

# LA FIRMA DIGITALE



@PEC



## Che cos'è la Firma Digitale – concetti

La *Firma Digitale* o *firma elettronica qualificata* è un particolare tipo di firma elettronica che, nell'ordinamento giuridico italiano, ha lo stesso valore legale di una tradizionale firma autografa apposta su carta.

La firma digitale è disciplinata dal "Codice dell'amministrazione digitale" (*D.lgs 82/2005*)

L'apposizione di firma digitale su un documento è un processo informatico di crittografia a chiave pubblica che consente al sottoscrittore di rendere manifesta l'autenticità del documento e al destinatario di verificarne la provenienza e l'integrità. In particolare la firma digitale garantisce:

- *Autenticità*: l'identità del sottoscrittore è sicura
- *Integrità*: certezza che il documento non è stato modificato dopo l'apposizione della firma
- *Non ripudio*: il documento firmato ha piena validità legale e non può essere ripudiato dal sottoscrittore

Tutto il processo di firma elettronica qualificata si basa su certificati digitali. Per tale motivo è fondamentale garantire l'affidabilità degli Enti autorizzati al rilascio di tali certificati. È stato quindi costituito un elenco di certificatori accreditati. L'elenco pubblico dei certificatori è mantenuto, sottoscritto digitalmente e reso disponibile in rete da *DigitPA*.)

Per maggiori dettagli sui certificatori accreditati:

- <http://www.digitpa.gov.it/firma-digitale/certificatori-accreditati>

## Che cos'è la Firma Digitale – concetti

- Esistono due tipi di formato possibili per i documenti firmati digitalmente:
  - *estensione .p7m - CADES*. Il formato di firma digitale CADES è uno dei più diffusi, poiché il file d'estensione .p7m della cosiddetta busta informatica, da esso prodotta, è riconosciuto dalla normativa vigente come valido per garantire l'interoperabilità tra i sistemi di firma digitale.
  - *estensione .pdf - PADES. PAdES*. è un acronimo che sta per PDF Advanced Electronic Signature. In buona sostanza, si tratta di una firma elettronica che, basando sul formato PDF le modalità e le tecnologie per l'identificazione dell'autore del documento e per le informazioni contenute nel documento originale (secondo la norma ETSI TS 102 778 e lo standard ISO 32000-1), garantisce le qualità necessarie per essere definita "firma elettronica avanzata" (con valore legale) secondo quanto individuato dalla Direttiva 1999/93/EC . Il formato Pades (\*.pdf) è ritenuto maggiormente attendibile del \*.p7m in quanto il formato pdf oltre che ad essere maggiormente leggibile per l'ampia diffusione dei software compatibili che ne permettono la lettura, è un formato che permette la firma di soli files di documenti. Il formato \*.p7m permette in teoria la firma anche di files eseguibili.

Per maggiori dettagli sulla firma digitale ed il suo utilizzo, si rimanda al sito di DigitPa:

- <http://www.digitpa.gov.it/firma-digitale>

## *Come dotarsi della Firma Digitale?*

Per dotarsi della firma digitale è necessario rivolgersi esclusivamente ai certificatori accreditati. Bisogna quindi registrarsi presso un ente di certificazione autorizzato (vedi elenco) e ottenere così una smart card con il certificato di firma digitale e relativo PIN.

N.B. Sebbene le procedure per la richiesta di firma digitale siano pressoché tutte identiche, per le modalità operative si rimanda ai singoli Enti. Va precisato comunque che, **in nessun caso**, è possibile ottenere un dispositivo di firma digitale senza incontrarsi personalmente con il certificatore o suo incaricato.

È necessario quindi dotare la propria postazione di un lettore di smart card o token usb e di software per effettuare le operazioni di firma e/o verifica dei documenti. Tra i numerosi software gratuiti che è possibile utilizzare, consigliamo l'applicativo ArubaSign rilasciato da Aruba s.p.a.

Solitamente, chi rilascia il certificato può fornire il kit completo di firma, composto da certificato, lettore e software.

Punti di rilascio capillari nel territorio:

- Camere di commercio (per le Aziende e professionisti)
- Ordini professionali
- CCNS (carta nazionale dei servizi) in molte regioni per singole provincie rilasciano i certificati di firma all'interno delle tessere sanitarie e forniscono gratuitamente i lettori di card.
- Aruba s.p.a. e altri autorizzati

## *Esempio: Firmare l'autocertificazione*

A titolo esemplificativo, di seguito vengono riportate alcune schermate in cui viene simulata la firma digitale dell'autocertificazione generata dal portale dell'Albo Fornitori Professionisti e Gare telematiche; la firma verrà apposta tramite ArubaSign, software distribuito da Aruba S.p.a., uno dei certificatori più utilizzati in Italia.

È possibile scaricare il software ArubaSign dal seguente indirizzo:

- <http://www.pec.it/Download.aspx>

*Generare l'autocertificazione e salvare il file in una cartella del proprio pc*

## AUTOCERTIFICAZIONE OBBLIGATORIA

---

Genera l'autocertificazione



\* Allega autocertificazione firmata digitalmente (\*.p7m - \*.pdf):

Sfoglia...

Nessun file selezionato.

Indietro

Salva e continua

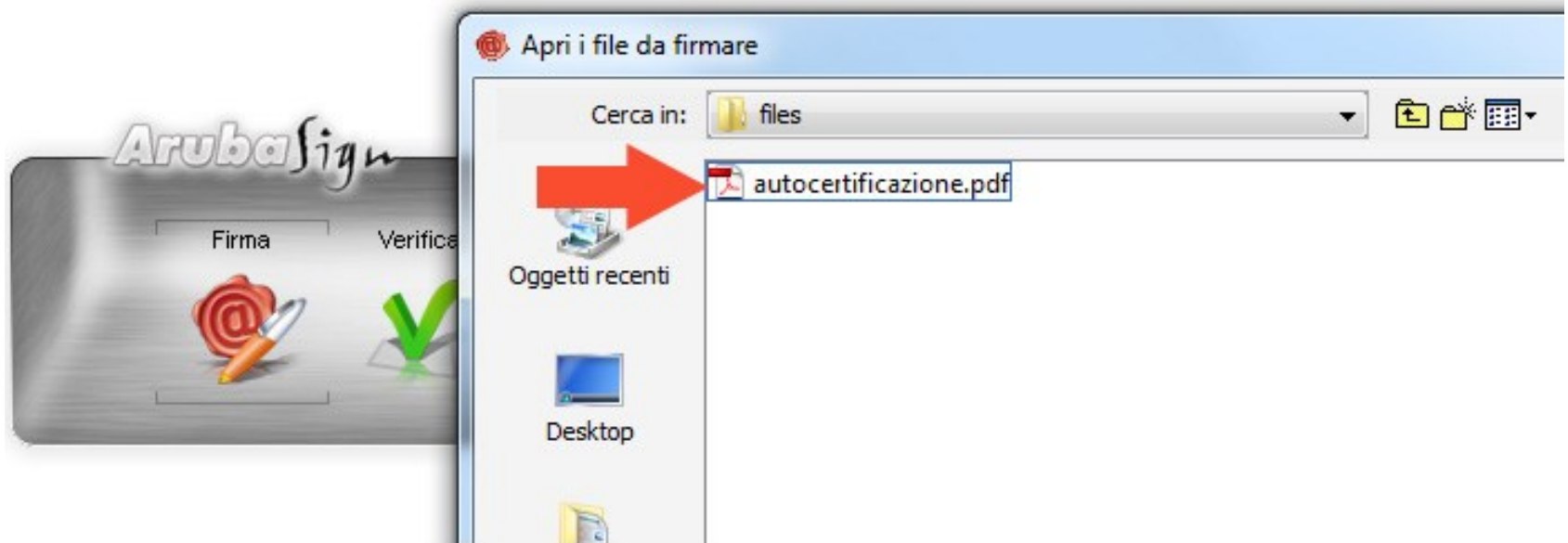
Richiedi abilitazione

\* I campi contrassegnati dall'asterisco rosso sono obbligatori

*Installare e avviare il software ArubaSign per la firma digitale*



*Selezionare il documento da firmare cliccando su “Firma”  
(verrà aperta una finestra di navigazione per selezionare il file desiderato)*



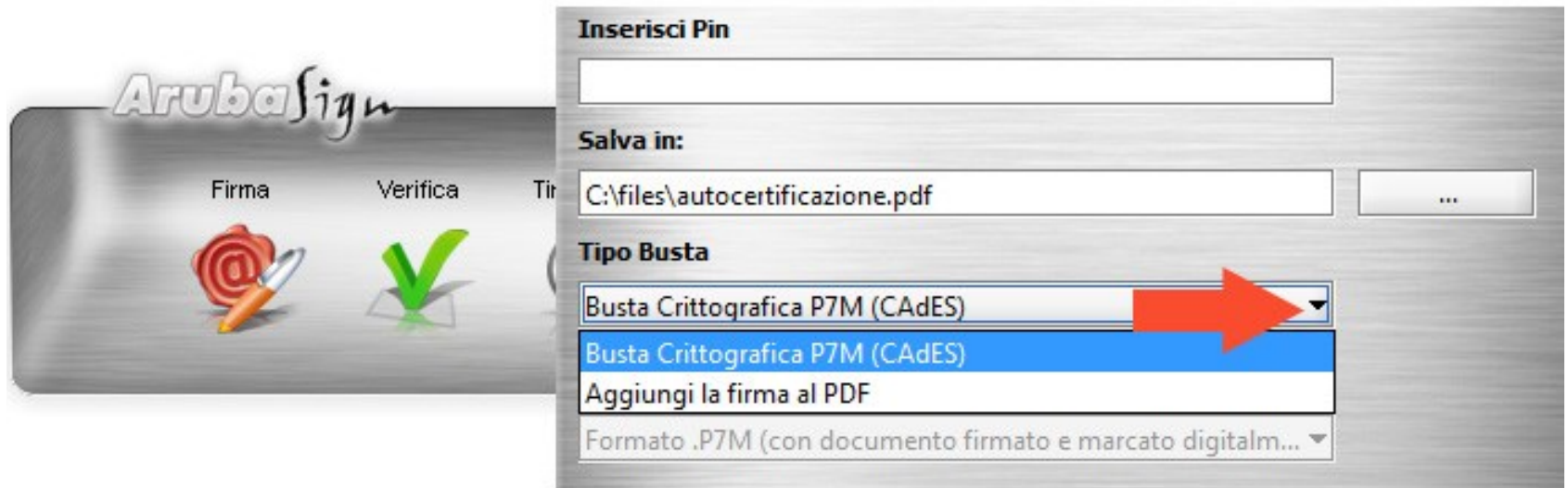


*Inserire il PIN, ovvero il codice univoco associato alla propria firma digitale  
(nella stessa finestra è possibile scegliere la cartella di destinazione del file dopo la firma)*



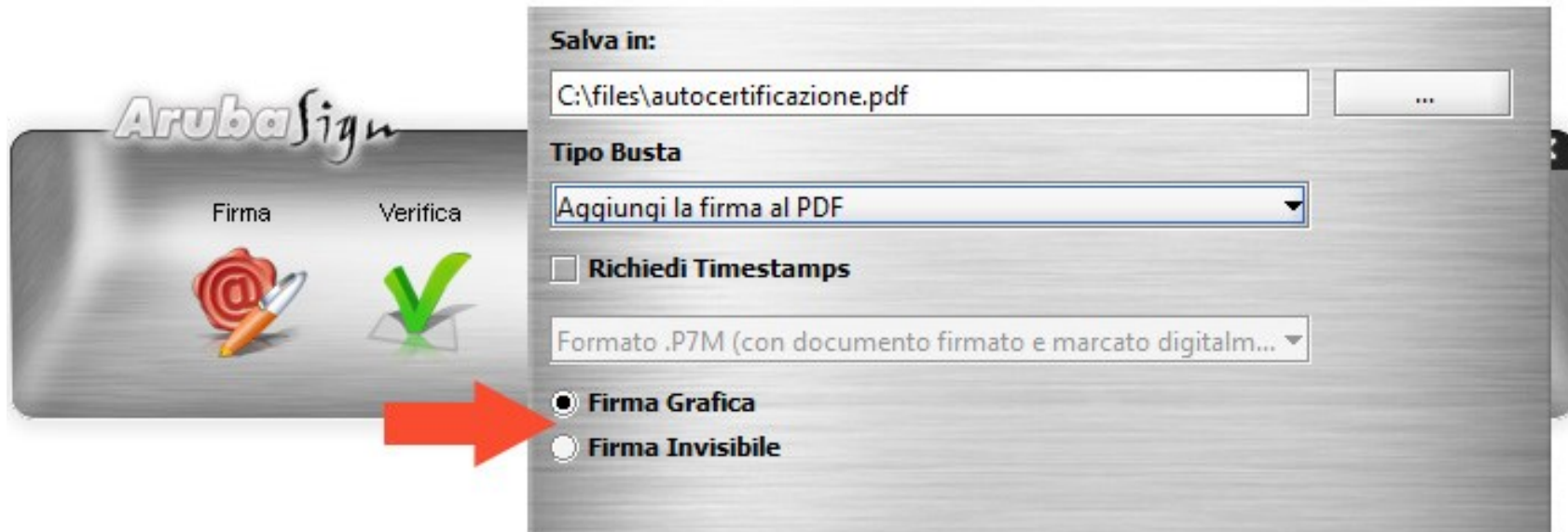
*Scegliere la tipologia di firma, se CAdES o PAdES\**

*(in caso venga scelto il formato PAdES, è necessario scegliere se inserire graficamente la propria firma da file, o invisibile)*



*Scegliere la tipologia di firma, se grafica o invisibile*

*(in caso si scelga di inserire graficamente la propria firma da file, il processo di firma avrà un passaggio aggiuntivo\*)*



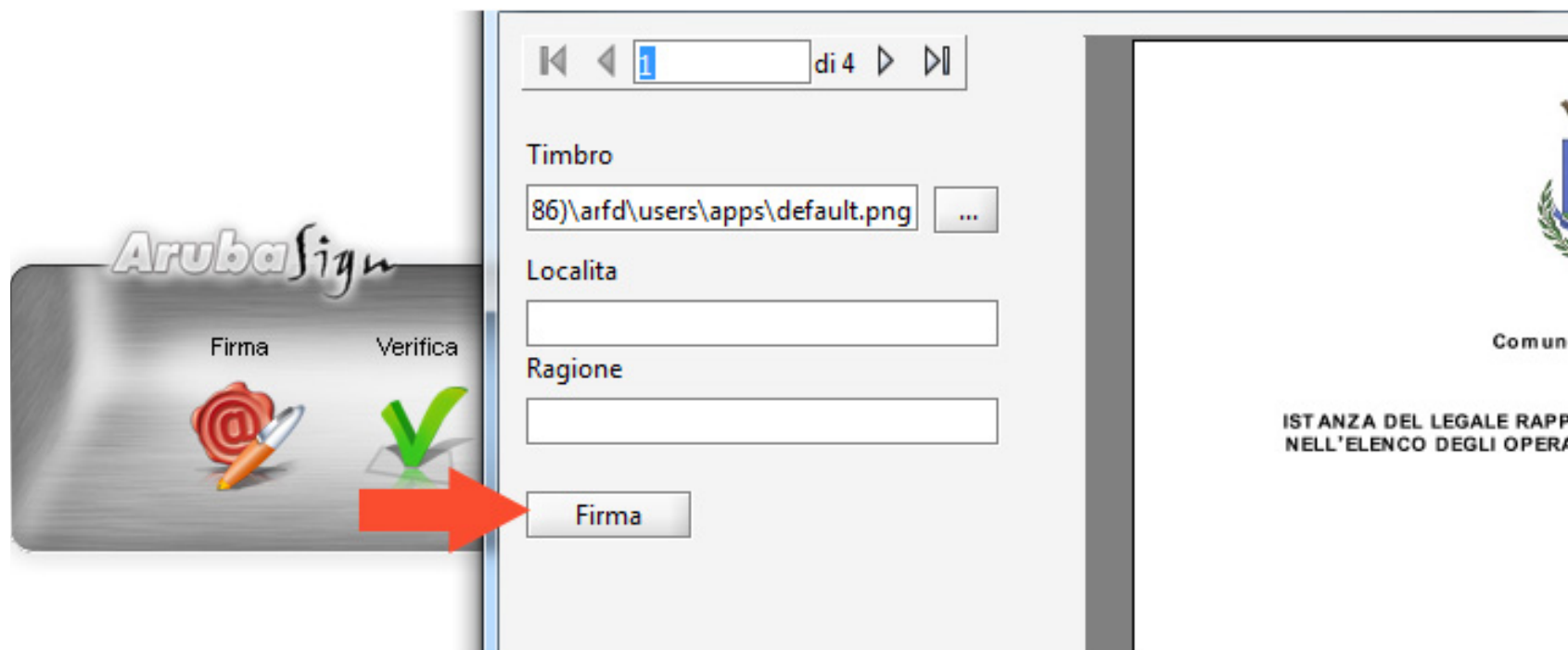
*Una volta inserito il pin cliccare sul pulsante "avanti"*



*Spuntare la dichiarazione come richiesto e poi cliccare sul pulsante "avanti"  
(nella stessa finestra è possibile aprire il file che si sta firmando attraverso il pulsante "Apri Documento")*



*\* Se è stato scelto di apporre una firma grafica verrà richiesto di selezionare il file della firma*



*Il documento è stato firmato correttamente e viene data conferma  
(nella stessa finestra viene mostrato il percorso in cui viene salvato il file firmato digitalmente)*

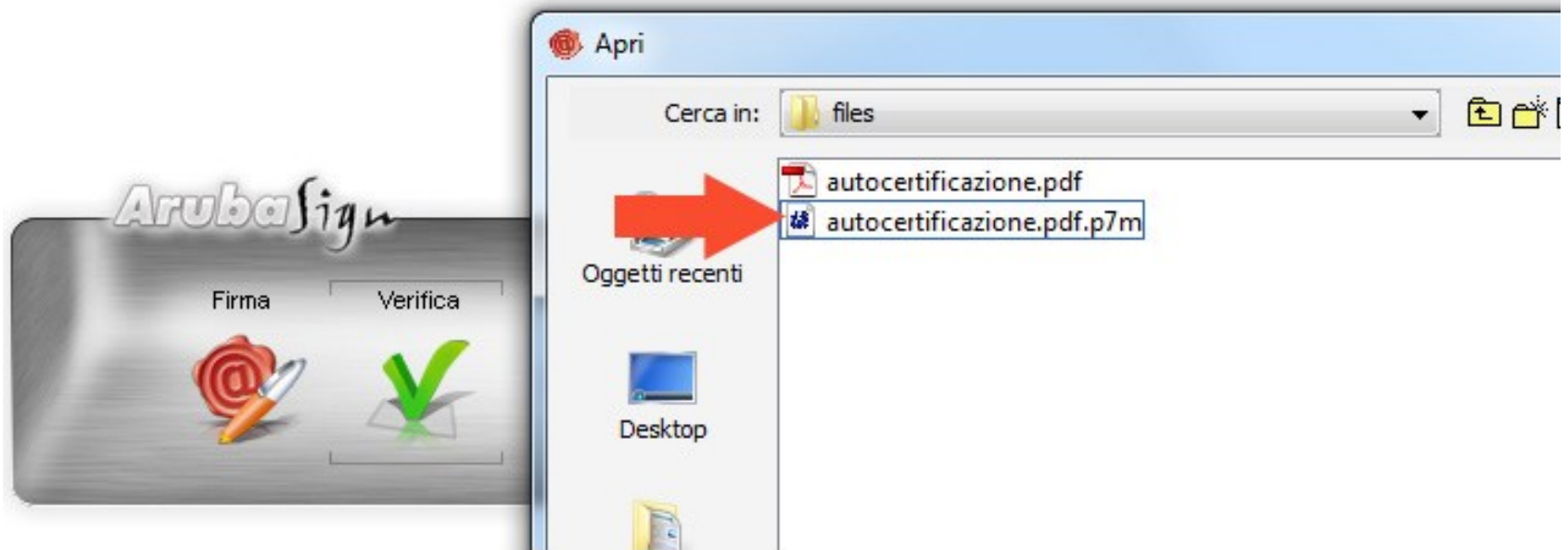


*Fase conclusiva. Verifica della firma digitale: cliccare su “verifica”  
(è possibile verificare con questi passaggi qualsiasi documento firmato digitalmente )*

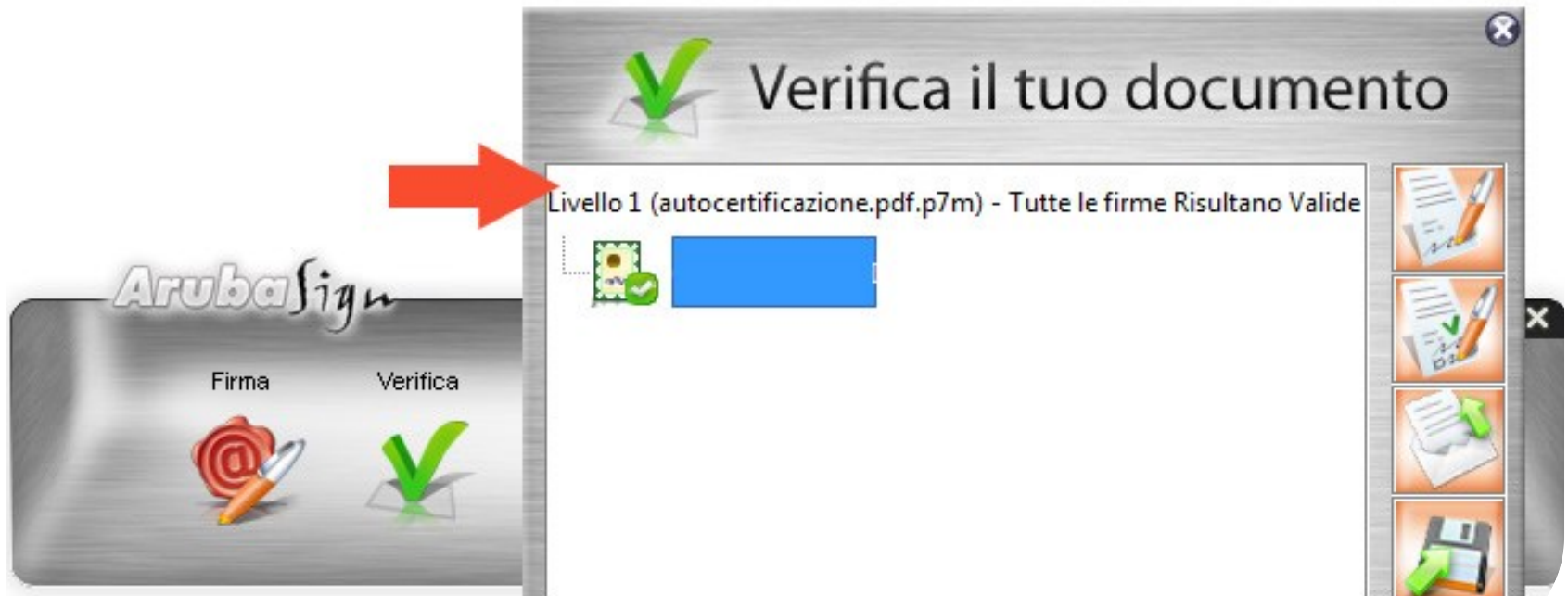




*Selezionare il file firmato digitalmente di cui si vuole verificare la firma e la validità  
(il file deve avere come estensione \*.pdf o \*.p7m)*



*Firma verificata e valida  
(vengono mostrati i dettagli sulla firma e sulla sua validità)*



# @PEC

La Posta Elettronica Certificata (denominata anche **Posta Certificata** o **PEC**) è il nuovo sistema di posta elettronica che consente di fornire al mittente garanzie sulla trasmissione e la ricezione dei messaggi.

L'invio e la consegna dei messaggi, infatti, vengono attestati tramite specifiche ricevute che il gestore del servizio rilascia al mittente e che conferiscono all'e-mail lo stesso valore di una raccomandata con ricevuta di ritorno (secondo quanto stabilito dal decreto [DPR 11 Febbraio 2005](#) che disciplina l'utilizzo della PEC.)

La **Posta Certificata** diventa così il mezzo di comunicazione più immediato e sicuro per la trasmissione di documenti, agevolando tutti quelli che sono gli iter burocratici tra i cittadini e pubbliche amministrazioni.

In più, oltre ad avere la certezza della ricezione, con il sistema di Posta Certificata è garantita la certezza del contenuto: i protocolli di sicurezza utilizzati fanno sì che non siano possibili modifiche al contenuto del messaggio e agli eventuali allegati.

**N.B.:** E' necessario chiarire che, una comunicazione di posta elettronica certificata, ha valore di raccomandata con ricevuta di ritorno solo nel caso in cui sia il mittente che il destinatario utilizzino indirizzi di posta certificata e che i messaggi siano inviati tramite i server di un gestore certificato.

Infatti, nel caso in cui venga inviato un messaggio da un' indirizzo di posta certificata a uno di posta elettronica ordinaria, il destinatario riceverà la Ricevuta di Accettazione (all'interno di un messaggio detto Busta di Trasporto contenente i Dati di Certificazione) ma NON quella di Avvenuta Consegna.

## Normativa di riferimento

- Legge 18 giugno 2009, n. 69 recante "Disposizioni per lo sviluppo economico, la semplificazione, la competitività nonché in materia di processo civile": Art.34.
- Circolare CNIPA CR/49 recante "Modalità di accreditamento all'elenco pubblico dei gestori di PEC";
- Decreto 2 novembre 2005 recante "Regole tecniche per la formazione, la trasmissione e la validazione, anche temporale, della posta elettronica certificata";
- DPR 11 febbraio 2005, n. 68 "Regolamento recante disposizioni per l'utilizzo della posta elettronica certificata, a norma dell'articolo 27 della legge 16 gennaio 2003, n. 3";
- Codice dell'Amministrazione Digitale: artt. 6, 45 e seguenti;
- "Direttiva per l'utilizzo della posta elettronica nelle pubbliche amministrazioni", emanata il 27 novembre 2003 dal Ministro dell'Innovazione e le Tecnologie di concerto con il Ministro per la Funzione Pubblica;
- DPR 28 dicembre 2000, n. 445 "Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa"