IDC
Analyze the Future

WHITE PAPER

Firma Digitale e formato PDF: evoluzione normativa e prospettive di applicazione

Sponsored by: **Adobe Systems**

Analista: Fabio Rizzotto

Gennaio 2007

WHITE PAPER

Firma Digitale e formato PDF: evoluzione normativa e prospettive di applicazione

Sponsored by: **Adobe Systems**

Analista: Fabio Rizzotto

Gennaio 2007

WHITE PAPER

Firma Digitale e formato PDF: evoluzione normativa e prospettive di applicazione

Sponsored by: Adobe Systems

IDC OPINION

Nell'ottica di una crescente introduzione dell'innovazione all'interno delle procedure di business, la firma digitale può consentire di estendere i benefici e il valore della gestione documentale, creando sinergie tra informazioni, tecnologie e processi.

La firma digitale non è stata la prima, e non sarà l'ultima, delle innovazioni con le quali individui e imprese (private e pubbliche) si sono confrontati negli ultimi anni. Le potenzialità di questa tecnologia sono numerose come i suoi campi di applicazione; altrettanto importanti sono i benefici in termini di automatizzazione delle procedure.

In questo scenario, particolare attenzione merita il protocollo di intesa tra il **Cnipa** (Centro nazionale per l'informatica nella pubblica amministrazione) e **Adobe Systems**, siglato nel febbraio 2006, che riconosce il **PDF** come formato valido ai fini della firma digitale. Si ritiene che l'apertura al formato PDF – che si affianca in questo modo al formato **PKCS#7** (il cosiddetto "**P7M**", il primo e unico standard previsto fino al 2005) possa contribuire ad accelerare l'innovazione, tramite la firma digitale, delle procedure a forte caratterizzazione documentale.

Il riconoscimento di Adobe PDF appare di particolare rilevanza in virtù non solo dei requisiti posseduti dal formato, ma anche della possibilità di far leva su un **fattore abilitante** quale il software **Adobe Reader** gratuito per la fase di verifica della firma digitale. La presenza del Reader, già ampiamente diffusa nelle organizzazioni, introduce elementi di **semplicità** per il riconoscimento delle firme digitali. La familiarità già acquisita dagli utenti può giocare un ruolo positivo per quella "presa di coscienza" che spesso ha rallentato l'introduzione delle nuove tecnologie.

Se l'apertura a nuovi formati è riconosciuta come un driver per lo sviluppo della firma digitale, è altrettanto vero che questa evoluzione dovrà confrontarsi con un contesto, quello della privacy e della sicurezza dei dati personali, che le continue minacce dell'era digitale tendono a rendere più vulnerabile.

Non va trascurato il fatto che la dimensione "digitale" della propria firma è, per molti, un grande passo logico, che spesso richiede di scardinare resistenze di carattere personale ed emotivo. La diffusione della firma digitale ad oggi ha già dimostrato che è possibile smontare la teoria della inconciliabilità tra evento originale, fisico (firma autografa) e procedura di apposizione digitale. La replicabilità dell'evento in una dimensione "virtuale" è possibile e la sua piena realizzabilità avrà bisogno anche di una sorta di "offensiva" comunicativa e culturale, che faccia capire quale ruolo possa rivestire la firma digitale e la disponibilità di nuovi formati di supporto, come il PDF, nella costruzione di processi documentali innovativi.

IN THIS WHITE PAPER

L'evoluzione delle tecnologie informatiche e i passi compiuti verso l'efficienza dei processi documentali

Di fronte ai mutamenti radicali dei mercati e agli scenari evolutivi, è naturale interrogarsi su ruolo e importanza che la gestione documentale possono giocare ai fini dell'efficienza e della produttività delle organizzazioni. La strada verso la **dematerializzazione** dei documenti è appena stata intrapresa e molto rimane da fare per allineare i processi documentali alle mutate esigenze di business.

Le nuove soluzioni tecnologiche hanno comunque già consentito un adeguamento dei sistemi informativi aziendali verso modelli più flessibili e al servizio dei processi. Ma come si realizza una strategia di gestione di documenti e contenuti che contempli le molteplici esigenze di business delle organizzazioni?

Diverse variabili entrano in gioco: i processi documentali risentono di fattori interni di carattere organizzativo, procedurale e infrastrutturale, e di aspetti esterni (ritmi tecnologici, normativa, mercati di sbocco). Di conseguenza, opportunità e percorsi di sviluppo risultano differenziati per aziende pubbliche e private, per settore o dimensione.

Esistono tuttavia principi evolutivi che accomunano tutte le organizzazioni e che ruotano attorno al concetto di **ciclo di vita** dei documenti: la sfida più grande per il futuro sarà individuare e strutturare percorsi, flussi di entrata/uscita e modelli di "collocazione" finali non solo coerenti con il business, ma il cui mantenimento e la cui evoluzione possano essere automatizzati, ovvero gestiti con limitati interventi manuali.

Grandi passi sono stati compiuti verso la **digitalizzazione** dei contenuti, tuttavia fino a qualche anno addietro è prevalsa una valenza "**statica**" dell'innovazione dei processi documentali (si pensi alla scansione, all'archiviazione dei documenti), mentre molto resta ancora da compiere per una reale sinergia tra piattaforme documentali e procedure di business.

Bisogna ancora, da un lato, investire nell'ottimizzazione del **workflow**, dall'altro rendere i documenti stessi più "**dinamici**" (*active* o *intelligent document*), il cui formato sia in grado di alimentarsi di contenuti e funzionalità a seconda delle fasi del proprio ciclo di vita (si pensi a funzioni interattive, di validazione e di calcolo automatico, piuttosto che alla possibilità di apporre una **firma digitale**).

In questi ultimi anni si è osservato come uno dei principali ostacoli all'efficienza dei processi documentali è, appunto, la mancanza di flussi strutturati, che insieme alle problematiche di "change management" possono diventare un rompicapo per i responsabili aziendali. Il tempo sta favorendo una progressiva "appropriazione" dell'innovazione da parte dei processi, nonché maggiore consapevolezza presso gli utenti, elementi di buon auspicio per gli obiettivi di efficienza e produttività.

La trasposizione di un processo dal contesto tradizionale a quello digitale rappresentano una grande opportunità non soltanto per le imprese private ma anche per la **Pubblica Amministrazione**. L'adeguamento dei sistemi informativi e il lancio di nuove iniziative online verso il cittadino devono essere mossi da elevati principi di **sicurezza**, affidabilità e, sempre più, di **interoperabilità**, per consentire integrazione

e normalizzazione dei processi all'interno del più ampio ecosistema delle strutture pubbliche.

Proprio in questo contesto, uno dei primi processi documentali su cui si è investito negli anni scorsi è stato il **protocollo**. L'automatizzazione della fase di ingresso dei documenti (protocollo informatico) ha permesso di superare i limiti della tradizionali modalità di registrazione, sostituendo al registro cartaceo un sistema di gestione e archiviazione basato sulla digitalizzazione degli originali e, successivamente, sulla trasmissione automatizzata dei documenti.

Protocollo e workflow sono parti essenziali di un processo ben più ampio e complesso che invade la sfera non soltanto delle organizzazioni ma anche quella **individuale**. Il Centro nazionale per l'informatica nella pubblica amministrazione (CNIPA) ha da tempo dettato le linee guida per l'ammodernamento dei processi pubblici, non solo a carattere interno ma anche di quelli rivolti al **cittadino**.

L'evoluzione tecnologica richiede quindi il supporto di standard e normative che la rendano "applicabile", ne definiscano le regole di diffusione, i contorni e i percorsi alternativi di sviluppo. Ma soprattutto i recenti interventi del legislatore hanno avuto l'obiettivo di elevare i documenti digitali **allo stesso piano** dei documenti cartacei ai fini della **validità legale** nell'ambito di specifici processi.

In tema di gestione documentale gli ultimi anni sono stati molto ricchi di produzione legislativa. Solo per fare qualche esempio si pensi ai seguenti:

- la "**conservazione digitale sostitutiva**", che ha di fatti legalizzato il documento informatico, equiparandolo a quello cartaceo ai fini della validità normativa. La "conservazione digitale sostitutiva" è uno strumento alternativo alla gestione cartacea e rappresenta una grande opportunità di snellimento dei volumi ed efficientamento dei processi documentali. Particolarmente importante è infatti la validità giuridica nel tempo, che assolve all'obbligo di conservazione pluriennale, garantita dalla marcatura temporale;

- la "**posta elettronica certificata**", che consente di attribuire valore legale all'invio e alla ricezione di documenti via e-mail. In tal modo la posta elettronica può diventare "posta certificata" e fungere ad esempio da normale raccomandata con avviso di ricevimento, fornendo attestazione del momento di invio, della consegna e del contenuto del messaggio consegnato;

- la possibilità di apporre una "**firma digitale**" a un documento informatico. Il legislatore è intervenuto per regolamentare l'utilizzo della firma digitale all'interno del documento informatico già nel 1997 (D.P.R. 513/97 e successive integrazioni).

La firma digitale e i processi documentali: gli scenari applicativi e il protocollo di intesa CNIPA – Adobe Systems

Dal punto di vista operativo, la firma digitale è il risultato di un processo realizzato attraverso una procedura informatica (cosiddetta validazione) che consente al sottoscrittore (tramite una chiave privata) di apporre la propria firma su uno o più documenti informatici e al destinatario di verificare la provenienza e l'integrità della stessa (tramite una chiave pubblica). Il sistema delle "chiavi" (cosiddette asimmetriche) deve essere certificato da un Ente (certificatore). La generazione della

firma avviene attraverso un apposito dispositivo (tipicamente una smart card o un token USB). Queste condizioni sono indispensabili per assicurare i tre requisiti di base che caratterizzano la firma digitale:

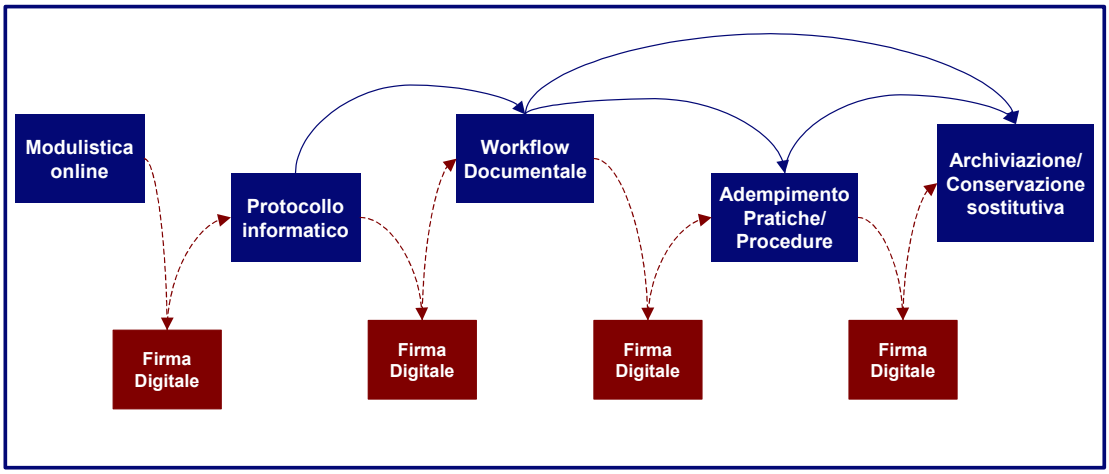
- **autenticità**, che riporta alla necessità di assicurare la certezza circa l'autenticità di chi sottoscrive il documento;
- **integrità**, ovvero la garanzia della protezione del contenuto del documento una volta apposta la firma;
- **non ripudio**, ovvero l'obbligo per il sottoscrittore di riconoscere una firma digitale da lui apposta. In pratica, questo principio assicura che l'apposizione non venga disconosciuta.

La firma digitale rappresenta una forma di firma elettronica cosiddetta "**pesante**", ovvero con piena validità giuridica a differenza di firme più "deboli" quali quella "elettronica generica" ed "elettronica avanzata", le quali nonostante le proprie caratteristiche (integrità per la prima, autenticità più integrità per la seconda) non vantano piena validità come la firma autografa (manca il requisito del "non ripudio").

La firma digitale rappresenta una grande opportunità per integrare le piattaforme tecnologiche di Document e Content Management con quei processi ancora caratterizzati da una forte componente manuale, fornendo un contributo prezioso all'innovazione dei servizi al cittadino, alle esigenza di interoperabilità tra enti pubblici e all'efficienza del ciclo di vita documentale nel suo complesso, anche nell'ambito delle organizzazioni private. Si veda a tal proposito l'esemplificazione presentata nella Figura 1, la quale mostra le possibilità per la firma digitale di "disarticolare" processi già parzialmente automatizzati, favorendo una reale integrazione tra procedure, informazioni e tecnologie.

FIGURA 1

Schema ipotetico di processo documentale e ruolo della firma digitale



Fonte: IDC, 2007

Come si è accennato, gli Enti Certificatori (Certification Authority) si occupano in modo specifico di servizi associati allo sviluppo e gestione di sistemi a chiave pubblica (PKI – Public Key Infrastructure) o firma digitale, secondo le regole dettate dalla normativa italiana. Esse assolvono il ruolo di "terza parte fidata". L'intervento del

Certificatore consente infatti di andare oltre la pura autenticazione (possibile attraverso la firma elettronica) per assicurare quella certezza legale che rende la firma digitale "non ripudiabile" e con medesima validità legale della firma autografa.

Molte delle Certification Authorities sono anche società di servizi IT, che hanno aggiunto alla propria offerta tradizionale di servizi di sicurezza anche il rilascio di policies e prodotti collegati alla gestione dei certificati digitali (PKI). Tra i loro obiettivi rientra anche quello di assicurare la piena interoperabilità dei certificati emessi relativamente non solo alla firma digitale, ma anche alla posta elettronica certificata (PEC).

Per il **cittadino**, la gestione di tutte quelle pratiche da evadere tramite la PA e che richiedono la sottoscrizione di una dichiarazione può passare sotto il controllo della firma digitale (modifiche a certificati anagrafici, denunce, richieste a norma di legge). Si tratta in questi casi di far tesoro dei progetti sperimentali in corso, dei fattori di successo e delle criticità, al fine di creare quel circolo virtuoso che, da un lato, ripropone un modello innovativo di servizio presso altri Enti, dall'altro alimenta maggiore fiducia presso l'utente finale.

I campi di applicazione per il **cittadino** spaziano anche oltre la relazione con il mondo pubblico: si pensi ad esempio alla gestione dei rapporti con banche e istituzioni finanziarie relativamente a servizi di Internet banking, online trading etc. La crescente diffusione dei servizi di home banking aumenta anche i rischi per la sicurezza: si pensi ad esempio al **phishing**, ovvero alle tecniche illegali utilizzate per ottenere l'accesso ad informazioni personali e riservate con l'obiettivo di violare e appropriarsi dell'identità altrui. Un problema rilevante, alla cui soluzione possono contribuire strumenti "forti" tra cui anche la **firma digitale**.

Le principali applicazioni che spingono l'adozione della firma digitale presso le **aziende private** sono legate a:

- scambio di documenti rilevanti con le Pubbliche Amministrazioni;
- applicazioni di eBusiness (ad esempio, la firma digitale su fatture elettroniche);
- conservazione a norma di legge, deposito telematico di bilanci presso le Camere di Commercio, Gestione della Contrattualista, Commesse e proposte di commesse, Modulistica.

In generale, un **driver** sarà in futuro la maggiore diffusione di dispositivi hardware di autentificazione (token, mouse con lettore d'impronta, strumenti biometrici, oltre ovviamente alle smart card). Nella categoria delle smart card rientrano, oltre a smart card di PKI aziendali, anche la carta d'identità elettronica e le cosiddette carte regionali/nazionale dei servizi, tutte innovazioni in grado di dare una spinta positiva alla diffusione di una cultura digitale applicata anche all'ambito personale.

La regolamentazione della firma digitale risale al 1997 ma è solo a metà anno 2000 che viene introdotto il formato di imbustamento **PKCS#7** (il cosiddetto "**P7M**") come standard unico per la firma digitale nel nostro Paese.

Di fatto, le caratteristiche di standard unico del P7M hanno evitato il proliferare di tecniche alternative per l'apposizione della firma digitale. È altrettanto vero che l'esigenza di identificare un modello unico per rispondere ai requisiti di sicurezza ha di fatti rallentato le opportunità di una diffusione più rapida.

Con l'evoluzione delle tecnologie e dei supporti di gestione dei flussi documentali si è reso opportuno introdurre nuove forme di regolamentazione, al fine di allargare le specifiche per la firma digitale ad altri formati. In particolare il Cnipa ha recentemente iniziato a introdurre nuove direttive per regolamentare l'utilizzo della firma digitale, che hanno riguardato i seguenti formati:

- **PDF** (Portable Document Format);
- **XML** (Extensible Markup Language), il linguaggio di riferimento per la strutturazione e lo scambio di dati.

All'inizio del 2006 è stato sancito un **protocollo di intesa** tra CNIPA e Adobe Systems Inc, in base al quale il formato **Adobe PDF** viene riconosciuto valido ai fini della firma digitale. L'accordo appare **significativo** per diverse ragioni:

- estende innanzitutto il riconoscimento a un formato diverso dal P7M, il primo e unico istituito nel 2000 e che ha guidato la diffusione della firma digitale allo stato odierno. Le indicazioni normative lasciavano aperta la possibilità di ulteriori formati per la firma digitale;
- riconosce al formato PDF quelle caratteristiche definite grazie alla Delibera CNIPA n. 4 del 2005, che ha dettato le regole per il riconoscimento e la **verifica** dei documenti informatici. In questa accezione, la disponibilità di specifiche pubbliche del formato e di **Adobe Reader**, diffuso pressoché in ogni organizzazione, rappresenta un validissimo attributo ai fini dell'estensione "**immediata**" degli strumenti di verifica di firma digitale.

Il formato PDF e la sfida della sicurezza del documento elettronico

La storia dell'innovazione insegna come l'introduzione di tecnologie abilitanti (si pensi a Internet) sia in grado di contribuire non solo allo sviluppo di nuove applicazioni, ma di dare anche impulso all'evoluzione dei modelli di vita nella società contemporanea.

La firma digitale è un'applicazione potenzialmente in grado di estendere la valenza digitale dei processi documentali, grazie alla possibilità di automatizzare quelle fasi del ciclo di vita, a forte impatto in termini di privacy e sicurezza, che non consentono ancora la completa automatizzazione delle procedure (determinando un effetto "**discontinuità**" sull'Information Life-cycle).

Dopo i primissimi anni in cui la firma digitale è rimasta nell'alveo della (quasi) sperimentazione e il maggiore impulso avvenuto tra il 2004 e il 2005, si ritiene che l'accordo **Cnipa-Adobe** possa rappresentare un momento di discontinuità positivo, in grado di dare una scossa alle trasformazioni che hanno invaso la gestione documentale.

A partire dal 1999 Adobe Systems ha iniziato ad arricchire il formato PDF con funzionalità di supporto alla firma digitale. Si evidenziano di seguito alcune delle caratteristiche del **formato PDF** ai fini del suo impiego per la firma digitale:

- la vastissima diffusione di **Adobe Reader**, che funge anche da **strumenti di verifica** della firma digitale, è determinante in quanto consente di estendere in maniera esponenziale il numero di utenti in grado di poter verificare una firma

digitale, se confrontato con la diffusione attuale di tools di verifica di firma digitale con il sistema P7M;

- grazie alle sue proprietà, il PDF assicura un contributo alle esigenze di interoperabilità della firma digitale. Il problema dell'interoperabilità nasce dalle possibili difficoltà di lettura e interazione tra certificati e dispositivi di firma diversi e soprattutto supportati da applicazioni diverse;

- il formato PDF consente di "**contestualizzare**" la firma digitale tramite "Campi Firma" che possono essere personalizzati dal punto di vista della collocazione grafica all'interno del documento;

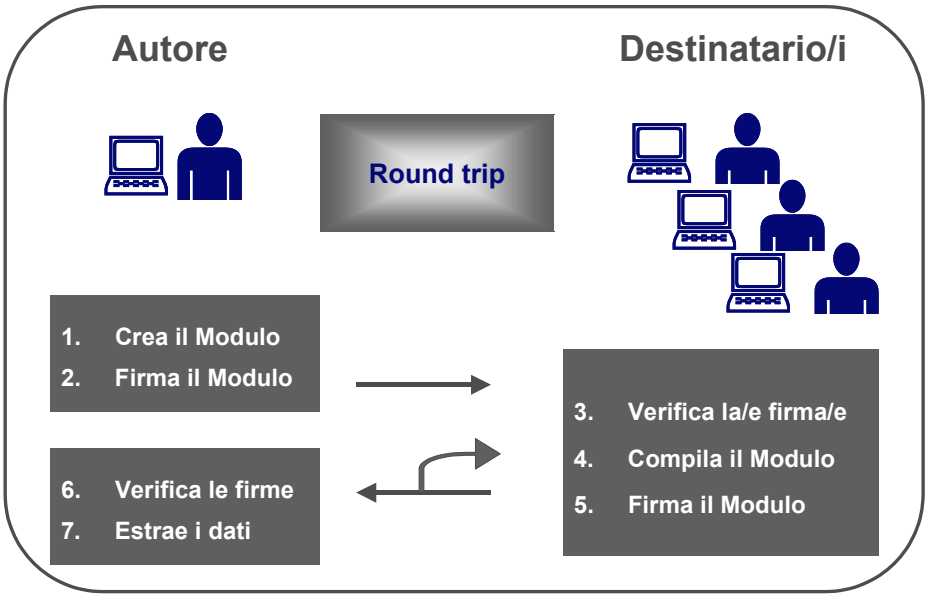
- supporta il trasporto di dati e metadati strutturati in formato **Xml**;

- è possibile apporre **firme multiple** al documento, intese come possibilità di firmare il documento successivamente all'apposizione della prima firma, da parte del sottoscrittore ma anche di altre persone che ad esempio sono coinvolte in processi collaborativi (iter di autorizzazione e approvazione).

La figura 2 illustra le possibilità di utilizzo della firma digitale nell'ambito di processi di collaborazione complessi, in cui può essere richiesta anche l'apposizione di firma multiple.

FIGURA 2

Esemplificazione di utilizzo della firma digitale in processi di approvazione complessi



Fonte: IDC-Adobe, 2006

Si ritiene che il **riconoscimento del PDF** come formato per la firma digitale rappresenti un passo in avanti nel processo avviato negli anni scorsi da parte del legislatore, impegnato attivamente nel regolare standard e modelli che facilitino la comprensione e l'accesso all'innovazione a fasce sempre più ampie di utenti e imprese, incidendo così positivamente sull'evoluzione della gestione elettronica documentale.

E' auspicabile una crescente diffusione della firma digitale all'interno delle imprese. Nuovi ambiti di applicazioni potrebbero aprirsi e andare a incidere significativamente sull'efficienza di processi gestiti ancora oggi in maniera tradizionale (deposito di bilanci, adempimenti civilistici e tributari, processi di fatturazione elettronica etc.).

E' fondamentale, a riguardo, adottare un approccio che coniughi la capacità di circoscrivere gli ambiti di intervento con una visione allagata sui processi aziendali. Le imprese che hanno già investito in infrastrutture di Document Management possono integrare gli strumenti di Workflow con le applicazioni per la Firma digitale al fine di creare "**Process Management**".

Ad esempio, è possibile creare, a livello infrastrutturale (Server), moduli o template PDF contenenti i campi da firmare. Il documento può essere firmato e rivisto dall'utente anche con il solo utilizzo del Reader collegato alla PKI aziendale. Il documento viene poi gestito dai sistemi di workflow e archiviazione esistenti che assicurano il ciclo di vita e la sinergia con il resto dei processi aziendali.

Il formato PDF, inoltre, può consentire di assicurare con relativa semplicità la validità legale di una firma digitale nel tempo. Tra i percorsi possibili merita un accenno la possibilità di apporre ad esempio una **marcatura temporale** alla firma digitale secondo i requisiti normativi. La marcatura temporale è una tecnica necessaria ad esempio per la conservazione digitale sostitutiva e ogni qualvolta è necessario certificare o attestare ora e data di emissione di un documento. In particolare, il PDF introduce un formato molto diffuso in un contesto, quello della marcatura temporale, che ad oggi appare ancora caratterizzato da diverse modalità di rappresentazione da parte dei fornitori di tali servizi.

Un caso di applicazione della firma digitale nella PA: il Tribunale di Cremona

Il **Tribunale di Cremona**, in collaborazione con **Adobe Systems Italia**, ha avviato nel 2004 un progetto di razionalizzazione ed efficienza dei processi a forte impatto sulla gestione documentale. Il progetto, denominato **DIGIT**, è stato finalizzato alla creazione del cosiddetto "Fascicolo Processuale Penale", la trasposizione dei fascicoli cartacei in formato elettronico (formato PDF) e la possibilità di utilizzare l'applicazione grazie agli strumenti Adobe.

Il progetto ha consentito in breve tempo di disporre di uno strumento digitale assolutamente allineato dal punto di vista della validità a quello cartaceo, ma con notevoli vantaggi dal punto di vista:

- della velocizzazione delle procedure;
- della riduzione dell'uso della carta e dei relativi costi, fino a realizzare non solo un ritorno dell'investimento ma di generare guardagni mediante un'accurata gestione dei diritti di copia.

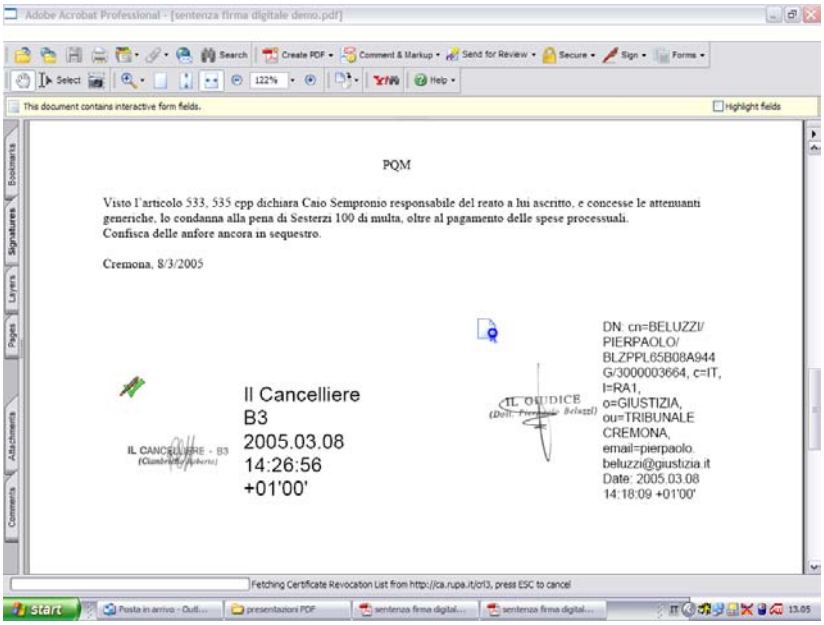
Parallelamente, le esigenze di **sicurezza** per i documenti prodotti in ambito giudiziario ha portato all'implementazione di Adobe Policy Server, la soluzione Adobe di Digital Rights Management (DRM) che consente un controllo dinamico e persistente della sicurezza dei documenti.

Inoltre, una visione "olistica" sui processi documentali ha consentito di estendere l'automatizzazione delle procedure anche alla fase della firma. A partire dal febbraio

2005, infatti, il Tribunale di Cremona ha iniziato a pubblicare alcune sentenze, correlate ai fascicoli digitali, attraverso l'apposizione della **firma digitale** del Giudice e del Cancelliere (si veda la Figura 3 che riporta un esempio di firma digitale applicata a una sentenza).

FIGURA 3

Esemplificazione di apposizione della firma digitale alla sentenza



Fonte: Adobe, 2006

La procedura prevede, nella modalità *certificazione*, che il documento venga utilizzato successivamente soltanto in due modalità:

- per l'inserimento di note o commenti;
- per la firma digitale da parte del cancelliere ai fini del deposito e dell'invio alla procura di competenza.

L'utente privato, grazie ad **Adobe Reader,** è in grado di visualizzare le caratteristiche delle firme digitali apposte, la cronologia delle modifiche effettuate successivamente all'apposizione della firma digitale da parte del Giudice, nonché i dettagli del procedimento di verifica della firma da parte del Certificatore che detiene il certificato del firmatario.

L'esperienza realizzata presso il Tribunale di Cremona dimostra come si possa sgombrare il campo da false o erronee convinzioni circa l'applicabilità dell'innovazione a processi o attività complesse, delicate e a forte impatto sulla sfera personale e quindi sulla sicurezza.

Conclusioni

Una delle caratteristiche dell'attuale società dell'informazione è la quantità, la varietà e la velocità con cui vengono introdotte le innovazioni tecnologiche. Non tutte, ovviamente, diventano "killer application", come è stato per la diffusione dell'email,

considerata massimo esponente di questa espressione. Tuttavia, sebbene poche innovazioni vengano elette a rango di "killer application", il loro impatto sull'innovazione dei processi può risultare molto significativo.

La maggior parte delle tecnologie introdotte di recente – all'interno della tematica **sicurezza** piuttosto che afferenti il tema della **gestione documentale** – hanno permesso di far evolvere i sistemi IT verso modelli più aderenti alle necessità di business.

La firma digitale arricchisce quel processo di digitalizzazione di documenti e procedure che ha già avuto inizio negli anni scorsi e ha consentito di far acquisire "valore legale" ai documenti elettronici.

Tuttavia, mentre il livello di copertura delle esigenze più "statiche" è stata da tempo intrapresa e appare sufficientemente coperta (con nuovi impulsi grazie ad esempio alla conservazione sostitutiva), il presidio dell'anima "dinamica" del processo appare molto più complessa e, quindi, ancora debole rispetto alle reali potenzialità.

L'innovazione di processo – per quanto sostenuta dall'ICT – ha toccato solo marginalmente procedure che invadono la sfera privata. I prossimi appuntamenti per le imprese e per chi sostiene una crescente applicazione della firma digitale saranno impegnativi. Superare le difficoltà significa anche avvicinare imprese e utenti alle novità introdotte dal legislatore e soprattutto ai possibili scenari evolutivi.

Un contributo alla sicurezza e alla maggiore standardizzazione dei processi relativi alla firma digitale può giungere dall'accordo **CNIPA – Adobe**, che riconosce al **formato PDF** le qualità e i requisiti necessari per l'applicazione e il riconoscimento della firma digitale. L'intesa è una delle tante "forme espressive" in tema di regolamentazione della firma digitale e del documento informatico. L'accordo evidenzia nuovi scenari che sono guidati dalla semplicità del supporto nativo e dalla familiarità con lo **strumento di verifica**, già ampiamente diffuso presso gli utenti.

IDC Italia - Viale Monza, 14 - 20127 Milano ITALY
Tel: +39 02 284571 - Fax: +39 02 28457.333

www.idc.com/italy