Firmare digitalmente documenti PDF con strumenti Open Source: Opensignpdf

Premessa.

All'inizio del 2006 la firma PDF (cioè la firma digitale secondo le specifiche PDF) divenne uno dei formati di firma digitale legalmente accettati in Italia. [0].

In precedenza, l'unico formato con valore legale sancito era il PKCS#7, che è un formato standard ma non di largo utilizzo per i documenti elettronici, ed è più una busta per il trasporto di informazioni crittografiche quale la firma digitale di un generico contenuto binario.

Poche settimane dopo noi del Servizio Sistema Informativo del Comune di Trento fummo contattati da Antonino Iacono, uno sviluppatore indipendente molto attivo nel campo degli strumenti Open Source per la firma digitale; Antonio è il creatore del progetto **OpenSignature** [2], vincitore nel 2004 del premio '"Open Source Contest" [3] come progetto più innovativo. Avevamo già collaborato molto fruttuosamente con Antonio per permettere l'utilizzo del nostro software **j4sign** in Linux, cosi reagimmo con interesse quando ci chiese di valutare un suo prototipo di strumento open source per firmare un generico documento PDF.

1. Pro e contro della Firma PDF.

Firmare file PDF è interessante per la notevole diffusione di questo formato; non si tratta di un formato indipendente, dato che il suo sviluppo non è resposabilità di un'organizzazione di standrdizzazione, ma non sono (nè saranno) richieste royalties per il suo utilizzo, sia in lettura che in scrittura, e le specifiche sono esaustive e pubblicamente disponibili [4].

La normativa italiana, inoltre, obbliga chi controlla lo sviluppo di un formato riconosciuto legale per la firma digitale a fornire a titolo gratuito uno strumento di verifica.

In generale i criteri per ammettere un nuovo formato è possibile sottoscrivere con il CNIPA uno specifico protocollo d'intesa, in cui il sottoscrittore si imoegna ad assicurare [1]:

a) *la disponibilità delle specifiche necessarie per lo sviluppo di prodotti di verifica o di generazione e eventuali librerie software necessarie per lo sviluppo di prodotti di verifica di firme digitali conformi al formato oggetto del protocollo d'intesa;*
b) *l'assenza di qualunque onere finanziario a carico di chi sviluppa, distribuisce o utilizza i prodotti menzionati al comma precedente;*
c) *la disponibilità di ogni modifica inerente a quanto indicato alla lettera a) con un anticipo di almeno 90 giorni rispetto alla data del rilascio di nuove versioni del prodotto che implementa il formato di busta crittografica oggetto del protocollo d'intesa;*
d) *la disponibilità, a titolo gratuito per uso personale, di un prodotto per verificare firme digitali del formato oggetto del protocollo d'intesa e visualizzare il documento informatico oggetto della sottoscrizione;*
e) *la capacità di utilizzare le informazioni contenute nell'elenco pubblico dei certificatori di cui all'Articolo 41 delle regole tecniche e nelle liste di revoca di cui all'Articolo 29 del*

citato provvedimento nel prodotto di verifica di cui al comma precedente.

Dato che la firma è una caratteristica del formato file, alcuni vantaggi pratici diventano possibili:

1. E' possibile firmare parti diverse di uno stesso documento con firme diverse, e fornire un suggerimento visuale riguardo sia al firmatario che all'ambito della firma.
2. E' possibile (ed è quello che lo strumento più diffuso per la visualizzazione PDF fa) rilevare quali parti del documento sono soggette a modifiche dinamiche, ed avvertirne il sottoscrittore (questo è proibito dalla legge italiana, cioè la firma di un contenuto digitale che cambia nel tempo non è valida).

Il problema principale della firma PDF è la mancanza di strumenti indipendenti che implementino le caratteristiche delle specifiche inerenti la firma digitale. In particolare, non c'è alcuno strumento Open Source che implementi firme MDP. MDP sta per "Modification Detection and Prevention", e le firme relative sono conosciute informalmente come "firme dell'autore", un particolare tipo di firme che "sigillano" il documento, garantendo all'autore la possibilità di ammettere solamente alcuni tipi di modifiche del contenuto, o nessuna modifica.

Ad esempio, un atto formale potrebbe essere soggetto a modifiche solo in alcune parti (ad esempio per aggiungere pareri o assensi da parte di qualche altra entità), e sigillata con la propria firma dal creatore per tutto il resto.

Opensignpdf è un tentativo di ovviare a questa carenza di strumenti per la Firma PDF nel dominio dell'Open Source.

2. Opensignpdf

Opensignpdf è scritto in Java, e basato sulla nota libreria java open source **iText** [5].

Il ruolo del Sistema Informativo del Comune di Trento nel progetto è stato concentrato in particolare nell'aggiungere il supporto per la Marcatura Temporale. La versione corrente è la 0.0.4, supporta smart cards per le quali è disponibile un'interfaccia pkcs11, e può essere usato per creare firme PDF "normali" e anche di tipo MDP.E'presente anche il supporto per servizi di Marcatura Temporale (Timestamping services) in linea con RFC 3161.

Il codice è liberamente accessibile con licenza GPL dalla sezione Download del sito Opensignature :

http://sourceforge.net/project/showfiles.php?group_id=67103&package_id=188602

Attualmente è possibile aggiungere firme semplici di tutto il contenuto, e anche firmare campi individuali.

Opensignpdf ha ricevuto l'interesse dei creatori della libreria iText per una possibile inclusione nel progetto principale. Sono inoltre giunti diversi consistenti contributi, sia in termini di codice, che di segnalazione di problematiche, anche a livello internazionale (Spagna, Svizzera, Ungheria, ..).

Riferimenti

[0] – 16 Febbraio 2006 – annuncio del Protocollo d'intesa CNIPA-Adobe .

[1] – CNIPA (Centro Nazionale per Linformatica nella Pubblica Amministrazione) - Deliberazione 5/2005, 17 Febbraio 2005 (in Italian).article 12.9.

[2] – Sito web di OpenSignature.

[3] – Vincitori dell “Open Source Context” .

[4] – Specifiche PDF .

[5] – Sito web di iText : http://www.lowagie.com/iText/ .