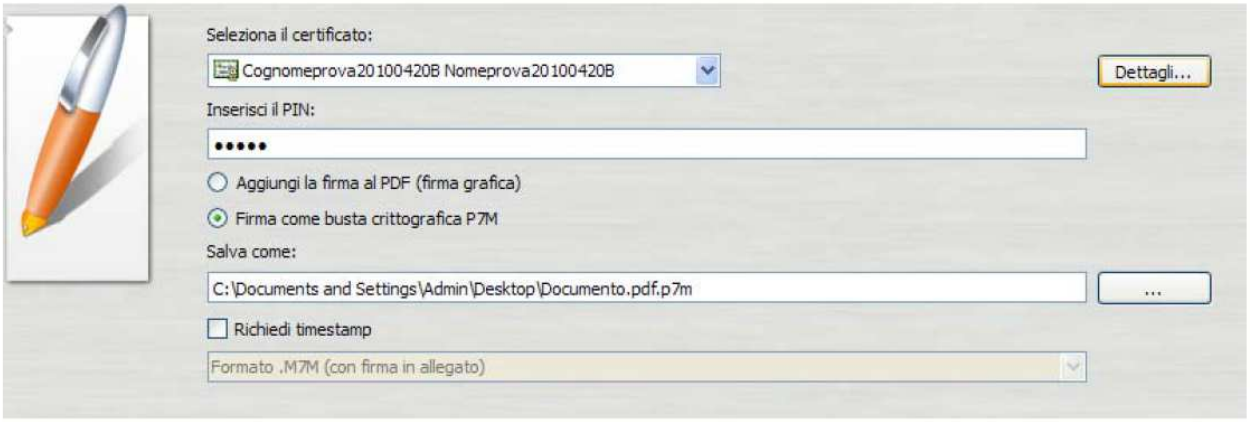
Formato di Firma digitale da adottare:

I Modelli convertiti in PDF/a dovranno essere firmati digitalmente in ***formato pkcs#7 meglio noto come p7m (Busta crittografica di firma)*** ed è quello che le Pubbliche Amministrazioni sono obbligate ad accettare (*Delibera CNIPA n. 45/2009 del 21 maggio 2009*).

Il nome del file firmato, ossia della busta, deve assumere l'ulteriore estensione "p7m" (*es:MURAD.pdf.p7m*). Le buste crittografiche possono contenere a loro volta buste crittografiche (*Firme Multiple*). In questo caso deve essere applicata una ulteriore estensione "p7m" (*es:MURAD.pdf.p7m.p7m*).

In commercio esistono dispositivi di firma digitale che oltre ad adottare come formato il pksc#7 utilizzano anche il formato PDF (*firma grafica*) come ad esempio i sistemi Aruba.
Il software ARUBASign, in dotazione a detti dispositivi, consente l'apposizione della firma digitale nel formato pksc#7 come sotto mostrato:

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



Il formato di firma digitale consentito dal SUAP di Civitavecchia è dunque il ***pkcs#7 meglio noto come p7m (Busta crittografica di firma).***

Verifica Firma digitale dei file *.pdf.p7m:

Per eseguire questa verifica, oltre che per rendere leggibile il contenuto del documento, sono utilizzati specifici software messi a disposizione dai fornitori dei dispositivi stessi.
In alternativa a quanto detto nella sezione del portale del SUAP di Civitavecchia *SPORTELLO UNICO → INFORMAZIONI GENERALI → UTILITY DOWNLOAD* è disponibile Dike 5.0.0.exe software che consente di apporre e verificare una o più firme digitali su qualunque tipo di file con estensione .p7m.

Firma digitale – Come funziona e contesto normativo

La Firma Digitale è l'equivalente informatico della firma autografa e ne ha il medesimo valore legale con in più il vantaggio della totale sicurezza.

La Firma Digitale è il risultato finale di un complesso algoritmo matematico che permette di firmare un documento informatico con la stessa validità di una firma autografa.

Il processo di Firma Digitale si basa sulla crittografia asimmetrica: ogni titolare dispone di una coppia di chiavi, una privata - segreta e custodita sulla Smart Card e protetta da un codice di accesso (PIN) - l'altra pubblica - custodita e pubblicata dall'Ente Certificatore - che viene usata per la verifica della firma. Le due chiavi sono correlate in maniera univoca, ma dalla chiave pubblica è impossibile risalire a quella privata.

La normativa italiana, attribuisce alla firma digitale lo stesso valore della firma autografa, rendendo pienamente validi ai fini di legge i documenti informatici sottoscritti digitalmente.
Il Codice dell'Amministrazione Digitale, emanato con il Decreto Legislativo 7 marzo 2005 n. 82, fissa i criteri e le modalità per la realizzazione, la sottoscrizione, la gestione e la trasmissione di documenti con strumenti informatici e telematici, validi e rilevanti a tutti gli effetti di legge.

La Deliberazione CNIPA 45/2009 del 21 maggio 2009 descrive le **REGOLE PER IL RICONOSCIMENTO E LA VERIFICA DEL DOCUMENTO INFORMATICO**, detta Deliberazione stabilisce inoltre che le pubbliche amministrazioni possono accettare documenti informatici sottoscritti con i formati di firma di cui ai commi 8 e 9 art.21, e di farne apposita menzione nei procedimenti amministrativi cui si applicano.