FIRMA DIGITALE

Cosa contiene il kit della firma digitale ?

Il kit della firma digitale contiene: un **lettore di smart card** (che si collega ad una porta USB del computer), una **smart sard**, una foglio di carta su cui è scritto il **codice PIN** associato alla smart card.
Il lettore di smart card ha un cavetto che permette di collegarlo su una porta USB del computer e ha uno slot in cui si inserisce la smart card. Viene accompagnato da un software (detto driver) che deve essere installato per permettere al sistema operativo (Windows) di comunicare con il lettore.
La smart card, che può essere acquistata anche separatamente dal lettore, ha un formato tale che può essere inserita all'interna del lettore ed è dotata di un chip di memoria su cui è memorizzato un file che rappresenta il **certificato digitale privato** rilasciato da un ente al titolare della firma. Questo certificato digitale contiene la chiave privata (segreta) che è un numero che serve alle applicazioni come chiave per la **crittografia** durante il processo di produzione della firma digitale. La smart card è uno strumento pratico e sicuro per conservare la chiave privata.
Il **codice PIN** (Personal Identification Number) è un numero che il titolare deve digitare ogni qualvolta desidera permettere ad una applicazione software di leggere il valore della chiave privata nella smart card al fine di produrre la firma digitale per uno specifico documento.
Il certificato pubblico che contiene la chiave pubblica che serve per la decrittografia dei dati, viene conservato dall'ente certificatore (Certification Authority) che garantisce l'identità del titolare della firma.

Quale garanzia è fornita dalla firma digitale nell'invio di un documento ?

La firma digitale allegata ad un documento garantisce:
- **autenticità**: la firma permette di verificare la veridicità dell'identità del mittente;
- **integrità**: la firma permette di verificare che i dati contenuti nel documento non sono stati modificati dal momento della firma;
- **non ripudio**: la firma impedisce che il mittente disconosca di aver firmato il documento;

Quali sono le differenze tra la firma autografa su carata e la firma digitale su file ?

	Firma autografa su carta	Firma digitale su file
Creazione	Viene creata manualmente	Viene creata da un software
Apposizione	La firma è parte integrante del documento	La firma è fuori dal documento, ad esempio in una firma elettronica semplice l'autenticazione attraverso user id o password o come file allegato
Verifica	La firma viene confrontata con una firma autenticata (metodo insicuro basato su perizia calligrafica)	mediante algoritmo di verifica pubblicamente noto e certificazione (metodo sicuro)
Documento copia	Distinguibile dall'originale	Indistinguibile dall'originale
Validità temporale	Senza limiti	Limitata dalla scadenza del certificato di firma
Automazione dei processi	Non è facilmente gestibile dai dispositivi elettronici	Per la sua natura digitale è fatta apposta per essere elaborata dai software e dai dispositivi elettronici.

Dove si può acquistare il kit di firma digitale ?

Un cittadino può dacquistare un kit di firma digitale rivolgendosi ai certificatori accreditati autorizzati da AgID (www.**agid**.gov.it) che garantiscono l’identità dei soggetti che utilizzano la firma digitale. AgID svolge attività di vigilanza sui certificatori. Le aziende più famose che offrono questo tipo di prodotto ci sono **Aruba** e **Poste Italiane**. Per quanto riguarda le aziende, dotarsi di firma digitale può essere un po’ più complicato. I titolari di aziende, devono infatti richiedere alla propria **Camera di Commercio** il kit per la firma digitale (di solito viene fornito quello con smart card) fornendo all’ente un documento di riconoscimento ed un indirizzo email validi.

Come si usa il kit di firma digitale ?

Installato il Kit sul proprio computer, attraverso il Software di Firma sarà possibile selezionare il documento elettronico da sottoporre a Firma Digitale e, previa attivazione di un account, alla Marcatura Temporale.

Al momento della Firma del documento, il software chiederà l’inserimento del codice di protezione del dispositivo (PIN) che - se correttamente inserito - procederà con la creazione del file firmato digitalmente.

Il file firmato assumerà l’estensione .p7m che si sommerà all’estensione del file originario. Pertanto firmando un documento .txt, al termine del processo di Firma Digitale il documento assumerà l’estensione .txt.p7m che rappresenta una busta informatica (CADES o PADES).

Tale busta incorpora al suo interno il documento originario, il Certificato del sottoscrittore ed un Hash del documento firmato con il Certificato del sottoscrittore.

Tali componenti consentiranno, in fase di verifica della Firma da parte del destinatario del documento firmato, di accertare che:

- il documento non sia stato modificato dopo la Firma
- il Certificato del sottoscrittore sia garantito da una Autorità di Certificazione (CA) inclusa nell’Elenco Pubblico dei Certificatori
- il Certificato del sottoscrittore non sia scaduto
- il Certificato del sottoscrittore non sia stato sospeso o revocato

Se tutte le verifiche daranno esito positivo, il documento sottoscritto digitalmente potrà essere considerato valido a tutti gli effetti di legge.

Come si appone la firma digitale ad un documento PDF ?

Uno dei programmi più usati per apporre la firma digitale è Adobe Acrobat, che permette di firmare documenti PDF e di trasformare altri tipi di file (ad esempio i file di Word) in file PDF per poi includere la firma digitale in questi ultimi. Per firmare un documento con Acrobat Reader, non devi far altro che importarlo nel programma e cliccare sul pulsante Firma, se presente nella barra degli strumenti, oppure prima sulla voce Strumenti collocata in alto a destra e poi sulla voce Firma e certificazione > Inserisci firma che si trova nella barra laterale di destra. Inserisci quindi il PIN e tutti i dati richiesti per la tua firma digitale (sono tutti compresi nel kit) e salva il file per convalidarlo. Trovi qualche esempio pratico anche sul sito di Poste Italiane.

Cos'è il token USB ?

E' un kit per la firma digitale che usa una pendrive come lettore e una SIM come smart card, costano circa 40 euro

Cos'è la firma digitale remota ?

Il servizio di Firma Remota rivoluziona il mondo della Firma Digitale coniugando la portabilità ad un sistema di autenticazione forte, cioè un’autenticazione a due fattori basata sull'utilizzo congiunto di due metodi di autenticazione individuale.

Grazie alla Firma Remota, per la sottoscrizione dei documenti digitali non sarà più necessaria la Smart Card ma sarà sufficiente utilizzare un computer collegato ad Internet, una OTP (One Time Password), generata attraverso un apposito dispositivo (Token, app per Smartphone) ed il Software di Firma Aruba Sign, attraverso il quale sarà possibile selezionare il documento elettronico da sottoporre a Firma Remota.

Per apporre la Firma Remota si può utilizzare esclusivamente il software Aruba Sign, che prevede la modalità di firma off-line (ovvero: si dovrà provvedere a firmare il documento in locale sul proprio computer). Per tale motivo la sottoscrizione digitale di documenti direttamente on-line potrebbe non essere consentita.

Le OTP (password dinamiche) sono considerate il sistema più sicuro per l’accesso ai sistemi informatici e vengono generate o distrutte direttamente all’interno dei dispositivi OTP. Trattandosi di password momentanee (scadono alcuni secondi dopo essere state generate) non rendendo necessaria all’utente finale la memorizzazione, eliminando di conseguenza i problemi ed i rischi - da tempo noti - relativi all’utilizzo delle tradizionali password statiche.

Il kit di Firma Digitale Remota non comprende il certificato di autenticazione di tipo CNS (Standard Carta Nazionale dei Servizi), pertanto il kit non può essere utilizzato per effettuare l’accesso ai portali web che consentono l’autenticazione tramite Smart Card.

Il dispositivo di Firma Remota può essere utilizzato anche per firmare documenti elettronici direttamente dal proprio iPad. Aruba mette infatti a disposizione l’applicazione: “Firma Digitale”, scaricabile in modo del tutto gratuito dall’Apple Store, grazie alla quale sarà possibile sottoscrivere digitalmente documenti in pochi semplici passaggi attraverso il proprio iPad. L’App “Firma Digitale” di Aruba può essere utilizzata in abbinamento con i dispositivi di firma remota di tipo OTP con Display o OTP Mobile, sarà sufficiente disporre di una connessione internet.

Qual'è il funzionamento che sta alla base della firma digitale ?

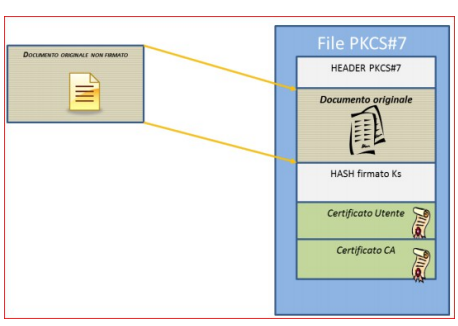
Il funzionamento si basa su una coppia di chiavi crittografiche, una privata e una pubblica. La chiave privata (segreta) è conservata in file detto certificato privato memorizzato nella smart card della persona che è titolare della firma e serve per firmare i documenti. La chiave pubblica è conservata dall'ente certificatore (Certification Authority) che ha rilasciato la firma e la mette a disposizione di chiunque voglia verificare l'autenticità e l'integrità di un documento firmato da quella persona.

Firma del documento

Supponiamo che si vuole firmare un documento contenuto in un file **documento.doc.pdf**.

Il software che viene usato per firmare un documento usa una funzione Hash per ottenere una impronta (fingerprint o digest) del documento, cioè una sequenza di 128 o 160 bit che rappresentano una riassunto del documento (ad ogni minimo cambiamento del documento corrisponde una impronta differente).

Il software chiede all'utente di digitare il PIN che permette di accedere alla smart card che contiene il certificato con la chiave privata in un file con estenzione **.cer** che contiene la chiave privata (sequenza di 1024 bit). Quindi usa la chiave privata



per crittografare l'impronta del documento ottenendo una sequenza binaria che costituisce la firma digitale (la sequenza di bit della firma digitale quindi dipende dal contenuto del file). Infine il software crea un file **documento.doc.p7m** che contiene il documento in chiaro, la firma digitale e il certificato pubblico da usare per la verifica (questo sistema di imbustamento è detto CADES, l'alternativa e il sistema PADES che viene usato per documenti in formato pdf). Questo è il file che costituisce il documento firmato che può essere inviato ad un'altra persona, azienda privata o ente pubblico.

Verifica del documento

Chi riceve il documento, può usare un qualsiasi software per la verifica di documenti firmati digitalmente, per esempio come Dike (scaricabile da www.firma.infocert.it). Innanzitutto il software legge dal file p7m il certificato pubblico del firmatario e lo sottopone alla Certification Authority (CA) che lo ha prodotto (per eseguire questa operazione il software necessita di una connessione a Internet). Il certificato pubblico contiene:

- numero di serie del certificatore
- identificazione della CA
- nome, cognome e data di nascita del titolare
- valore della chiave pubblica
- algoritmo di generazione e verifica
- data di inizio e data di fine del periodo di validità delle chiavi

La CA fornisce al software la garanzia dell'autenticità del certificato pubblico (cioè che l'ha emesso lei e che il contenuto è corretto) , la validità legale del certificato (cioè che non è scaduto) e la garanzia che il titolare non risulta ne revocato ne sospeso.
Quindi il software usa la chiave pubblica contenuta nel certificato pubblico del firmatario per decrittografare la firma digitale e ottenere l'impronta (digest) calcolato dal software che ha firmato il documento. Quindi usa la stessa funzione hash (descritta dal certificato pubblico) per ricavare l'impronta (digest) del documento in chiaro e la confronta con l'impronta ricavata dalla firma. Se le due impronte sono uguali significa che il documento è **autentico** (firmato dalla persona specificato sul certificato) e **integro** (non è stato modificato dal momento in cui è stato firmato).