

A proposito del “contrassegno elettronico/timbro digitale”

di Romano Oneda¹

“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.” (CAD, art.23-ter c.5)

Un articolo di Luigi Foglia e Francesca Giannuzzi, “Il ‘nuovo glifo: nostalgia del passato?’, pubblicato il 12 aprile scorso e consultabile al link http://saperi.forumpa.it/story/55866/il-nuovo-glifo-nostalgia-del-passato?utm_source=FORUMPANET&utm_medium=2011-04-13, con osservazioni critiche importanti ed acute, ulteriormente supportate da autorevoli interventi a commento di vari autori, mi hanno stimolato, complici anche le ferie pasquali, a formulare qualche ulteriore osservazione critica sul tema del timbro digitale. Naturalmente mi adeguo anch'io ai toni parzialmente attenuati, nell'attesa dei chiarimenti promessi con le Linee guida, proprio per evitare di partire a testa bassa su bersagli che potrebbero poi rivelarsi non più tali.

E tuttavia le finalità esposte a piene lettere nel testo del CAD sopra citato, vale a dire “assicurare la provenienza e la conformità” e “consentire la verifica automatica della conformità...” appaiono chiaramente specificate e tecnicamente vincolanti, per cui, a mio giudizio, non dovremmo aspettarci da DigitPA grandi novità con le future Linee guida, ma piuttosto una consacrazione dello status sperimentale già esistente (Gazzetta ufficiale ‘securizzata’, tagliandini dello stipendio dei dipendenti statali, e altre iniziative varie in atto).

Si tratterà allora di vedere, e su questo punto vorrei offrire un modesto contributo con questo articolo, se le finalità da raggiungere sono già state, almeno in parte, conseguite con le attività ‘pionieristiche’ citate o se invece si tratta di problemi obiettivamente difficili da affrontare, se non addirittura impossibili da conseguire.

Il discorso sulla conformità mi ha fatto emergere dalla memoria il ricordo di un episodio di veramente tanti anni fa, quando, appena laureato e alle prese con i vari concorsi cui inviare domanda di partecipazione, scelsi di richiedere una copia notarile per il mio diploma fresco di compilazione.

Al ritiro trovai un foglio di carta bollata interamente scritto a mano dal notaio (le macchine per scrivere comunque esistevano già...), con bolli e timbri vari, ma che comunque stonava miseramente al confronto con la pergamena di laurea, ricca di ori, di grafica solenne e di ceralacche: era la copia conforme, così come praticata da secoli, in attesa di venir poi velocemente soppiantata dalla copia fotostatica/copia conforme che riportava fedelmente tutto quanto di testuale stava scritto sul diploma, dava conto dei nomi e delle qualifiche dei firmatari, e si ingegnava pazientemente (la cosa che più mi aveva stupito) nel descrivere l'aspetto grafico del sigillo rettorale, tanto che mi era venuto da pensare che forse avrebbe avuto maggiore successo di conformità un abbozzo di disegnano.

¹ Docente di Informatica Giuridica presso l'Università di Pavia.

Nonostante l'aspetto diversissimo si trattava di testi-messaggi equipollenti, conformi nel senso appunto di una comunità di forma, con riferimento al corretto esercizio della strategia di copia testuale consentita dalla scrittura.

Attualmente, abituati come siamo all'utilizzo pressoché esclusivo delle fotocopie, che ci restituiscono una versione appunto 'fotografica' dell'originale, difficilmente teniamo in considerazione gli aspetti tecnico-procedurali della copia 'umana', prassi secolare ma abbandonata, che però riassume interesse e valenza rilevante nel momento in cui dobbiamo istruire/programmare il computer a leggere la nostra scrittura (OCR): i problemi dell'intelligenza artificiale posta di fronte agli ardui compiti del riconoscimento della scrittura come forma significativa rinviano ad una meditazione e ad un approfondimento delle strategie mentali che ci consentono la lettura.

Le scritture alfabetiche e sillabiche utilizzano un insieme definito di poche decine di simboli (caratteri, lettere), con i quali vengono costruite sequenze e unità più complesse (parole, frasi), e infine il testo.

La strategia umana che consente questo risultato è appunto il meccanismo della percezione, che provvede ad incasellare i dati sensoriali sempre diversi in insiemi omogenei, costruzioni mentali astratte che offrono la possibilità di gestire la diversità sotto il profilo della comunità di appartenenza ad una classe logica, nel nostro caso quella del grafema.

E così le inesauribili diversità idiografiche della scrittura manuale, cui si sono aggiunte di recente le acrobazie grafiche di molti font informatici 'griffati', sono ricondotte dal meccanismo percettivo a poche decine di grafemi, attraverso operazioni mentali di grande sofisticazione, tra l'altro non ancora sufficientemente chiarite.

Un esercizio mentale di grande valenza didattica potrebbe essere il tentativo di esplicitare i criteri per cui l'aspetto grafico (glifo, allografo) di una lettera alfabetica, ad esempio la 'a' disegnata dal font Courier New, venga classificato come appartenente allo stesso grafema di un glifo 'a' chirografo, scritto a mano da noi: operazione che l'uomo compie con routine automatiche inconse, ma come istruire una macchina sulle operazioni da fare? La valenza didattica esplicita risiede naturalmente nel fatto che non possiamo rendere chiare alla macchina operazioni che non siano previamente chiare a noi.

La procedura di copia manuale, compiuta attraverso l'operatore umano, può svolgersi appunto grazie al fatto che ogni glifo riconosciuto (percepito) come appartenente ad una determinata classe grafemica risulta testualmente equipollente a tutti gli altri membri della stessa classe, per cui tutti sono titolati a 'rappresentare' il fonema, che come classe astratta di per sé può essere rappresentata solo dai suoi membri: un insieme di gatti, come è ben noto, non è un gatto...

Ed è così che grafie individuali, umane o meccaniche, anche diversissime graficamente, sono però in grado di veicolare lo stesso testo-significante, inteso appunto come sequenza di grafemi, Urtext che genera e contiene tutte le infinite possibilità della sua realizzazione fisica.

Il compito difficile, in certi casi forse impossibile, dell'OCR consiste allora nel discernere ed isolare, nella selva di puntini scanditi linearmente sul foglio scritto, degli schemi (pattern) la cui configurazione possa essere riconducibile ad un allografo di qualche grafema che il programma conosce, per cui l'operatore meccanico che emula la percezione umana possa mapparla con un codice.

Se l'operazione ha successo otterremo una sequenza di codici che, opportunamente stampati, potranno produrre un testo riconoscibile dalla parte umana come equivalente all'originale: perché abbia successo occorre però che il programma abbia già una qualche informazione sulla tipologia grafica (font) e sulla consistenza numerica (sistema grafematico) dei glifi da sottoporre a riconoscimento, pena il fallimento di qualche operazione di classificazione (chi abbia anche una sola volta affrontato la lettura di un libro dei secoli scorsi digitalizzato da Google e sottoposto ad OCR mi capirà al volo).

Un'illusione poi tipicamente umana, non rara anche in chi non è digiuno di informatica, si disvela proprio nel meravigliarsi, di fronte ad una fotografia digitale riproducente un testo, magari soltanto un cartello di avviso con poche parole, delle difficoltà dei programmi OCR a leggerci e riconoscerci un testo, considerato che noi umani invece lo scopriamo e leggiamo immediatamente.

Veniamo allora ad affrontare il nocciolo della questione, e cioè l'utilizzo del supporto cartaceo non per la rappresentazione di qualche decina di grafemi testuali ma per la memorizzazione di simboli binari. E' chiaro che qui scrittura e lettura non saranno più orientati ad una interfaccia antropomorfa, ma saranno di competenza esclusiva della macchina: le più comuni soluzioni di questo genere si affidano a codici alfanumerici, ma soprattutto a codici a barre monodimensionali e bidimensionali.

Le matrici della codifica bidimensionale Data Matrix, che esamineremo meglio più avanti e che ci sono familiari tra l'altro per essere state adottate sui fogli della Gazzetta ufficiale 'securizzata', rappresentano i valori 0 e 1 dei bit proprio attraverso i quadratini bianchi e neri (simboli); ma mentre l'uomo non procede molto oltre questa scoperta, la macchina di scansione decodifica rapidamente e con precisione la sequenza di bit a noi celata.

Occorre anche sottolineare che la codifica Data Matrix è ben attrezzata contro l'eventualità di errori di lettura dovuti a problemi del supporto (strappi, discontinuità di inchiostatura ecc.), grazie a bit aggiuntivi di informazione ridondante e a codici di correzione evoluti, tanto che può assicurare una lettura precisa anche in condizioni precarie. Inoltre non si potrebbe avere una lettura dubbia o errata, perché verrebbe immediatamente segnalata l'illeggibilità dei glifi.

Quindi, sotto un certo aspetto, potremmo non avere difficoltà a considerare anche la carta come un ulteriore supporto di memorizzazione (appunto un remake dai tempi dei nastri e schede perforate), ingannevolmente alla portata della nostra percezione visiva, accanto ai meglio noti e più efficienti supporti ottici e magnetici, non accessibili ai nostri sensi e che pure si giovano di efficienti algoritmi di correzione degli errori (errori di lettura assai frequenti, ma comunque trasparenti all'utente grazie ai controlli e rettifiche preventivi).

Come tutti i supporti di memorizzazione affidabili, quindi anche la carta, come del resto anche il metallo e gli altri supporti utilizzabili da Data Matrix, garantisce un percorso di scrittura che ne assicura la corretta reversibilità, generando in lettura la medesima sequenza di bit originari della scrittura.

È di tutta evidenza allora che i glifi di Data Matrix, essendo in grado di codificare sequenze binarie qualsivoglia, possono tranquillamente memorizzare anche documenti provvisti di firma digitale: l'unico problema potrebbe essere costituito dalla capienza delle matrici, che nella configurazione massimale (144*144, raramente utilizzata) arriva a 1556 byte (nemmeno le duemila battute della classica cartella dattilografata), per cui può risultare necessario costituire dei raggruppamenti.

Naturalmente in tutto questo discorso abbiamo dato per scontato di essere in possesso di attrezzature hardware e di software adeguati e specifici, condizione sine qua non perché l'interpretazione dei glifi risulti ineccepibile, ma anche situazione di disponibilità non frequente, se si superano certi limiti matriciali (i telefoni cellulari, ad es. riescono a leggere solo matrici di dimensioni molto ridotte).

Tanto premesso sull'affidabilità della codifica Data Matrix in ordine alla scrittura/lettura di dati binari, occorre ora esaminare la relazione tra una determinata sequenza di dati binari e la sua rappresentazione stampata come testo durevole su carta, oppure mostrata come testo effimero su di un monitor.

In questi casi ci troviamo di fronte ad interfacce specificamente costruite per le esigenze umane, al termine di un percorso che parte sì da una sequenza di bit, ma che poi si snoda in varie deviazioni di scelte di cui poi è difficile, se non impossibile, recuperare il cammino inverso. Mentre un essere umano legge senza problemi il messaggio stampato sul foglio di carta, la macchina ha bisogno di una scansione preliminare che le permetta di acquisire digitalmente una mappa del foglio, il cui risultato sarà anche funzione delle caratteristiche e delle impostazioni dello scanner, oltre che dei micromovimenti della scansione meccanica.

Questo per sottolineare che il risultato della scansione avrà comunque delle componenti aleatorie: chi non ne fosse convinto può semplicemente provare a scandire più volte di seguito uno stesso foglio stampato, senza cambiare alcuna impostazione di scansione e limitandosi semplicemente a dare un nome diverso alla mappa di bit risultante.

Ricaverà presumibilmente dei file della stessa lunghezza in byte, quindi apparentemente identici e di identica visualizzazione, ma se poi, con l'ausilio di un editor esadecimale, andrà a comparare la sequenza di bit dei vari file troverà che presentano comunque numerose differenze: ecco che già le prospettive di partenza non risultano affatto promettenti, e che eventuali funzioni di hash protesterebbero vigorosamente.

Ma su questa mappa di bit dovrà poi impegnarsi a fondo il programma di OCR, con risultati chiaramente malsicuri se i glifi utilizzati nella stampa non sono quelli tipici dei font standard, o se all'interno del testo compaiono parole di lingue diverse, o se si verificano comunque difficoltà di lettura e di categorizzazione: chiunque abbia utilizzato un programma del genere, per quanto raffinato, sa benissimo che occorre poi comunque rivedere il testo in uscita, perché non vengono date garanzie sulla precisione dell'esito (del resto anche gli umani talvolta si devono cimentare con scritture al limite dell'illeggibilità...).

Il risultato dell'elaborazione OCR sarà poi un file di testo, in una codifica che potrebbe essere ASCII, con le sue varie estensioni, o UNICODE, nei suoi vari formati (16,32,UTF8 ecc.), o altre, un file di testo che poi potrebbe assumere la formattazione caratteristica e specifica di un qualche editor testuale (Word ecc.), magari anche in una particolare versione e/o edizione, e così via distinguendo: come si può sapere se una semplicissima 'a' era stata originalmente codificata con un byte, con due, con quattro, o con una qualunque altra codifica? Il risultato di stampa è sempre lo stesso.

Dovremmo essere oramai convinti dell'impossibilità costituzionale di riuscire a ripercorrere a ritroso la via che porta da un foglio stampato con caratteri testuali alla sequenza di bit originaria, per poterla ricostruire con certezza e precisione: si tratta evidentemente di una procedura one-way,

agevole in un senso ma impraticabile nell'altro. Questo perché le informazioni fornite sul foglio stampato dai glifi dei font sono tutte *ad usum hominis*, non ci sono qui strutture informative sui bit, ridondanze predisposte per la correzione degli errori o codici di controllo utilizzabili dalla macchina, sono soltanto disegni che attendono l'intervento della vista e delle funzioni percettive dell'uomo per acquisire senso e significato.

Rimane allora da esaminare il possibile significato e funzione della scelta di compresenza, su una stessa superficie cartacea, da una parte di glifi specificamente idonei alla lettura elettronica ma inaffrontabili da un occhio umano (codici a barre bidimensionali) e dall'altra di glifi rappresentativi di grafemi (testo), perfetti per l'umano ma irrisolvibili di fatto irrisolvibili per la macchina, anche ben dotata di intelligenza artificiale, se l'obiettivo che le si pone è quello di ricostruire il cammino retrogrado verso i bit del testo di partenza.

Direi che si tratta di una situazione tipica di separati in casa: non si intravede, nelle soluzioni prospettate in Italia ma nemmeno in altre nazioni, una qualche possibilità di colloquio, di interfacciamento attraverso la classica 'connessione logica' tra le due realtà conviventi sullo stesso supporto, tale da reggere le conseguenti necessità di rigorosa verifica. E' ben vero che i codici a barre ci restituiscono un certificato, una firma digitale ed eventualmente anche il documento oggetto della firma, tutto controllabile ed ineccepibile, ma è anche vero che, in sede di verifica, mentre abbiamo a disposizione l'impronta firmata digitalmente non abbiamo alcun modo di recuperare quella originale del documento che ha generato la stampa. Di conseguenza non abbiamo la possibilità di mettere al lavoro quelle funzioni di hash che, incorruttibili mastini a guardia dei bit, ci darebbero la garanzia o il diniego dell'integrità attraverso il confronto delle sequenze originali.

La soluzione proposta nel quaderno CONSIP del 2006 "La firma digitale 'su carta' " (<http://www.consip.it/on-line/Home/RicercaGenerale/documento1115.html>), per quanto si può capire, consisterebbe nel confronto tra la bitmap del documento firmato digitalmente e codificato nelle barre 2D, e quella ricavabile da un documento pure elettronico da sottoporre a verifica, oppure, e questo è il caso che più ci interessa, nel confronto tra la bitmap firmata e quella (una delle quasi infinite possibili, data l'indefinitezza dei parametri di scansione, DPI e caratteristiche elettromeccaniche varie) ricavabile dalla digitalizzazione del foglio di carta e dalla successiva codifica in pdf. E' evidente che qui le funzioni di hash tipiche della firma digitale non hanno alcuna possibilità di utilizzo né avrebbe senso il proporle, e si dovrebbe trattare sostanzialmente di una comparazione automatica tra i pixel delle due bitmap, rappresentate visualmente sullo schermo, in modo da indicare i punti o le regioni sede di varianti e discrepanze. Insomma, una specie di suggeritore elettronico, un occhio meccanico di ausilio a chi, dovendo verificare la conformità di due documenti, abbia bisogno di aiuto.

In effetti, come abbiamo visto, la dichiarazione di conformità umana e quella digitale riposano su basi e livelli del tutto differenti: due testi che un notaio non avrebbe nessuna difficoltà a validare come assolutamente conformi possono al contrario essere rappresentazioni identiche di sequenze di bit diversissime.

La stessa rappresentazione documentale che osserviamo sul monitor del computer, appena prima di approvarla per la firma digitale, non ci dà di fatto molte garanzie sulla fedeltà e corrispondenza con quanto è soggiacente a livello di bit, anche senza dover andare a pensare a macro o a istruzioni maligne.

Dunque, una volta doverosamente ridimensionate le affermazioni enfatiche e sostanzialmente azzardate del documento Consip, come, a p.27: “In questo modo il documento cartaceo sarà protetto con lo stesso livello di sicurezza adottato con l’uso della firma digitale nel caso dei documenti elettronici, senza che sia in alcun modo interrotta la catena del “trust” che procede dall’autore del documento fino al fruitore finale.”, potremmo magari apprezzare il servizio dell’applicazione viewer fornita nei limiti di quello che dovrebbe fare, e cioè servire per una comparazione visuale dei documenti in pdf. E’ quello che ho cercato di verificare con qualche prova di cui ora riferirò brevemente.

Gazzetta ufficiale ‘securizzata’

Sempre citando dal documento Consip (p.28): “La verifica di un documento reso ‘sicuro’ consente di stabilirne l’autenticità, l’integrità e la non-ripudiabilità. Analogamente alla fase di produzione, il processo si applica al documento in formato elettronico (pdf, tif, bmp, ecc.). Qualora si intenda verificare lo stesso documento, una volta stampato sarà sufficiente effettuare una scansione con l’apposito software di seguito denominato Viewer. L’acquisizione in formato elettronico del documento cartaceo da verificare può essere effettuata attraverso un comunissimo scanner, rendendo possibile la verifica da parte di qualsiasi persona o ente.”

Confidando nelle sopraccitate rassicuranti affermazioni, e dotato come sono appunto di comunissimi scanner, ho cercato di fare qualche esperimento concreto con la Gazzetta ufficiale ‘securizzata’, mettendomi nei panni di un cittadino comune, magari un ‘casalingo vogherese’ un po’ informatizzato, che volesse sperimentare il valore aggiunto di sicurezza fornito dai glifi impressi sulla Gazzetta ufficiale.

Il punto di partenza dell’esperimento è naturalmente il sito della Gazzetta ufficiale (<http://www.gazzettaufficiale.it/>), da cui è possibile scaricare gratuitamente, in versione pdf securizzata, il sommario di una copia risalente ad una data non anteriore ai sessanta giorni. Con il link, disponibile nella stessa pagina, al Guritel, troviamo anche la presentazione (<http://dbase.ipzs.it/indispol/presentazione/index.html>) del procedimento di securizzazione e le istruzioni per la verifica di autenticità. Viene fornito il link per scaricare il viewer da installare sul proprio computer (<http://dbase.ipzs.it/indispol/download/SPViewerSetupIPZS.exe>), precisando che “L’applicativo consente di controllare una pagina di G.U. sia in formato PDF che in formato cartaceo: in quest’ultimo caso deve essere preventivamente scannerizzata e trasformata in formato PDF. Nel caso si desideri “verificare” una pagina cartacea e’ necessario utilizzare scanner compatibili con lo standard *Twain*; per ogni informazione sull’utilizzazione dell’applicativo si rimanda alle indicazioni riportate sullo stesso”.

L’applicativo fornito si chiama “SecurePaper Viewer 2.3.4” con intestazione “Istituto poligrafico e Zecca dello Stato S.p.a. - Verifica di autenticità della Gazzetta Ufficiale della Repubblica Italiana”: è un prodotto della Land S.r.l. (www.land.it). Appena avviato mi segnala cortesemente la disponibilità di un aggiornamento consigliato, che io mi affretto ad accettare; in effetti viene scaricato il file ‘spviewer_2_3_7_rev690.zip’, e però al termine dell’installazione appare l’avviso “Impossibile aggiornare il Viewer, i seguenti plugin non possono essere aggiornati: Plugin SKIN IPZS. Per aggiornare il viewer disinstallare manualmente i seguenti plugin e poi procedere di nuovo con l’aggiornamento.”

Nonostante vari tentativi, anche con privilegi amministrativi, il plugin incriminato non si lascia disinstallare, e per di più in fase di successivo riavvio l’applicativo richiede di essere reinstallato,

perché non trova più il plugin di ‘customizzazione grafica’: insomma, un loop infinito, ed il casalingo comincia ad avere qualche dubbio... ; per fortuna gli sovviene del fatto che lo stesso applicativo viene pure utilizzato per la verifica del DURC, per cui dal link http://www.sportellounicoprevidenziale.it/DURCWeb/theme/documentation/SPViewerSetupINAIL_2_3_7.exe riesco finalmente ad ottenere la versione aggiornata.

Ho quindi utilizzato il programma per attivare le due fasi del processo di verifica, così come indicate dalla presentazione, e cioè:

- un primo livello di verifica per accertare, senza necessità di collegamento internet, il certificato di provenienza, gli estremi ed il tipo di G.U. comprensivo di numero di pagina.
- un secondo livello di verifica per evidenziare, attraverso la rete telematica, eventuali differenze tra il testo originale (archiviato sui server del Poligrafico) e quello riprodotto in "locale" rilevando, dal confronto, eventuali alterazioni di contenuto.

Ho allora scaricato il sommario della Serie generale del 14 aprile (SG086.pdf) e l’ho indicato al viewer come file (in alternativa allo scanner) da utilizzare come sorgente, nella selezione proposta in apertura. Il programma mostra l’anteprima della pagina iniziale e le miniature delle cinque pagine contenute nel file, consentendo la scelta della pagina da verificare.

Sono ben visibili, al fondo di ogni pagina e allineati a destra, quattro simboli (matrici di glifi) Data Matrix di dimensione 104x104 e articolati su sedici regioni di dati, simboli con una capacità massima di 814 byte (in base256) ognuno, per cui la possibilità di memorizzazione complessiva dei quattro non supera di molto i 3200 byte: decisamente insufficienti per contenere una bitmap della pagina e appena sufficienti per ospitare un certificato, una firma digitale e qualche indicazione testuale.

Confermando la scelta di una pagina da analizzare, il programma la analizza ad alta risoluzione e provvede a decodificare il contenuto delle matrici, annunciando poi che ‘La pagina è certificata’ (qualunque cosa significhi tale affermazione) ed offrendo la possibilità di visionare il certificato e le informazioni (presumibilmente il contenuto testuale firmato digitalmente).

Se si esaminano i dettagli del certificato però l’impressione che se ne ricava è pessima: ne risulta un prodotto faldate, evidentemente (si spera) una bozza di lavoro, compilata senza minimamente tener conto delle regole nazionali e internazionali in materia, rilasciata da IPZS a se stesso, quindi senza nessuna garanzia ed autorità legale se non quel credito che possiamo essere disposti a concedere sulla parola. Inoltre non c’è traccia di quanto preannunciato nella presentazione già citata a proposito della firma del responsabile:”_La ‘firma digitale’, apposta dal responsabile della pubblicazione (Ministero della Giustizia), assicura la conformità del contenuto della Gazzetta Ufficiale in versione digitale ovvero che l’oggetto della sottoscrizione non ha subito alcuna alterazione rispetto alla versione cartacea.”

Di conseguenza, ben lungi dall’essere un certificato qualificato, il nostro ha tutta l’apparenza di un certificato piuttosto squalificato.

Cliccando poi su ‘Informazioni’ ci viene fornito il testo letterale “Gazzetta Ufficiale n. 86 del 14-04-2011 Serie Generale Pagina n. 1 del sommario”, che dovrebbe essere, presumo, il documento sottoposto a firma digitale, in modo da non consentire di alterare l’indicazione della pagina della Gazzetta cui fa riferimento.

Viene anche offerta la possibilità di salvare il testo sopra indicato come busta PKCS#7, con l'estensione canonica .p7m, il che mi aveva reso particolarmente soddisfatto, perché finalmente sarebbero state rese possibili verifiche indipendenti sul documento e sulla sua firma digitale. Si può immaginare la mia delusione quando ho dovuto constatare che il file, pur salvato automaticamente con l'estensione .p7m, era in realtà un comunissimo file di testo, che riproduceva esattamente quanto sopra mostrato nella finestrella delle informazioni. Sarebbe lecito chiedersi se i 'sistemisti' di IPZS (così si denominano nel certificato) hanno qualche pallida idea della struttura di una busta PKCS#7 e del perché non hanno avvisato l'utenza del fatto che in realtà viene salvato un file di testo, ma penso che, purtroppo, la spiegazione sia analoga a quella del certificato sopra esaminato.

Poiché poi, come si vedrà, risulta codificato nei glifi anche il link al file pdf relativo alla pagina specifica 'securizzata' giacente sul server Guritel, sembra logico presumere che anche il link faccia parte del testo documentale firmato digitalmente, anche se non mostrato tra le informazioni.

Successivamente l'applicativo SecureViewer propone la possibilità di eseguire il confronto della pagina sotto esame con quella 'ufficiale' depositata sul server IPZS (ma non memorizzata nei glifi, per i motivi di spazio già indicati): cliccando su 'avanti' il programma, se risulta disponibile un collegamento Internet, scarica la pagina. Nel mio caso (14 aprile) il link era: http://www.gazzettaufficiale.it/spws_retrieve/gusec?hash=1c8d3868a8bed41b14d97a0d61fd5bd9bb5ced1bb48bf80a73c89cca1f2e4036ddb98fffe28b42454b8ed9faaa888e2248d5d036cd1165c1713b01d8c124bd012011086g00002011-04-140001.

Viene così scaricata (come *gu.pdf*) la pagina richiesta per il confronto visuale del contenuto: è importante comunque rilevare che il collegamento previsto non è sicuro, anche se sarebbe bastato ben poco per passare ad 'https': ulteriore leggerezza che non depone certo a favore del rispetto delle esigenze della sicurezza tanto decantata.

In presenza delle due versioni in pdf l'applicativo procede ad un confronto delle bitmap, per quanto si può presumere, e segnala alla fine dell'esame i punti di divergenza riscontrati; è possibile zoomare ampiamente i pixel non coincidenti in modo da individuare chiaramente le differenze riscontrate dalla procedura automatica.

Ho fatto qualche esperimento con pagine della citata G.U. lievemente modificata, e l'applicativo ha correttamente evidenziato le discrasie introdotte. Appare chiaro comunque che la valutazione finale sulla conformità o sull'accettabilità delle differenze non può che spettare al giudizio umano, per cui si conferma il ruolo ausiliario di un simile automatismo strumentale.

Per ulteriore esperimento ho anche sottoposto all'esame del viewer una pagina bianca, contenente soltanto i glifi della G.U. sopra indicata: il programma mi ha subito garantito che 'la pagina è certificata', ma non è il caso di stracciarsi le vesti, sappiamo ormai che l'affermazione si riferisce soltanto a quanto è contenuto nei glifi Data Matrix, del resto della pagina il programma non ne sa ancora nulla. Solamente quando gli si dice di scaricare la pagina 'ufficiale' per effettuare il confronto tra le due versioni visuali inizia un intenso lavoro di elaborazione, protrattosi nel mio computer per più di dieci minuti, al termine del quale annuncia di aver trovato '7 difformità' (le sette zone bianche del documento): probabilmente qualche routine di controllo preliminare in più avrebbe ridotto soprattutto l'attesa dell'utente, comunque non si può negare lo scrupolo nell'investigazione...

Rimarrebbe ora, *last but not least*, il caso più importante, quello per cui si giustifica la proposta di adozione del timbro digitale e della ‘securizzazione’ del cartaceo, verificata attraverso l’acquisizione via scanner e la conseguente digitalizzazione.

Qui purtroppo i miei esperimenti casalinghi sono risultati fallimentari, ed ho di conseguenza ben poco da riferire, mentre sarei ben lieto di apprendere da altri sperimentatori di esiti coronati da successo.

Nonostante la già citata assicurazione di Consip (“L’acquisizione in formato elettronico del documento cartaceo da verificare può essere effettuata attraverso un comunissimo scanner, rendendo possibile la verifica da parte di qualsiasi persona o ente.”) le mie prove, effettuate con tre tipi diversi di scanner (TWAIN compatibili, of course), sia con uscita diretta in formato .pdf sia con uscita .bmp trasformata poi in .pdf hanno monotonamente generato nel viewer il disperante messaggio ‘non è stato possibile decodificare i glifi del documento acquisito’. Anche il mio scanner laser a pistola, che legge al volo i simboli Data Matrix codificati su due regioni nei documenti più comuni (bancari, bollette luce e gas, Agenzia delle entrate, Inpdap, Inps ecc.) arretra confuso e intimidito davanti alle sedici regioni dei simboli della Gazzetta ufficiale, per cui è lecito pensare che probabilmente non saranno tanto comuni (tanto meno ‘comunissimi’) gli scanner in grado di affrontare con sicurezza questo tipo di decodifica, e nemmeno tanto frequenti le dotazioni di tali strumenti presso le persone comuni o gli enti con cui il cittadino ha più frequentemente a che fare.

Conclusioni

Dall’esame della sperimentazione effettuata dall’IPZS con la G.U. securizzata emerge chiaramente, a mio giudizio, l’inadeguatezza della soluzione adottata in rapporto alle finalità conclamate: il timbro digitale non è in grado, costituzionalmente, di rapportarsi ad altro che non sia digitale, per cui non sembra ipotizzabile né credibile una operazione di ‘securizzazione’ di un documento cartaceo rappresentato a stampa con grafemi.

Questa tesi trova recente conferma, tra l’altro, anche nel documento **ETSI SR 003 232 V.1.1.1** (2011-02), che si occupa, tra l’altro, di *Printable Representations of Electronic Signatures*, e che, al punto 4.2, chiaramente afferma: “The encoding of graphics and text formatting cannot be precisely created from a printed document. It is only possible to verify a printable signature reference with the original digitally encoded document.”

Sarebbe interessante ed importante che qualche volonteroso proseguisse nell’esame così avviato, con strumenti non specialistici, dando conto delle specifiche adottate nella securizzazione del cedolino elettronico, del DURC ed eventualmente di altre sperimentazioni analoghe: sarebbe una condivisione di esperienze senza dubbio utile anche a chi avrà il compito di definire le caratteristiche tecniche del timbro digitale.

Come ultimissima annotazione, segnalo che da almeno una settimana il sito della Gazzetta ufficiale ha sospeso, tra l’altro, il servizio di fornitura gratuita dei sommari securizzati in pdf; un avviso promette comunque una rapida cessazione dei messaggi ‘not found’ da parte del server e la ripresa delle funzionalità consuete.