White Paper

ADOBE® PDF PER LA FIRMA DIGITALE
CARATTERISTICHE E APPLICAZIONI

Andrea Valle

Adobe

Adobe® PDF per la Firma Digitale
Caratteristiche e Applicazioni

Sommario

1. Introduzione

Sulla scia della notevole evoluzione nei sistemi informatici a cui abbiamo assistito negli ultimi anni, si sono diffuse varie tecnologie e soluzioni per la gestione elettronica dei documenti. Il loro scopo è garantire maggiore efficienza rispetto alla tradizionale carta, consentendo per esempio di sfruttare la trasmissione telematica e via Internet oltre che di reperire e controllare in pochi secondi da un normale PC l'equivalente di migliaia di pagine stampate.

Poche tecnologie però sono riuscite a mettere a punto un documento digitale equivalente se non migliore del documento cartaceo. Tra queste spicca il formato Adobe PDF (Portable Document Format) affermatosi non solo grazie alla disponibilità di un visualizzatore gratuito (il diffusissimo Adobe Reader reperibile virtualmente per qualsiasi piattaforma informatica), ma soprattutto per un'ampia serie di caratteristiche e proprietà che ne fanno il formato ideale per la gestione elettronica dei documenti.

Il PDF, nato oltre dieci anni fa come semplice formato documentale indipendente dalla piattaforma hardware e stampabile ad alta qualità, si è evoluto in un formato "intelligente" capace di rappresentare non solo testo e grafica ma anche dati, metadati e logica applicativa, con in più funzioni di sicurezza allo stato dell'arte che ne consentono il controllo e ne accrescono l'affidabilità. Inoltre, in Italia, il formato Adobe PDF è stato riconosciuto come standard di riferimento per la firma digitale in seguito alla sottoscrizione di un protocollo d'intesa tra il CNIPA (Centro Nazionale per l'Informatica nella Pubblica Amministrazione) e Adobe Systems Inc. , avvenuta il 16 febbraio 2006, che individua nel formato i requisiti richiesti dall'articolo 12, comma 9 della Deliberazione CNIPA n. 4/2005, in particolare per quanto concerne la disponibilità pubblica e gratuita sia delle specifiche del formato sia di un prodotto di verifica quale Adobe Reader, il diffuso visualizzatore di file Adobe PDF.

Il quadro normativo della firma digitale in Italia è in realtà molto più ampio. In particolare, si segnalano le fonti seguenti:

- Il Codice dell'Amministrazione Digitale, entrato in vigore il 1° gennaio 2006, disciplina l'utilizzo dell'informazione digitale nelle PA: creazione, gestione e conservazione, trasmissione e disponibilità. Per ulteriori informazioni, consultare: *www.cnipa.gov.it/site/it-IT/Normativa/Leggi,_Decreti_e_Direttive/*
- La Deliberazione n. 4/2005 stabilisce le regole per il riconoscimento e la verifica del documento informatico. Per ulteriori informazioni, consultare: *www.cnipa.gov.it/site/it-IT/Normativa/Leggi,_Decreti_e_Direttive/*
- Il DPCM 13/01/2004 stabilisce le regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione anche temporale dei documenti informatici. Per ulteriori informazioni, consultare: *www.privacy.it/dpcm20040113.html*

Alla pagina *www.cnipa.gov.it/site/it-IT/Attivit%C3%Ao/Firma_digitale* del sito CNIPA è possibile reperire informazioni generali sulla definizione di firma elettronica, firma elettronica qualificata e firma digitale secondo quanto stabilito dalla normativa italiana ed europea.

2. Il formato PDF per la firma digitale e la marcatura temporale

Sin dal 1999 il formato PDF ha introdotto nelle sue specifiche, disponibili pubblicamente sul sito *www.adobe.com*, un supporto standard e documentato per funzionalità di firma digitale. Esso utilizza tecniche standard conformi anche a quanto previsto dalla vigente normativa europea ed italiana. Nella pagina seguente sono elencate alcune caratteristiche tecniche essenziali.

- Formato della firma digitale: PKCS#7/CMS v.1.5 detached (conforme all'RFC2315) DER encoded
- Algoritmo dell'impronta (hash): SHA-1 o SHA-256
- Algoritmo crittografico: RSA con chiavi asimmetriche a 1024 o 2048 bit
- Formato dei certificati digitali: X.509 v.3
- Gestione completa della catena dei certificati
- Gestione delle liste di revoca dei certificati mediante CRL e OCSP
- Supporto della marcatura temporale (timestamp) conforme all'RFC3161

Le specifiche tecniche del formato di firma PDF sono anche documentate nell'RFC3778 (*www.ietf.org/rfc/rfc3778.txt*). Le applicazioni che implementano in modo completo le specifiche PDF per la firma digitale possono utilizzare diversi metodi per l'attuazione dei processi crittografici necessari alla firma digitale stessa. A titolo di esempio, il software gratuito Adobe Reader, nella versione attualmente disponibile, consente di accedere al registro dei certificati gestito dal sistema operativo Microsoft Windows mediante il livello CryptoAPI, che permette di utilizzare in modo semplice e immediato anche dispositivi sicuri (come SmartCard o Token USB) compatibili con questo sistema (mediante driver CSP). In alternativa, è possibile utilizzare direttamente driver sviluppati secondo lo standard PKCS#11 tramite i quali è possibile controllare direttamente dispositivi sicuri di firma anche su sistemi operativi non Microsoft (per esempio Linux e Mac OS).

2.1 Caratteristiche distintive della firma digitale nel formato PDF

La firma digitale nel formato PDF, in quanto funzionalità nativa, offre un'ampia serie di caratteristiche non presenti in altri prodotti software disponibili sul mercato. Questi prodotti infatti utilizzano generalmente una busta PKCS#7 di tipo "signed and enveloped data" (formato .P7M), un formato caratterizzato da numerose limitazioni d'uso.

Di seguito sono elencate alcune caratteristiche distintive della soluzione PDF che presentano sensibili vantaggi rispetto alla soluzione P7M.

2.1.1 Disponibilità diffusa di un verificatore gratuito

Nell'ottica di favorire la diffusione di strumenti per la firma digitale non si può ignorare la difficoltà che molti utenti possono trovare nel reperire un'applicazione di verifica di file con firma digitale P7M. Malgrado gli sforzi operati dal CNIPA e dai Certificatori Accreditati, sono ancora poche in numero assoluto le persone in possesso dei programmi in grado di verificare e leggere file P7M. Al contrario la stragrande maggioranza degli utenti di personal computer (circa il 90% secondo le stime più recenti) sono in grado di riconoscere un file PDF e di utilizzare il visualizzatore Adobe Reader gratuito, ottenendo implicitamente la possibilità di verificare le eventuali firme digitali in esso contenute.

2.1.2 Accesso immediato al documento firmato

Il documento PDF con firma digitale non subisce alcuna trasformazione in altro formato. Il formato P7M imbusta invece il documento firmato nascondendolo in un nuovo file e impedendo così l'accesso al documento a chi sia sprovvisto di un'applicazione compatibile. Per accedere al documento firmato P7M occorre inoltre "sbustarlo", con la conseguente duplicazione tra documento firmato e non firmato. Nel caso di documenti con più firme la duplicazione si moltiplica, essendo richiesti tanti sbustamenti quante sono le firme apposte al documento. È poi necessario considerare che sono di norma molte più le persone che necessitano di leggere e verificare documenti firmati da altri che non quelle che devono crearli e firmarli. Il formato PDF offre in definitiva funzionalità di firma digitale trasparenti rispetto all'esigenza primaria di accedere con facilità ai documenti firmati.

2.1.3 Gestione di firme multiple

Il formato PDF consente di apporre firme digitali multiple come sigilli alle revisioni o alle nuove versioni di un documento. Vi è perciò la possibilità di apportare modifiche al documento successive alla firma senza invalidare quest'ultima. Questa funzionalità, non disponibile con il formato P7M, sfrutta la caratteristica del PDF di effettuare il salvataggio incrementale dei dati ed è fondamentale quando la firma è utilizzata in processi in cui più persone collaborano ad un unico documento modificandolo e apponendovi la propria firma digitale in tempi successivi. Un ambito in cui questa caratteristica è indispensabile è quello della modulistica elettronica, dove i processi tipicamente prevedono che più persone interagiscano con lo stesso documento aggiungendo e sottoscrivendo i propri dati in tempi successivi.

2.1.4 Gestione dell'aspetto visivo della firma digitale nel documento

Questa caratteristica consente di associare all'operazione di firma digitale una rappresentazione grafica di informazioni mediante "campi firma" liberamente posizionabili all'interno delle pagine del documento. È possibile per esempio raffigurare l'autografo del firmatario oppure mostrare una semplice trascrizione dei dati distintivi del suo certificato di firma digitale. I "campi firma" permettono inoltre di contestualizzare l'apposizione di una firma digitale nel contenuto del documento, così come è naturale fare con un autografo su un documento cartaceo. Il caso esemplare è quello delle clausole vessatorie di un contratto, laddove una persona può essere chiamata ad esprimere un consenso anche più volte all'interno di un unico documento. Questa funzionalità è molto apprezzata anche come elemento di riduzione del "digital divide" verso coloro che non sono del tutto avvezzi alle tecniche informatiche e che spesso, con la gestione digitale dei documenti, temono di non vedere completamente rispettata l'espressione della propria volontà.

I campi firma consentono di contestualizzare la validità della firma a sezioni differenti di un documento. Più persone possono sottoscrivere parti diverse di un unico documento dando una chiara percezione di cosa ciascuno abbia sottoscritto, esattamente come avviene con la carta.

2.1.5 Possibilità di associare informazioni sul luogo e il motivo della firma

Questa funzionalità consente di comunicare la ragione per cui viene applicata una firma digitale ad un documento. Le informazioni, personalizzabili e opzionali, vengono sottoposte al processo di sottoscrizione in quanto sono firmate digitalmente con il documento e quindi forniscono un ulteriore contesto informativo per la firma digitale apposta al documento.

2.1.6 Possibilità di controlli sulle caratteristiche di una firma

I "campi firma" consentono anche di controllare le tipologie di firma apponibili ad un documento PDF. È possibile per esempio imporre all'utente l'uso di un particolare tipo di certificato di firma (ad esempio un certificato "qualificato" ovvero emesso da Certificatori conformi con quanto disposto dall'art. 27 del CAD.") oppure rendere obbligatoria la scelta del motivo della firma (magari per forzare una scelta tra "accetto le clausole" oppure "non accetto"). Il vantaggio è che questi controlli sono veicolati attraverso i documenti da firmare e non come caratteristiche dell'applicazione di firma utilizzata, come avviene con altre soluzioni. Questa caratteristica consente il massimo controllo delle funzioni di firma digitale, senza imporre complicazioni per la distribuzione o l'aggiornamento di applicazioni dedicate.

2.1.7 Garanzia di interoperabilità riconosciuta a livello nazionale e internazionale

Lo scopo dell'interoperabilità della firma digitale è favorirne l'utilizzo esteso, indipendentemente dal tipo di certificato, dal dispositivo di firma o dall'applicazione di firma. A tale scopo, in Italia, il CNIPA ha introdotto nella normativa dapprima il riconoscimento del solo formato P7M, consentendo un sostanziale allineamento dei servizi e delle applicazioni fornite dai Certificatori qualificati, e più recentemente con la Deliberazione n.4/2005 ha stabilito la possibilità di estendere ad altri il riconoscimento di "formato legale". Il formato PDF è stato riconosciuto come formato di firma digitale opponibile a terzi mediante la stipula di un Protocollo d'Intesa tra CNIPA e Adobe siglato il 16 febbraio 2006.
Al di fuori della realtà italiana, la mancanza di regolamentazione ai fini dell'interoperabilità per la firma digitale contribuisce all'utilizzo del PDF, formato già ampiamente diffuso per la gestione documentale in ambito internazionale. Dal punto di vista applicativo il formato PDF è in grado di gestire firme apposte mediante l'uso di certificati e dispositivi di firma diversi tra loro senza presentare alcun problema di interoperabilità, a differenza di altre soluzioni che tendono a non consentire l'utilizzo di dispositivi di firma differenti da quello fornito dal produttore dell'applicazione.

Uscendo dall'ambito nazionale, questa esigenza si rafforza ulteriormente non esistendo iniziative di interoperabilità volte a favorire una compatibilità tra applicazioni disponibili a livello di nazioni.

Il formato PDF in questo senso gioca un ruolo di primaria importanza per consentire la piena e libera circolazione di documenti sottoscritti digitalmente, consentendone la verifica con il solo Adobe Reader.

2.1.8 Controllo implicito della dinamicità del documento

Alcuni dei prodotti più utilizzati per la produzione di documenti e di fogli di calcolo non sono in grado di proteggerli da modifiche apportate da macro o altro codice in essi annidati. Queste istruzioni non sono visibili all'utente, specialmente a quello meno esperto, e possono a sua insaputa produrre modifiche alla "presentazione" del documento stesso. Per esempio, una fattura emessa per 1000 euro può diventare di 10.000 euro senza alcun intervento sulla stringa di bit che compongono il documento e quindi senza che la firma digitale ne sia inficiata. Solo per determinati formati semplici (TIFF, TXT) il visualizzatore nativo è esente da tali rischi. Questo limita la capacità di controllare ciò che accade al documento generato dai tipi di prodotti, citati sopra, appena prima dell'apposizione della firma o appena dopo la sua verifica. Infatti vi è una netta separazione tra la gestione operata dal programma di firma e quella svolta dal visualizzatore durante la quale il programma di firma perde il controllo della staticità della rappresentazione del documento. Questo ha contribuito ad alimentare i timori per quei documenti che incorporano elementi "dinamici" (quali macroistruzioni o altro codice eseguibile), in grado cioè di mutare l'aspetto del documento all'insaputa del programma di firma digitale e anche dell'utente. Nel PDF, essendo la firma supportata nativamente, il visualizzatore (Adobe Reader) identifica, segnala e addirittura può evitare all'utente ogni eventuale alterazione successiva alla verifica di una firma digitale.

2.1.9 Possibilità di associare una marca temporale alla firma

La marca temporale è tecnicamente una firma digitale, associata al documento da una terza parte fidata, che possiede la caratteristica di collegare un identificativo del documento (il suo digest) a un momento (data e ora) determinato in modo affidabile. Il suo scopo è collocare temporalmente il documento oggetto della marcatura. Mentre la firma digitale non è in grado di stabilire l'esistenza di un dato documento in un preciso istante (ma solo la sua integrità ed autenticità), la marca temporale lo consente proprio grazie all'informazione temporale rilasciata dalla terza parte fidata.

La normativa italiana prevede che i Certificatori Accreditati possano rilasciare servizi di marcatura temporale ricorrendo a sistemi compatibili con il protocollo RFC3161. Purtroppo però non è stata definita una modalità comune e interoperabile comune con cui rappresentare in modo univoco le marche temporali associate ad un dato documento. Permangono perciò sul mercato soluzioni che appongono marche temporali ai documenti con modalità tra loro incompatibili, con conseguente assenza di interoperabilità tra i diversi operatori: alcune soluzioni per apporre la marca temporale imbustano ulteriormente il file già firmato, mentre altre rappresentano la marca temporale mediante un file separato dal documento.

Il formato PDF consente di associare una marca temporale in formato RFC3161 ad una firma digitale. Questo significa che il file firmato e marcato temporalmente continua ad essere un file PDF senza l'aggiunta di suffissi o file esterni al documento.

Anche per la marca temporale continua inoltre a valere quanto detto per la firma digitale: il controllo della validità della marca temporale è svolto con continuità dall'applicazione di visualizzazione (Adobe Reader) ed ogni variazione nella staticità del documento è identificata e segnalata all'utente.

Infine, ma non meno importante, la soluzione PDF consente di realizzare una piena interoperabilità tra i servizi di marcatura temporale offerti dai Certificatori, eliminando l'onere a carico degli utenti di dotarsi dei differenti prodotti di verifica in grado di leggere le diverse tipologie di formati in uso.

2.1.10 PDF: un formato all-in-one ideale per molteplici applicazioni

Il formato PDF consente di incorporare in un unico file tutte le caratteristiche di un documento elettronico evoluto. Oltre alla firma digitale e alla marca temporale, è possibile inglobare anche dati strutturati in formato XML.

Questa caratteristica consente di realizzare applicazioni efficienti nell'ambito di soluzioni quali il Protocollo Informatico e la Fatturazione Elettronica.

Nel caso del Protocollo Informatico, in un unico file PDF è possibile memorizzare il documento vero e proprio unitamente alla cosiddetta "segnatura di protocollo", un file XML che ne rappresenta i dati anagrafici del sistema di protocollatura.

Nell'applicazione di Fattura Elettronica il file PDF unisce alla nota qualità di presentazione delle informazioni testuali e grafiche la capacità di trasportare la firma

digitale del soggetto emittente, la marca o il riferimento temporale e infine i dati contabili in formato XML, secondo le specifiche definite da standard di mercato quale il CBI (Corporate Banking Interbancario - *www.acbi.it*)

3. In breve

Ad oggi, la soluzione PDF per la firma digitale non ha eguali in nessun altro formato per quanto riguarda l'usabilità e le funzionalità.

Il formato PDF si affianca al P7M il quale, essendo l'unico formato in uso in Italia fino al febbraio 2006, ha guadagnato una posizione di leadership indiscutibile in quanto a diffusione, anche favorito dal non essere necessariamente associato ai prodotti di uno o più fornitori, venendo implementato attraverso vari tool di sviluppo tra cui anche alcune librerie open source. Il CNIPA stesso però prevede nei prossimi anni la graduale diffusione del formato PDF per la rappresentazione di firme digitali proprio in virtù delle sue caratteristiche esclusive che soddisfano parecchi requisiti non supportati dal formato P7M. Bisogna però segnalare che per potere scambiare documenti PDF firmati con una Pubblica Amministrazione è necessario che essa comunichi ufficialmente tale possibilità, anche sul proprio sito web.

3.1 F.A.Q.

Si fa spesso una certa confusione tra i termini "formato PDF", "Adobe Acrobat" e "documenti PDF" (prodotti o manipolati da Adobe Acrobat e da altri software), o quanto meno li si considera la stessa cosa. Le tre entità sono invece decisamente distinte, anche se presentano punti in comune. È vero per esempio che Adobe Acrobat produce documenti in formato PDF, ma è altrettanto vero che un file PDF prodotto da un'altra applicazione (o addirittura "scritto a mano") può essere profondamente differente dai PDF di Adobe Acrobat.

Qualsiasi caratteristica che non sia inclusa nelle specifiche del formato PDF, ma particolare o addirittura esclusiva di Adobe Acrobat non va vista come una proprietà generale del formato, ma solo come una sua possibile applicazione. Le domande e risposte che seguono rappresentano una sintesi di quesiti e osservazioni che sono state raccolte tra gli utenti e che si ritiene opportuno chiarire ed approfondire per contribuire alla diffusione della conoscenza su un argomento così specifico come la firma digitale che sempre più diventa argomento di discussione anche tra non esperti di tecnologia o diritto.

D: La firma di file inclusi in una busta PKCS#7 comporta l'aggiunta al file originario di circa 4 Kbyte. Per la firma in un file PDF vengono aggiunti almeno 16 Kbyte più un ulteriore carico, se si utilizza anche il simbolo grafico (immagine della firma), che varia in funzione della risoluzione e dei colori impiegati. In casi estremi, il "peso" del documento può dunque aumentare di diverse centinaia di Kbyte, è vero?
R: Quest'affermazione necessita di chiarimenti.
La firma nel PDF è tecnicamente un PKCS#7 di tipo "detached", perciò equivalente al formato P7M (qui chiamato "busta PKCS#7") dal punto di vista computazionale.
Le eventuali differenze possono essere ricondotte al fatto che Adobe Acrobat prevede l'inserimento nell'oggetto PKCS#7 di tutta la catena completa dei certificati, operazione non necessariamente svolta da altri programmi che generano file firmati in formato P7M. In realtà questa operazione è facoltativa nel formato PDF ed è quindi possibile produrre PDF firmati nativamente dalle dimensioni sostanzialmente equivalenti a quelle di un PDF firmato in P7M.
Il simbolo grafico aggiunge al file la sua dimensione, ma questo è ovvio se si vuole ottenere una funzione così utile e accattivante, del resto assolutamente facoltativa secondo il formato PDF (ed anche con Acrobat). Va, infine, sdrammatizzata questa affermazione, in quanto, molto spesso, a parità di caratteristiche grafiche un documento in formato PDF è di dimensioni inferiori a quelle del formato originario, per cui le cose si possono ritenere ampiamente compensate.

D: Apporre più firme allo stesso documento può apparire una pratica alquanto complessa e complicata. Innanzitutto, le firme successive modificano il file e la verifica della prima firma è comunque possibile, ma potrebbe essere fuorviante per utenti poco esperti. Particolari opzioni di firma impediscono di aggiungerne altre. Le firme sono solo ricorsive, ovvero non è possibile la firma congiunta e paritetica permessa invece nella busta PKCS#7 che ha un "content" unico ed una zona per le firme. È così?

R: Nello sviluppo delle funzionalità di firma per il formato PDF, Adobe ha sempre considerato il concetto di "carta elettronica" come metafora della carta fisica. Ciò può avere come conseguenza che molte scelte architetturali del formato possono rappresentare scenari differenti da quelli ispiratori di altri formati di firma ma è comunque vero che firme multiple possono essere apposte con estrema facilità, come apporne una sola.
La possibilità di apporre più firme ad un unico documento non va vista in modo negativo. È a paragone molto più problematico il fatto che nel formato P7M per ogni firma apposta ad un documento venga creata una nuova "busta crittografica" intorno al file, con la conseguenza di avere alla fine una "matrioska" di firme che costringe a ripercorrere con una certa complessità il procedimento contrario in fase di verifica. Senza considerare che ad ogni passaggio viene creato un nuovo file che, di fatto, è ancora un file intermedio di difficile interpretazione per l'operatore umano.
Con il PDF le firme multiple sono gestite in modo trasparente per l'utente che le ritrova tutte elencate in ordine cronologico di apposizione in un unico pannello firme di facile lettura nell'unico file PDF, fruibile nello stesso identico modo di un PDF non firmato. È possibile, inoltre, verificare tutte queste firme con Acrobat Reader, senza alcun costo e senza alcuna difficoltà anche per l'utente che ignori i meccanismi della firma digitale.
Corretta è la segnalazione della mancanza della firma paritetica, sebbene sarà oggetto di una futura rivisitazione del formato PDF. Ad oggi, questa non appare comunque una mancanza rilevante nella quasi totalità dei processi a cui la firma digitale viene applicata.
Al contrario, le firme ricorsive rappresentano la tipica sequenzialità di apposizione di firme multiple ad un foglio di carta nella normale esperienza quotidiana. Va sottolineato, infine, che è una scelta del primo firmatario impedire l'aggiunta di altre firme e questo non è certo un impedimento, ma un'ulteriore misura di sicurezza.

D: La firma, inclusa in un documento in formato PDF, altera l'impronta del documento, il che implica la non verificabilità nei sistemi di protocollo informatico secondo le specifiche AIPA (ora CNIPA)?
R: Normalmente un documento prima si firma e poi viene protocollato. Anche la penna che firma un foglio di carta lo modifica, il P7M altera addirittura l'intero documento oggetto della firma, nascondendolo dentro la busta crittografica e cambiando estensione al file rendendolo nuovamente leggibile solo mediante l'elaborazione da parte di un programma specializzato. Questo sembra proprio essere un falso problema, infatti l'alterazione nel PDF si risolve in due necessarie modifiche: la creazione del cosiddetto "campo firma" (l'equivalente dell'inchiostro per la firma su carta) e la "nicchia" nel file all'interno della quale viene iniettato il PKCS#7 detached che costituisce la firma vera e propria.
Non viene quindi inficiata la verificabilità laddove si utilizzino sistemi di protocollo: questi possono prendere in carico un file PDF firmato nativamente come farebbero con qualsiasi altro documento elettronico.

D: Utilizzando la firma digitale nativa in PDF non è possibile apporre la marca temporale all'interno del documento, ma solo all'esterno costringendo perciò ad avere un client fornito dalle CA.
Dall'interno di Acrobat non si richiede la marca temporale, ma viene aggiunto solo il riferimento temporale basato sulla data e ora del computer, inaffidabile e non valido ai fini dell'opponibilità a terzi e della validità nel tempo quando il certificato di firma usato sarà scaduto.
In caso di firme multiple l'eventuale marca temporale aggiunta con un file esterno non è più verificabile in quanto il file risulta alterato rispetto a quanto marcato dopo la prima firma. È vero tutto questo?
R: A partire dalla versione 1.6 delle specifiche del formato PDF (supportata a partire dalla versione 7.0 di Adobe Acrobat) è stata introdotta la possibilità di apporre al documento una o più marche temporali associate a firme digitali. La marca è conforme all'RFC3161 (standard di riferimento per questo tipo di servizio) e supporta pienamente i servizi per i Certificatori che sono conformi a questa specifica.
Aggiungere alla firma il "SigningTime" è una pura scelta del firmatario. In ogni caso, il file ottenuto è ancora un PDF leggibile e verificabile con il Reader gratuito, a beneficio dell'usabilità della soluzione e della sua interoperabilità e indipendenza dal fornitore di servizi.

D: La firma si può apporre solo con Adobe Acrobat, mentre con Adobe Reader si può solo verificare la firma. La produzione di PDF firmati in maniera automatica, per esempio fatture, costringe all'uso di strumenti di sviluppo costosi. Gli strumenti di creazione

PDF a basso costo, come quelli gratuiti sarebbero a questo punto esclusi. Pur avendo un sistema di alto costo da gestire, per l'apposizione delle marche temporali occorrerebbe sempre dotarsi di un client esterno. È così?
R: Essendo il formato PDF aperto e pubblico, è sempre possibile che prodotti alternativi ad Adobe Acrobat siano migliorati fino a supportare funzioni evolute come la firma digitale. Al momento esistono già alcuni tool open source in grado di apporre la firma secondo il formato PDF. Ma Adobe Acrobat ha funzioni ben più numerose e produttive della sola firma digitale. In ogni caso, anche con il software gratuito Adobe Reader è possibile, in determinate condizioni, apporre firme digitali e marche temporali, oltre che verificarle, senza gravare di alcun onere economico il firmatario. Questa possibilità è data dalla tecnologia Adobe Reader Extensions che comporta un costo soltanto per chi attiva il documento da firmare (per esempio un modulo di raccolta dati, come quelli proposti alcuni enti pubblici) e nessun costo per chi lo compila e firma con Adobe Reader.

D: Si possono riscontrare problemi con i font inclusi (o esclusi) nel file firmato? La rappresentazione di quanto firmato può variare presentando font diversi nel sistema in cui il file è stato firmato e in quello in cui viene effettuata la verifica della firma?
R: Assolutamente no, è vero il contrario. Una delle caratteristiche principali del documento PDF è appunto la capacità di inglobare al suo interno tutti gli elementi in grado di garantire stabilità di presentazione grafica indipendentemente dalla piattaforma e dall'applicazione di origine. Adobe Acrobat supporta pienamente set di caratteri sia orientali sia europei, perciò non si vedono i problemi segnalati; anzi sono disponibili garanzie di portabilità e di compatibilità superiori a quelle di qualsiasi altro formato documentale.

D: Per l'apposizione della firma digitale nativa in PDF esistono alcune limitazioni in merito ai contenuti:

- I contenuti audio e video non sono consentiti;
- JavaScript e avvio di file eseguibili non sono consentiti;
- Tutti i font devono essere inclusi nel file e devono essere legalmente includibili per uso universale;
- I colori devono essere definiti in modalità indipendente dal dispositivo;
- La crittografia non è consentita.

È vero tutto questo?
R: Quanto rilevato si può riferire al formato PDF/A. Se è così, è scorretto il riferimento al formato PDF per la firma digitale.
Il PDF/A (lo standard PDF/A-1, altrimenti noto come ISO 19005-1, basato sulla specifica PDF 1.4) è una profilazione del formato PDF intesa per l'archiviazione a lungo termine di documenti elettronici. In essa il gruppo di lavoro ISO (costituito da rappresentanti delle maggiori aziende dell'IT mondiale e di prestigiose istituzioni governative e accademiche) ha ritenuto di rendere necessario, o di impedire, l'uso di talune caratteristiche del formato PDF con lo scopo di garantire la stabilità della presentazione dei contenuti del documento nel tempo. Questo non significa che non sia possibile firmare digitalmente un file PDF/A oppure che un PDF firmato debba necessariamente essere conforme allo standard PDF/A o alla versione PDF 1.4.
Gli elementi elencati nella domanda sono di norma "nemici" della longevità del documento perciò occorre scegliere se privilegiare il loro utilizzo oppure ottenere la garanzia di stabilità del documento nel tempo.
In entrambi i casi sarà sempre possibile apporre la firma digitale.

Per ulteriori informazioni sulla firma digitale con il formato Adobe PDF, consultare:
www.adobe.com/it/firmadigitale

Better by Adobe.™

Adobe

Adobe Systems Italia
Centro Direzionale Colleoni, Palazzo Taurus A3
Viale Colleoni, 5 - 20041 Agrate Brianza (MI)
www.adobe.com/it