SOFTWARE

Per quanto riguarda gli ambienti software per apporre **firme digitali** è necessario distinguere tra le soluzioni che **non hanno valore legale** (come ad esempio *Acrobat Reader DC*, *FastStone Photo Resizer* o *DigiSigner*) e quelle invece **con valore legale**.

Tra le soluzioni con valore legale più usate ricordiamo **Aruba Key**. Dopo essersi rivolti all'azienda di riferimento (Aruba) per la consegna e l'attivazione del kit per la firma digitale, è necessario scaricare i **driver** e avvalersi del **software** dal rispettivo sito.

A software avviato viene presentata un'icona cliccabile per l'**applicazione della firma digitale**. Dopo aver cliccato l'icona, verrà richiesto di scegliere il **file da firmare**, inserire il **PIN del dispositivo** di firma del kit ed infine il **tipo di firma** da applicare.

I tipi di firma più comuni sono i seguenti:

- **Busta crittografica P7M (CAdES)** – crea un nuovo file in formato **P7M** che contiene il documento originale e i file della firma digitale. Si può applicare a tutti i tipi di documenti.
- **Firma PDF** – crea un file PDF con firma inclusa, la quale può essere invisibile o grafica.
- **Firma XML (XAdES)** – crea un nuovo file in formato **P7M**. Applicabile a tutti i tipi di documenti.

Dopo aver apposto la firma, i documenti possono essere verificati tramite l'apposita funzionalità annessa al software.

AMBIENTE SICURO

L'efficacia delle firme digitali è garantita se c'è un **legame indissolubile tra il firmatario e la sua chiave privata.**

Paradossalmente è necessario proteggere la chiave privata dell'utente dall'utente stesso!

Un malintenzionato potrebbe far trapelare la sua *chiave privata* e negare di aver firmato un documento che in realtà ha effettivamente firmato.

Per ovviare a questo problema entra in gioco il dispositivo fidato (che prende il nome di "**ambiente sicuro**") la cui funzione è stabilire un legame indissolubile tra l'utente e la sua chiave privata. È importante dunque che l'utente abbia cura del dispositivo di firma fornitogli e che sia scrupoloso nel suo uso.

Tale dispositivo farà in modo di autenticare l'utente al **momento effettivo della firma**; inoltre, l'applicazione di un "*timestamp*" (data e ora precise della firma) farà in modo di non sollevare nessun problema di **ripudiabilità**.

RIFERIMENTI

- http://www.c3t.it/projects/awareness/articoli&brochure/firme_digitali_applicazioni/

LE APPLICAZIONI PER LA FIRMA DIGITALE

Scopri come dare valore legale ai tuoi documenti, quali sono i metodi e i software per la firma digitale

POR FESR 2014-2020 obiettivo Crescita e Occupazione (CreO)

COS'È LA FIRMA DIGITALE

La firma digitale è il risultato di una procedura informatica basata su tecniche crittografiche che consente di associare in modo indissolubile un **numero binario** (la firma) a un documento in formato elettronico, ovvero ad un altro insieme di bit che rappresenta fatti, atti o dati giuridicamente rilevanti. E' indispensabile per conferire validità legale ai documenti digitali in una serie di contesti come la sottoscrizione di contratti, di dichiarazioni o di atti amministrativi nel pubblico e nel privato.

2 COME FIRMARE

Per firmare, viene usato un software che iniziata la procedura di firma calcola l'*impronta digitale* del documento tramite una cosiddetta **funzione di hash** (a ogni documento diverso corrisponde un'impronta diversa). La lunghezza dell'impronta allo stato dell'arte deve essere di 256 bit.
Calcolata l'impronta, il software la invia all' "ambiente sicuro" dove è custodita la *chiave privata* (dispositivo di firma). Per attivarla, è necessario validare il **PIN** inserito dal titolare della firma. A questo punto il dispositivo di firma procede alla **cifratura dell'impronta** del documento con la *chiave privata*. Il risultato dell'operazione è la **firma digitale del documento**.
E' indispensabile associare la firma al documento e questo avviene attraverso specifici formati. Per esempio se utilizziamo il **PDF** il formato è denominato **PAdES**.

3 COME VERIFICARE

Per verificare la firma, il destinatario utilizza uno specifico software che estrae la *chiave pubblica* dal certificato del titolare. Spacchetta il file con documento e firma. Ricalcola l'impronta e decifrando con la *chiave pubblica* la firma del titolare **può verificare se l'impronta del mittente e quella ricalcolata dal destinatario sono identiche**.
In caso positivo la firma è valida. In caso contrario la firma non è valida e bisogna indagare sullo specifico errore che ha impedito la validazione.

1 DISPOSITIVI DI FIRMA

La **firma digitale** si ottiene dai prestatori di servizi fiduciari presenti in una serie di elenchi di fiducia gestiti dai singoli stati membri europei.

Esistono diversi prodotti di firma digitale generalmente costituiti da un *device*, solitamente una **smart card**, che contiene un certificato di firma digitale rinnovabile ed un dispositivo che serve per leggere la smart card.

Inoltre, sul mercato è possibile trovare da un po' di anni anche un kit costituito da una **chiavetta USB** che include il certificato di firma digitale (solitamente contenuto in una sim card da inserire all'interno della chiavetta.

Infine, esistono dispositivi di **firma digitale remota** che permettono di firmare documenti, anche massivamente, grazie alle soluzioni in cloud. Operano mediante dei dispositivi
firma virtuali accessibili solo mediante sistemi di accesso "sicuro" con dispositivi fisici che forniscono delle password usa e getta mediante una **chiavetta OTP** (simili a quelle utilizzate dalle banche), app per smartphone o messaggi sms.

In pratica, bisogna rivolgersi a uno dei provider qualificati (che in Italia sono in tutto 18 📋) per ottenere il kit di installazione e i relativi dettagli sulla procedura. Le azioni da fare per chi vuole iniziare ad utilizzare una firma digitale sono:

1. individuare uno provider che vende i kit di firma digitale;
2. essere identificati da un pubblico ufficiale;
3. attivare il kit acquistato;
4. usare il software specifico per apporre la propria firma digitale su un certo documento;

📋
- Actalis
- Aruba PEC
- Banca D'Italia
- Cedacri
- Comando C4 Difesa dello Stato Maggiore della Difesa
- In. Te. Sa
- Consiglio nazionale dottori commercialisti ed esperti contabili
- Consiglio nazionale del notariato
- IntesaSanPaolo
- Intesi Group
- Lombardia Informatica
- Lottomatica
- Namirial
- NexiPayments
- Poste Italiane
- Telecom Italia trust technologies
- Zucchetti
- Infocert