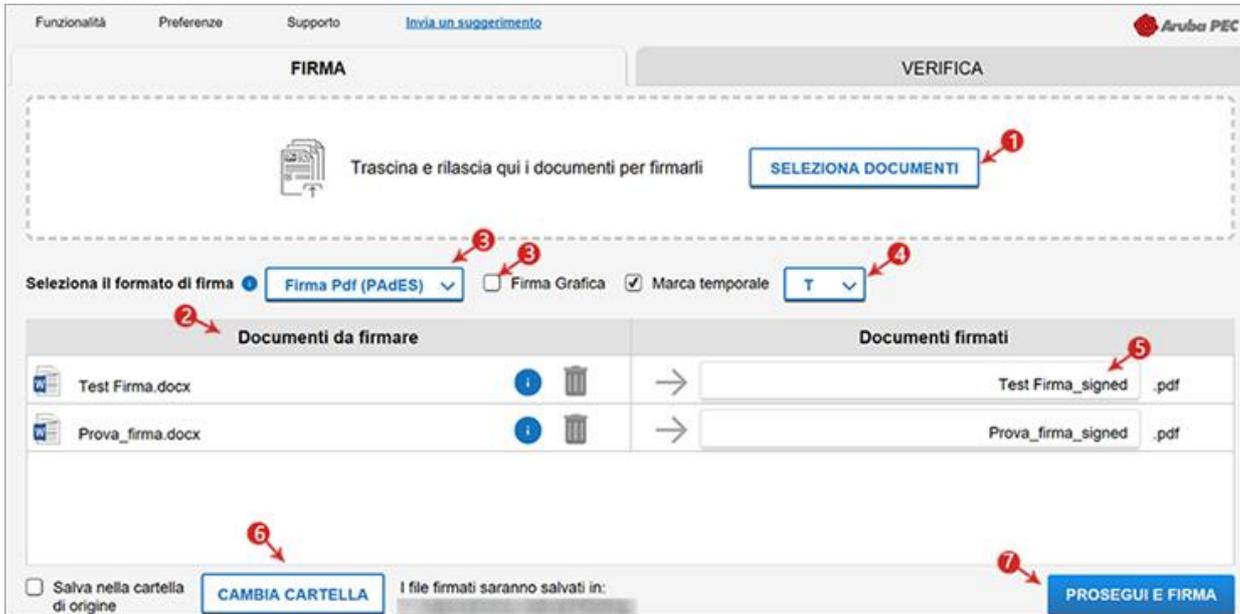
Il formato di firma **PADES** è applicabile ai soli file **.PDF, .doc, .docx, .xls, .xlsx** (supporto a MS Word w MS Excel versione 2007 o superiore).

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:

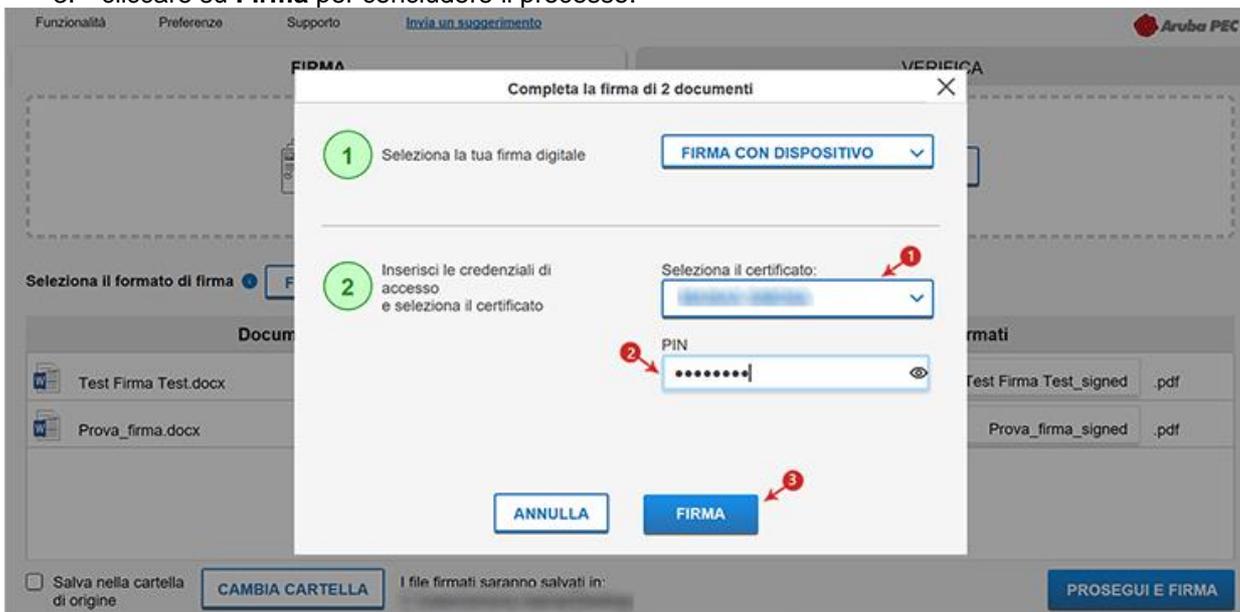
1. trascinare o selezionare uno o più documenti e/o una intera cartella;
2. il singolo/i documenti caricati/o sono visibili all'apposita schermata **Documenti da firmare**;
3. dall'apposito menu a tendina **Seleziona il formato di firma** selezionare come tipologia di **Firma PAdES** per firmare il file in formato .PDF e rimuovere il Flag su Firma Grafica;
4. se in possesso di marche temporali, oltre alla firma, è possibile apporre al file una marcatura temporale. Inserire il flag in corrispondenza della voce **Marca Temporale**;

- dalla finestra **Documenti firmati** rinominare, se desiderato, eventuali file prima di apporre la firma;
- 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;
- clickare su **Prosegui e Firma** per continuare. Sono firmati tutti i documenti presenti alla finestra Documenti da firmare:



Alla schermata Completa la firma di documenti:

- assicurarsi che sia selezionato il certificato per la firma digitale (in formato cognome - nome);
- inserire il **PIN** di protezione della Smart Card;
- clickare 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.

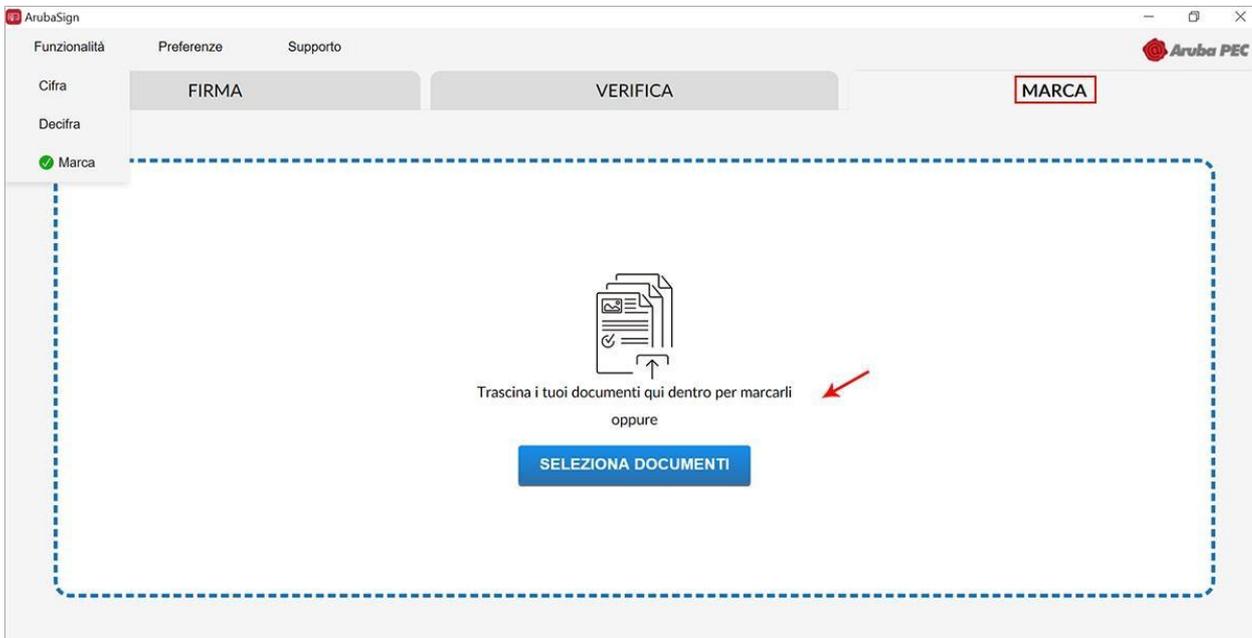
Su **Visualizza Documenti** sono visibili i documenti firmati e salvati in formato .p7m, cliccare su **Chiudi** per terminare l'operazione:



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

7.9 Apposizione di Marche Temporali - Firma Digitale

Per apporre una Marca Temporale accedere su **Funzionalità** e poi su **Marca**, se non precedentemente configurato verrà popolato sulla destra la scheda, quindi trascinare o selezionare il file che si desidera cifrare:



Alla pagina visualizzata:

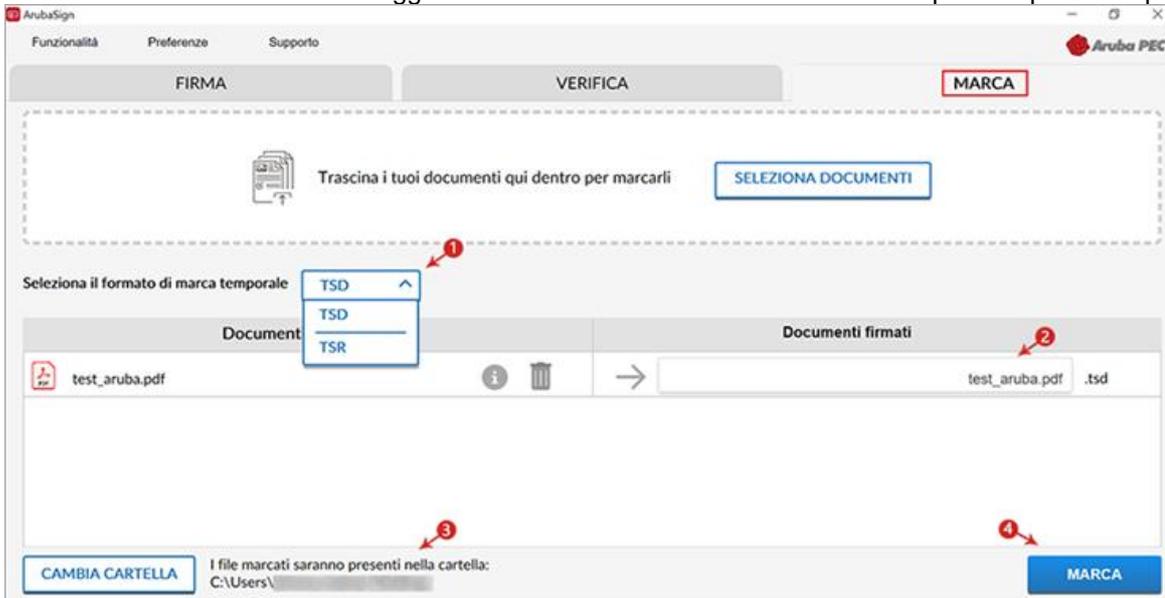
- selezionare il formato di salvataggio della marca temporale. Scegliere tra:
 - TSR**: Il file creato contiene solo l'impronta del file, non tutto il file, e la Marca Temporale in formato TSR è separata dal documento. Pertanto, per verifica il file TSR, è indispensabile possedere anche il documento 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:

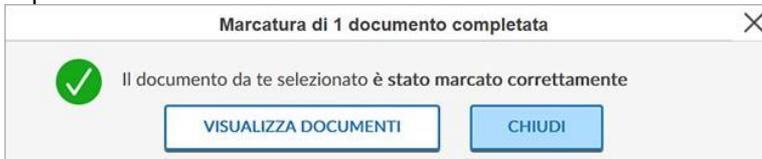
- la **password** è preimpostata a seguito della configurazione dell'account di marcatura temporale;
- il **percorso di destinazione del file** inserito è la cartella su cui risiede il file originale.

- dalla finestra **Documenti firmati** rinominare, se desiderato, eventuali file prima di apporre la firma;

3. il documento è disponibile nella cartella indicata in fase di apposizione della marcatura stessa;
4. cliccare **Marca** al messaggio che notifica la corretta marcatura del file per completare l'operazione:



Il file è disponibile nella cartella indicata in fase di apposizione della marcatura stessa. Cliccare **Chiudi** per completare l'operazione:



7.10 Verifica di file firmati - Firma Digitale

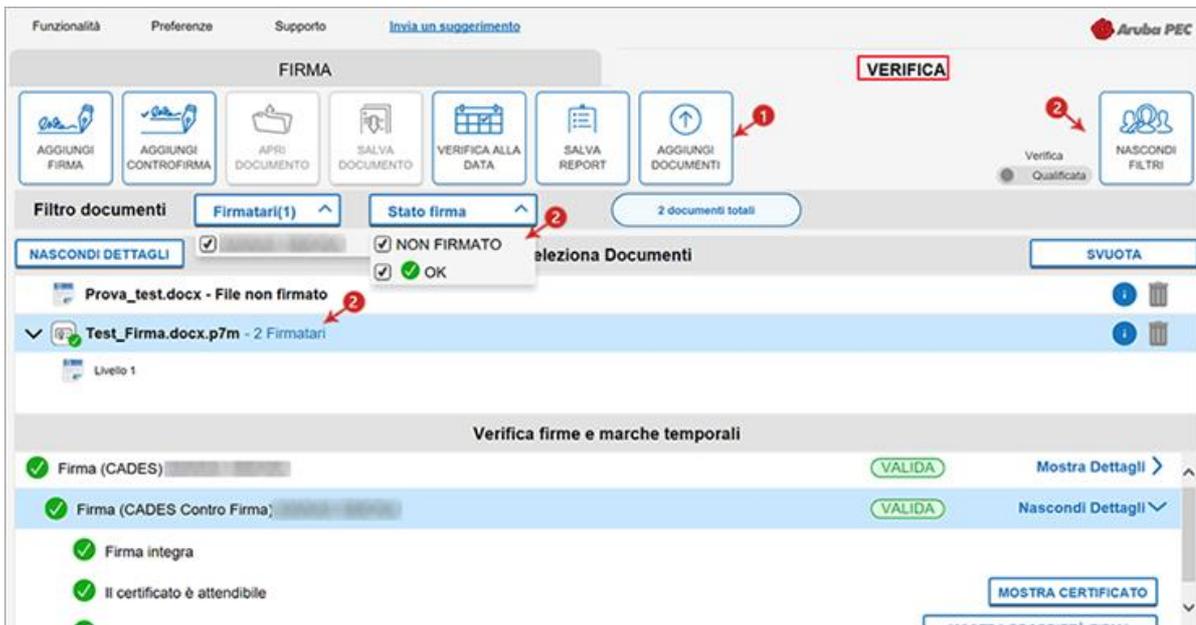
La verifica dei file firmati permette di verificare la validità legale del certificato.

Per verificare uno o più file firmati con Aruba Sign, trascinare o selezionare il documento nella scheda **Verifica**



Alla schermata visualizzata è possibile:

1. verificare ulteriori file firmati trascinandoli da locale o su **Aggiungi Documento**;
2. da **Mostra/Nascondi Filtri** 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 **Selezione documenti**:



3. verifica firme e marche temporali sono visibili le firme presenti all'interno del file:

- **Firma valida**

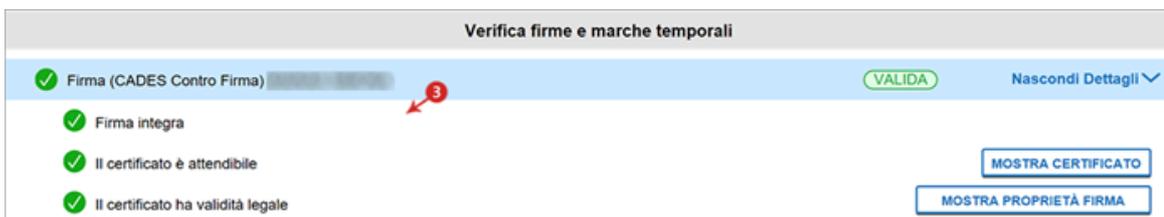
Attesta il formato della firma e che il documento non è stato alterato dopo la firma;

- **Il certificato è attendibile**

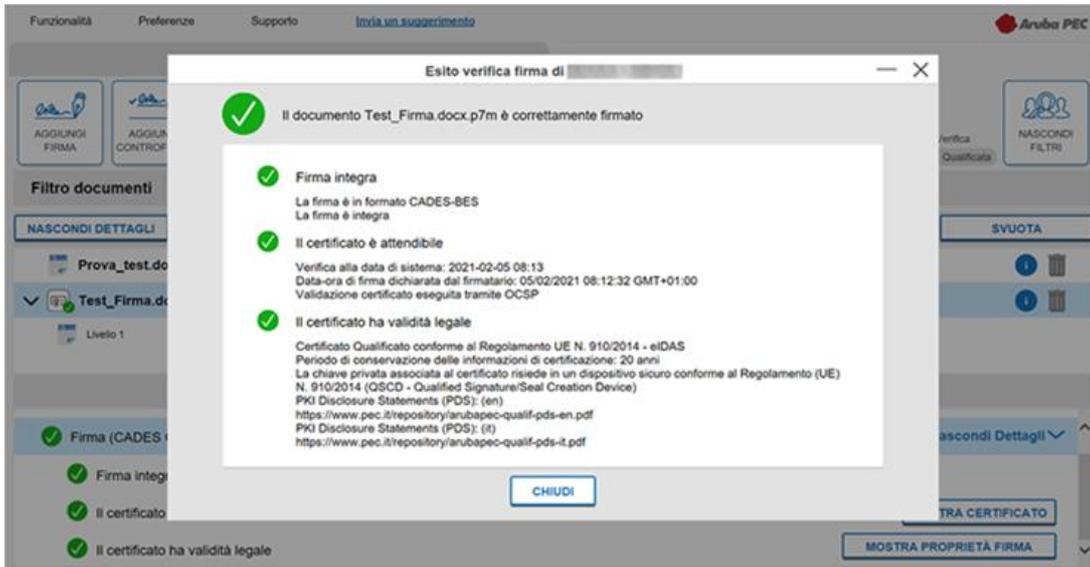
Il messaggio indica che il certificato del sottoscrittore è garantito da una Autorità di Certificazione inclusa nell'Elenco Pubblico dei Certificatori e che non risulta scaduto alla data della Verifica;

- **Il certificato ha validità legale**

Attesta che il certificato del sottoscrittore è un certificato di Firma Digitale qualificato:



da **Mostra Proprietà Firma** è possibile verificare la validità della firma apposta, in particolare:



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.

7.11 Verifica di Marca Temporale in formato TSR - Firma Digitale

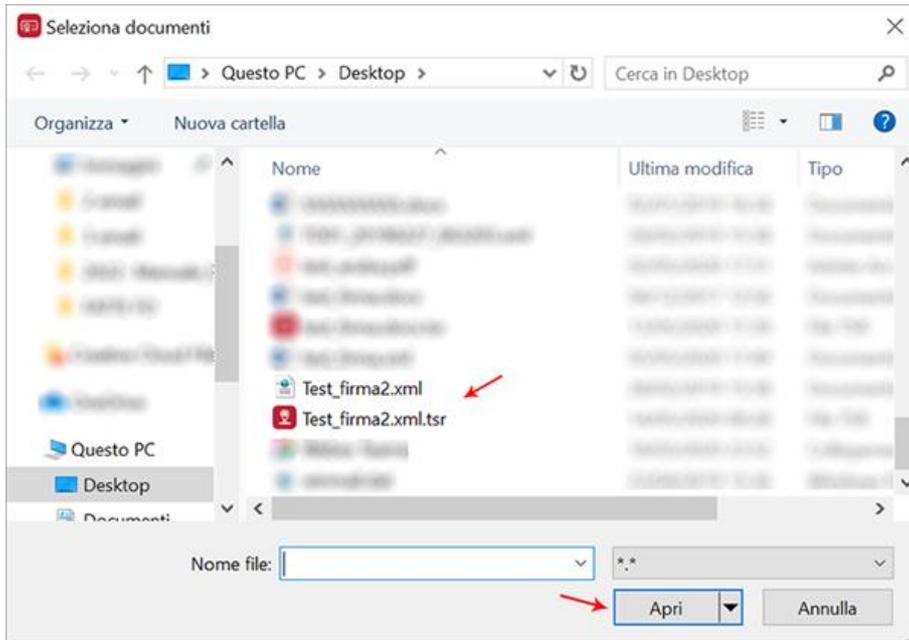
58

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 verificare uno o più file marcati in formato TSR con Aruba Sign, trascinare o selezionare il documento all'interno della scheda **Verifica**:



Selezionare da locale il file originario e il file associato alla marca stessa, quindi cliccare su **Apri**:



Alla schermata visualizzata è possibile:

1. visualizzare il file marcato;
2. su **Verifica firme e Marche Temporali** sono visibili le marche presenti all'interno del file;
 - **Marca valida**

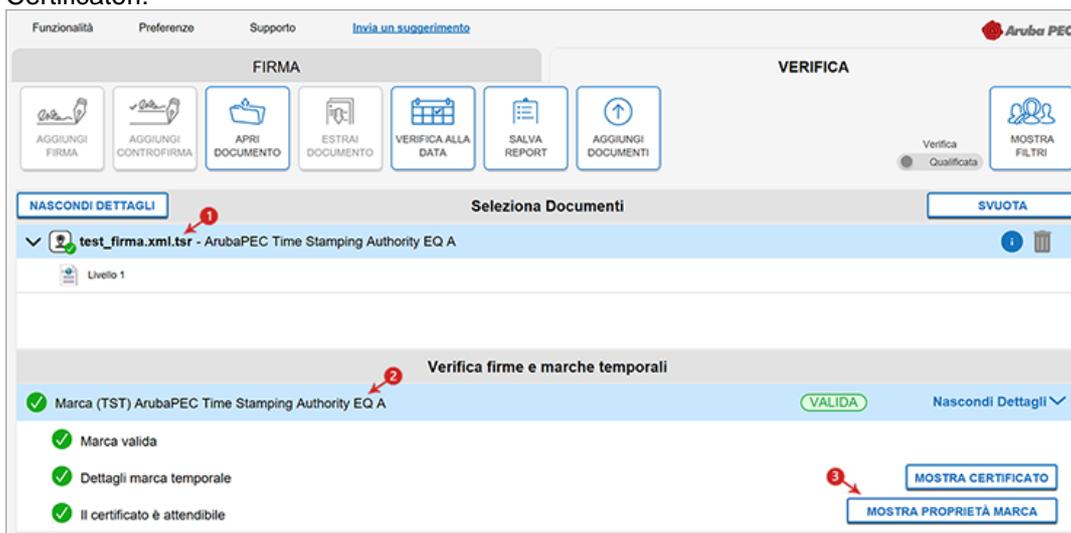
Indica che la marca temporale è integra ed è correttamente associata al documento selezionato;

- **Dettagli marca temporale**

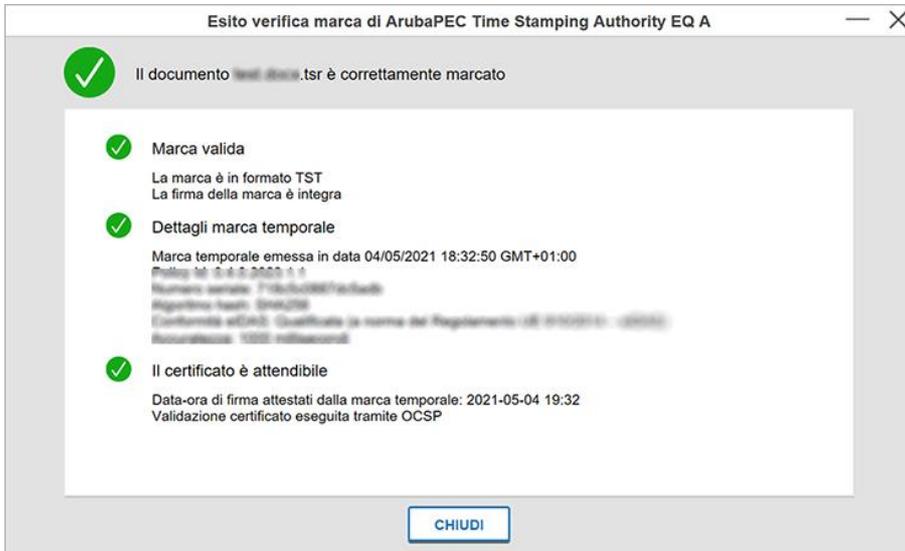
Sono riportate le specifiche della marca stessa;

- **Il certificato è attendibile**

Attesta che la Marca Temporale è rilasciata da un'Autorità di Certificazione inclusa nell'Elenco Pubblico dei Certificatori:



3. da **Mostra Proprietà Marca** è possibile verificare la validità della firma apposta:



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.

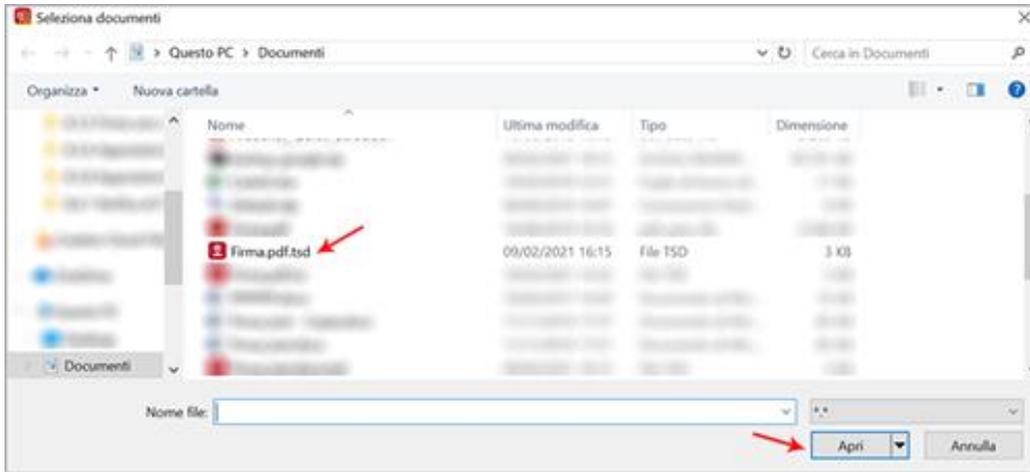
L'orario di marcatura e Firma Digitale si riferisce all'orario UTC (Tempo Coordinato Universale) riferimento da cui sono calcolati tutti gli altri fusi orari del mondo e indicato per essere sempre lo stesso in ogni parte del mondo. In **Italia**, nel periodo estivo (ora legale), l'orario è 2 ore avanti rispetto alla UTC (Tempo Coordinato Universale), in inverno (ora solare) l'orario è avanti di un'ora sulla UTC.

7.12 Verifica di Marca Temporale in formato TSD - 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 verificare uno o più file marcati in formato TSD con Aruba Sign, trascinare o selezionare il documento all'interno della scheda **Verifica**:



Selezionare da locale il file associato alla marca stessa, quindi cliccare su **Apri**:



Alla schermata visualizzata è possibile:

1. visualizzare il file marcato;
2. su **Verifica firme e Marche Temporali** sono visibili le marche presenti all'interno del file;

- **Marca valida**

Indica che la marca temporale è integra ed è correttamente associata al documento selezionato;

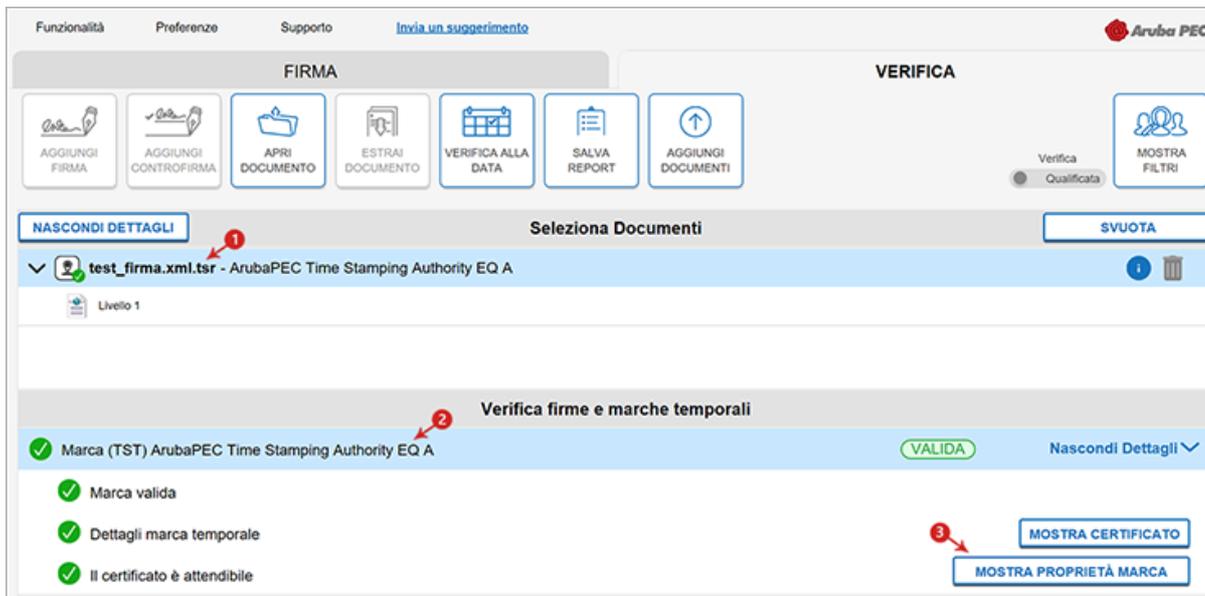
- **Dettagli marca temporale**

Sono riportate le specifiche della marca stessa;

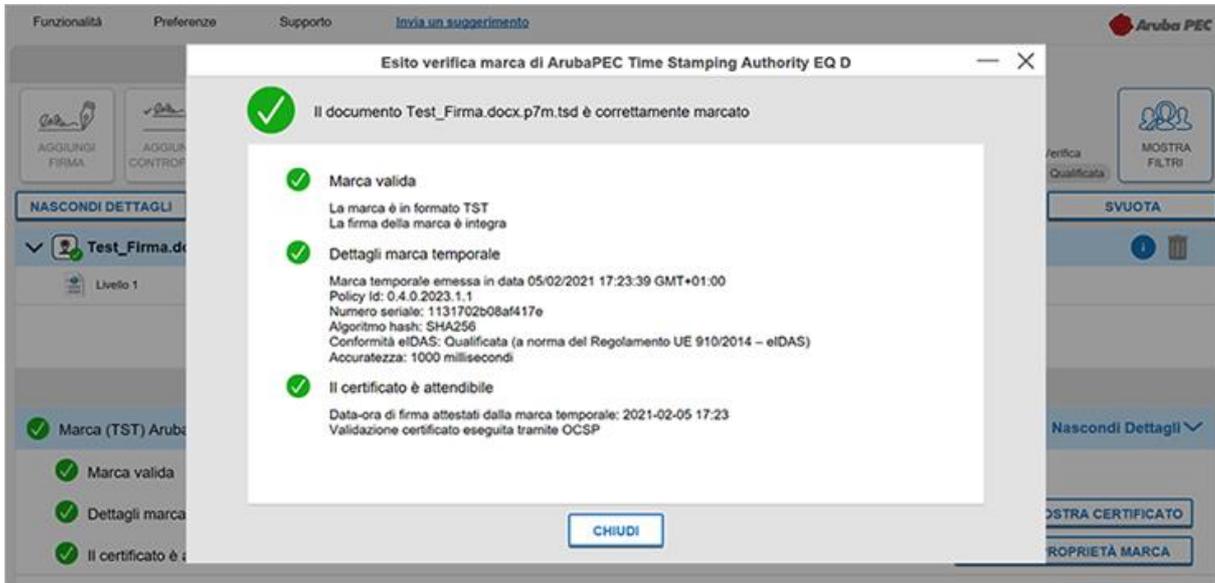
- **Il certificato è attendibile**

Attesta che la Marca Temporale è rilasciata da un'Autorità di Certificazione inclusa nell'Elenco Pubblico dei Certificatori:

61



3. da **Mostra Proprietà Marca** è possibile verificare la validità della firma apposta:



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.

L'orario di marcatura e Firma Digitale si riferisce all'orario UTC (Tempo Coordinato Universale) riferimento da cui sono calcolati tutti gli altri fusi orari del mondo e indicato per essere sempre lo stesso in ogni parte del mondo. In Italia, nel periodo estivo (ora legale), l'orario è 2 ore avanti rispetto alla UTC (Tempo Coordinato Universale), in inverno (ora solare) l'orario è avanti di un'ora sulla UTC.

8 Funzioni disponibili Home Page Aruba Sign

8.1 Gestione PIN/PUK

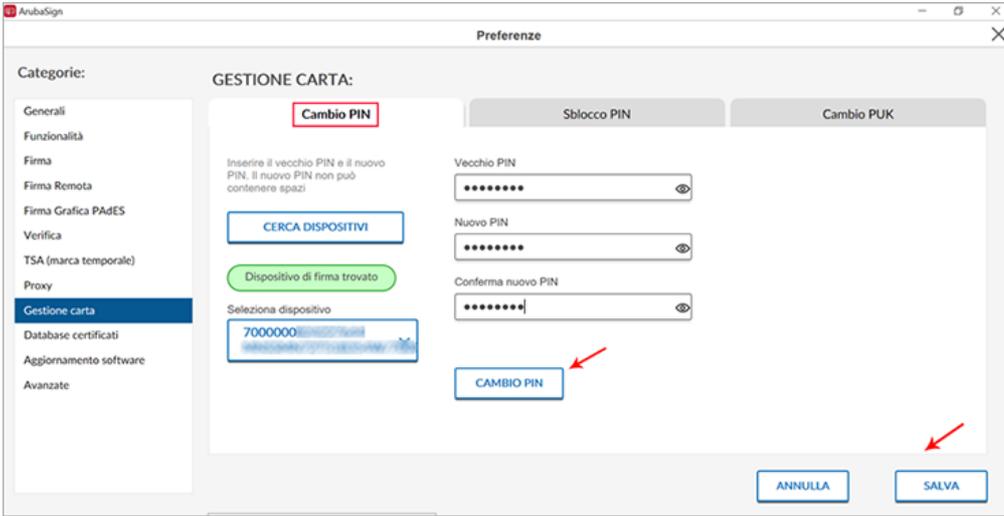
Il menu Gestione Carta di Aruba Sign consente la gestione del PIN e PUK della Smart Card e la visualizzazione delle informazioni relative alla carta stessa. Di seguito il dettaglio delle operazioni possibili:

Cambiare il PIN della Smart Card - Aruba Sign

Per cambiare il PIN della Smart Card, tramite l'utilizzo di una Firma Digitale, accedere su **Gestione Carta**.

Al tab **Cambio PIN** inserire:

- PIN precedente;
- impostare e confermare un nuovo codice PIN;
- cliccare su **Cambio PIN** e poi su **Salva**:



Per impostare il codice PIN è 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 PIN composti almeno da 5 numeri.

Sbloccare il PIN della Smart Card - Aruba Sign

Per sbloccare il PIN della Smart Card, tramite l'utilizzo di una Firma Digitale, accedere su Gestione Carta.

Al tab **Sblocco PIN** inserire:

- codice PUK della Smart Card;
- impostare e confermare un nuovo codice PIN;
- cliccare su **Sblocca PIN** e poi su **Salva**:

63



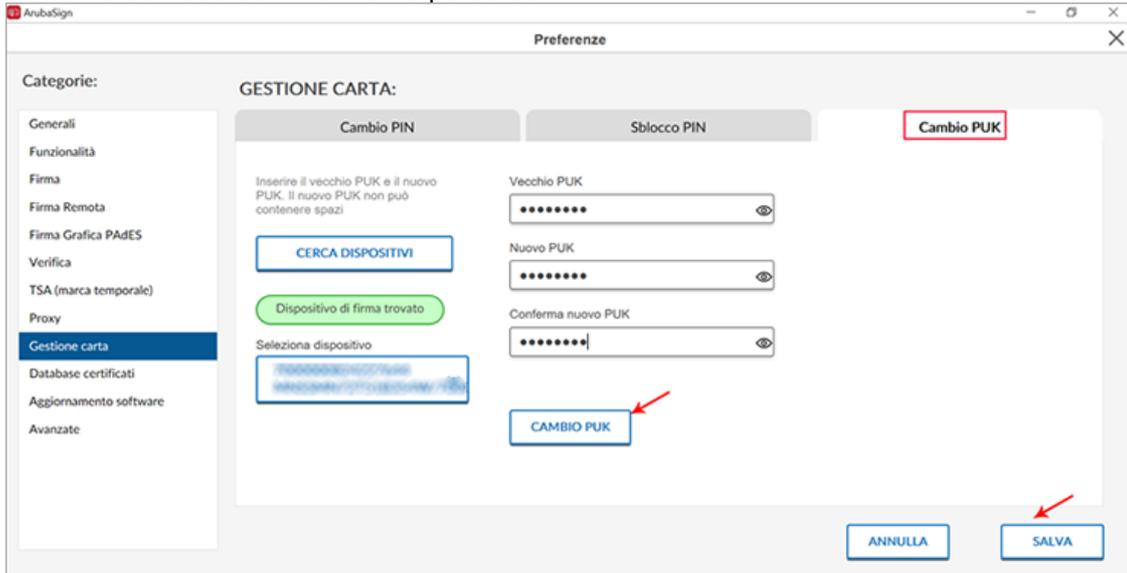
Per impostare il codice PIN è obbligatorio l'utilizzo di soli caratteri numerici (0,1,2,3,4,5,6,7,8 e 9). In alcun modo sono ammessi caratteri alfabetici (a,b,A,B, etc..). Ai fini della sicurezza si consiglia l'utilizzo di codici PIN composti almeno da 5 numeri.

Cambiare il PUK della Smart Card - Aruba Sign

Per cambiare il PUK della Smart Card, tramite l'utilizzo di una Firma Digitale, accedere su Gestione Carta.

Al tab **Cambio PUK** inserire:

- vecchio PUK della Smart Card;
- impostare e confermare un nuovo codice PUK;
- cliccare su **Cambio PUK** e poi su **Salva**:



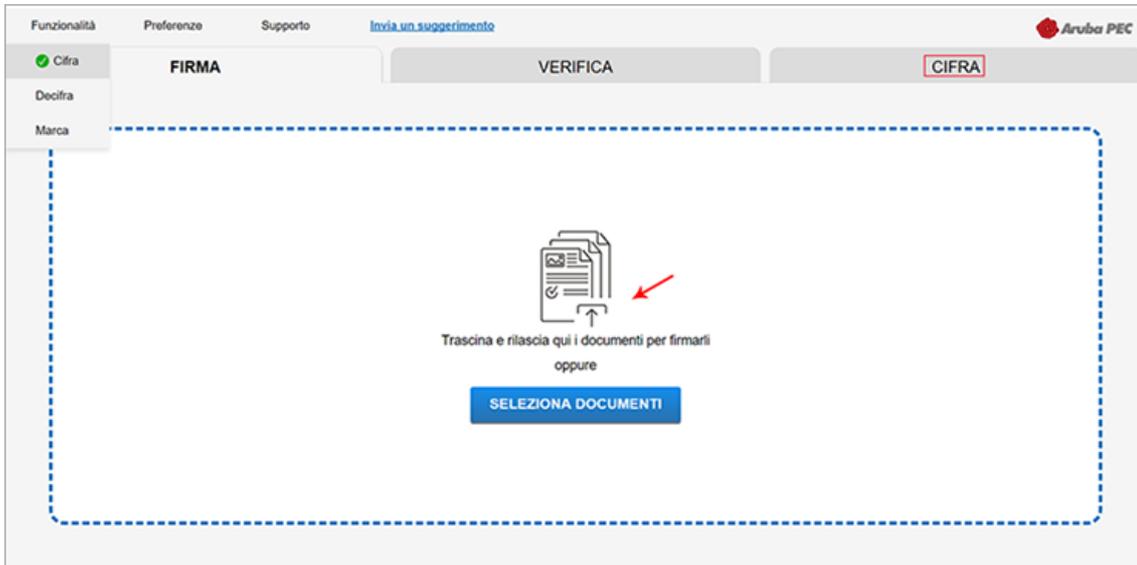
Per impostare il codice PUK è obbligatorio l'utilizzo di soli caratteri numerici (0,1,2,3,4,5,6,7,8 e 9). In alcun modo sono ammessi caratteri alfabetici (a,b,A,B, etc..). Ai fini della sicurezza si consiglia l'utilizzo di codici PIN composti almeno da 5 numeri.

8.2 Cifra e Decifra un file Aruba Sign Windows

La cifratura del file permette la protezione del file stesso, trasformandolo in un documento non immediatamente intellegibile.

Una volta cifrato, il file può essere aperto solo ed esclusivamente con chiave pubblica (anche in caso di successiva scadenza del certificato) **e visualizzato e decifrato solo ed esclusivamente dal destinatario/i indicato/i in fase di cifratura stessa. Per cifrare un file occorre prima esportare su locale il certificato di Autenticazione CNS** in formato .cer (formato del Certificato) e solo successivamente procedere a eseguire la cifratura.

Per **cifrare** un file, [esportare il certificato di autenticazione CNS in formato .cer](#), accedere su **Funzionalità** e poi su **Cifra**, se non precedentemente configurato verrà popolato sulla destra la scheda, quindi trascinare o selezionare il file che si desidera cifrare:



Una volta caricato il file, lo stesso è visibile nella finestra **Documenti da cifrare**. Per procedere:

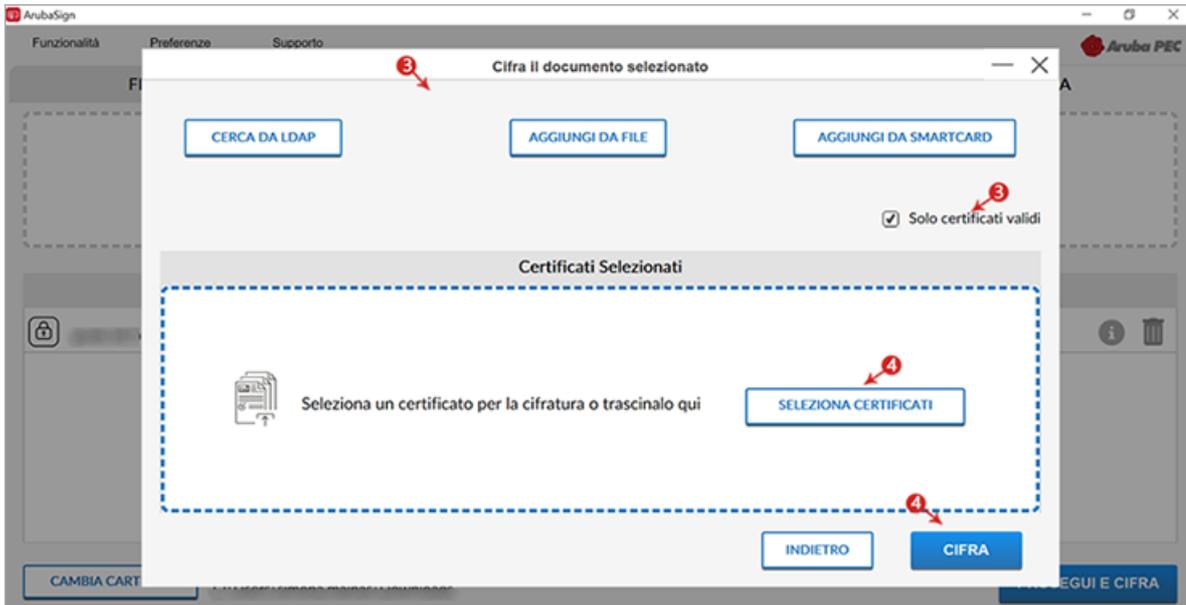
1. verificare la correttezza del percorso su cui salvare il file cifrato, o selezionare una nuova cartella utilizzando il pulsante indicato in figura;
2. cliccare su **Prosegui e Cifra**:



3. nella schermata successiva è possibile scegliere 3 diverse modalità per cercare un certificato:
 - Cerca da LDAP
 - Aggiungi da File
 - Aggiungi da Smart Card

In alternativa selezionare attraverso la spunta solo i certificati validi.

4. è possibile inoltre su **Selezione Certificato** ricercare all'interno delle cartelle presenti nel PC dei certificati e infine cliccare su **Cifra**:



Il programma di cifratura crea un file con **estensione .p7e** che **include il file originale**. Il documento è visibile nella cartella di destinazione indicata in fase di creazione.
Se l'operazione è stata eseguita correttamente si visualizza una schermata di conferma.

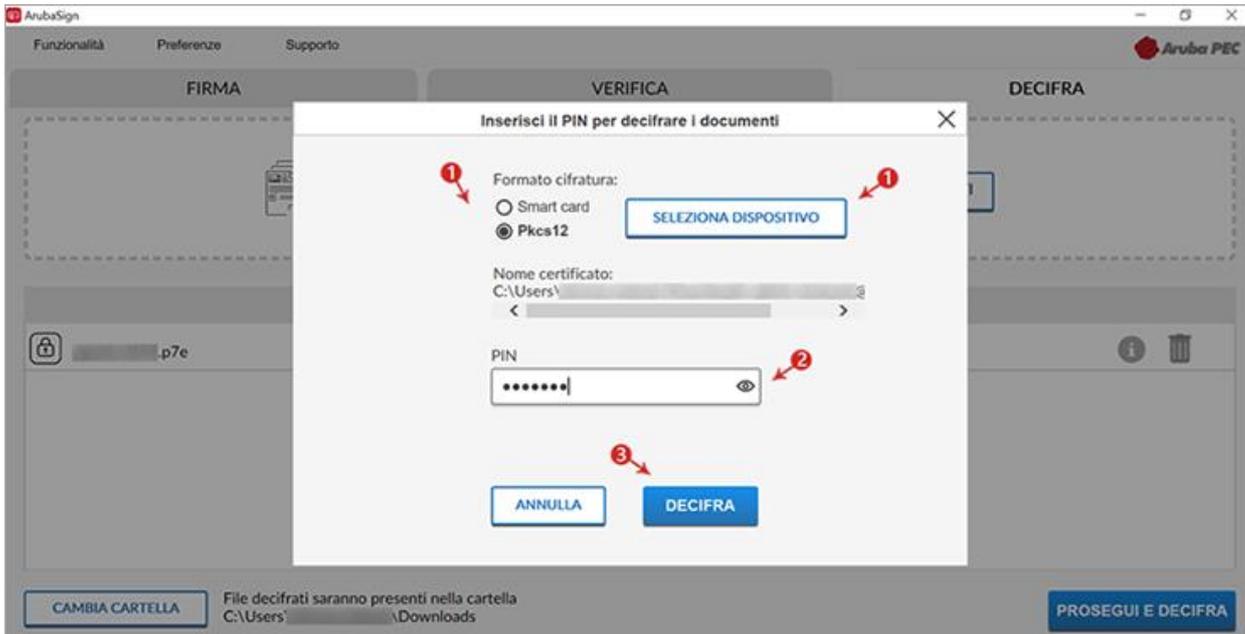
Per **decifrare** un file con Aruba Sign, trascinare o selezionare il file cifrato (formato .p7e) nella sezione **Decifra**:



Arubasign verifica che nella Smart Card sia presente almeno uno dei certificati indicati nella fase di cifratura.

Alla schermata visualizzata:

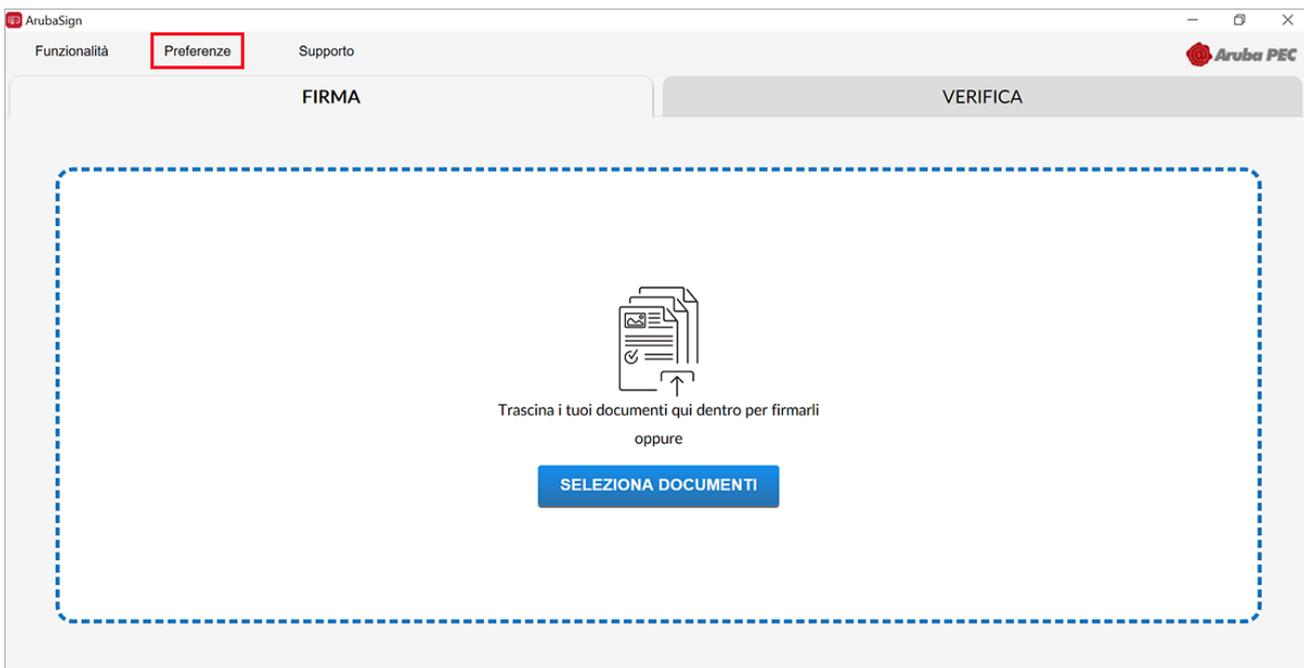
1. è possibile scegliere l'opzione **Smart card** o **Pkcs12** in questo caso selezionare il dispositivo;
2. inserire il **PIN** della Smart Card;
3. cliccare su **Decifra** per proseguire:



Se l'operazione è stata eseguita correttamente si visualizza la schermata di conferma.

8.3 Configurazione Proxy http Aruba Sign

La configurazione dei parametri **Proxy HTTP**, tramite l'utilizzo del Software Aruba Sign, permette di svolgere le operazioni di verifica di un file firmato, aggiornamento, controllo, stato di revoca e richiesta di Marche Temporali qualora la postazione si trovi dietro Proxy HTTP. Per procedere, aprire il menu **Preferenze**:



Quindi allo specifico Tab **Proxy** è possibile scegliere:

- Nessun Proxy
- Configurazione Manuale
- Configurazione di sistema

Se si sceglie la Configurazione manuale impostare i relativi parametri e salvarli:

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

9 Import e verifica certificato Firma Digitale

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 e la verifica corretta dei certificati.

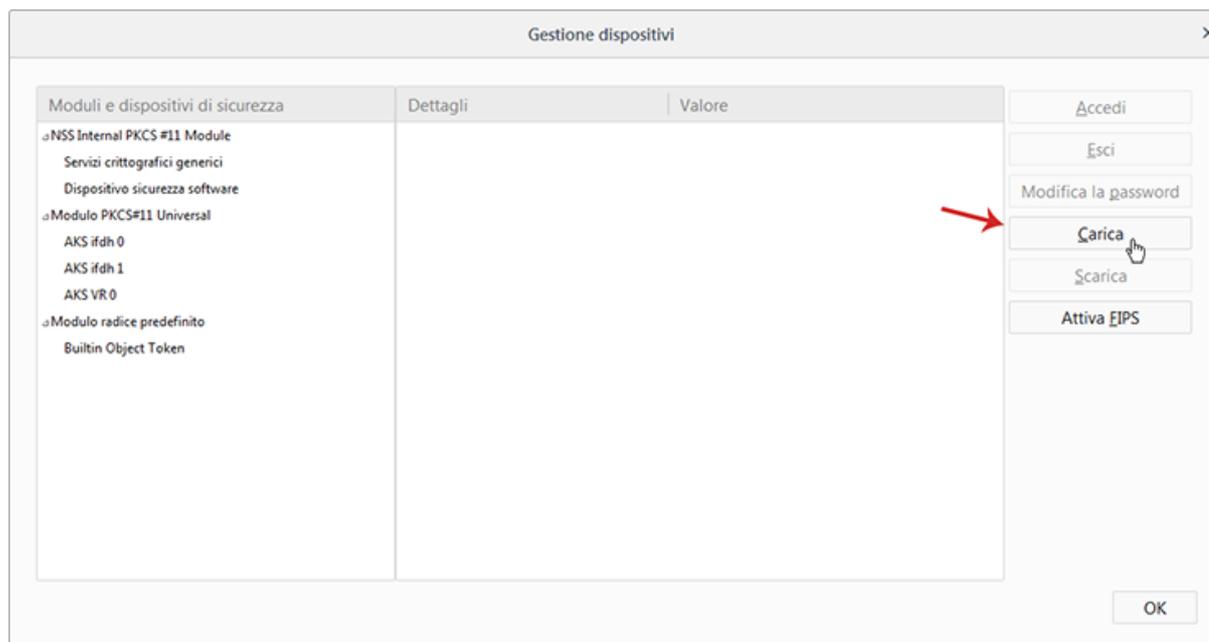
La funzione Import Certificato per Aruba Sign è **automatica su Edge e Google Chrome**.

9.1 Import certificato

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:

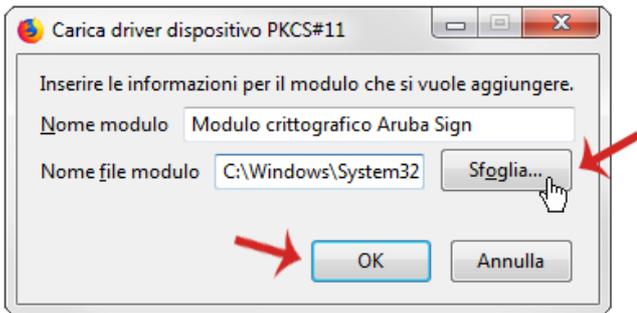
1. avviare Mozilla Firefox;
2. da **Strumenti** (visibile in alto a destra nell'icona con 3 trattini orizzontali), scegliere Impostazioni;
3. da **Privacy e sicurezza** in alto a sinistra, scorrere fino a visualizzare paragrafo **Sicurezza** in fondo alla pagina, quindi selezionare il tab **Dispositivi di Sicurezza**;
4. dal pannello **Gestione Dispositivi**, cliccare su **Carica**:

68

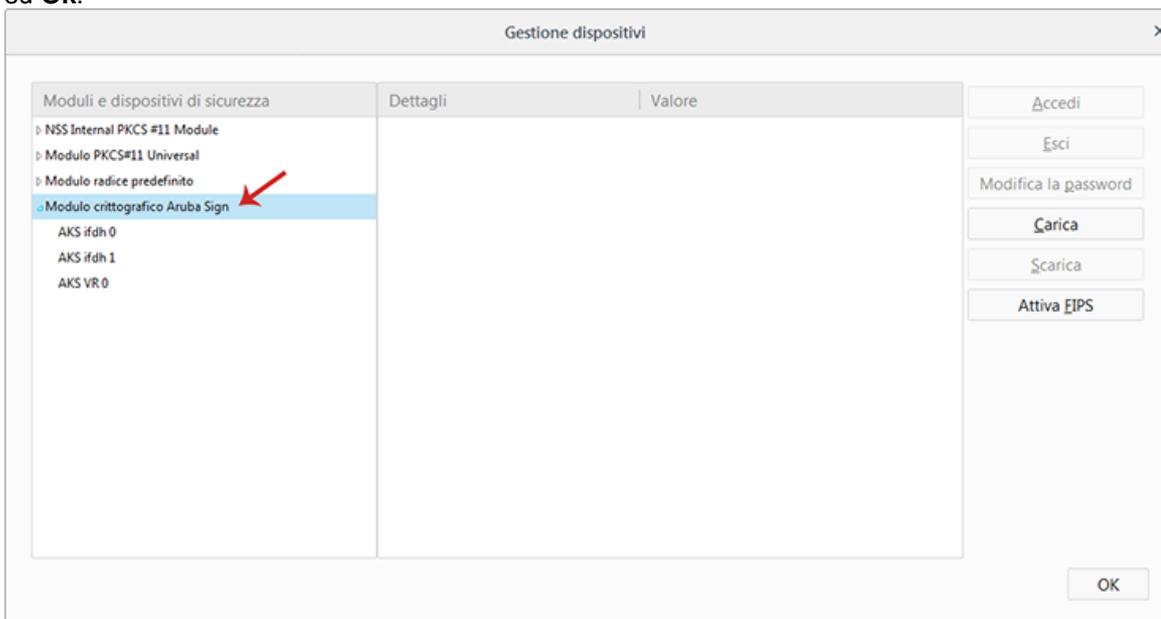


5. al tab **Carica dispositivo PKCS#11** visualizzato, procedere come di seguito indicato:

- 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:



Verificare che all'interno della finestra **Gestione dispositivi** compaia il nuovo modulo appena aggiunto quindi cliccare su **OK**:



Terminata tale procedura l'import manuale dei certificati sarà andato a buon fine e **sarà 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 su Elimina**. L'azione potrebbe causare l'eliminazione dei certificati CNS e Firma Digitale all'interno della Smart Card e l'impossibilità di recuperarli.

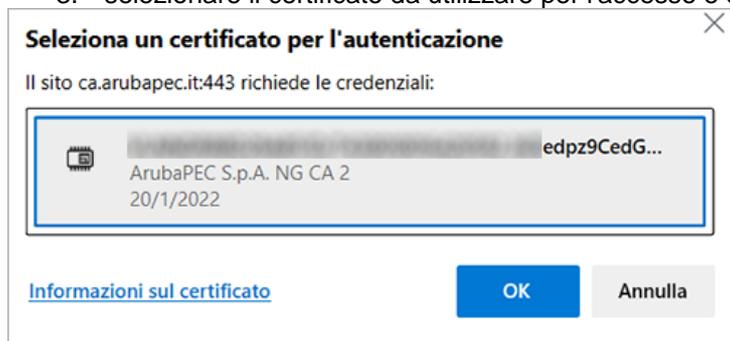
9.2 Verifica certificati

Una volta completata la procedura di Import Certificato, per verificare la corretta installazione del certificato, procedere come di seguito indicato. La procedura è esemplificata con i Browser Edge, Google Chrome e Mozilla Firefox.

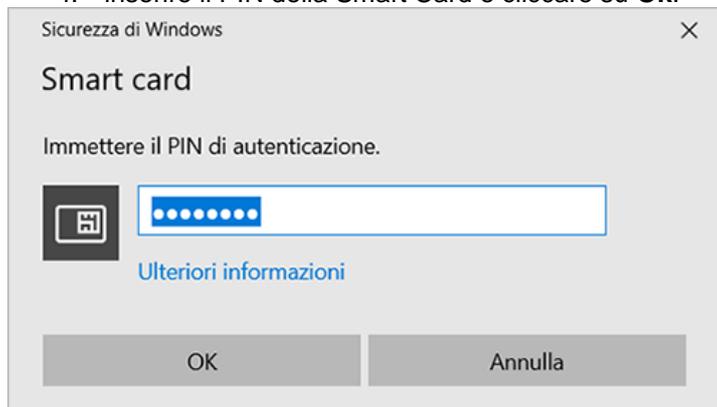
Verifica corretta importazione certificato Aruba Sign su Edge

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

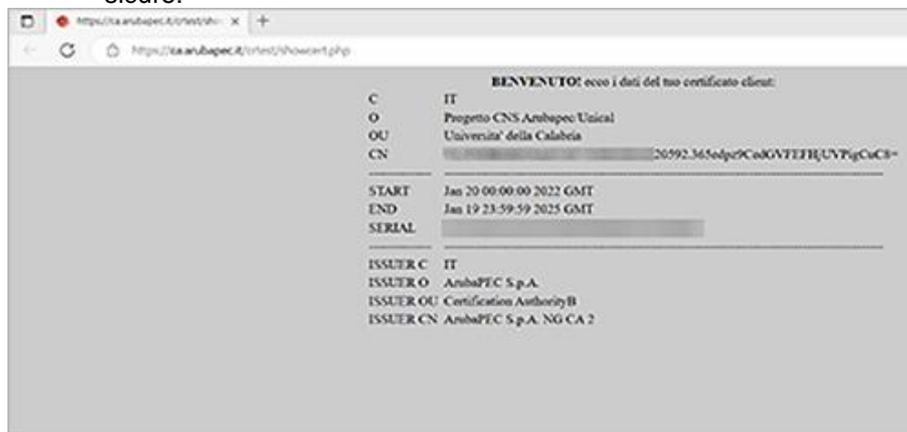
1. avviare **Microsoft Edge**;
2. collegarsi al link <https://ca.arubapec.it/crtest/showcert.php>;
3. selezionare il certificato da utilizzare per l'accesso e cliccare su **Ok**:



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



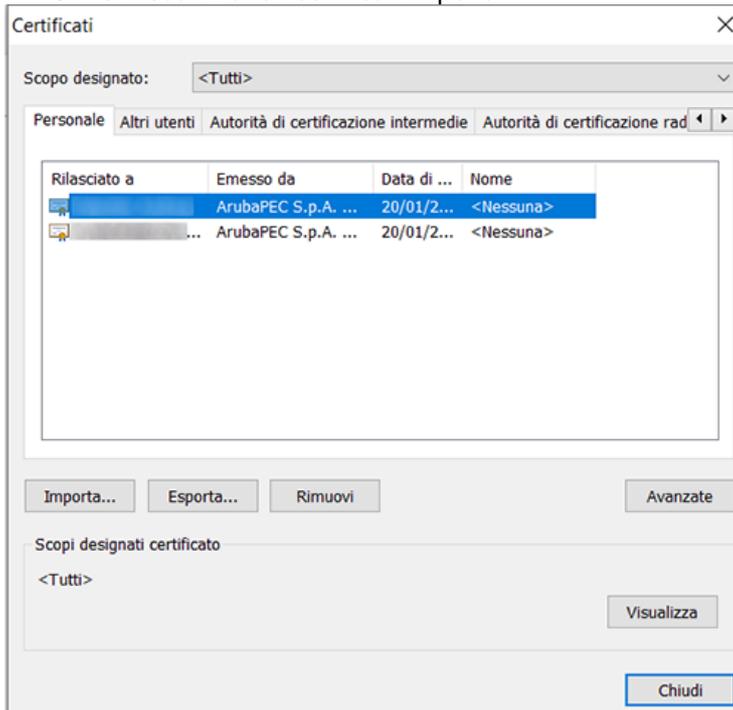
5. verificare che il browser mostri la pagina riepilogativa contenente i dati del certificato usato per l'accesso sicuro:



Verificare la corretta importazione del certificato da **Strumenti** di Edge.

Questa procedura consente di verificare l'effettivo caricamento dei certificati, e quindi il corretto esito della procedura di "Import Certificato":

1. avviare **Edge**;
2. selezionare dal menu in alto a destra l'icona con **3 puntini orizzontali** e cliccare su **Impostazioni**;
3. sulla colonna di destra cliccare su **Privacy, ricerca e servizi**;
4. scorrere al paragrafo **Sicurezza** e cliccare su **Gestisci Certificati**;
5. si visualizzano i certificati importati:

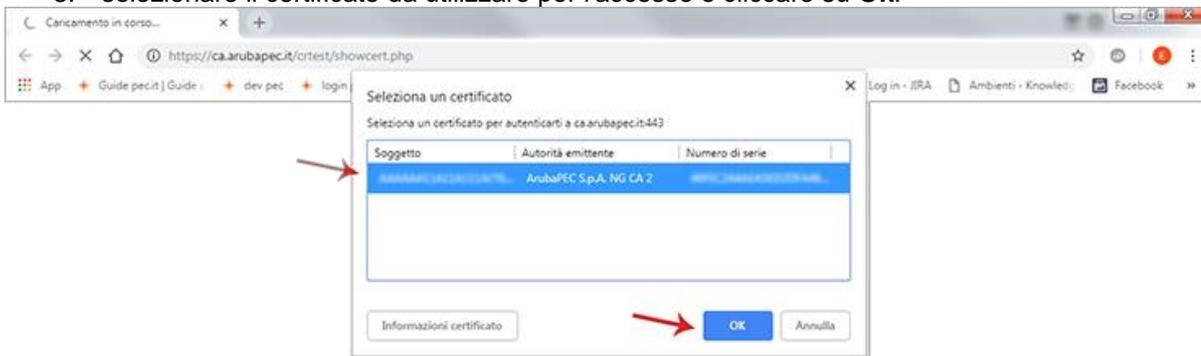


71

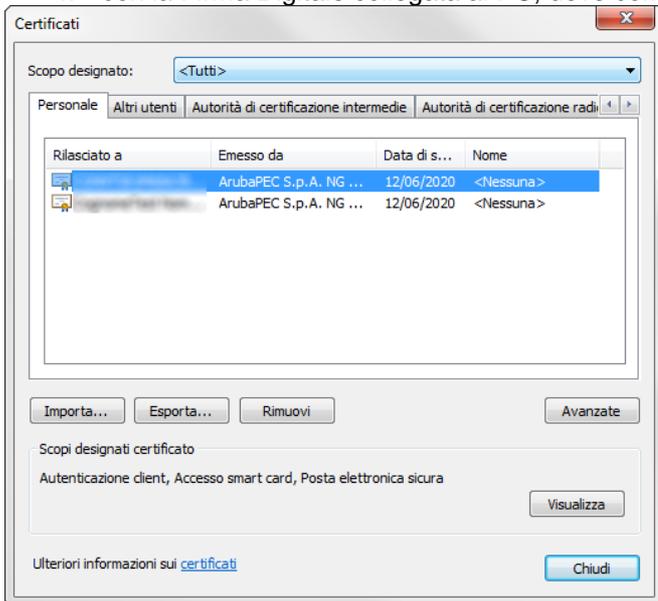
Verifica corretta importazione certificato Aruba Sign su Google Chrome

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

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. con la Firma Digitale collegata al PC, deve comparire in elenco il codice fiscale:

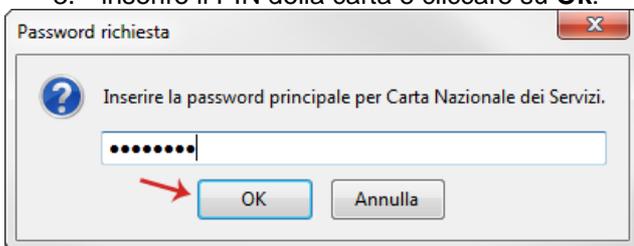


Verifica corretta importazione certificato Aruba Sign su Mozilla Firefox

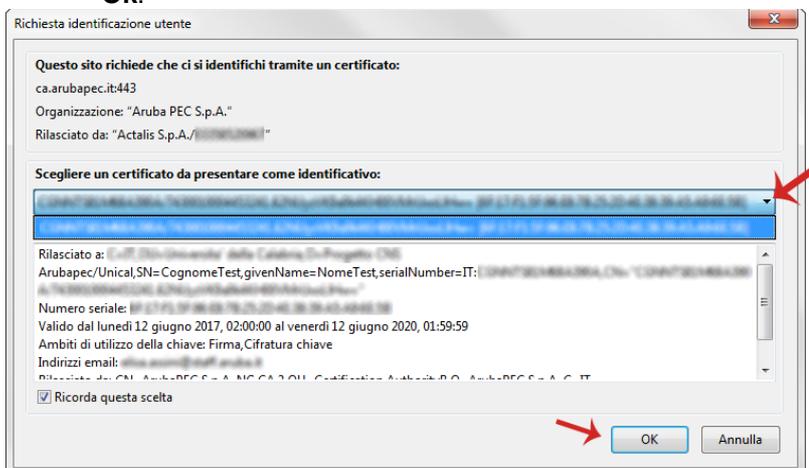
Questa procedura consente l'accesso a un sito di test con il proprio certificato CNS:

1. avviare **Mozilla Firefox**;
2. collegarsi al link <https://ca.arubapec.it/crtest/showcert.php>;
3. inserire il PIN della carta e cliccare su **Ok**:

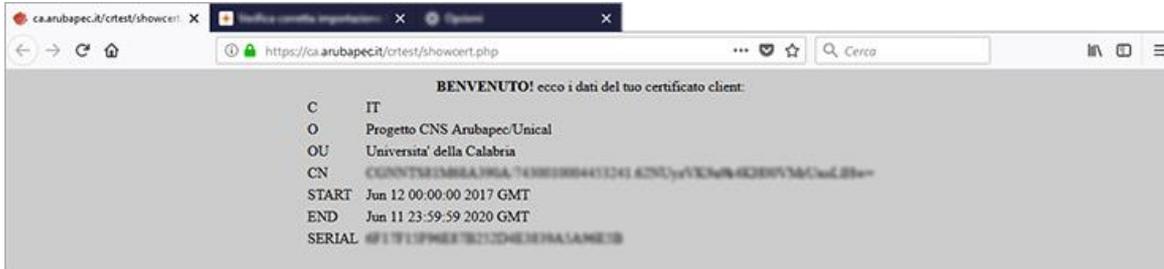
73



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



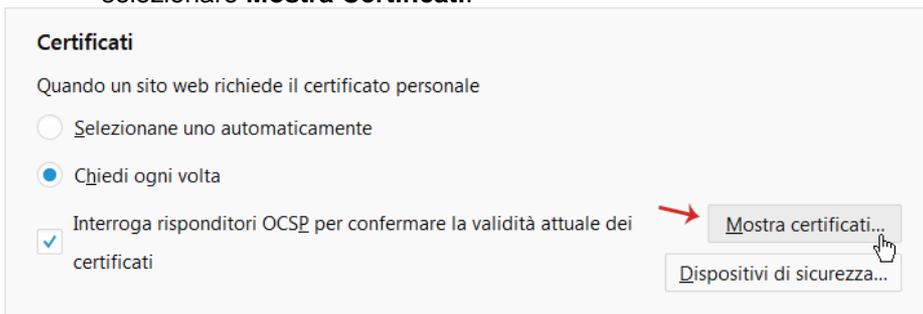
5. verificare che il browser mostri la pagina riepilogativa contenente i dati del certificato usato per l'accesso sicuro:



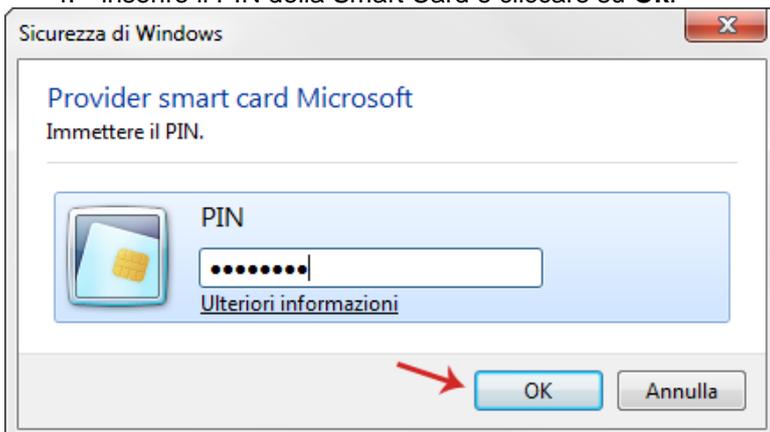
Verificare la corretta importazione del Certificato da "Strumenti" di Mozilla Firefox:

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

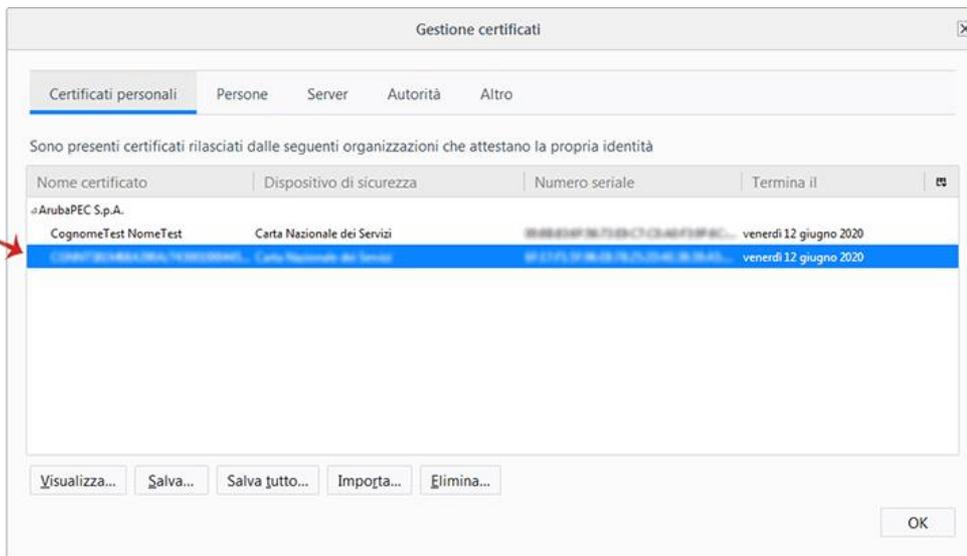
1. avviare **Mozilla Firefox**;
2. da Strumenti in alto a destra, scegliere **Opzioni**;
3. da **Privacy e sicurezza** in alto a sinistra, scorrere fino a visualizzare Certificati in fondo alla pagina, quindi selezionare **Mostra Certificati**:



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

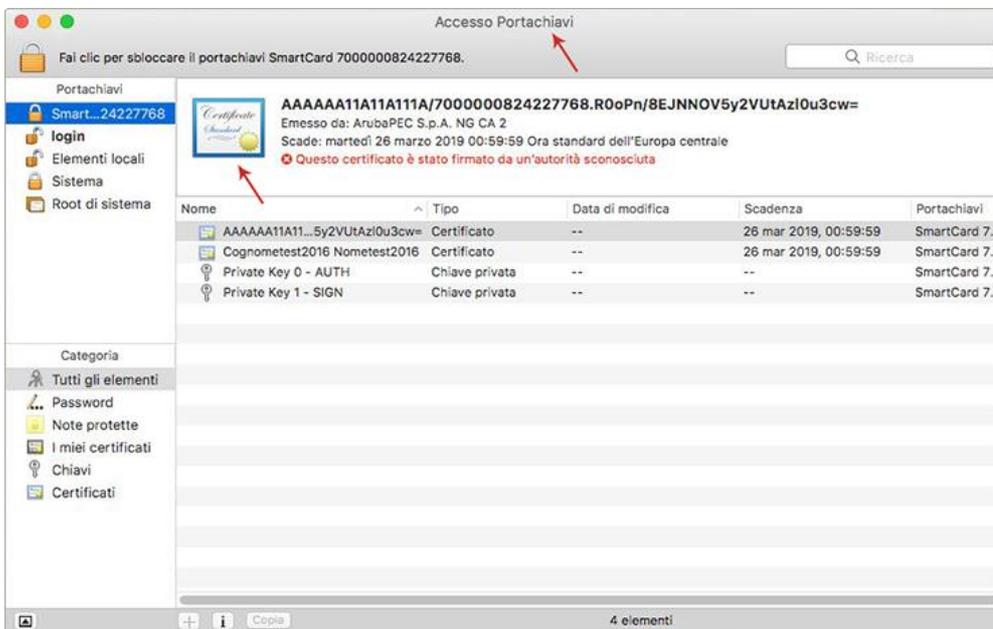


5. dal tab Certificati Personali verificare che siano visibili i certificati installati:



9.3 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:

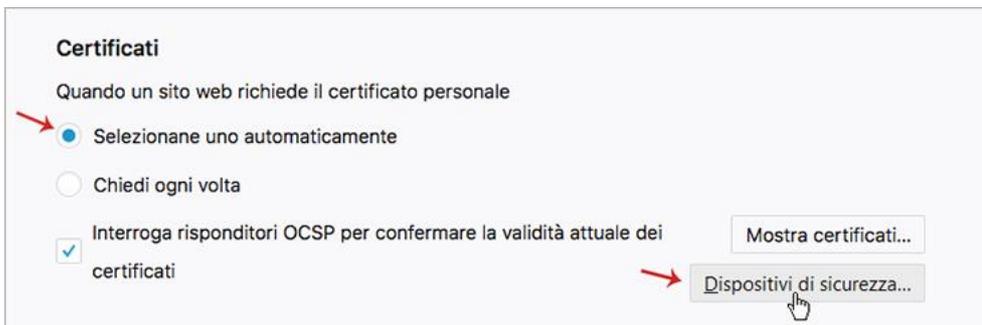


Dalla **versione 10.6 alla 10.9 di Mac** per poter utilizzare Safari per autenticazioni tramite Smart Card, si rimanda alle guide specifiche del produttore (il certificato deve essere scaricato con codice fiscale in formato .cer tramite Aruba Sign). In alternativa è possibile utilizzare Mozilla Firefox per autenticazioni tramite Smart Card..

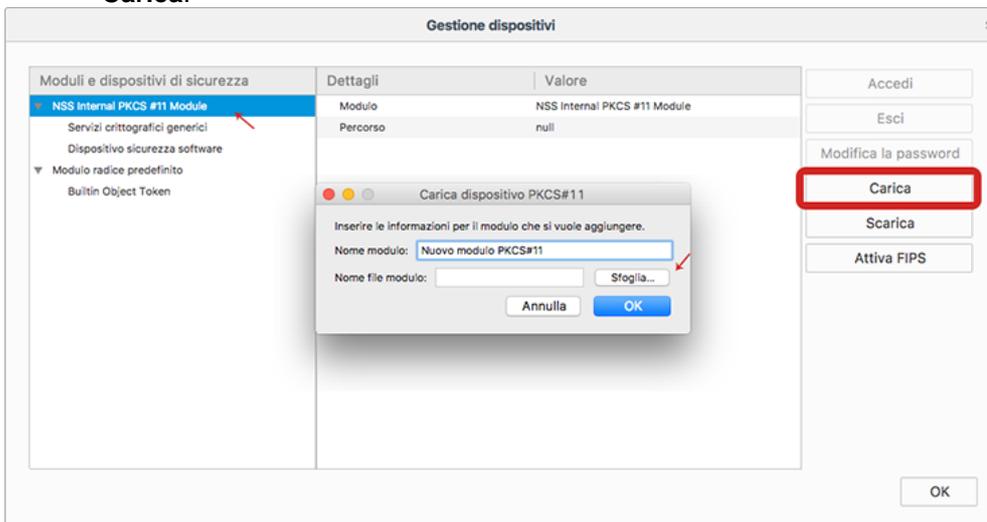
9.4 Import Certificato su Mozilla Firefox - Aruba Sign Mac

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 procedere:

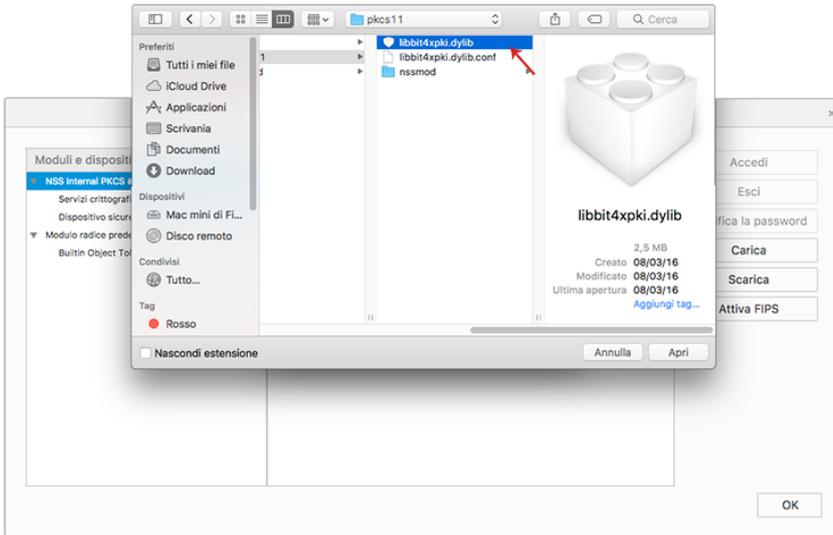
1. avviare **Mozilla Firefox**;
2. dall'icona **Strumenti** in alto a destra, scegliere **Preferenze**;
3. da **Privacy e sicurezza** in alto a sinistra, scorrere fino a visualizzare **Certificati** in fondo alla pagina;
4. spuntare l'opzione **Selezionane uno automaticamente** quindi **Dispositivi di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



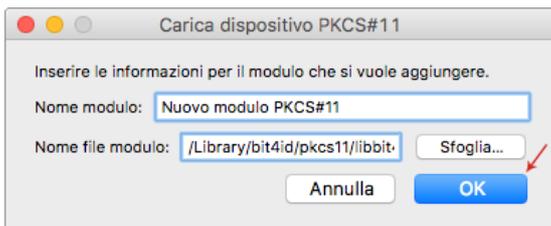
5. nella finestra **Gestione dispositivi** selezionare a sinistra **NSS Internal PKCS # 11 Module** poi cliccare su **Carica**:



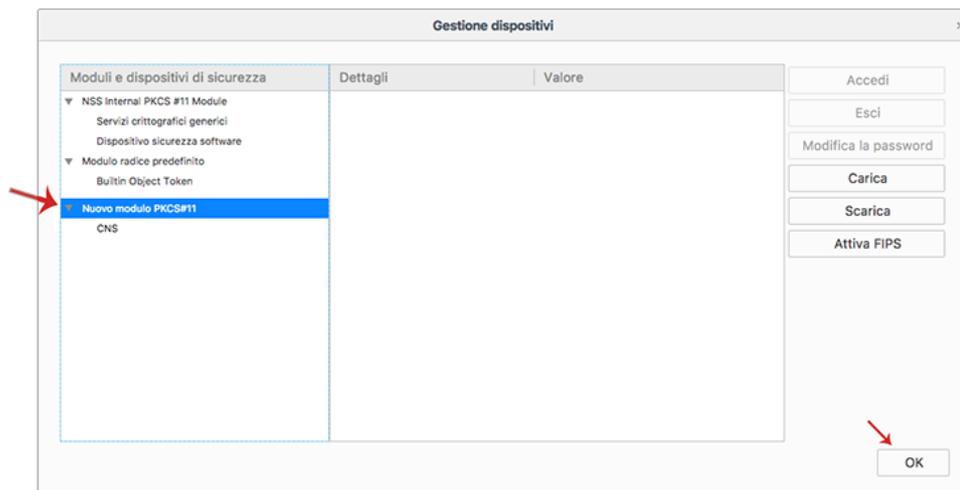
6. al Tab **Carica dispositivo PKCS#11** visualizzato utilizzare **Sfogli** per spostarsi all'interno della directory e selezionare il file **bit4xпки.dylib**:



7. verificare che il campo Nome file modulo sia valorizzato con il percorso della libreria selezionata utilizzando il tasto **Sfoggia** 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 su Elimina. L'azione potrebbe causare l'eliminazione dei certificati CNS e Firma digitale all'interno della Smart Card e l'impossibilità di recuperarli.