Firma Digitale per il Consiglio Nazionale degli Ingegneri

Roma 15 ottobre 2009

:: Firma Digitale ::

La Firma Digitale è il risultato di una procedura informatica che garantisce l'autenticità e l'integrità di messaggi e documenti scambiati e archiviati con mezzi informatici, al pari di quanto svolto dalla firma autografa per i documenti tradizionali.

La Firma Digitale è nata con l'obbiettivo di trasferire su digitale il concetto di *firma autografa su carta.*

Attraverso la Firma Digitale si riescono quindi a garantire i seguenti 3 requisiti:

Autenticità: Con un documento firmato digitalmente si può essere certi dell'identità del sottoscrittore;

Integrità: Sicurezza che il documento informatico non è stato modificato dopo la sua sottoscrizione;

Non ripudio: Il documento informatico sottoscritto con firma digitale, ha piena validità legale e non può essere ripudiato dal sottoscrittore.

:: Marca Temporale ::

La Marca Temporale è il risultato della procedura informatica, con cui si attribuisce, ad uno o più documenti informatici, un riferimento temporale opponibile ai terzi.

Le marche temporali permettono quindi di associare una data e ora, certe e legalmente valide, ai documenti ai quali sono apposte (cfr. Art. 20, comma 3 Codice dell'Amministrazione Digitale Dlgs 82/2005).

:: Quadro normativo ::

- **Deliberazione 18 maggio 2006:** Regole tecniche per la definizione del profilo di busta crittografica per la firma digitale in linguaggio XML. (Deliberazione n. 34/06). (GU n. 230 del 3-10-2006)
- **CIRCOLARE 6 settembre 2005, n.48:** Modalità per presentare la domanda di iscrizione nell'elenco pubblico dei certificatori di cui all'articolo 28, comma 1, del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445.(G.U. 13 settembre 2005, n. 213)
- **Decreto legislativo 7 marzo 2005, n. 82:** Codice dell'amministrazione digitale pubblicato in G.U. del 16 maggio 2005, n. 112 - S.O. n. 93
- **Deliberazione CNIPA 4/2005, 17 febbraio 2005:** Regole per il riconoscimento e la verifica del documento informatico. (G.U. 3 marzo 2005, n. 51)
- **DPCM 13 Gennaio 2004:** Regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici. (GU n. 98 del 27-4-2004)

[per approfondimenti: http://www.cnipa.gov.it]

:: Come funziona la Firma Digitale ::

Per la creazione e la verifica delle firme digitali è necessario utilizzare una **coppia di chiavi** digitali asimmetriche, attribuite in maniera univoca ad un soggetto detto Titolare della coppia di chiavi.

La prima, **chiave privata** destinata ad essere conosciuta solo dal Titolare, è utilizzata per la generazione della firma digitale da apporre al documento, la seconda, **chiave pubblica**, viene utilizzata per verificare l'autenticità della firma.

Caratteristica di tale metodo, detto crittografia a chiave asimmetrica, è che, firmato il documento con la chiave privata, la firma può essere verificata con successo esclusivamente con la corrispondente chiave pubblica.

La sicurezza è garantita dalla impossibilità di ricostruire la chiave privata (segreta) a partire da quella pubblica, anche se le due chiavi sono univocamente collegate.

:: Come funziona la Marca Temporale ::

La marcatura temporale è un servizio online (TSA Time Stamping Authority) rilasciato da un **Certificatore Accreditato.**

Tale servizio consiste nella generazione e successiva sottoscrizione, ad opera del Certificatore, di un **riferimento temporale** opponibile ai terzi e associato in modo univoco ad un ben determinato documento.

Un file marcato temporalmente contiene quindi al suo interno il documento del quale si è richiesta la validazione temporale e la marca temporale emessa dal Certificatore.

Il tempo, cui fanno riferimento le marche temporali di Aruba Pec, è riferito al Tempo Universale Coordinato (UTC), ed è assicurato da una costante sincronizzazione con il segnale emesso dall'Istituto Nazionale di Ricerca Metrologica (INRIM, ex IEN) .

:: Gli attori ::

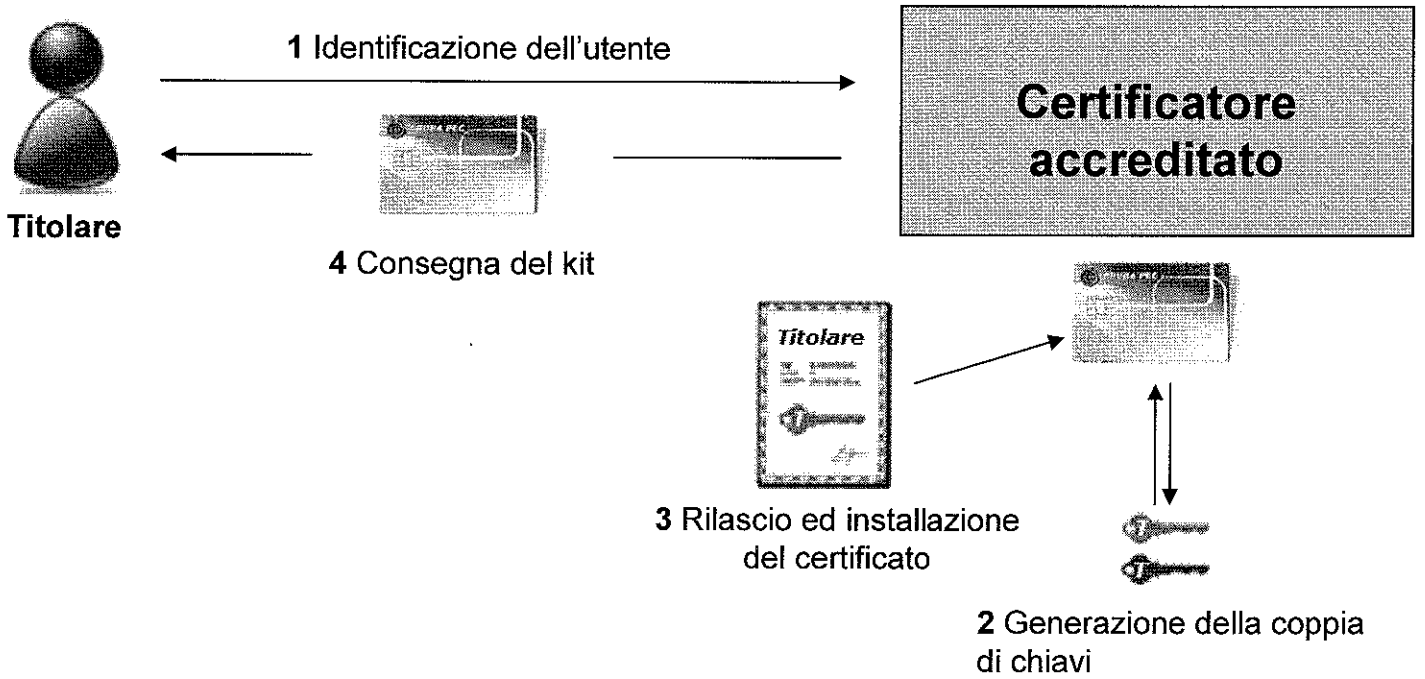
- **Titolare:** La persona fisica cui è attribuita la firma digitale e che ha accesso al dispositivo che contiene la coppia di chiavi per la creazione della firma digitale;
- **Certificatore (CA):** Il soggetto pubblico o privato che presta servizi di certificazione delle firme digitali e che fornisce altri servizi connessi con queste ultime (ad esempio Marcatura Temporale). Esso rilascia certificati qualificati conformi alla Direttiva europea 1999/93/CE e nazionale in materia di firma digitale. Deve inoltre, ai sensi della normativa vigente, aver richiesto ed ottenuto il riconoscimento del possesso dei requisiti del livello più elevato, in termini di qualità e di sicurezza (accreditamento);
- **CNIPA:** L'ente ministeriale che esercita funzioni di controllo e vigilanza sull'operato delle CA accreditate attraverso la raccolta di dati, visite ispettive e test di interoperabilità.
- **Utente:** Colui che ha la necessità di verificare la validità di una firma digitale e/o di una eventuale marca temporale ad essa associata.

:: Cos'è un Certificato Qualificato ::

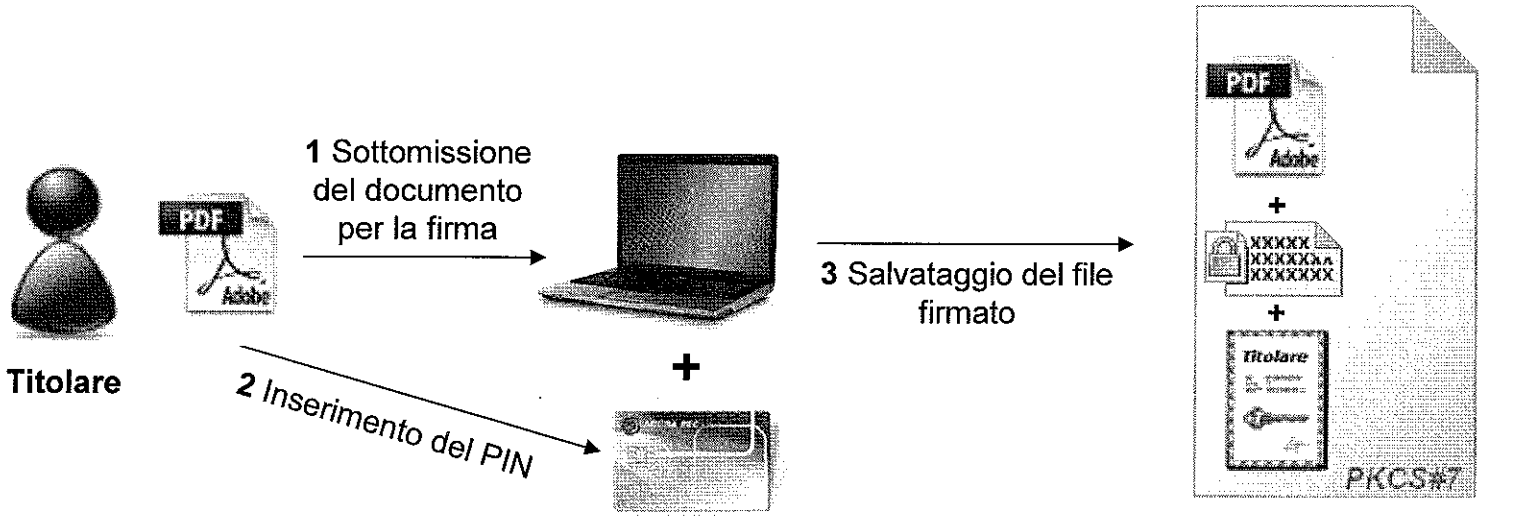
Un certificato qualificato è lo strumento che permette di distribuire pubblicamente le chiavi pubbliche rendendole note agli utenti finali con garanzia di autenticità e integrità.
All'interno di un certificato qualificato troviamo i seguenti elementi informativi principali:

- **Ragione sociale** o **denominazione** dell'Ente che ha rilasciato il certificato;
- **Dati del Titolare** del certificato (nome, cognome, CF, Organizzazione di appartenenza, Titolo o Carica etc...);
- **Durata** del certificato (solitamente 3 anni);
- **Chiave pubblica** del Titolare del certificato;
- **Firma Digitale** dell'Ente Certificatore a garanzia dell'autenticità ed integrità di tutte le informazioni contenute nel certificato (comprese ovviamente quelle dei punti di cui sopra).

:: Il rilascio del kit di Firma Digitale ::

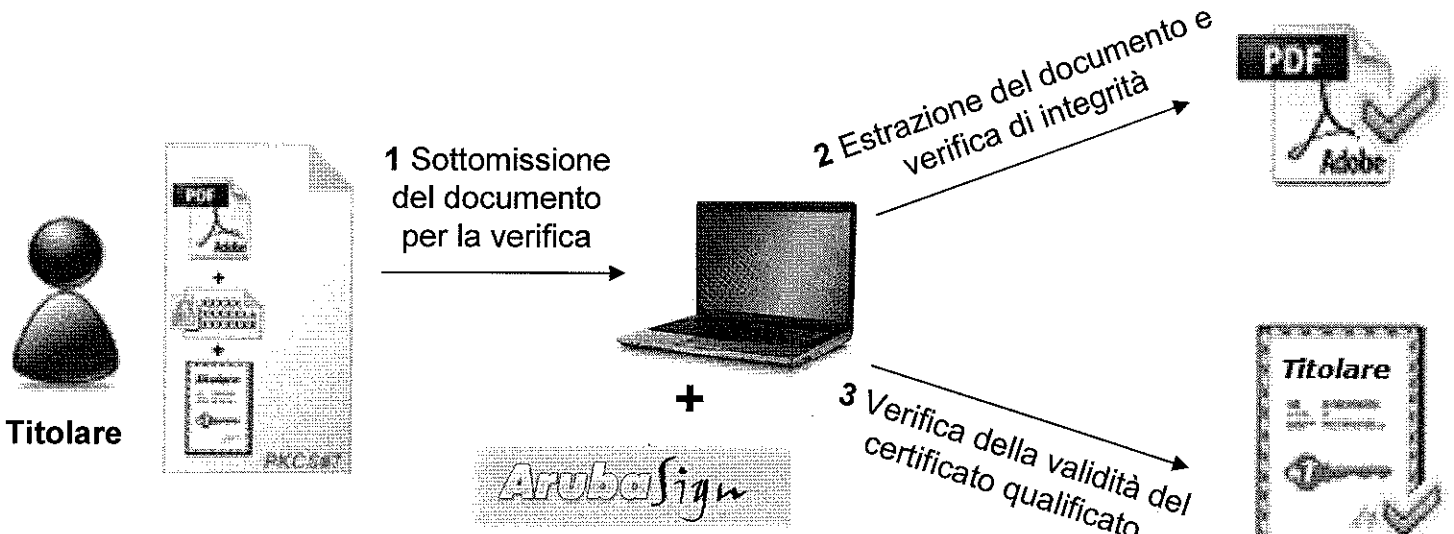


:: Firma di un file ::



Il file firmato viene salvato automaticamente all'interno della directory di lavoro assumendo l'ulteriore estensione **.p7m**

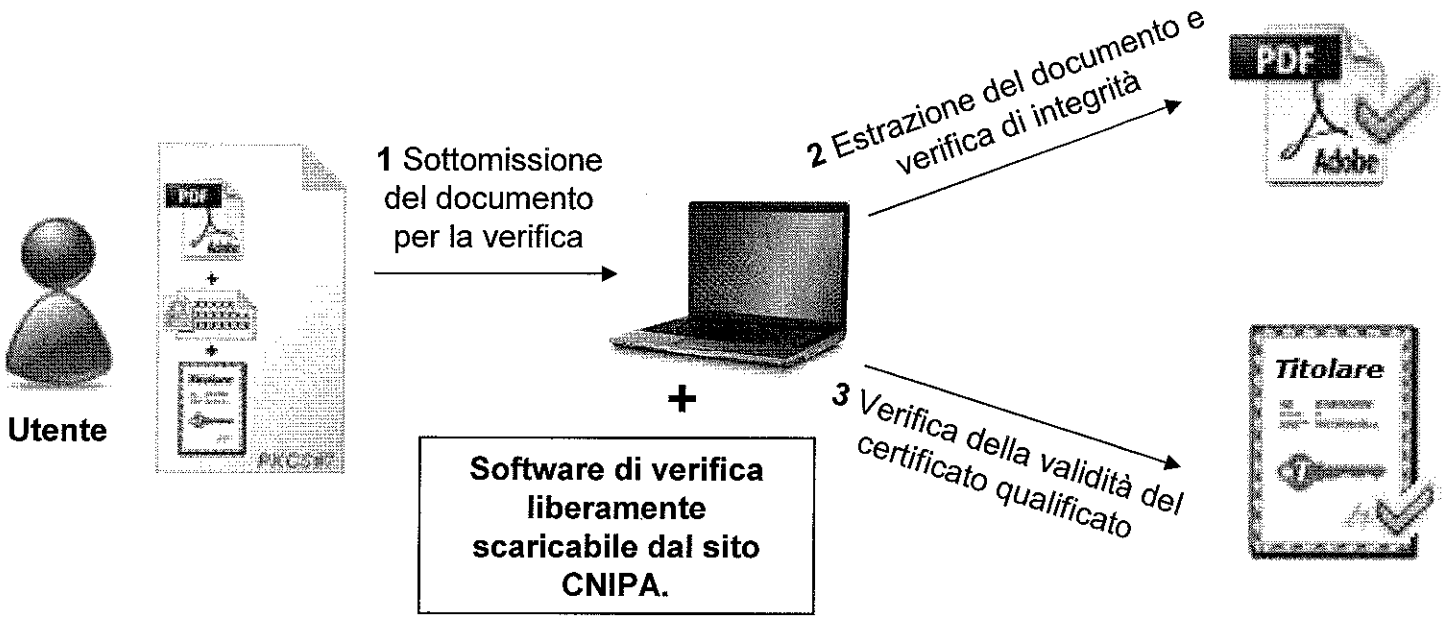
:: Verifica della firma ::



- Il documento non deve aver subito modifiche dopo l'apposizione della firma.

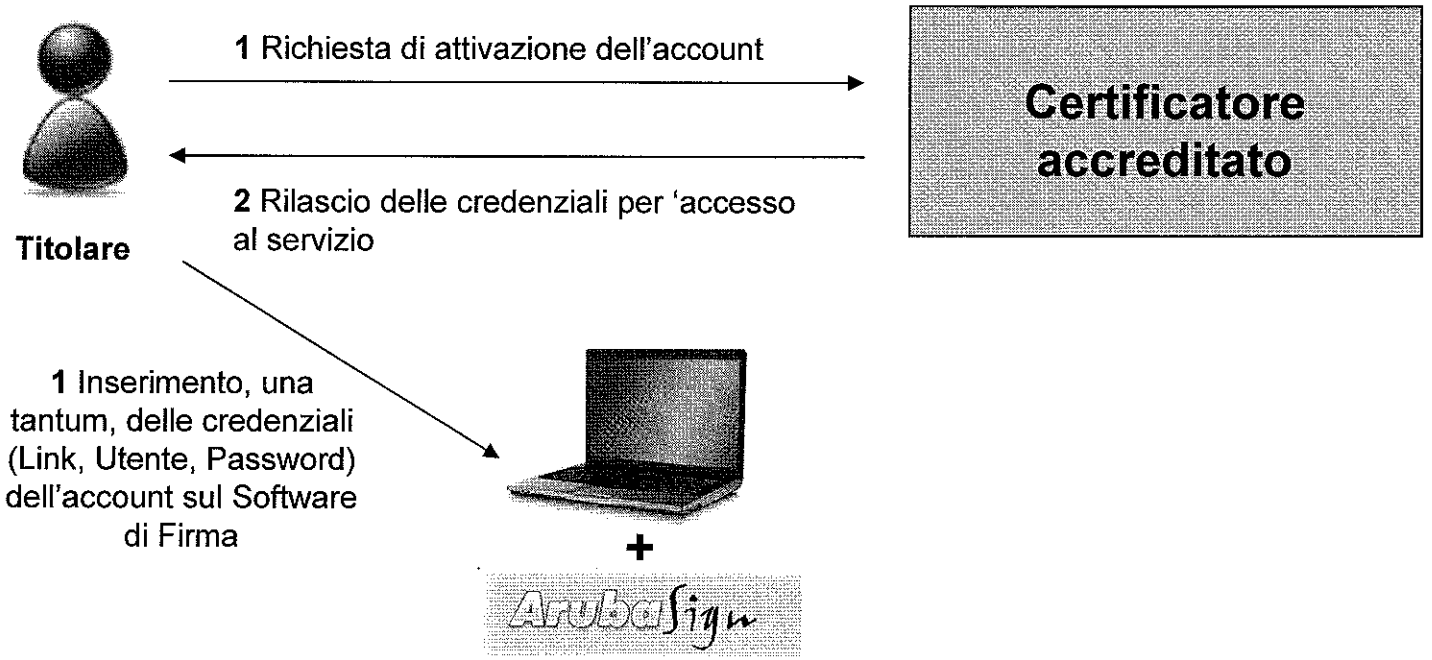
- Il certificato del sottoscrittore sia garantito da una CA accreditata al CNIPA.
- Il certificato del sottoscrittore non sia scaduto.
- Il certificato del sottoscrittore non sia stato revocato o sospeso.

:: Interoperabilità della Firma Digitale ::

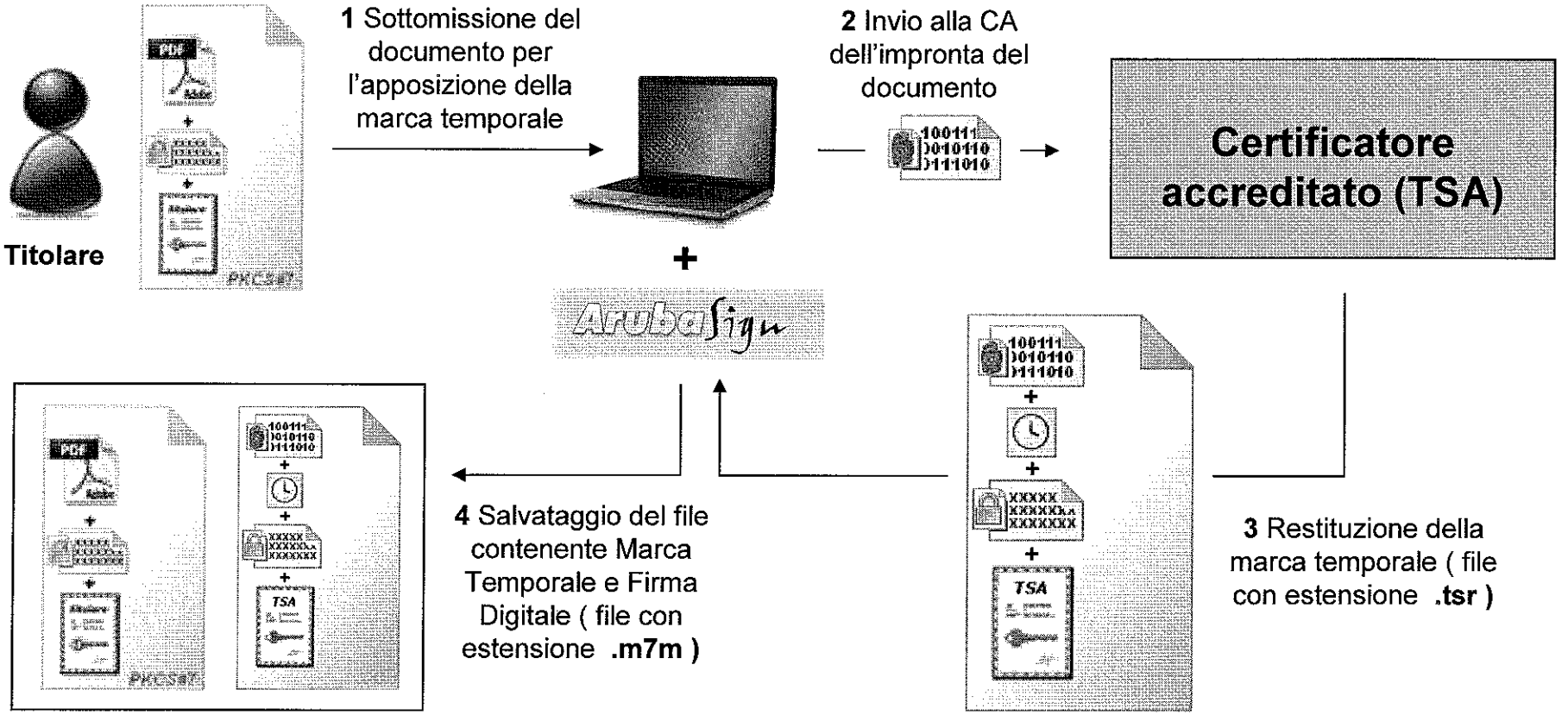


- Il documento non deve aver subito modifiche dopo l'apposizione della firma.
- Il certificato del sottoscrittore sia garantito da una CA accreditata al CNIPA.
- Il certificato del sottoscrittore non sia scaduto.
- Il certificato del sottoscrittore non sia stato revocato o sospeso.

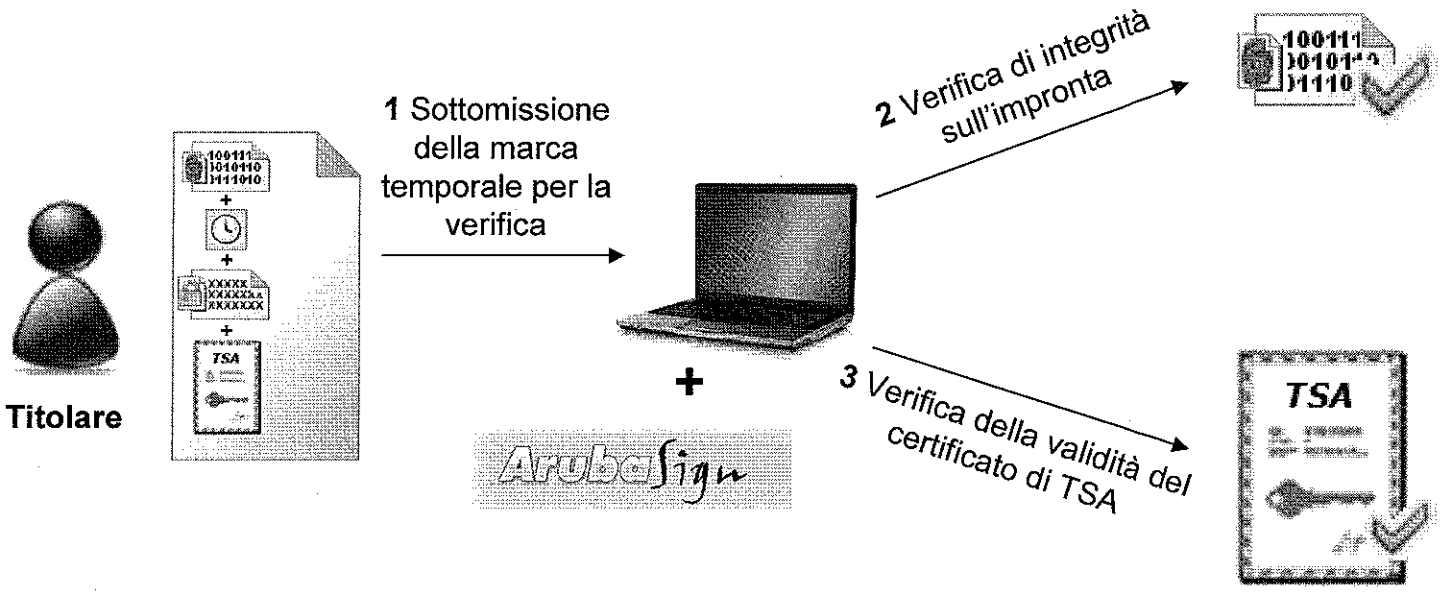
:: Il rilascio e configurazione dell'account di Marcatura Temporale ::



:: Marcatura temporale di un file firmato ::



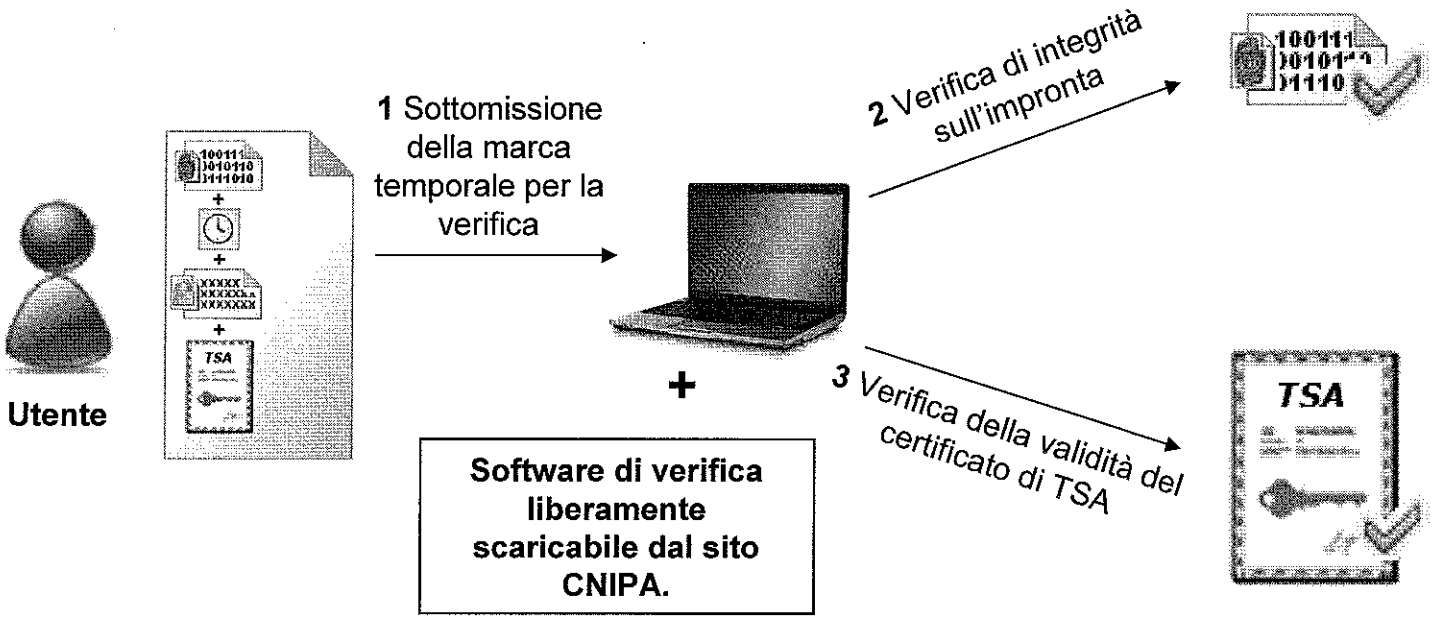
:: Verifica di un file marcato temporalmente ::



- L'impronta relativa al documento per cui si è richiesta la validazione temporale non deve aver subito modifiche dopo l'apposizione della firma da parte della TSA.

- Il certificato della TSA che ha rilasciato la Marca Temporale sia garantito da una CA accreditata al CNIPA.
- Il certificato della TSA non sia scaduto.
- Il certificato della TSA non sia stato revocato o sospeso.

::Interoperabilità delle Marche Temporali ::



- L'impronta relativa al documento per cui si è richiesta la validazione temporale non deve aver subito modifiche dopo l'apposizione della firma da parte della TSA.

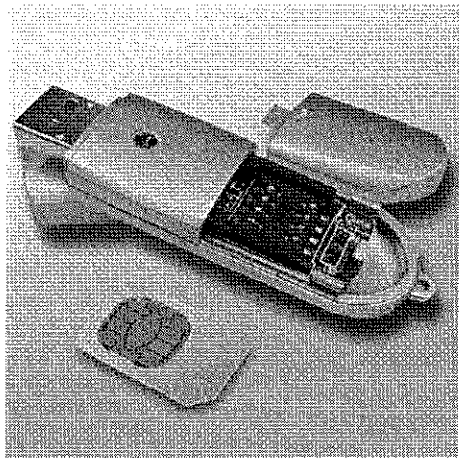
- Il certificato della TSA che ha rilasciato la Marca Temporale sia garantito da una CA accreditata al CNIPA.
- Il certificato della TSA non sia scaduto.
- Il certificato della TSA non sia stato revocato o sospeso.

:: La Firma Digitale per il CNI ::

:: Kit di Firma Digitale ::

- Kit di Firma Digitale formato Standard
  - Smart card formato standard ISO-CR80
  - Lettore di Smart Card "da tavolo"

- Kit di Firma Digitale formato Token
  - Smart card formato plug-in
  - Lettore di Smart Card formato "Token"



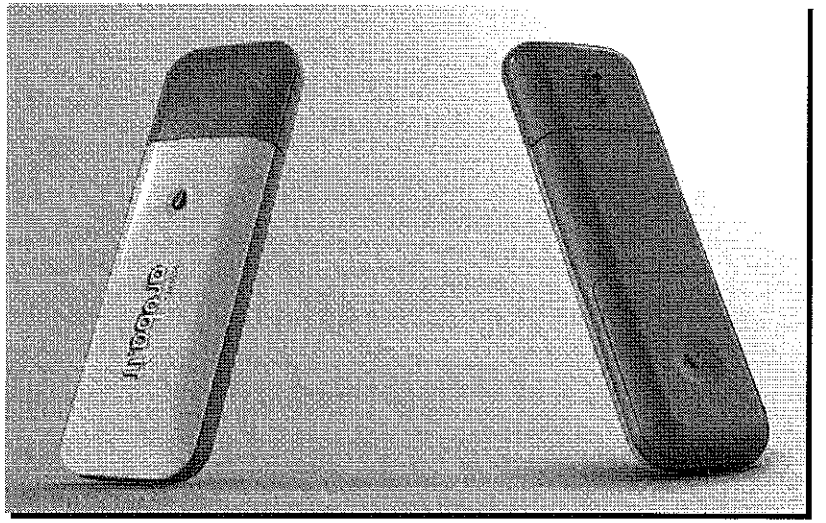
Entrambe le tipologie di Kit richiedono l'installazione dei driver della Smart card, del lettore di Smart Card e del software di Firma Digitale.

:: ArubaKEY ::

Aruba Key è il dispositivo USB evoluto che permette di **portare sempre con sé la propria Firma Digitale e Marca Temporale**.

Aruba Key **non necessita di installazione HW o SW**, ed è sempre pronta per sottoscrivere digitalmente e marcare temporalmente documenti informatici.

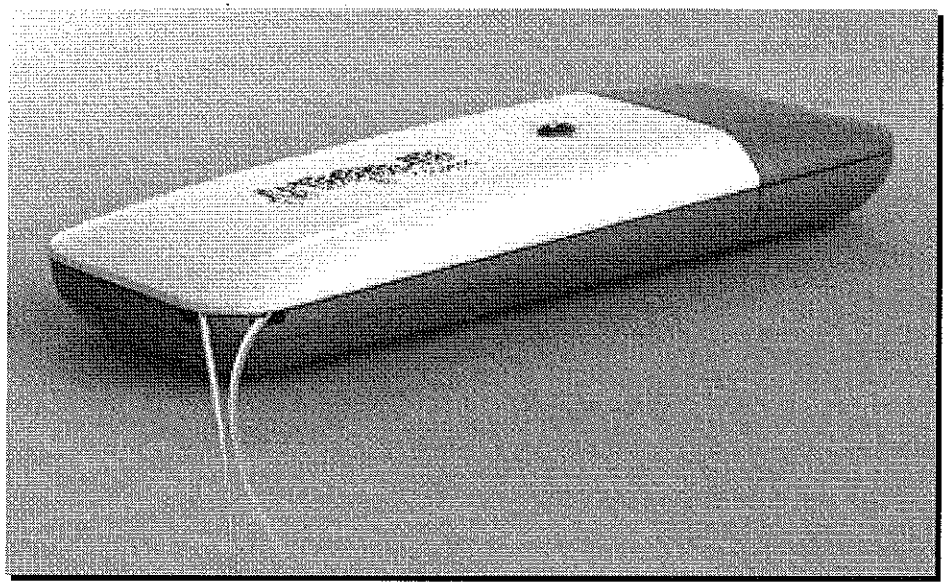
Aruba Key inoltre può essere anche utilizzata per **l'autenticazione sicura nei Siti web**.



:: ArubaKEY ::

Aruba Key è il nuovo dispositivo di firma digitale di Aruba PEC, che integra:

- una smart card in formato SIM
- un lettore di smart card
- una memoria flash di 1 GB

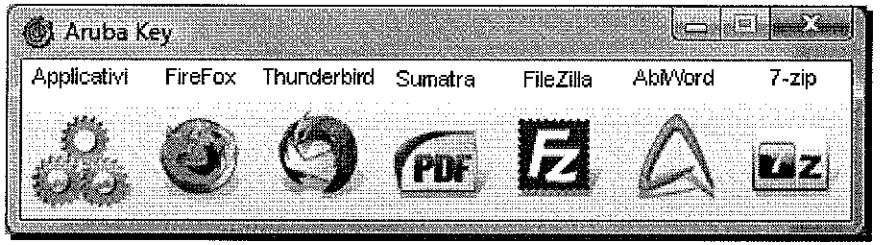


[Firma Digitale per il CNI]

:: ArubaKEY ::

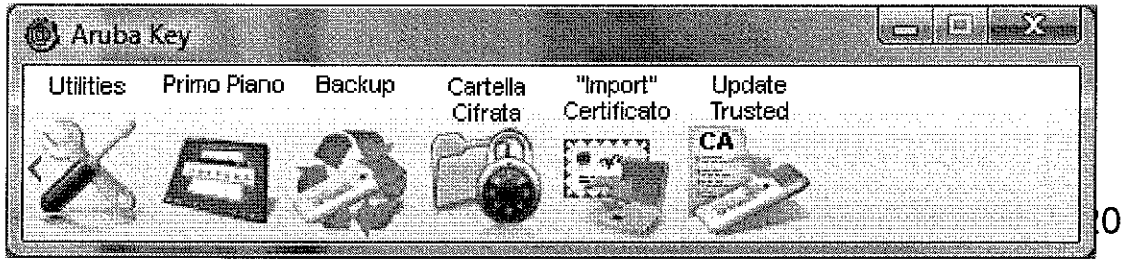
In essa sono memorizzate tutte le applicazione necessarie per l'Utente:

1. Software di firma digitale
2. Software di verifica dei file firmati digitalmente
3. FireFox e Thinderbird in versione portable
4. Un editor di testo per la creazione di documenti .doc
5. Un visualizzatore di file PDF
6. Un software per l'apertura di file compressi



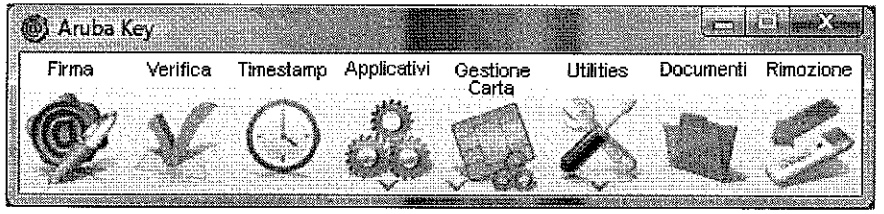
Sono disponibili funzionalità di:

- Update automatico del repository delle Root CA pubblicate del CNIPA (EPC)
- Cartella Cifrata



:: ArubaKEY ::

Collegando **Aruba Key** al PC, apparirà una barra di strumenti, dalla quale è possibile effettuare le operazioni di firma e verifica, oppure richiamare le altre applicazioni presenti all'interno della memoria.



Grazie alla funzione "drag&drop", è possibile firmare digitalmente, marcare temporalmente un file, oppure verificarne uno già firmato e/o marcato, semplicemente trascinando il file sul relativo pulsante.

Il pacchetto software preinstallato consente all'Utente di disporre di circa 900Mb per l'archiviazione di documenti, ai quali è possibile accedere rapidamente, selezionando l'opportuna icona sulla barra degli strumenti.

In caso di particolari esigenze del Cliente, è possibile personalizzare il pacchetto software preinstallato.

:: ArubaKEY ::

- **Portabilità:** Con ArubaKEY si è in grado di poter disporre della propria firma digitale e marca temporale anche senza l'installazione di alcun driver e/o applicazione su qualsiasi PC ospite.
- **Validità legale:** La firma digitale produce gli stessi effetti della firma autografa (ex art. 2702 c.c.). Inoltre l'utilizzo del dispositivo di firma si presume riconducibile al titolare, salvo che questi dia prova contraria.
- **Semplicità:** Una volta collegata l'ArubaKEY al PC sarà possibile, attraverso il software di firma, selezionare fin da subito il documento elettronico da firmare e/o marcare temporalmente. In alternativa è possibile avvalersi anche della funzionalità "drug&drop" per velocizzare ulteriormente il processo di firma e/o marcatura file.
- **Sicurezza:** Utilizzo di dispositivi certificati CC EAL4+, autenticazione del sottoscrittore a due fattori, utilizzo di algoritmi e meccanismi crittografici estremamente robusti.
- **Economicità:** La Firma Digitale unitamente al servizio di Marcatura Temporale consentono di informatizzare la gestione documentale. Si evitano quindi le costose inefficienze legate alla gestione cartacea dei documenti quali ad esempio: difficoltà di condivisione e archiviazione, tempi di ricerca elevati, smarrimenti, perdite, facilità di errori ed altro ancora.

:: La Firma Digitale per il CNI ::

:: Kit di Firma Digitale – Flusso richiesta ::

★ L'Ordine dovrà essere nominato come Incaricato alla Registrazione di ArubaPEC (cfr. modulo allegato)

★ L'Ordine pubblicherà sul proprio portale (in area riservata) e/o trasmetterà direttamente agli iscritti (ad es. via mail) la modulistica necessaria per ottenere il Kit di Firma Digitale:

- ★ Offerta economica
- ★ Modulo unico di registrazione e richiesta certificato
- ★ Condizioni generali di contratto (solo presa visione)

★ L'iscritto dovrà restituire ad ArubaPEC via fax al numero 0575-862022 o via mail alla casella amministrazione@ca.arubapec.it la seguente documentazione, opportunamente compilata e sottoscritta:

- ★ Offerta economica
- ★ Modulo unico di registrazione e richiesta certificato

:: La Firma Digitale per il CNI ::

:: Kit di Firma Digitale – Flusso richiesta ::

- ArubaPEC provvederà poi a svolgere in totale autonomia le seguenti operazioni:
  - Verifica documentazione
  - Emissione certificati
  - Preparazione Kit di Firma Digitale
  - Spedizione Kit di Firma Digitale all'Ordine
- L'Ordine infine dovrà solamente effettuare la consegna dei Kit di Firma Digitale agli iscritti raccogliendo la documentazione in originale
- La documentazione così raccolta dovrà essere restituita periodicamente ad ArubaPEC

:: La Firma Digitale per il CNI ::

:: Kit di Firma Digitale – Tabella Costi ::

Descrizione	Costo unitario
Kit di Firma Digitale formato Standard	€ 17,50 + IVA
Kit di Firma Digitale formato Token	€ 19,50 + IVA
ArubaKEY	€ 39,50 + IVA

GRAZIE PER L'ATTENZIONE

Simone Braccagni
Amministratore Unico
Simone.braccagni@staff.aruba.it
348-6299009

Andrea Sassetti
Direttore Certification Authority
Andra.sassetti@ca.arubapec.it

Luca Oliva
Referente commerciale
luca.oliva@staff.aruba.it
340-5114508