Il timbro digitale: una soluzione tecnologica per l'autenticazione di documenti stampati

versione 2.0
18 dicembre 2006

Francesco Grasso - CNIPA
Gaetano Santucci - CNIPA

SOMMARIO

1 Premessa ... 3
1.1 Documenti elettronici e documenti cartacei ... 3
1.2 Struttura del documento ... 3
1.3 Attività del CNIPA ... 4
2 Campo e modalità di applicazione ... 5
2.1 Rilascio di documenti ufficiali ... 5
2.1.1 Il meccanismo di generazione e di verifica ... 6
2.2 Uso interno alle amministrazioni ... 8
2.3 Documenti certificanti un pagamento ... 10
2.4 Uso per la logistica ... 11
2.5 Altri possibili impieghi ... 11
2.5.1 Documenti stampati con parti riservate ... 11
2.5.2 Accessibilità ... 12
2.6 Applicazioni e progetti in Italia ... 13
2.6.1 Cedolino elettronico dei dipendenti pubblici ... 13
2.6.2 I servizi di Postel ... 15
2.6.3 Securizzazione della ECDL per AICA ... 15
2.6.4 Certificato di proprietà degli autoveicoli ... 16
2.7 Applicazioni e progetti in altri Paesi ... 16
2.7.1 Europa ... 16
2.7.2 Stati Uniti ... 17
3 Tecnologie disponibili ... 19
3.1 Codici bidimensionali ... 19
3.1.1 PDF417 ... 19
3.1.2 Maxicode ... 20
3.1.3 DataMatrix ECC200 ... 20
3.1.4 Dataglyph ... 20
3.1.5 2D-Plus ... 21
4 L'offerta di mercato ... 23
4.1 Land/Postel ... 23
4.2 Secure Edge ... 24
4.3 Modalità di pagamento di Land/Postel e Secure Edge ... 24
4.4 Everis (precedentemente DMR Consulting) ... 25
4.5 Xerox ... 25
5 Bibliografia ... 26

1 Premessa

1.1 Documenti elettronici e documenti cartacei

Nel vari Paesi europei esiste a oggi, pur con regolamenti e orientamenti differenti, una normativa che regola il riconoscimento d'autenticità dei documenti elettronici. In Italia, il Codice dell'amministrazione digitale del 7/03/2005 prevede la firma digitale come soluzione tecnica per garantire ai documenti elettronici i valori di integrità, non modificabilità e non ripudio.

Tradizionalmente, al contrario, il riconoscimento d'autenticità di un documento cartaceo si basa su elementi quali il tipo di carta, la filigrana, stampe sofisticate, inchiostri speciali, timbri e firma autografa.

Questa differenza fa sì che, quando un documento elettronico viene stampato, si ha una cosiddetta "interruzione della catena del valore" della firma digitale.

A seguito di un processo di stampa tradizionale, infatti, gli attributi d'integrità, certezza del mittente, non ripudio e di data certa di creazione e/o di firma sono definitivamente persi: il documento stampato necessita nuovamente di una firma tradizionale, perdendo così i vantaggi di essere nato in formato elettronico e di essere stato firmato digitalmente [1].

Nell'ambito della Pubblica Amministrazione, e nel rapporto tra questa e i suoi utenti (cittadini e imprese) esistono tuttora numerose situazioni in cui documenti dei quali occorre garantire l'autenticità possono attraversare, nel corso del loro ciclo di vita, uno o più passaggi attraverso la carta.

Esiste senz'altro l'esigenza di proteggere tali documenti in tutte le fasi del loro ciclo di vita, indipendentemente dal supporto – elettronico o cartaceo – utilizzato. Questa indipendenza potrebbe essere possibile se si stampassero, contestualmente al contenuto del documento, le informazioni necessarie a controllarne l'autenticità già presenti nel documento stesso, ad esempio:

- una rappresentazione alternativa e non alterabile del contenuto del documento;
- la certificazione della fonte che ha emesso il documento.

Nel proseguo del documento, indicheremo convenzionalmente la stampa di tutte o parte di queste informazioni con il termine "**timbro digitale**". Per timbro digitale si può intendere quindi una rappresentazione convenzionale di informazioni contenute nel documento elettronico (tutte o parte di esse), stampabile, riconoscibile con strumenti elettronici, ottenuta utilizzando una codifica grafica definita.

1.2 Struttura del documento

Il presente documento contiene:

- un'analisi dei vari contesti di applicazione delle tecnologie per la generazione e la verifica del timbro digitale; sono esaminati i pro e i contro di soluzioni di questo tipo rispetto alle alternative più tradizionali, illustrando anche le più significative esperienze condotte in Italia e/o all'estero;
- un esame delle tecnologie a oggi esistenti per applicare al documento cartaceo i meccanismi di autenticazione propri del mezzo elettronico;
- l'offerta di mercato, sotto il profilo tecnico;
- una serie di riferimenti a documentazione tecnica e a siti web di interesse su questa tematica.

1.3 Attività del CNIPA

Il presente documento è stato redatto a seguito di uno studio iniziale, a cui si prevede di far seguire:

- la definizione di un piano di sperimentazione dei principali prodotti disponibili sul mercato; la sperimentazione sarà condotta presso il laboratorio del CNIPA con il coinvolgimento dei fornitori e di altri esperti;
- ulteriori studi finalizzati, in prospettiva, a fornire elementi e considerazioni tecniche per eventuali future iniziative legislative;
- l'eventuale costituzione di un gruppo di lavoro aperto, oltre che a personale del CNIPA, alle amministrazioni interessate a questa tematica. A questo proposito, si sottolinea che un'importante fonte che è stata utilizzata nel corso dello studio iniziale è costituita dall'esperienza congiunta di Consip e del Ministero dell'Economia e Finanze per il progetto del cedolino elettronico per i dipendenti pubblici. I risultati di tale esperienza, che ha impegnato risorse di Consip e del Ministero per più di diciotto mesi, sono citati più volte all'interno di questo documento.

2 Campo e modalità di applicazione

Esistono diversi ambiti che richiedono oggi, e richiederanno ancora per diverso tempo, la coesistenza di documenti elettronici e cartacei. Si propone nel seguito una possibile categorizzazione dei **contesti di applicazione**.

- **Rilascio di documenti** ufficiali da una pubblica amministrazione a cittadini e/o imprese. In questa tipologia di documenti ricadono ad esempio concessioni, nulla osta, certificati anagrafici, abilitazioni, licenze, autorizzazioni, permessi di soggiorno, visti, attestati, visure catastali e commerciali, certificati di proprietà di veicoli.

- **Uso interno** a una o più amministrazioni, per scambio di documenti (ad esempio per processi autorizzativi o per altri tipi di flusso documentale) tra gruppi chiusi di utenti o tra uffici diversi, in integrazione con i sistemi di gestione documentale delle amministrazioni.

- Generazione di **documenti comprovanti un pagamento** o un credito. Ad esempio, i documenti in questione possono essere ricevute di servizi ticketless[1] o di transazioni on-line, ricevute di bonifici, estratto conto contributivi, pagamenti tasse e imposte on-line, abbonamenti o iscrizioni a servizi pubblici, biglietti di lotterie.

- Uso per **logistica**, ad esempio, per il controllo delle merci e delle spedizioni, per le bolle d'accompagnamento.

Nei prossimi paragrafi vengono analizzati nel dettaglio questi ambiti di applicazione. Un successivo paragrafo è dedicato all'esame di casi che non sembrano rientrare in nessuno dei contesti elencati.

2.1 Rilascio di documenti ufficiali

A oggi la carta è, di fatto, il mezzo più diffuso per la circolazione e la conservazione di documenti ufficiali. Nonostante la forte spinta in atto al processo di dematerializzazione, il supporto cartaceo è ben lungi dall'essere abbandonato, anche a causa di una serie di problematiche non solo tecniche, ma, soprattutto, organizzative, gestionali ed economiche.

Ad esempio, la gran parte delle aziende e dei cittadini sono ormai in grado di ricevere documenti da amministrazioni in forma elettronica, ma non sono sempre in grado di conservarli in questa forma per la durata di validità dei documenti stessi.

Inoltre, l'uso più comune che viene fatto dei documenti ufficiali è allegarli a domande o ad altra documentazione da presentare, in forma cartacea, in vari contesti.

Nell'esempio illustrato nella figura seguente, una pubblica amministrazione locale emette un certificato a un'azienda o a un cittadino, che lo deve allegare a una domanda presentata a un altro privato, oppure a un'azienda, o a una seconda amministrazione locale (es. una ASL).

Per questi motivi, il cittadino o l'azienda che riceve il documento ufficiale da parte dell'amministrazione in forma elettronica deve poi stamparlo. E' questo dunque un evidente ambito di applicazione di soluzioni per "riportare su carta" le garanzie di sicurezza proprie del documento elettronico.

[1] Ad esempio, nel caso di acquisto on-line di un biglietto ferroviario, la ricevuta è attualmente costituita da una e-mail che viene inviata dal sito di Trenitalia all'acquirente. Il servizio è definito "ticketless" in quanto in nessun momento viene stampato un vero e proprio "biglietto".

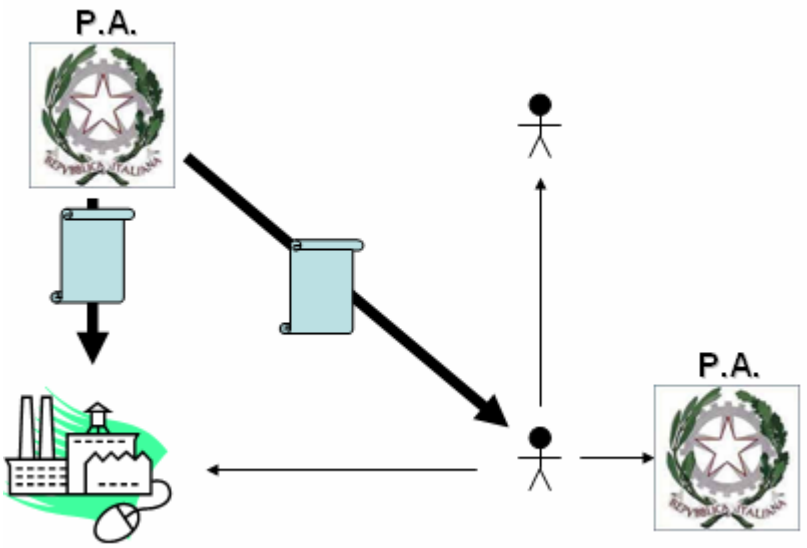


Figura 1: rilascio di documenti ufficiali - scenario

Si noti che essere in grado di rendere sicure le stampe dei documenti elettronici potrebbe costituire una soluzione pragmatica (presumibilmente la carta non sarà eliminata nel prossimo futuro) al problema della sicurezza nei documenti ufficiali, e allo stesso tempo un fattore abilitante alla diffusione della firma digitale.

Soluzioni di questo tipo non devono perciò essere giudicate "in controtendenza" rispetto al desiderato processo di dematerializzazione, ma anzi sono con ogni probabilità propedeutiche ad esso. Sono infatti soluzioni che consentono di procedere alla dematerializzazione con gradualità, tenendo conto che gli investimenti necessari alla transizione dal supporto cartaceo a quello elettronico costituiscono spesso un vincolo economico a tale transizione. Si deve insomma tener conto che non tutte le amministrazioni sono immediatamente in grado di adottare, per ragioni di carattere tecnico, organizzativo ed economico, sistemi di gestione dei documenti completamente digitali.

2.1.1 Il meccanismo di generazione e di verifica

Nell'ambito in esame (il rilascio di documenti ufficiali), un possibile meccanismo per la sicurezza del documento stampato è descritto nel seguito.

Rilascio

1. L'amministrazione rilascia il documento su supporto elettronico, dopo averlo firmato digitalmente. Il documento dovrà contenere, al proprio interno, il timbro digitale (vedi precedente definizione).
2. Il destinatario del documento (cittadino o impresa) ottiene il documento su supporto elettronico, ad esempio scaricandolo dal sito dell'amministrazione, o ricevendolo via posta elettronica.
3. Il destinatario visualizza e stampa il documento ricevuto con un software già disponibile (es. un browser), senza la necessità di acquistare software apposito. Nel caso in cui sia necessario utilizzare un plug-in[2] o un modulo ad hoc, questo dovrà essere fornito gratuitamente dall'amministrazione. Il formato e le caratteristiche del timbro digitale dovranno permettere la sua stampa anche con stampanti a basso costo normalmente reperibili in commercio.

[2] Un plug-in è un componente software che si aggiunge a un browser per l'esecuzione di particolari funzioni.

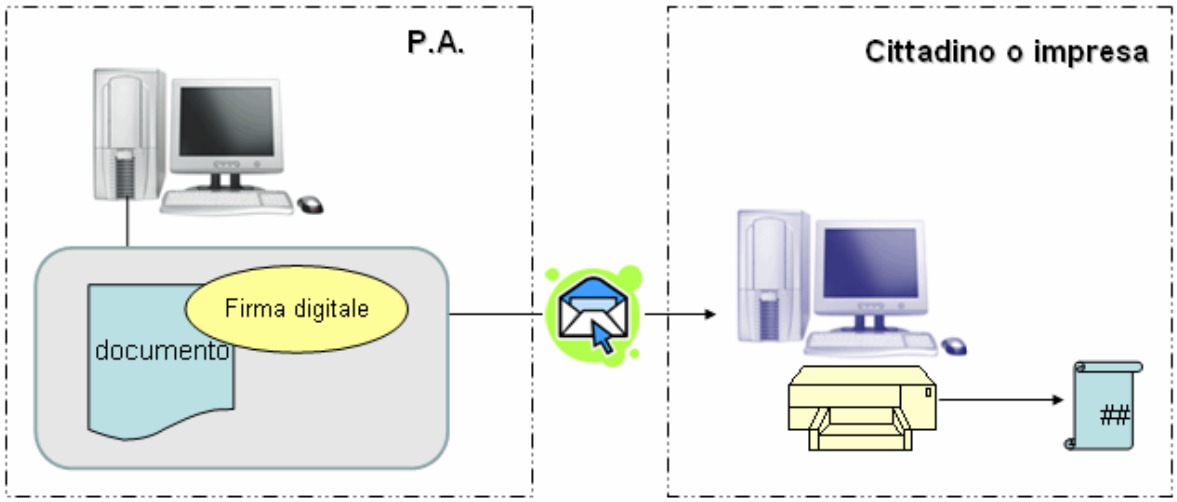


Figura 2: processo per il rilascio

In alternativa, l'amministrazione potrebbe rilasciare il documento già su supporto cartaceo all'utente (consegnandolo di persona, o via posta ordinaria). In questo caso, la stampa avviene negli uffici dell'amministrazione, per cui l'utente non ha più la necessità di dotarsi del software apposito citato al precedente punto 3, e neppure di una stampante. Il processo alternativo è rappresentato nella figura seguente.

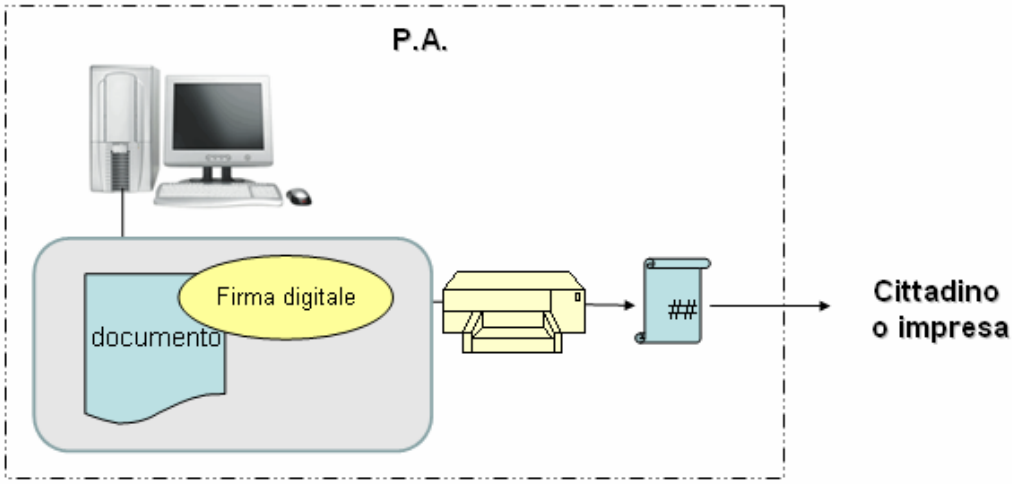


Figura 3: processo alternativo per il rilascio

In questo secondo processo, il timbro digitale potrebbe esistere solo sulla versione stampata del documento (il timbro viene generato solo in fase di stampa), mentre l'amministrazione potrebbe conservare una copia solo dell'originale elettronico, firmato digitalmente ma non contenente il timbro.

Verifica

1. In ogni momento il documento stampato potrà essere sottoposto a verifica. Per questo, il documento stampato dovrà essere inserito in uno scanner, che ne produrrà una versione elettronica. Dovrà essere possibile adoperare scanner di basso costo, normalmente reperibili in commercio.
2. Si verificherà la firma digitale contenuta nel documento elettronico prodotto al passo precedente. Per far questo, non dovrà essere necessario dotarsi di un software a pagamento.

Possibilmente, il modulo o il plug-in necessario si scaricherà gratuitamente dallo stesso sito web dell'amministrazione che ha rilasciato il documento.

3. La verifica di cui al passo precedente dovrà garantire che il documento sia stato effettivamente emesso dall'amministrazione, e che il suo contenuto non sia stato alterato dopo l'emissione.

Figura 4: processo di verifica

Vantaggi previsti

Il livello di sicurezza del processo descritto è molto più alto rispetto a quanto attualmente disponibile (si pensi alla facilità di falsificare una firma autografa o un timbro tradizionale a inchiostro).

E' possibile stampare il documento quante volte si vuole, e tutte le copie saranno ugualmente sicure. Ciò potrebbe rendere inutile l'attuale ricorso alla cosiddetta "copia conforme"[3].

Problematiche connesse

Per realizzare il processo descritto è chiaramente necessario **l'uso di una stampante e di uno scanner**, ma questi sono dispositivi già normalmente usati dalle aziende e dai privati, e il loro costo – comunque non elevato – può essere considerato un investimento per ottenere un grado di sicurezza sui documenti cartacei molto superiore a quello attuale.

Più complesso è il **problema dell'interoperabilità**. Il meccanismo descritto è certamente in grado di funzionare se tutti i soggetti coinvolti dispongono della stessa tecnologia o di tecnologie compatibili tra loro. Tuttavia, come sarà illustrato nel capitolo 4 di questo documento, sono oggi presenti sul mercato numerose tecnologie e formati di timbri digitali alternativi tra loro. Eventuali organizzazioni (enti, imprese) che dispongono di una tecnologia A potrebbero non essere in grado di verificare e gestire i documenti emessi da organizzazioni che usano tecnologia B. La messa a disposizione in forma gratuita dei moduli software per la verifica non risolve completamente il problema. Si pensi alla necessità di disporre, sui PC di un'organizzazione, di **tutti** i moduli software per la verifica esistenti sul mercato, magari incompatibili tra loro, e senza chiare indicazioni su quale modulo adoperare di volta in volta.

2.2 Uso interno alle amministrazioni

Esistono tuttora ambiti nei quali documenti scambiati all'interno di una stessa pubblica amministrazione attraversano una fase cartacea.

Un primo esempio è costituito da documenti amministrativi quali note di servizio, certificazioni di corsi svolti, valutazioni o altri documenti archiviati, per esempio, nel fascicolo dei dipendenti. Avviene di norma, in molti uffici, che se un dipendente fa richiesta di un estratto del suo fascicolo,

[3] Si parla ovviamente solo dal punto di vista tecnico. Per eliminare effettivamente la necessità della copia conforme occorre una modifica dell'attuale normativa.

questo gli venga rilasciato su supporto cartaceo. Ma anche in caso di rilascio in forma elettronica, questi documenti vengono normalmente stampati dal dipendente e conservati su supporto cartaceo. Successivamente, avviene che tali documenti vengano poi allegati a domande, ad esempio per partecipazione a concorsi interni o di un'altra P.A., e debbano perciò essere nuovamente gestiti dagli uffici della stessa o di un'altra amministrazione.

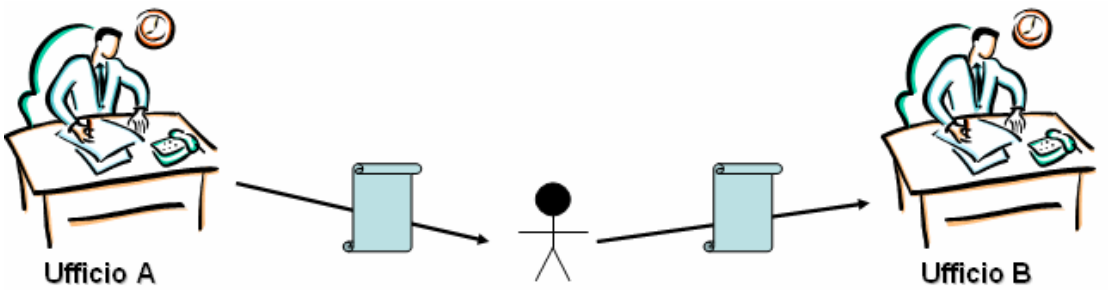


Figura 5: uso interno alle amministrazioni - scenario

Come secondo esempio si può pensare a un processo di raccolta di informazioni che preveda l'uso di formulari o di moduli cartacei. Benché l'uso di "form" elettroniche si stia diffondendo, ci sono tuttora molte aree in cui la modulistica continua ad essere cartacea per oggettive difficoltà di tipo tecnico, logistico o organizzativo. In questi casi il documento che viene scambiato è uno stampato contenente:

- alcune informazioni "statiche" prodotte dall'ufficio di partenza,
- campi da riempire a cura del rispondente.

Il formulario compilato e riconsegnato deve poi essere gestito dall'ufficio competente, che può essere lo stesso ufficio di partenza o un altro dell'amministrazione (si pensi, come esempio, ai questionari delle rilevazioni Istat).

Nei casi descritti, e in tutti gli ambiti della stessa tipologia, l'introduzione dei timbri digitali può essere una buona soluzione. Rispetto ai processi di rilascio e verifica illustrati al paragrafo 2.1.1, le maggiori differenze sono le seguenti:

- **Unicità dell'autore** del documento. Tutti i documenti di questa categoria, per definizione, sono rilasciati dalla stessa amministrazione. Non c'è dunque bisogno che il timbro digitale riporti informazioni sull'autore, in quanto esso è già definito.
- La **verifica del documento è un'operazione più "limitata"** rispetto a quanto visto al paragrafo 2.1.1, in quanto i soggetti che hanno interesse a verificare il documento stampato sono solo gli uffici che lo ricevono in forma cartacea e devono gestire il proseguo del suo ciclo di vita (con riferimento al primo esempio, l'ufficio del personale). Per questo motivo, è accettabile anche un meccanismo di verifica che imponga hardware e/o software specializzato (es. scanner costosi, o moduli software a pagamento), in quanto tali prodotti specializzati non dovranno comunque avere grande diffusione.
- Per gli stessi motivi del punto precedente, l'esigenza di **interoperabilità** tra le varie tecnologie è **molto inferiore** (in questo ambito, la soluzione scelta potrebbe essere "chiusa" senza tuttavia generare particolari problemi).
- Per questa categoria di documenti, è utile che il timbro digitale faciliti anche un eventuale lavoro di **data entry**. Con riferimento all'esempio precedente (questionario di rilevazione), se il timbro digitale contiene al suo interno la codifica delle informazioni già presenti sul modulo prima della compilazione dello stesso da parte del rispondente, esse possono essere facilmente riportate in digitale senza l'uso di tecnologie costose quali ad esempio un OCR.
- In generale, per questa categoria di documenti, i **requisiti di sicurezza sono meno stringenti**. Lo scambio di documenti avviene infatti all'interno di un "gruppo chiuso" di utenti, per cui la

falsificazione o la modifica non autorizzata di un documento sono eventi in generale meno probabili rispetto ai casi descritti nel paragrafo 2.1 (in alcuni ambiti, l'eventualità di una contraffazione o di un'alterazione del documento semplicemente non ha senso).

- Il processo di rilascio e verifica deve essere **compatibile con il sistema di protocollo e di gestione documentale** usato nell'ambito dell'amministrazione (o che l'amministrazione ha intenzione di realizzare). In prospettiva, è necessaria un'integrazione tra il processo di gestione delle fasi cartacee dei documenti e il resto del sistema documentale. Ancora una volta, soluzioni di questo tipo non devono essere viste "in controtendenza" rispetto all'introduzione di sistemi informatici "paperless", essendo anzi un fattore abilitante alla diffusione di questi ultimi, nonché un modo per superare i vincoli economici e permettere una gradualità di sostituzione del cartaceo con il digitale.

2.3 Documenti certificanti un pagamento

I documenti che rientrano in questa categoria si possono ulteriormente suddividere in due gruppi:

- documenti rilasciati da un'amministrazione come ricevuta di un pagamento da parte di un cittadino o di un'azienda (ad esempio pagamento di un tributo o del canone di un servizio pubblico);
- documenti che certificano un pagamento effettuato da un'amministrazione (ad esempio stipendi dei dipendenti, rimborsi fiscali, bonus bebé).

La documentazione di questo tipo viene oggi rilasciata generalmente in forma cartacea, e conservata sempre in questa forma dal destinatario. In molti casi, gli stessi documenti (in originale o in copia) vengono successivamente presentati ad altre amministrazioni perché richiesti in altri procedimenti (si pensi ad esempio agli allegati alla dichiarazione dei redditi), oppure a soggetti terzi quali banche o servizi finanziari, ad esempio per la concessione di prestiti.

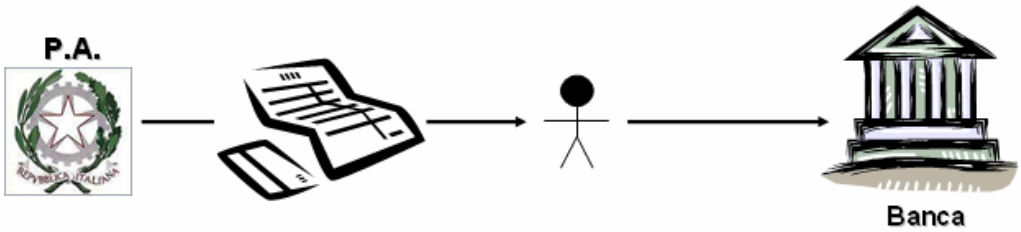


Figura 6: documenti relativi a pagamenti - scenario

E' immediato comprendere l'utilità del timbro digitale, negli ambiti descritti, per garantire la sicurezza nello scambio dei documenti. Il processo per il rilascio e la verifica illustrati al paragrafo 2.1 sono in generale applicabili anche in questo contesto, tenendo presente i punti seguenti:

- Dato il contenuto dei documenti di questa categoria (informazioni di tipo finanziario), i **requisiti di sicurezza** sono **molto alti**. E' difatti questo l'ambito in cui è più necessario tutelarsi da falsificazioni e contraffazioni. Ciò può giustificare anche investimenti per l'acquisto di apparecchiature o moduli software, confrontando questi investimenti con i costi della "non sicurezza" (in termini di soldi persi per truffe e contenziosi legali).
- A differenza dei casi illustrati nei paragrafi precedenti, dove i documenti sono generici e di struttura indefinita, i documenti di questa categoria hanno una **struttura in massima parte prefissata**. Nel caso di una fattura, ad esempio, sarà sempre presente sul documento un campo con l'importo, un campo con la data e un campo col codice fiscale (o la partita IVA) di chi ha versato il pagamento. Data questa staticità della struttura, il timbro digitale potrebbe limitarsi a "proteggere" solo i campi significativi del documento, e non l'intero contenuto, con possibili vantaggi sulle dimensioni del timbro digitale e sulla velocità del processo di verifica.

– Per assicurare il funzionamento del meccanismo, è necessario stipulare **accordi con il settore bancario** e dei servizi finanziari, affinché anche tale settore concordi sul processo di rilascio/verifica e sugli standard tecnologici su cui tale processo si basa.

2.4 Uso per la logistica

In questa categoria ricadono gli scambi di documenti relativi a beni da inventariare o da movimentare (es. bolle di accompagnamento, documenti di carico/scarico, archivi di magazzino, eccetera).

Si tratta di un ambito applicativo nel quale tradizionalmente si impiegano, come contenitore di informazioni, i codici a barre, tecnologia che può essere considerata la generazione precedente dei timbri digitali.

Il vantaggio di utilizzare timbri digitali rispetto ai codici a barre è essenzialmente legata alla maggiore quantità di informazioni che i timbri digitali possono contenere rispetto ai codici a barre. Tipicamente, i codici a barre usati in ambito "logistica - gestione merci" contengono semplicemente un indice per un database esterno al documento; al contrario, il timbro digitale può già contenere al suo interno tutte le informazioni necessarie, rendendo il documento autoconsistente e permettendo la gestione del sistema anche in mancanza della connessione con il database esterno[4].

Anche in questo contesto, inoltre, i timbri digitali potrebbero ridurre la necessità di eventuale data entry manuale, nel caso in cui le informazioni da acquisire dal documento cartaceo (ad esempio una bolla di accompagnamento) siano contenute anche all'interno del timbro digitale.

2.5 Altri possibili impieghi

2.5.1 Documenti stampati con parti riservate

Con i timbri digitali si possono realizzare documenti cartacei che riportino stampate, e leggibili direttamente, solo le informazioni pubbliche del documento, mantenendo tutte le informazioni riservate e/o sensibili crittografate all'interno dello stampato. L'accesso a queste informazioni sarà consentito solo a coloro che hanno le necessarie autorizzazioni. Nella figura seguente viene illustrato un possibile processo di codifica e di recupero delle informazioni.

[4] In questo contesto non va dimenticato che una tecnologia in via di espansione è quella dell'RFID.

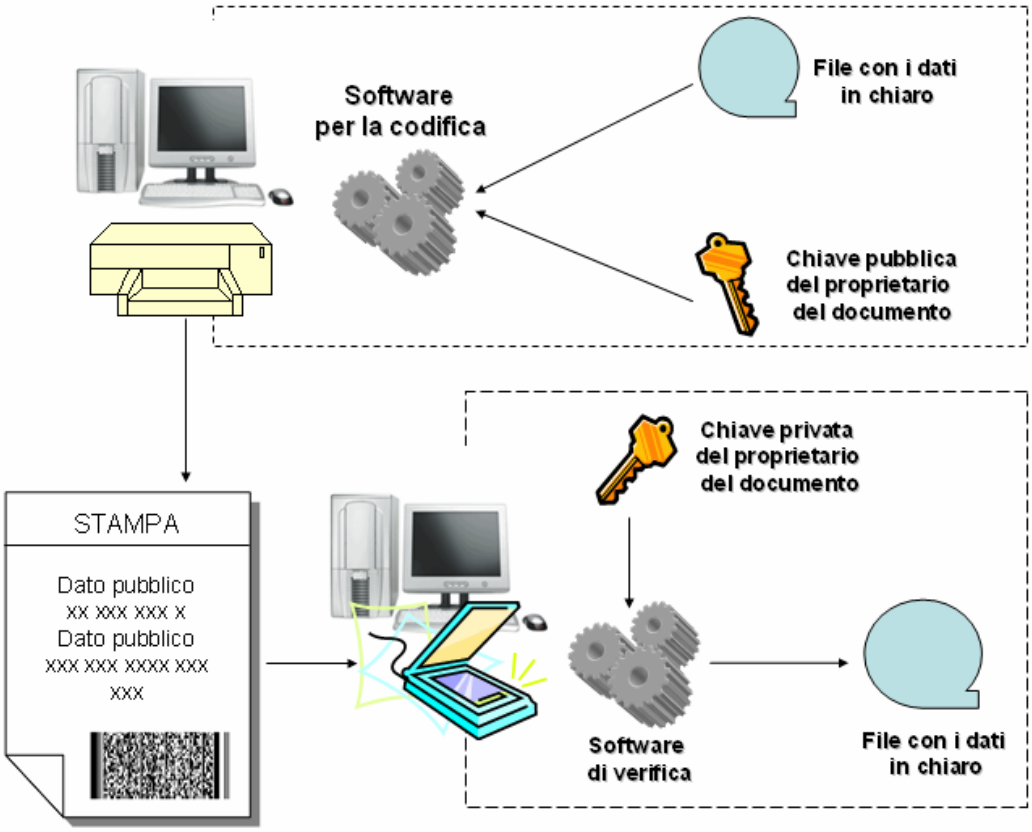


Figura 7: documenti con parti riservate - processo

I contesti di applicazione sono ad esempio le cartelle mediche, i risultati di esami clinici, in generale i documenti con problematiche di privacy.

2.5.2 Accessibilità

Per l'accesso a documenti elettronici da parte di persone disabili sono disponibili sul mercato numerose tecnologie assistive. Ad esempio, per i non vedenti, è diffuso l'uso di software del tipo "screen reader" in grado di convertire un testo nel suo equivalente sonoro. Anche in questo caso, il passaggio dei documenti su supporto cartaceo annulla questa possibilità: il ricevente disabile potrebbe riportare il documento in elettronico mediante uno scanner, ma otterrebbe una bitmap non più leggibile dal software "screen reader", a meno di non usare un OCR, programmi in genere costosi e che comunque non garantiscono il perfetto recupero del testo originario.

Si tratta di una problematica che è possibile affrontare con soluzioni basate sui timbri digitali. In questo caso, il documento cartaceo da rilasciare alla persona disabile può contenere, all'interno del timbro digitale, il testo codificato del documento stesso, o parte di esso. Durante la verifica, tale testo può essere facilmente recuperato dal timbro, senza necessità di un OCR.

Una seconda possibilità (ancora alla fase di studio) potrebbe essere inserire all'interno del timbro non il testo ma il file audio corrispondente (la "lettura" del documento). In questo modo il ricevente disabile potrebbe accedere al contenuto del documento in via sonora.

Il processo di recupero delle informazioni è rappresentato, nei due casi, nella figura seguente.

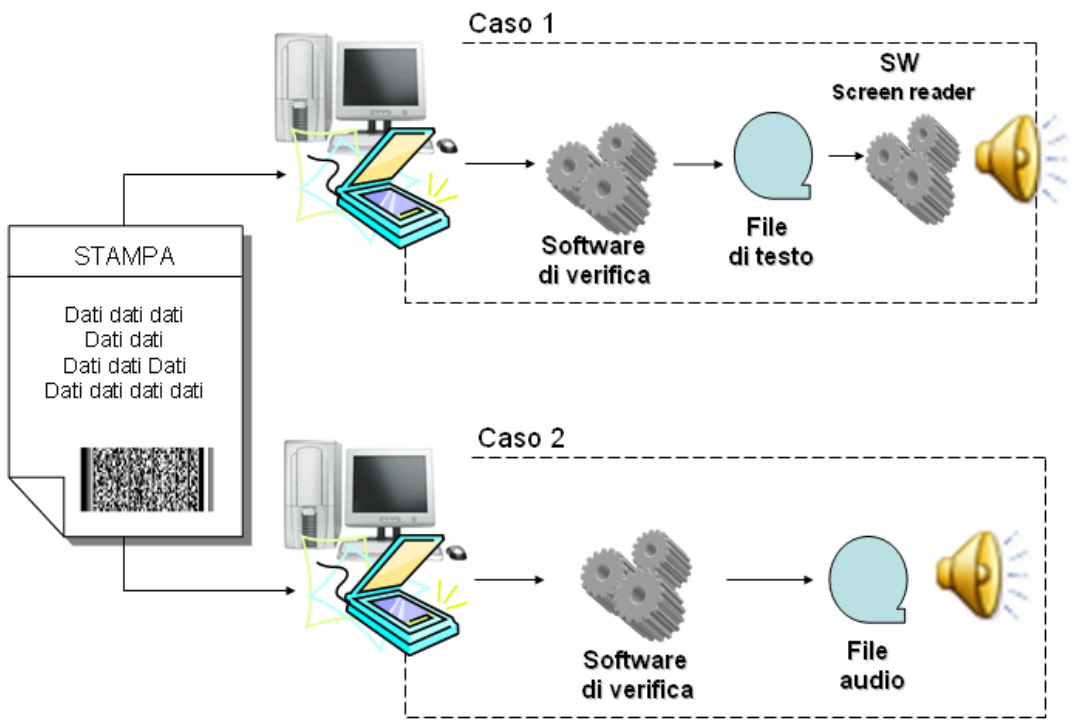


Figura 8: applicazione per l'accessibilità

Si segnala che in data 6/4/2006 è stata presentata all'Ufficio Italiano Brevetti e Marchi una domanda di brevetto (num. RM2006A000196) su un "procedimento denominato AudioSign, e relativa tecnologia abilitante, per la rappresentazione di segnali acustici firmati digitalmente e per la loro verifica quando richiesto, finalizzata all'accesso ai servizi di firma digitale anche da parte di coloro che a causa di disabilità visiva necessitano di opportune tecnologie assistive" [2].

2.6 Applicazioni e progetti in Italia

2.6.1 Cedolino elettronico dei dipendenti pubblici

Consip sta conducendo da più di un anno, per conto del Ministero dell'Economia e delle Finanze, il progetto "e-Cedolino", finalizzato ad adeguare il servizio reso dal Service Personale Tesoro (SPT) del Ministero agli adempimenti previsti dal comma 197 dell'art. 1 della legge Finanziaria 2005.

Il progetto si prefigge, in una prima fase, di rendere SPT in grado di inviare il cedolino per il pagamento delle competenze stipendiali mediante lo strumento della posta elettronica. In una seconda fase, si prevede la realizzazione di un portale web di servizi per SPT che consenta la richiesta e l'erogazione on-line di certificazioni e documenti (lo stesso cedolino, ma anche ad esempio i modelli CUD).

Nell'ambito di questo progetto, è previsto il primo vero *deployment* su vasta scala, almeno in Italia, delle tecnologie basate su timbri digitali nel contesto della securizzazione dei documenti cartacei[5].

In sintesi, la securizzazione del cedolino avviene tramite apposizione di un timbro digitale[6]. L'esigenza principale che vuole essere soddisfatta dalla securizzazione è dimostrare l'autenticità del

[5] Relativamente a questa esperienza sarà a breve disponibile un documento Consip che ne illustrerà nel dettaglio gli aspetti realizzativi.
[6] Tramite un applicativo sviluppato della società Land. Nel progetto di realizzazione è stata coinvolta anche la società Postel.

cedolino stampato (ad esempio per i dipendenti che vogliono accedere a finanziamenti bancari) sia certificando l'autore del documento, sia assicurando l'integrità dei dati rappresentati.

Il processo di creazione del cedolino securizzato - secondo le informazioni pervenute da Consip - può essere illustrato nei seguenti passi:

1. a partire dal file di stampa in formato PCL5 prodotto da SPT viene estratta l'immagine in formato bitmap del cedolino;
2. tale bitmap viene imbustata, anche mediante una apposita infrastruttura hardware, assieme alle informazioni di firma digitale in un file PKCS#7 (.p7m);
3. l'insieme dei dati così ottenuto viene rappresentato graficamente[7], applicando anche un codice per la rilevazione e la correzione degli errori per garantire una resistenza ai danneggiamenti e alle imprecisioni di stampa e lettura;
4. il timbro digitale ottenuto al passo precedente, e costituito da 8 diversi elementi grafici, viene apposto in calce al cedolino, senza coprire alcun dato;
5. il cedolino completo di timbro digitale viene inserito in formato PCL5 nel sistema di archiviazione e indicizzazione di SPT[8].

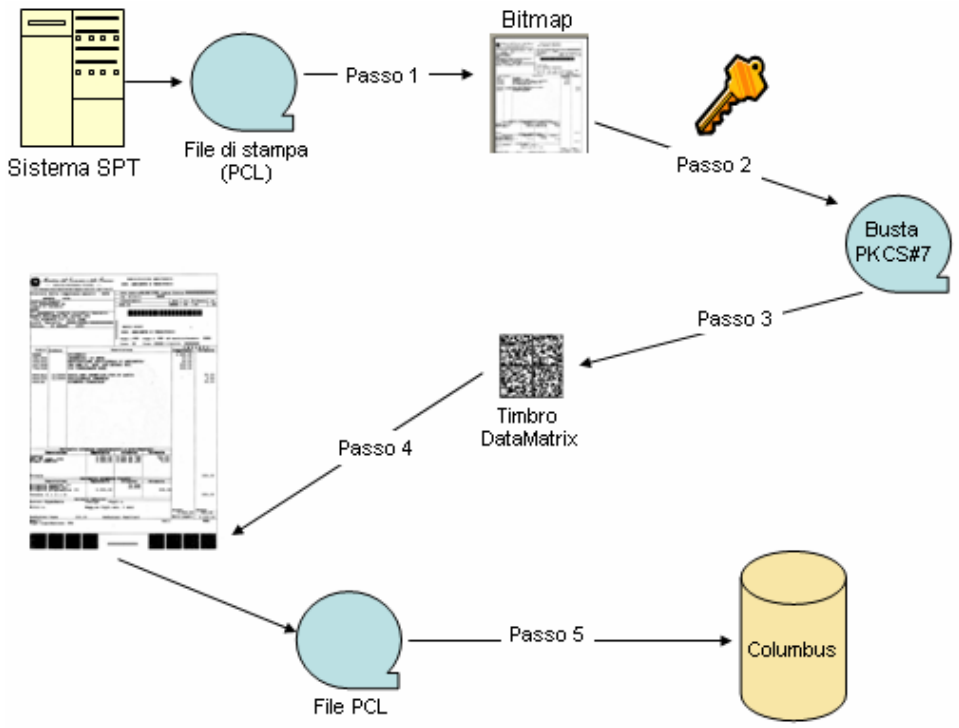


Figura 9: cedolino elettronico - processo

Per quanto riguarda la seconda fase, tuttora in atto, si sta realizzando un *web service* che consenta una securizzazione **indipendente dal formato dei documenti** e che supporti le tecnologie di firma digitale. Tale servizio, come accennato precedentemente, consentirà il rilascio di certificazioni e documenti timbrati digitalmente e sarà accessibile a tutti gli uffici del Ministero (si prevedono 50.000-60.000 utenze).

[7] In codifica DataMatrix.
[8] Software Columbus.

2.6.2 I servizi di Postel

Postel è attiva nel campo delle soluzioni basate sui timbri digitali con un servizio online, denominato "Secure Paper", contestuale e accessorio a quello di "Posta Ibrida" [3]. Il servizio[9] è compatibile con la tecnologia della firma digitale.

Il servizio consente agli utenti l'invio a Postel di documenti elettronici (è supportata una buona varietà di formati). Questi documenti vengono recapitati da Postel ai destinatari in una forma cartacea completa di timbro digitale, che garantisce le proprietà di autenticità, integrità e non ripudio del documento elettronico di partenza. In sostanza, l'utente:

1. invia al servizio Postel il documento elettronico,
2. il servizio Postel provvede a securizzarlo apponendo su di esso il timbro digitale che ne codifica il contenuto,
3. il servizio Postel manda in stampa il documento completo di timbro,
4. il servizio Postel invia il documento in forma cartacea al destinatario desiderato.

Il destinatario può verificare l'integrità del documento ricevuto con l'ausilio di uno scanner e di un apposito viewer.

In via sperimentale, è attualmente allo studio la possibilità di applicare questa soluzione anche all'interno del servizio della "raccomandata on-line". Il meccanismo previsto è analogo al precedente:

1. l'utente invia al servizio la raccomandata in forma elettronica;
2. il servizio provvede a generarne una copia cartacea, completa di timbro digitale, e a inviarla al destinatario.

2.6.3 Securizzazione della ECDL per AICA

Dal gennaio 2004 presso l'AICA (Associazione Italiana per l'Informatica e il Calcolo Automatico) è in esercizio un'applicazione[10] per la securizzazione del documento ECDL (European Computer Driving License) tramite l'apposizione di un timbro digitale in codifica 2D-Plus contenente i dati da proteggere del documento stesso. In figura, un esempio di documento ECDL securizzato (il timbro digitale è visibile in basso, sopra il logo dell'AICA).

[9] Basato sulla codifica DataMatrix e su componenti applicativi sviluppati dalla società Land.
[10] Realizzata dalla società Secure Edge.

European Computer Driving Licence

Questo diploma attesta che

Mario Rossi

Ha superato i sette esami della
"Patente Europea di Guida del Computer"

Concetti Base della IT
Gestione dei Documenti
Elaborazione Testi
Fogli Elettronici
Basi di Dati
Presentazione/Disegno
Reti informatiche

Data: 25/03/2004 Il Presidente AICA ID: AV369xtF04

AICA
Associazione Italiana
per l'Informatica ed il
Calcolo Automatico

2.6.4 Certificato di proprietà degli autoveicoli

L'applicazione, il cui uso sperimentale inizierà presso la regione Piemonte entro la fine 2006, è stata realizzata per l'ACI (tramite ACI informatica). Lo scopo è la securizzazione del certificato di proprietà dei veicoli. Il timbro digitale utilizzato è in codifica 2D-Plus. L'applicazione è stata realizzata dalla società Secure Edge. In figura, un esempio del documento securizzato (il timbro digitale è visibile in basso a sinistra).

2.7 Applicazioni e progetti in altri Paesi

2.7.1 Europa

DMR Consulting (oggi Everis) ha realizzato un progetto per la gestione della fatturazione elettronica per conto del gruppo MAPFRE. Il progetto prevede la firma digitale, l'uso di una

codifica PDF417 (descritto nel prossimo capitolo) sulle fatture stampate, e l'integrazione con il sistema ERP.

Una seconda realizzazione di DMR Consulting è il progetto di gestione documentale CIRCE per la Direzione Generale del Ministero dell'Economia spagnolo. Il progetto prevede l'uso della firma digitale e della codifica PDF417 per garantire l'integrità e l'autenticità anche sulle versioni stampate dei documenti[11].

La società austriaca TEC-IT ha realizzato soluzioni basate su timbri digitali per:

- il gruppo BMW (soluzione per scambi documentali interni tra impiegati e tra l'azienda e i fornitori);
- Hitachi (soluzione per la gestione della supply chain, integrata con SAP, in cui i moduli cartacei sono sostituiti da documenti elettronici in formato PDF contenenti timbri digitali);
- Croce Rossa austriaca (soluzione per la trasmissione sicura dei risultati dei test per l'epatite e l'HIV).
- Beep!, azienda olandese leader nel settore del ticketing elettronico (soluzione per fatturazione elettronica a prova di truffa).

2.7.2 Stati Uniti

Negli Stati Uniti sono da citare almeno due applicazioni basate sui timbri digitali.

La prima si trova nello stato di New York e riguarda le patenti di guida. Le informazioni anagrafiche e biometriche del proprietario della patente sono riportate sotto forma di timbro sulla patente stessa (vedi foto, tratta dal sito web della codifica PDF417 [4]).

La seconda applicazione opera nello stato del Connecticut, e riguarda la tessera per i servizi sociali. Anche in questo caso il timbro, basato sulla codifica PDF417, contiene le informazioni anagrafiche e biometriche (anche le impronte digitali) del proprietario della tessera (vedi figura).

[11] A questo proposito, si citano le norme che regolano la certificazione dei documenti elettronici in Spagna:
- decreto ministeriale HAC/3134 del 5/12/2002,
- risoluzione 2/2003 del direttore generale dell'agenzia statale dell'amministrazione tributaria,
- decreto reale 1496 del 28/11/2003,
- L. 59/2003 sulla firma elettronica.

STATE OF CONNECTICUT
600 890 1919 19191
Sue Sample
SAMPLE

3 Tecnologie disponibili

3.1 Codici bidimensionali

Le tecnologie attualmente disponibili per rappresentare informazioni in maniera convenzionale, graficamente, su una superficie piana (cartacea o meno) sono, come detto, evoluzioni del tradizionale codice a barre. A differenza di quest'ultimo, che presentava le informazioni in maniera lineare (monodimensionale), le tecnologie attuali rappresentano le informazioni su due dimensioni. Sono perciò definiti "codici bidimensionali".

Attualmente esistono circa 20 codifiche differenti sul mercato. Tra le più diffuse, sono da citare la codifica PDF417, il Maxicode, il DataMatrix, il Datagliph. Questi quattro tipi di codifica vengono descritti in dettaglio nei prossimi paragrafi.

3.1.1 PDF417

Il PDF417 è un simbolismo grafico inventato da Ynjiun Wang nel 1991 per conto della Symbol Technologies, ed è stato diffuso in modalità open source sia per quanto concerne la codifica che la decodifica.

I brevetti correlati sono riportati all'indirizzo www.symbol.com/category.php?category=675. La codifica PDF417 è stata recentemente approvata come standard ISO/IEC (15438:2006)[12]. Il nome è l'acronimo di "Portable data file", e la sigla 417 indica che l'unità di dati elementare (di seguito "codeword") è composta da quattro barre e da quattro spazi, con larghezza totale pari a 17 volte lo spessore di una barra verticale. Un timbro in codifica PDF417 ha l'aspetto grafico rappresentato in figura.

Esso è formato da un minimo di tre righe a un massimo di novanta. Ciascuna riga è formata da:

- una zona libera, costituita da un spazi bianchi prima;
- una sequenza di riconoscimento, che identifica la codifica PDF417;
- una zona sinistra con i dati sotto forma di codeword (da 1 a 30);
- una zona destra con ulteriori informazioni relative alla riga;
- un codice di stop;
- una zona libera.

Un timbro in codifica PDF417 può contenere al massimo 928 codeword, ed è possibile dedicarne fino a 510 per il recupero errori. E' possibile leggere correttamente un timbro con un'area danneggiata fino a circa il 55%.

Un timbro con questa codifica può contenere fino a 2710 cifre o 1850 caratteri alfanumerici. Se i dati da rappresentare sono di più, è possibile stampare più timbri di questo tipo da leggere in sequenza. Questo tipo di codifica consente una scansione anche non esattamente in orizzontale, ed essendo open source non necessita di licenze d'uso.

[12] ISO/IEC 15438:2006, "PDF417 bar code symbology specification", di cui al link: http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=43816

3.1.2 Maxicode

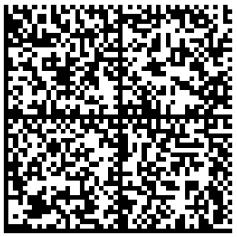
La codifica Maxicode è stata creata nel 1992 da UPS (la compagnia di Atlanta leader mondiale nel settore delle spedizioni). Un timbro Maxicode è della dimensione di un pollice quadrato, e presenta una serie di cerchi concentrici al centro ("occhio di bue") circondati a loro volta da un percorso di punti esagonali (vedi figura).

Un timbro Maxicode può memorizzare informazioni costituite da 93 caratteri, ed è possibile utilizzare una catena di 8 timbri Maxicode per ampliare il contenuto informativo. La gestione degli errori viene effettuata mediante il codice Reed-Solomon error, che consente l'intercettazione di errori dovuti al danneggiamento di una porzione del simbolo.

Come nel caso del PDF417, anche la codifica Maxicode è di pubblico dominio, per cui l'utilizzo è gratuito.

3.1.3 DataMatrix ECC200

DataMatrix è un codice bidimensionale costituito da moduli quadrati bianchi e neri distribuiti su percorsi rettangolari o quadrati. Ciascun modulo della matrice rappresenta un bit. Di solito un modulo bianco indica uno '0' e un modulo nero indica un '1'. In figura, l'aspetto tipico di un timbro DataMatrix.



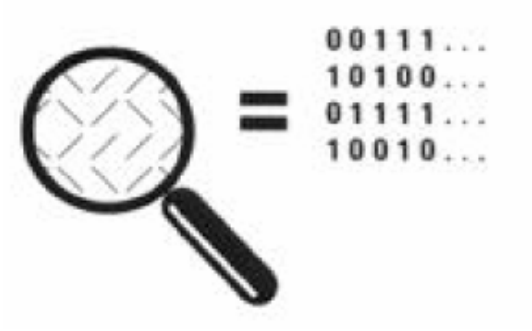
Generalmente un timbro DataMatrix contiene circa 2.335 caratteri alfanumerici o 3.116 caratteri numerici. La versione più recente di DataMatrix è la ECC200, che supporta i metodi avanzati di codifica, check e correzione degli errori secondo gli algoritmi Reed-Solomon. Questa codifica è di dominio pubblico.

La EIA (Electronic Industries Alliance) raccomanda l'uso della codifica DataMatrix per etichettare i componenti elettronici. DataMatrix è stato recentemente approvato come standard ISO/IEC (16022:2006)[13].

3.1.4 Dataglyph

Il Dataglyph [5] è una codifica di proprietà della Xerox, costituito da "glifi", ovvero linee trasversali orientate di 45° (per intendersi '/' e '\') a ciascuno dei quali è attribuito un valore '0' piuttosto che '1' (vedi figura).

[13] ISO/IEC 16022:2006, "Data Matrix bar code symbology specification", di cui al link: http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=44230



Un timbro Dataglyph stampato appare come un'area grigia. Poiché il contenuto informativo è legato all'inclinazione dei glifi e non al loro colore o intensità, è possibile utilizzare i glifi anche per creare un'immagine sul foglio stampato (ad esempio un logo). Combinando tale caratteristica con un'alta resistenza all'errore, è possibile in teoria stampare il timbro come "sfondo" al documento cartaceo (effetto filigrana).

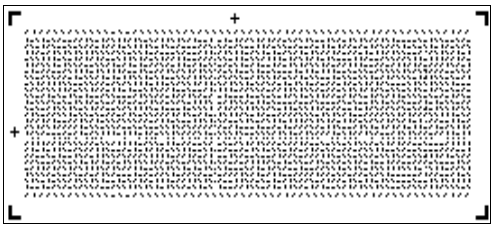
Un'altra importante caratteristica del Dataglyph è la possibilità di modificare la sua forma, quindi di "allargarsi" allo scopo di contenere quantità sempre più grandi di dati. Xerox afferma che la massima grandezza, rappresentata da 769 x 769 glifi, può contenere 63.740 byte di dati (la densità di dati per unità di superficie è quindi piuttosto bassa)[14].

Il brevetto che copre la tecnologia Dataglyph è lo United States Patent 6641053 del 4 Novembre 2003, visionabile all'indirizzo *http://www.patentstorm.us/patents/6641053-fulltext.html*.

3.1.5 2D-Plus

Il 2D-Plus è una codifica proprietaria sviluppata e brevettata dalla società Secure Edge nel 2005. Il brevetto europeo ha data 8/11/2006, num. EP1720118, ed è rintracciabile all'indirizzo internet: *http://v3.espacenet.com/textdoc?DB=EPODOC&IDX=EP1720118&F=0*.
Per questa codifica è stata inoltre depositata una domanda di brevetto USA (`Ref: US11/318,826`) in data 5/5/2006.

Il 2D-Plus è stato esplicitamente progettato per massimizzare la densità dei dati. Il formato grafico presenta una struttura quadrangolare, con dimensioni definibili a piacere dall'utente. Attualmente la dimensione massima testata è di 7" x 8". In figura, l'aspetto tipico di un timbro in codifica 2D-Plus.



Le sue caratteristiche sono:

- formato grafico di struttura quadrangolare ma di dimensione variabile per contenere i dati necessari;
- percentuale massima di errore tollerabile selezionabile (dal 5% al 50%) in fase di creazione del timbro;
- codice a correzione di errore Reed-Solomon;

[14] La densità dipende comunque dalla risoluzione di stampa: a 400dpi può memorizzare 500 Byte di dati per pollice quadrato con un grado di correzione d'errore pari al 27%, a 600dpi la densità sale a 1 KB per pollice quadrato.

- dati da codificare visti e gestiti come sequenze binarie pure, il che elimina qualsiasi vincolo relativo al set di caratteri da utilizzare;
- densità delle informazioni variabile a seconda della tipologia di hardware impiegato per la creazione del timbro e per la sua riacquisizione, secondo la tabella seguente.

densità di byte per pollice quadrato	densità di stampa (in dpi)	Acquisizione (in dpi)	Tipo apparati (non proprietari)
3.750	300	600	Stampante/scanner off the shelf
15.000	600	1.200	Stampante professionale Scanner off the shelf
60.000	1.200	2.400	Stampa su pellicola Scanner off the shelf
240.000	2.400	4.800	Stampa su pellicola Scanner professionale

4 L'offerta di mercato

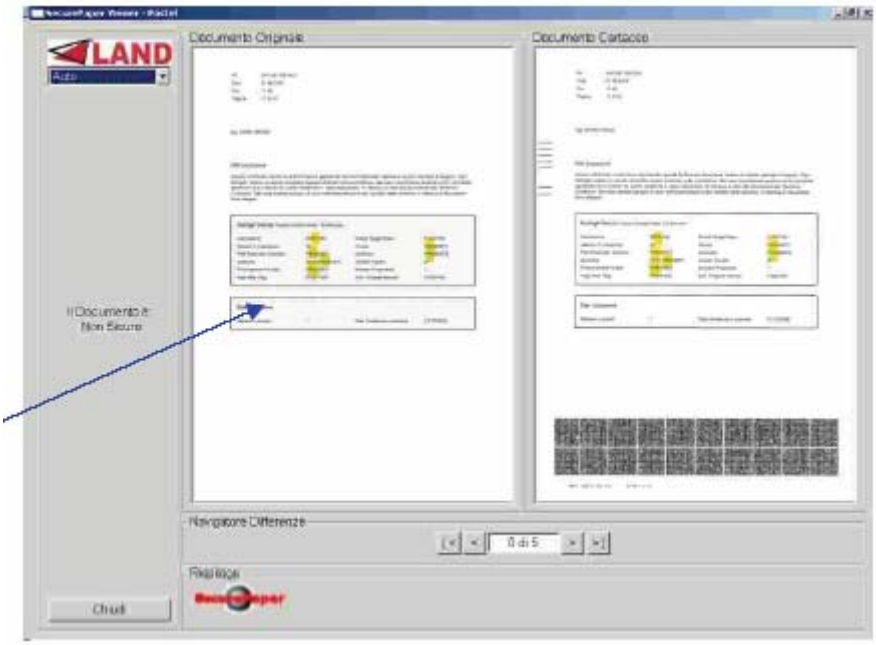
In questo paragrafo vengono esaminate, sotto l'aspetto tecnico ed economico, i prodotti commerciali maggiormente diffusi sul mercato italiano. Si sono prese in considerazione le offerte commerciali[15] delle aziende Land/Postel, Secure Edge, Everis e Xerox, in quanto tali aziende hanno già una o più soluzioni basate sui timbri digitali già implementate in Europa o negli Stati Uniti.

4.1 Land/Postel

La soluzione progettata e sviluppata da Land [6], chiamata **Secure Paper**[16], è distribuita in via esclusiva dalla società Postel s.p.a. E' attualmente basata sulla codifica DataMatrix[17], e prevede di riportare all'interno del timbro digitale l'intero contenuto del documento da securizzare.

L'offerta commerciale proposta da Postel s.p.a. prevede tre moduli software:

1. Una componente server, da integrare all'interno di un'infrastruttura di gestione documentale, per la generazione del timbro in modalità batch su grandi quantità di documenti, disponibile su varie piattaforme (Windows, Linux, Unix).
2. Un modulo client per la verifica, per il momento disponibile sulla sola piattaforma Windows. Questo secondo modulo è essenzialmente un visualizzatore, la cui interfaccia è riportata nella figura seguente. Come si vede, è possibile effettuare un confronto visivo – assistito dal software che indica i punti in cui sono state riscontrate differenze - tra il documento cartaceo scansionato (a destra) e il contenuto del timbro riportato in chiaro (a sinistra).



3. Un modulo definito "stampante virtuale", che consente la stampa del timbro digitale, in modalità interattiva, su documenti di vari formati. Questo modulo è disponibile su piattaforma Windows.

[15] Si sottolinea comunque che questo settore è in rapida evoluzione, e che nuovi attori possono entrare o uscire dal mercato con rapidità.
[16] Per questa soluzione è stata presentata, in data 2/2/2004, la domanda all'ufficio italiano dei brevetti num. RM2004A000055, dal titolo "Metodo e sistema per la verifica della conformità all'originale di un documento cartaceo".
[17] Land ha comunque intenzione di sperimentare in futuro altre implementazioni di questa soluzione, basate su codifiche differenti da DataMatrix, ad esempio Dataglyph.

Tra gli utilizzatori della soluzione Secure Paper si può citare il Ministero dell'Economia e Finanze.

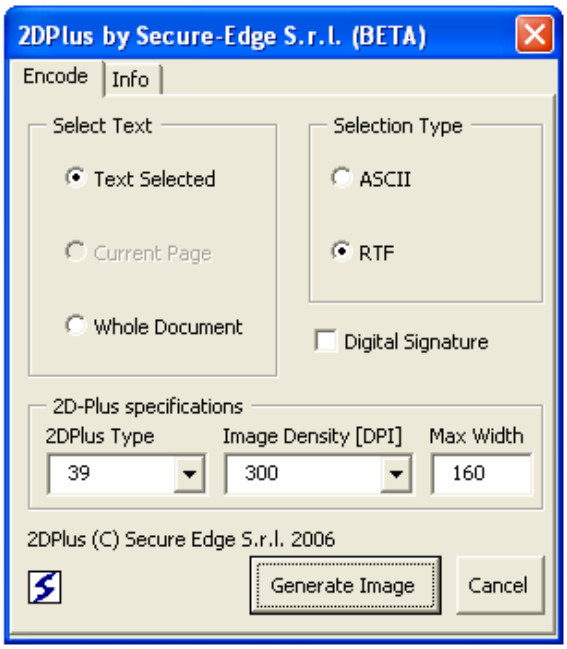
4.2 Secure Edge

La società Secure Edge [7] opera nel campo dei timbri digitali sin dal 2001. La sua soluzione, denominata Paper e-Sign [8], è basata sulla codifica proprietaria 2D-Plus. Il brevetto italiano che la copre è il numero 0001323223 del 06/08/2004[18], "Procedimento per l'autenticazione di documenti a stampa tramite firma digitale, e per la loro verifica quando richiesto".

La suite Paper e-Sign prevede una componente "server" (Appliance Paper e-Sign) per la realizzazione del timbro. Questa componente, che comprende un dispositivo HSM (Hardware Security Module), provvede all'operazione di firma digitale del documento e alla generazione del timbro corrispondente.

La suite prevede inoltre una componente "client" (Verifica Paper e-Sign) per la verifica del timbro. Tale componente effettua le seguenti funzioni:

- controllo di integrità dei dati;
- verifica il certificato presente sul documento;
- prospetto a video dei dati in chiaro.



La componente client è disponibile su piattaforma Windows e su PDA con sistema operativo Pocket PC.

E' inoltre disponibile un plug-in per la suite Adobe LiveCycle, che si integra con il modulo "BarCoded Forms", e un plug-in per Microsoft Word, da utilizzare all'interno del suddetto programma di videoscrittura, e richiamabile con un pulsante sulla barra comandi.

Nella figura a fianco è mostrata la maschera di quest'ultimo plug-in. I comandi della maschera permettono di specificare la densità, la grandezza del timbro e il tipo di codifica utilizzata. E' possibile generare un timbro che contenga un testo selezionato oppure l'intero documento, in formato ASCII oppure in formato RTF.

Tra le soluzioni realizzate da Secure Edge, oltre alle già citate applicazioni per l'AICA e per l'ACI, è da citare il nulla osta apparecchiature da gioco, per l'Amministrazione Autonoma dei Monopoli di Stato (tramite SOGEI), in esercizio da gennaio 2006.

4.3 Modalità di pagamento di Land/Postel e Secure Edge

L'offerta commerciale dei fornitori di cui sopra prevede due modalità di pagamento per le licenze d'uso. La prima modalità è basata sul numero di "form" (tipologie di documenti da gestire), mentre la seconda è basata sul numero di "tag" (timbri emessi) o di "click" (pagine securizzate).

La prima modalità prevede un prezzo unitario "una tantum" per singola form. Normalmente tale prezzo unitario decresce all'aumentare del numero complessivo delle form, con un andamento "a gradino". E' previsto inoltre un canone per il servizio di manutenzione, con un importo annuale pari a una percentuale (intorno al 18-20%) del prezzo "una tantum" di cui sopra.

[18] La domanda di brevetto era del 15-03-2001.

La seconda modalità prevede un prezzo unitario per ogni timbro emesso o pagina securizzata. Anche in questo caso il prezzo unitario ha un andamento a gradino, decrescente al crescere del numero complessivo di tag o di click. Normalmente non è previsto un canone annuo per la manutenzione.

La scelta tra le due modalità dipende dall'applicazione da implementare: se si prevede di inserire il timbro digitale su un gran numero di documenti dello stesso tipo (per esempio nel caso del cedolino elettronico), sarà più conveniente la prima modalità; viceversa, se si prevede di gestire un numero limitato di documenti ma di molti tipi diversi (per esempio il rilascio di certificazioni varie) sarà più conveniente la seconda modalità.

In caso di acquisizione di soli servizi di securizzazione di documenti e non di licenze d'uso, sono inoltre possibili modalità di pagamento alternative.

4.4 Everis (precedentemente DMR Consulting)

La soluzione Everis [9] si basa sulla codifica PDF417, e non presenta costi di licenze d'uso (il prodotto è open source), ma solo un costo per l'integrazione dei componenti nell'infrastruttura tecnologica e applicativa del cliente.

Dunque, da un punto di vista economico, è difficile confrontare questa soluzione con le precedenti. E' comunque utile riportare le seguenti considerazioni:

- Il costo della soluzione Everis, coincidendo con i costi di integrazione, non dipende dal numero di "tag" emessi.
- Viceversa, il costo potrebbe dipendere dal numero di "form", in quanto applicazioni che gestiscono più tipologie di documento richiedono presumibilmente un maggiore onere di realizzazione.
- I costi di integrazione, comunque, non sono nulli per le soluzioni illustrate nei precedenti paragrafi: è presumibile infatti che ogni applicazione necessiti di un certo lavoro di personalizzazione del prodotto software di base.

4.5 Xerox

Xerox non offre (almeno in Italia) una soluzione completa, ma solo la tecnologia di base (Dataglyph) su cui implementare un'applicazione. La sua offerta si concretizza quindi in un Software Developer Kit, venduto a licenza d'uso per singolo progetto, basato sul linguaggio C con librerie predefinite per le piattaforme Windows, Linux, Solaris, MacOS X, MVS.

Negli Stati Uniti, soluzioni software Xerox basate sui Dataglyph sono usate da industrie produttrici di componentistica per aerei (in questo caso, i timbri bidimensionali possono anche essere apposti direttamente sul pezzo, e letti da sensori appositi, ad esempio pistole ottiche), da Case farmaceutiche e da assicurazioni.

5 Bibliografia

[1] Articolo XXXIX Convegno Annuale AICA Settembre 2001:
"Paper e-Sign: la firma digitale su carta"
www.secure-edge.com/img/pdf/Paper e-Sign articolo per AICA [1.2].pdf

[2] Sito relativo al procedimento AudioSign:
www.audiosign.it

[3] Sito del servizio di posta ibrida:
www.postel.it

[4] Informazioni sulla codifica PDF417:
www.pdf417.com

[5] Informazioni sulla tecnologia Dataglyph:
www.xerox.com/downloads/usa/en/d/Dataglyphtech.pdf
www.parc.com/research/projects/dataglyphs/

[6] Sito web della società Land:
www.land.it

[7] Sito web della società Secure Edge:
www.secure-edge.com

[8] Sito web sulla tecnologia Paper e-Sign:
www.paperesign.com

[9] Sito web della società Everis:
www.everis.com

[10] Articolo su Iged num. 3/2006 “La dematerializzazione dei documenti: ostacoli e soluzioni”
www.secure-edge.com/2D-Plus/2D-Plus_dematerializzazione.pdf

[11] Ufficio Italiano dei Brevetti:
www.uibm.gov.it