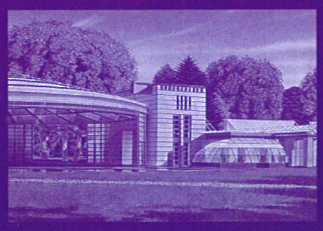
AICA 2001



VILLA ERBA
CERNOBBIO (CO)

TECNOLOGIE INNOVAZIONE E SOCIETÀ

19 - 22 Settembre 2001

Paper e-Sign®: la firma digitale su carta

Paper e-Sign®: digital signature on paper

Sandro Fontana
Secure Edge S.r.l.
sfontana@secure-edge.com s.fontana@computer.org

ACM, AICA, ICSA, IEEE, ISOC, USENIX

Abstract

La tecnologia di firma digitale è accettata ogni giorno di più come la soluzione che permette lo scambio di documenti rispettando le caratteristiche d'integrità, non ripudiabilità ed autenticità. La catena del valore del documento elettronico è così rinforzata, consentendo nuove possibilità nel B-to-c e nel B-to-b. Il mondo reale però necessita ancora della carta e qui nascono i problemi, perché il processo di stampa interrompe la catena del valore della firma digitale.
L'articolo che segue, introduce una metodologia che permette agli utenti di mantenere inalterata questa catena del valore ed in alcune situazioni di renderla ancora più robusta.

The digital signature technology is being accepted more and more as the solution that enables the exchange of digital documents fulfilling the requirements of integrity, non-repudiation, and authenticity. The value chain of electronic documents is thus reinforced, allowing new possibilities for B-to-c and B-to-b. In everyday life though, we still need paper documents but the printing process breaks the value chain of digitally signed documents.
The following article introduces a methodology that allows the user to maintain unaltered the value chain of digital signatures. Moreover, in some cases, it reinforces the process

1. Concetti Generali

1.1. Firma Digitale

La firma digitale, anche se tra difficoltà e vincoli legali [DPC 99] e pratici, sta divenendo una realtà che abilita, di fatto, lo scambio legale e formale di documenti in formato elettronico, grazie agli attributi di certezza del mittente, integrità e non ripudio che implica in se.

La catena del valore del documento elettronico viene così enormemente irrobustita, consentendo nuove possibilità nell'e-commerce e nel Biz-to-B. Il mondo reale però necessita ancora della carta e proprio qui nascono i problemi, perché il processo di stampa interrompe la catena del valore di un documento elettronico firmato.

Le leggi in Italia ed in Europa, anche se con regolamenti [DPR 97] ed orientamenti differenti, consentono ed accettano l'utilizzo delle tecniche della crittografia a chiave pubblica allo scopo di realizzare una firma digitale legalmente valida.

Proprio in relazione alla firma digitale, ci si è però trovati davanti ad una "interruzione" della catena del valore della firma quando il documento elettronico viene stampato.

1.2. La catena del valore della firma digitale

Il processo classico di stampa di un documento elettronico, interrompe la catena del valore del documento stesso per vari aspetti:

- il documento non è più banalmente acquisibile, gestibile e trasferibile se non dopo un processo di data entry che comporta impegno di tempo e plausibilmente introdurrà delle variazioni se non errori rispetto all'originale

- dal punto di vista della firma digitale, gli attributi d'autenticità, integrità e non ripudio sono persi per sempre.

In un processo di stampa tradizionale, infatti, gli attributi d'integrità, certezza del mittente, non ripudio ed eventualmente di una data certa di creazione e/o firma, non vengono riportati sulla carta e sono definitivamente persi; il documento a questo punto necessita nuovamente di una firma tradizionale, perdendo così gli enormi vantaggi di essere nato in formato elettronico e di essere stato firmato con le tecniche della firma digitale.

1.3. Paper e-Sign® : una soluzione possibile

La soluzione a questo problema consiste nella stampa, non solo del semplice documento, ma anche di quanto necessario per mantenere e verificare gli attributi legati al processo di firma digitale.

Allo scopo di estendere la catena del valore della firma digitale ai documenti cartacei, è stata definita una speciale modalità d'uso [ANG 01] denominata Paper e-Sign®.

Tramite questa modalità d'uso, qualsiasi documento firmato con le "classiche" tecniche di firma digitale può essere stampato mantenendo le sue caratteristiche ed attributi originali.

Con Paper e-Sign® la stampa del documento differisce da una stampa comune solo per l'aggiunta di

un'immagine grafica (GCM), assimilabile ad un codice a barre bidimensionale che contiene i dati del documento che sono stati firmati e la loro firma

Successivamente sarà sufficiente rileggere quest'immagine tramite un lettore di codice a barre bidimensionale od uno scanner piano, per avere di nuovo disponibile in formato digitale, il documento firmato.

Le caratteristiche di questa modalità d'uso si prestano naturalmente alla missione di interfacciare la raffinata tecnologia della firma digitale con servizi di largo consumo.

Prescrizioni mediche, biglietteria aerea, bollo auto ed in generale ricevute di transazioni on-line, sono esempi di servizi che potrebbero essere rivoluzionati dall'introduzione di questa metodologia.

Condensando i dati salienti di un documento in un'immagine grafica sulla carta stampata, Paper e-Sign® può essere utilizzato per creare da remoto documenti cartacei firmati inequivocabilmente e la cui validità può essere verificata in modo immediato.

La metodologia è totalmente compatibile con gli standard crittografici riconosciuti.: X.509 [ITU-T 97], PKCS [RSA 99].

1.3.1. Codici a barre 2D

Le aziende leader nel settore dei codici a barre già da molti anni hanno sviluppato una tecnologia detta dei codici a barre 2D, che permette di codificare in un'immagine di pochi pollici quadrati alcune migliaia di caratteri.

Le esigenze applicative hanno portato allo sviluppo di diverse famiglie di codici che oggi sono supportate da altrettante famiglie di prodotti: lettori laser/CCD, stampanti, scanner.

Solo per avere un'idea dei codici disponibili citiamo: i codici bidimensionali "Stacked" che permettono di codificare circa 2000 caratteri, il "PDF417" che permette di codificare fino a 2000 caratteri, il codice "MaxiCode" che permette di codificare 138 cifre, il codice "DataMatrix" che può codificare fino a 2334 caratteri ASCII a 7 bit o 1558 caratteri ASCII a 8 bit o 3116 cifre o il codice DataGlyph™ (XEROX) che può codificare fino a 59Kbyte (vedi fig. 1 e 2)..

Fig 1: PDF417

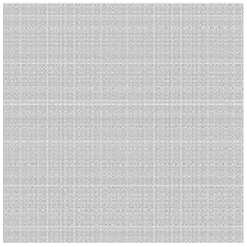


Fig 2: DataGliph ™

I diversi codici si differenziano anche per i settori di mercato per i quali sono stati sviluppati in quanto

presentano differenti caratteristiche di leggibilità e resistenza ai difetti e velocità d'acquisizione.

1.3.2. La carta come "layer" di trasporto

Con questa metodologia la carta assume un nuovo ruolo, posizionandosi come una speciale "Rete di Trasporto", o vista in ottica OSI, come Gateway possibile tra due reti digitali.

I dati stampati usando la tecnologia Paper e-Sign® da un "end-point" di una rete, possono, infatti, essere trasportati (manualmente) fino ad un "end-point" di una diversa rete e lì essere riacquisiti istantaneamente e con la certezza che tutte le informazioni fornite siano integre, in altre parole che queste informazioni non siano state modificate o corrotte durante il "trasporto": la carta diventa quindi un canale digitale sicuro.

1.3.3. Motivazioni all'utilizzo della soluzione Paper e-Sign®

1.3.3.1. Protezione antifalsificazione

Un documento stampato con questa modalità d'uso è intrinsecamente non falsificabile: qualunque variazione della parte testo, non sarà rispecchiata dal contenuto del GCM e naturalmente non è possibile la generazione di un GCM falso proprio in quanto difeso dalla crittografia a chiave pubblica utilizzata della firma digitale.

1.3.3.2. Distribuzione remota

In questo modo è finalmente possibile inviare in forma elettronica, ad esempio via e-mail, anche quei documenti che necessitando di forma cartacea, normalmente avrebbero avuto l'obbligo di essere consegnati di persona.

Il documento inviato da un punto centrale verso la periferia, può essere stampato mantenendo inalterate le sue caratteristiche di autenticità ed infalsificabilità.

1.3.3.3. Risparmio sull'acquisto e sulla gestione della carta speciale

Nei casi in cui si stampava già in remoto questo tipo di documenti, la soluzione più comune è stata quella di produrli da stazioni di lavoro specializzate, magari in enti o uffici preposti, usando speciale carta filigrana o carta con speciali immagini olografiche antifalsificazione.

I costi di questo tipo di carta ed i costi ancora più grandi associati alla gestione di questa carta speciale, sono a questo punto totalmente evitabili.

E' ovvio che del punto di vista servizio, è ora possibile che l'utente finale riceva direttamente questo documento in formato elettronico per poterlo stampare comodamente a casa su di una normale stampante

da PC.

1.3.3.4. Riacquisizione del dato

Un ulteriore anello della catena del valore è la riacquisizione del dato.

In caso di necessità di acquisire i dati presenti su un documento stampato, la prassi è sempre stata quella di riacquisire le informazioni ridigitandole di nuovo, con un enorme spreco di tempo e con la quasi certezza di introdurre errori o variazioni rispetto al documento originario.

Questa metodologia evita totalmente il data entry di queste informazioni, in quanto queste possono essere acquisite automaticamente attraverso la lettura del GCM ed inoltre l'acquisizione effettuata in questa modalità è garantita, esente da errori o variazioni rispetto al documento originale firmato.

1.3.3.5. Verifica off line

Ancora un aspetto importante è la non necessità di essere "on line" durante la verifica di un documento contenente la tecnologia Paper e-Sign®.

Questo documento è, infatti, completo di dati e firma e la sua acquisizione, la verifica e l'eventuale riutilizzazione dei dati in esso contenuti sono eventi totalmente autonomi, quindi non necessitano di controlli on line.

Naturalmente dipenderà dalle caratteristiche dell'applicazione, relativamente alla verifica della firma digitale, la necessità o meno di accesso alla CRL (Certification Revocation List) della CA che ha emesso il certificato.

1.3.3.6. Privacy

Un punto che deve essere preso in considerazione ormai da tutte le aziende è la gestione dei dati dal punto di vista della Privacy.

La legge 675 [Lex 96] tra i suoi vari aspetti, obbliga le Aziende che trattano dati di terzi, di servirsi di sistemi di protezione da accessi non autorizzati alla lettura o al trattamento dei dati.

Quando i dati o i documenti sono stampati, il rischio di violazioni della privacy diventa elevatissimo ed in alcuni ambiti certo.

Questa metodologia aiuta anche in questo senso: un documento riservato potrà quindi essere stampato solo nelle parti non sensibili, lasciando che tutto il resto dei dati rimangano presenti all'interno del GCM, eventualmente cifrati.

In questo modo durante la manipolazione del documento stampato, nessun inserviente, segretaria od impiegato comunque non autorizzato, potrà leggerne il contenuto, trovandosi di fronte alla sola rappresentazione grafica dei dati.

Ambienti particolarmente adatti a questa modalità d'uso sono ad esempio tutti quelli che trattano dati sensibili, come ospedali, cliniche, studi medici ovvero aziende che trattano dati particolarmente riservati.

2. Implementazione della tecnologia Paper e-Sign®

La necessità di trasformare il brevetto in un prodotto commerciale, ci ha portato ad identificare la realizzazione di un Appliance (sistema integrato Hardware e Software) quale soluzione generale al problema in tutti quei casi in cui la produzione di documenti è centralizzata.

I protocolli di colloquio previsti con i server applicativi sono HTTP/HTTPS o SMTP.

Il sistema presenta inoltre due interfacce di rete, in quanto ha integrata la funzionalità di High Availability (HA) che sfrutta una delle connessioni di rete per trasmettersi il segnale di Heart Beat.

2.1. Tool di verifica Off Line

Il tool di verifica è un prodotto generico che non entra nel merito dell'applicazione ma si limita ad acquisire un GCM, a decodificarlo, verificare la firma con le chiavi di firma preimpostate e quindi visualizza i dati presenti nel GCM.

L'acquisizione del GCM può essere realizzata con strumenti diversi: lettori di codici a barre 2D in tecnologia CCD, lettori di codici a barre 2D in tecnologia Laser e scanner piani.

Il software di base per la verifica è costituito da un'applicazione per Windows che interfaccia un lettore di codici a barre 2D per l'acquisizione del GCM.

Dopo la lettura del GCM, il software presenta una finestra in cui è visualizzato il contenuto del GCM e dopo averne verificata la firma, evidenzia l'esito dell'operazione che potrà essere: firma valida, firma non valida oppure GCM corrotto qualora il codice grafico presenti un numero di difetti maggiore di quello che può essere corretto dai codici a correzione introdotti.

Vengono inoltre fornite le API e tutta la documentazione necessaria per l'integrazione di applicazioni.

3. Riferimenti

Ulteriori riferimenti e documentazione sugli sviluppi possono essere trovati sul sito:

www.secure-edge.com

Bibliografia

[ANG 01]. Angelucci M., Di Piazza L.,Fontana S., Pascalucci A., brevetto di modalità d'uso "Procedimento per l'autenticazione di documenti a stampa tramite firma digitale e per la loro verifica quando richiesto ", marzo 2001

[DPC 99] DPCM 8.2.1999, "Regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, di documenti informatici, ai sensi dell'art.3, comma 1, del decreto del Presidente della Repubblica 10 novembre 1997, n.513", febbraio 1999

[DPR 97] DPR 513/97, "Regolamento recante criteri e modalità per la formazione, l'archiviazione e la trasmissione di documenti con strumenti informatici e telematici, a norma dell'art.15 comma 2, della legge 15 marzo 1997, n.59", novembre 1999

[ITU 97] ITU-T Recommendation X.509, " the directory: authentication framework" 1997

[Lex 96] Legge 675/96, "Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali", 31.12.1996

[RSA 99] RSA Data Security, Inc., " Public-Key Cryptography Standards (PKCS) ", RSA Laboratories Technical Note 1991/1999