Il Timbro Digitale

Quando la firma digitale incontra la carta

AUTORE
SANDRO FONTANA

INTRODUZIONE

Oggi si parla di banda larga, di dematerializzazione e di cloud computing/storage, come se la carta fosse poco usata e comunque evitabile.

Nella realtà di tutti i giorni, però, siamo sì sempre più interconnessi, ma continuiamo a fare affidamento su una serie di processi, abitudini ed infrastrutture che non possono prescindere da documenti stampati.

Questi documenti, inoltre, sono in genere preparati da computer e poi ... stampati, magari su supporti speciali anti-contraffazione, e spesso spediti per posta ordinaria: questo spreco potrebbe essere eliminato gestendoli direttamente in formato elettronico, con la garanzia di integrità, di autenticità e valore legale grazie alla firma digitale.

Già dal 2001 per ovviare alla perdita degli attributi d'integrità, autenticazione e non ripudio di un documento firmato digitalmente, allorché lo si stampa, proponevamo l'uso dei codici bidimensionali, presentando il concetto di *"Firma digitale su Carta"* durante il congresso annuale AICA di quell'anno[1] Il termine Timbro Digitale fu poi introdotto da uno studio CNIPA del 2006, relativo all'autenticazione dei documenti stampati.

La garanzia di cui si parla, si basa sulla presenza di firme elettroniche/digitali, a norma di legge, all'interno del Timbro Digitale; è bene ricordare che in questo contesto è d'obbligo che all'interno del codice bidimensionale, sia presente il contenuto del documento.

I vantaggi di questo modo di operare sono molti; in primis, il documento, che poi sarà stampato, può essere ricevuto tramite posta elettronica o prelevato da un portale Internet e mantenere tutte le sue caratteristiche di integrità ed autenticità: risparmio di tempo e di carburante (con conseguente riduzione dell'inquinamento), migliore utilizzo delle risorse umane presso gli uffici eroganti: globalmente parlando, un migliore utilizzo delle risorse umane ed una più grande efficienza di gestione.

Il documento è, poi, non falsificabile e, proprio per come è pensato ideato il Timbro Digitale, è sempre possibile ricostruire il documento informatico firmato digitalmente.

TECNOLOGIE PRESENTI SUL MERCATO

L'idea di base è semplice: inserire i dati del documento e la relativa firma digitale all'interno di un codice bidimensionale, in modo che si possa generare un documento cartaceo non falsificabile e verificabile anche off-line.

In realtà l'uso di un codice bidimensionale è solo uno egli elementi necessari a formulare un sistema solido e affidabile, ma è l'elemento immediatamente evidente e quindi ce ne occupiamo subito.

Le proposte in commercio, si differenziano sia per la tipologia dei codici bidimensionali utilizzati, sia per il reale contenuto di questi codici.

La gran parte di soluzioni, si basa sull'uso di codici bidimensionali industriali (CBI) quali QrCode, Datamatrix, PDF417, MaxiCode.

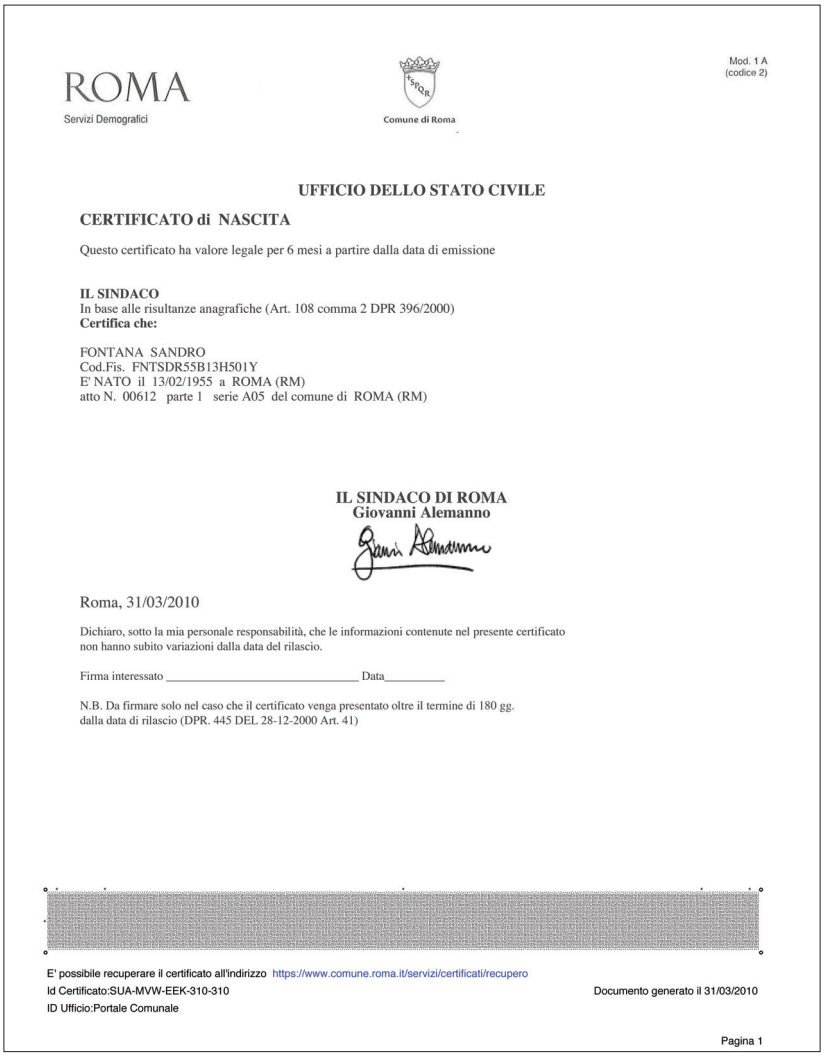
Sono anche disponibili alcune proposte basate sull'uso del QrCode, che non sono dissimili dall'uso che si fa in pubblicità di questo codice. IL QrCode può diventare abbastanza leggero (a bassa densità di informazione), tanto da poter essere letto dalla fotocamera di uno smartphone.

Come nell'uso in pubblicità, all'interno di un QrCode di questo tipo, trovano spazio poche decine di caratteri: quelli necessari per contenere una *"tinyURL"* che lo smartphone utilizzerà per accedere ad un sito su Internet.

Se per la pubblicità di un prodotto, l'indirizzamento sul sito del produttore fornisce un valore aggiunto, nel caso di una applicazione di Timbro Digitale, questa soluzione non è applicabile in modo banale.

Se applicato, ad esempio, ad un certificato anagrafico ciò comporta che la URL contenuta nel codice debba puntare ad un servizio, attivato appositamente dal Comune emittente, il quale dovrà controllare il download di documenti creati dall'utenza; dovrà quindi gestire un repository aperto su Internet in cui inserire i documenti creati su richiesta di un cittadino e rimuoverli alla loro scadenza e ..., soprattutto, dovrà gestire la sicurezza globale del servizio ed un sistema di credenziali per l'accesso: i documenti di questo tipo non sono infatti documenti pubblici.

In queste condizioni l'automatismo dell'accesso da smartphone, che funziona in pubblicità, è bloccato



ROMA
Servizi Demografici

Comune di Roma

Mod. 1 A
(codice 2)

UFFICIO DELLO STATO CIVILE

CERTIFICATO di NASCITA

Questo certificato ha valore legale per 6 mesi a partire dalla data di emissione

IL SINDACO
In base alle risultanze anagrafiche (Art. 108 comma 2 DPR 396/2000)
Certifica che:

FONTANA SANDRO
Cod.Fis. FNTSDR55B13H501Y
E' NATO il 13/02/1955 a ROMA (RM)
atto N. 00612 parte 1 serie A05 del comune di ROMA (RM)

IL SINDACO DI ROMA
Giovanni Alemanno

Roma, 31/03/2010

Dichiaro, sotto la mia personale responsabilità, che le informazioni contenute nel presente certificato non hanno subito variazioni dalla data del rilascio.

Firma interessato _____ Data_____

N.B. Da firmare solo nel caso che il certificato venga presentato oltre il termine di 180 gg. dalla data di rilascio (DPR. 445 DEL 28-12-2000 Art. 41)

E' possibile recuperare il certificato all'indirizzo https://www.comune.roma.it/servizi/certificati/recupero
Id Certificato:SUA-MVW-EEK-310-310
ID Ufficio:Portale Comunale

Documento generato il 31/03/2010

Pagina 1

In figura
Il certificato di nascita dell'autore rilasciato on-line dal portale del Comune di Roma

dalla necessità di una fase di autenticazione; inoltre non è detto che chi che deve verificare il documento in questione, abbia le credenziali necessarie ad accedere a quel particolare servizio.
Altre soluzioni inseriscono i dati del documento direttamente nel codice, magari usando più codici dello stesso tipo, ad esempio Datamatrix, per distribuire tra questi il carico dovuto alla quantità di informazioni da gestire.
L'uso di gruppi di codici, comporta alcune negatività: in queste condizioni non si possono usare lettori di codici standard ne tantomeno smartphone; per la lettura dell'insieme dei codici deve necessariamente essere usato lo scanner piano.
Inoltre essendo codici separati, anche la gestione del codice a correzione di errore (ECC) presente all'interno di ogni codice stampato rimane separata. Questo comporta che l'eventuale non lettura di uno solo dei codici del gruppo, comprometta la lettura dell'intera informazione distribuita. Per ovviare a questo evento, l'unica possibilità è quella di aggiungere uno o più codici ulteriori per la gestione di una sorta di codice di parità.
L'aggravio di spazio occupato e la minore efficienza sono evidenti.
In alcune di queste realizzazioni, inoltre, il software fornito per la lettura e la verifica del contenuto dei codici bidimensionali non consente l'estrazione del file firmato digitalmente; questo fatto è molto grave, in quanto non consente, all'utente che sta verificando il documento, l'utilizzo di un software di sua fiducia per poter validare la firma digitale. La mancanza di questa funzione, banale da implementare, lascia qualche dubbio sul reale contenuto dei codici bidimensionali stampati[2].

UN APPROCCIO DIVERSO

Quando iniziammo a pensare alla soluzione del problema della stampa dei documenti firmati digitalmente ci confrontammo a lungo, sia con potenziali Clienti sia con grandi Operatori nell'ICT, ed effettuammo svariati test con i più diffusi codici bidimensionali industriali: DataMatrix, QrCode, PDF417, DataGlyphs. Dopo due progetti andati in esercizio utilizzando il codice bidimensionale PDF417 ed una serie di ulteriori studi, divennero però evidenti alcuni i limiti dei CBI esistenti.
Limiti che derivavano dalla necessità, a nostro avviso, di contenere l'intero

In figura
Un timbro digitale 2D-Plus

documento informatico sottoscritto con firma digitale e non solo una sua parte o suoi riferimenti esterni.
Prima di tutto i CBI prevedono la gestione di dati in formato testo o decimale: inserire informazione generica (binaria) comporta uno spreco di un terzo dello spazio disponibile.
Secondo. La loro forma geometrica è fissa, generalmente quadrata e questo fatto limita molto la possibilità di stampare il codice stesso in posizioni specifiche del documento.
Terzo punto, molto importante: la quantità di informazioni che è possibile inserire in un singolo CBI non è grande; certo, i CBI sono più capienti di un semplice codice a barre, ma concretamente parlando, i 1.500 byte di capienza massima, non sono sufficienti per le esigenze di memorizzazione di un documento elettronico firmato. Da qui, come sopra ricordato, la necessità di usare più codici per avere più spazio a disposizione.
Quarto ed ultimo punto, forse la considerazione più importante visti gli obiettivi del Timbro Digitale: il codice a correzione di errore (ECC) da usare per rendere la stampa di un codice resistente all'usura, è implicito all'interno del singolo CBI. Questa caratteristica, positiva nel classico uso per la logistica di un singolo codice, diventa un problema quando si cerca di superare il limite della scarsa quantità di memorizzazione.
Infatti per aumentare la capacità del singolo CBI, l'unica possibilità è ... usarne più di uno: l'applicazione che genera il CBI può distribuire i dati da gestire, su più di un codice, ma non può agire a livello di un unico codice a correzione di errore; questo comporta che ogni CBI ha la sua struttura di ripristino dati e ... la perdita di una singola istanza di uno solo dei codici, compromette tutta l'informazione.

Alla luce di tutto ciò, decidemmo di progettare un codice bidimensionale ad hoc, con le caratteristiche necessarie a realizzare una completa Firma Digitale su Carta.
Il nuovo codice bidimensionale, il cui nome depositato è 2D-Plus, fu studiato per avere dei plus per ognuno dei punti sopra indicati; esso fu poi brevettato in Italia, in Europa e negli USA.
Inoltre, siccome la definizione di *"Firma digitale su Carta"* poteva creare ambiguità e diffidenze nel mondo legale, fu deciso che sarebbe stato meglio impiegare, per identificare un codice 2D-Plus contenente un intero documento informatico sottoscritto con firma digitale, il termine Timbro

Digitale ideato dal CNIPA.
La sua forma è quadrangolare e la grandezza del codice è proporzionale alla quantità di informazione che deve contenere (le dimensioni sono dinamiche nel rapporto altezza/larghezza): il codice 2D-Plus da stampare quindi è sempre uno solo.
La densità dei dati contenuti è la più elevata esistente; espressa in byte essa corrisponde a 3.750 byte/inch2 ovvero a 588 byte/cm2.
Il 2D-Plus è nato per contenere dati in forma binaria; quindi non ha problemi a gestire qualsiasi formato.
In ultimo, ma importante, il codice a correzione di errore (ECC) adottato è il ReedSolomon, lo standard più utilizzato al mondo ed è realizzato in modo controllato ed omogeneo su tutta la superficie del 2D-Plus.
Tale gestione del codice a correzione di errore rende il 2D-Plus particolarmente resistente ad elementi di disturbo, come macchie, graffi etc. ...
Come sopra accennato, il solo codice bidimensionale non è sufficiente a fornire una soluzione completa di Timbro Digitale: avendo a che fare con la firma digitale a norma, non si può prescindere dall'integrazione di infrastrutture hardware, dall'implementazione di software, dalla definizione di politiche di sicurezza reali e da competenza e specializzazione sulla sicurezza informatica.
In questo contesto, tenendo sempre presente la robustezza e la sicurezza informatica della soluzione, si è scelto di fornire appliance dedicati alla creazione di Timbro Digitale 2D-Plus ed apparati per la gestione dei dispositivi sicuri di firma.
È stata, poi, particolarmente curata la definizione di politiche di sicurezza e di procedure organizzative di supporto alla implementazione di pro-

getti in cui è gestita la firma digitale.
Naturalmente tutta la piattaforma è conforme, e viene mantenuta aggiornata, alla normativa corrente.
Infine, pur trattandosi di un prodotto proprietario, tutta la documentazione relativa alla Piattaforma Tecnologica ed alla sua implementazione, comprese le politiche di sicurezza suggerite, è sempre stata disponibile e liberamente scaricabile dal nostro portale: *www.timbrodigitale.com*.

A completamento della proposta relativa alla Piattaforma tecnologica, uno dei suoi punti di forza risulta essere il software di decodifica, un vero *"coltellino svizzero"* nel settore.
Il software è naturalmente di uso gratuito e liberamente scaricabile dal nostro portale. Esso può pilotare scanner piani, leggere direttamente immagini o file PDF contenenti il codice 2D-Plus, gestire questi codici da clipboard o leggere e verificare file p7m (sia nel formato PKCS#7 che CAdES).
Tra le sue funzioni base c'è quella di poter sempre salvare su disco il contenuto del codice 2D-Plus; in questo modo, il contenuto del codice 2D-Plus, cioè un file P7M, rimane sempre a disposizione dell'utente e la verifica della firma digitale ad esso applicata, può essere così effettuata da un software di fiducia dell'utente stesso.

Le applicazioni in esercizio sono molte, a partire dal documento *"nulla Osta per macchine da gioco"*, ai cedolini, ai certificati anagrafici on line o ai documenti per gli studenti universitari.
Potendo parlare solo di ciò che si conosce, attualmente circa 70 piattaforme sul territorio italiano creano documenti con Timbro Digitale, utilizzando 2D-Plus. Queste piattaforme sono in esercizio per fornire servizi a circa 100 comuni d'Italia e più di 10 Università.

Le applicazioni possibili sarebbero molte ed importanti. Quelle che sono state realizzate sono solo alcune di quelle possibili; altri documenti potrebbero sfruttare questa tecnologia: carta di identità cartacea, visti per immigrati, permessi di soggiorno, ricette mediche etc.

CAD ART. 23- TER, COMMA 5: ENTRA IN SCENA IL CONTRASSEGNO ELETTRONICO

"Al fine di assicurare la provenienza e la conformità all'originale, sulle copie analogiche di documenti informatici, è apposto a stampa, sulla base dei criteri definiti con linee guida emanate da DigitPA, un contrassegno generato elettronicamente, formato nel rispetto delle regole tecniche stabilite ai sensi dell'articolo 71 e tale da consentire la verifica automatica della conformità del documento analogico a quello informatico."

In *"contrassegno generato elettronicamente"*, si riesce facilmente a vedere una tecnica assimilabile a quella usata nella generazione di un Timbro Digitale.
Ci sono però due importanti considerazioni da fare:

- la prima è che questo comma, si sta preoccupando di dare valenza di copia conforme ad una copia analogica di documento informatico;
- la seconda è ... che prescrive qualcosa di non realizzabile: *"la verifica automatica della conformità"*

Per quanto riguarda il primo punto, è necessario ricordare che la Tecnologia di Timbro Digitale, è orientata al trasporto dell'intero documento informatico. Pensare di dover valutare la carta come una copia conforme analogica, quando si ha a disposizione il documento informatico originale, sembra un controsenso.
Fermo restando che non ci sono ancora indicazioni sui criteri e linee guida da adottare, il secondo punto non sembra, comunque, raggiungibile.
Anche avendo a disposizione dal Timbro Digitale, pardon, dal contrassegno elettronico, tutto il documento originale, avere una procedura che consenta automaticamente di sapere se una copia analogica è conforme o meno, è un obiettivo che non si può conseguire (a meno, forse, di tempi e costi di elaborazione che non rendono praticabile la scelta).
È pure vero che il Diritto è pieno di norme che si riferiscono alle copie conformi all'originale, e la cosa non può essere ignorata, anche se la gran parte di queste norme sono state pensate quando l'informatica non era presente nella nostra vita e non sempre sono state, o è stato possibile, adeguarle.
Quindi, se di copia conforme all'originale bisogna parlare, ecco il nostro contributo: per controllare la conformità di una copia analogica all'originale, quale strumento migliore può esserci se non il documento originale stesso?

In questa visione ed in attesa di criteri e linee guida esplicativi, un Timbro Digitale che contenga l'intero documento informatico sottoscritto con firma digitale, è sicuramente anche un perfetto contrassegno elettronico.

NOTE

[1] Un elenco di link a riferimenti, studi ed altra documentazione esplicativa, è liberamente disponibile qui: http://www.secure-edge.com/Appliance_PeS/doc/bibliography

[2] R. Oneda, Università di Pavia - A proposito del *"contrassegno elettronico/timbro digitale"* - http://ig.unipv.it/timbrodigitale.pdf

SANDRO FONTANA
Chief Technology Officer
Secure Edge