

eSign HowTo

versione 0.2

gennaio 2005

a cura di

andrea guido sommaruga

viale tunisia, 25 - 20124 - milano

retro della copertina

inserito pensando alla gestione della stampa in fronte retro

Indice

1	Scopo del documento.....	2
1.1	Introduzione.....	2
1.2	Obiettivi.....	2
1.3	Altri documenti correlati.....	2
2	Cenni storici.....	3
3	La firma elettronica.....	4
3.1	Chiavi pubbliche e chiavi private.....	6
3.2	La legislazione in materia.....	8
3.3	nota sui formati di file.....	9
4	Come funziona il meccanismo delle firme elettroniche.....	11
4.1	firma di più persone.....	11
4.2	documento segreto.....	12
5	Breve glossario sulla crittografia.....	13
5.1	Programmi per Firmare e Crittografare.....	14
6	Crediti, Ringraziamenti, Licenza.....	17
6.1	Crediti.....	17
6.2	Ringraziamenti.....	17
6.3	Licenza.....	17
7	Impaginazione di questo documento.....	18

1 Scopo del documento

Con questo documento ci proponiamo di illustrare la firma elettronica o firma digitale per consentire agli utenti di avvicinarsi a questa tecnologia con cui un domani dovremo interagire di frequente.

1.1 Introduzione

Questo documento nasce come una libera raccolta di idee e suggerimenti con accenni ai programmi normalmente utilizzati mettendone in luce pregi e difetti.

Non è scritto pensando di sostituire i manuali di istruzione o i readme dei programmi di posta elettronica o dei sistemi operativi. Questo manuale si pone l'obiettivo di spiegare “**cosa fare**” e non “**come fare**”. Per le istruzioni operative rimandiamo alle istruzioni dei singoli programmi applicativi.

1.2 Obiettivi

L'obiettivo è forse ambizioso: vorremmo illustrare in linea di principio la firma elettronica e la crittografia toccando i vari aspetti tra cui.

La firma elettronica

La crittografia

Il valore legale

1.3 Altri documenti correlati

Per approfondimenti in merito agli argomenti trattati in questo documento è possibile consultare anche gli altri documenti correlati:

- **eDocHowTo** note sui documenti in formato elettronico
- **eMailHowTo** note sulla firma digitale e sulla crittografia
- **Schede Software Libero** schede programmi

2 Cenni storici

Parlando di firme si pensa subito a documenti ufficiali. Vediamo una breve introduzione al concetto di documento in senso lato.

Un documento non è altro che un testo scritto su un qualsiasi supporto che soddisfi almeno i seguenti requisiti minimi:

- Inalterabilità
- Paternità
- Data certa

Nei requisiti minimi volutamente non compare nulla in merito alla veridicità del contenuto.

Con i sistemi tradizionali i documenti venivano redatti su carta con inchiostro inalterabile, senza lasciare spazi o righe libere, firmati e timbrati su tutte le pagine magari davanti ad un Notaio che poneva una data ed ora certa.

Le nuove tecnologie hanno progressivamente spostato documenti dal tradizionale formato cartaceo al nuovo formato digitale. Questo passaggio non è comunque indolore, per dare piena valenza ad un documento digitale occorre essere in grado di soddisfare i requisiti minimi precedentemente illustrati.

Con la firma digitale è quindi possibile dare ad un documento digitale il pieno valore legale.

Attenzione un documento in forma elettronica firmato digitalmente resta valido (con firma verificabile) solo in forma elettronica. Non avrà mai valore una sua stampa: si deve sempre avere il documento elettronico originale per poterne verificare la firma.

Un documento firmato digitalmente nasce e vive solo in forma elettronica.

3 La firma elettronica

La diffusione di Internet ha agevolato il diffondersi della posta elettronica (email) con la quale è facilissimo inviare documenti in forma elettronica a persone anche molto distanti tra loro. Il documento generato e trasmesso in forma elettronica deve potere combattere ad armi pari con il tradizionale foglio di carta, deve quindi avere tutte le caratteristiche che gli attribuiscono "valore legale".

Firmare digitalmente un documento equivale ad attribuirgli una paternità certa e garantire l'inalterabilità del contenuto, ciò è reso possibile dai **programmi di firma elettronica**.

Con la firma autografa si aggiunge informazione al documento, la sigla che si pone sulla pagina marchia in qualche modo il foglio e può essere ricondotta all'autore in base all'impronta personale che diamo alla nostra calligrafia.

La firma elettronica, analogamente alla tradizionale firma autografa, consiste nell'aggiunta di informazioni ad un documento mediante elaborazione del medesimo con opportuni programmi di firma (in realtà di crittografia). Con questo trattamento vengono aggiunte al documento originale tutte le informazioni che servono ai programmi per verificarne paternità ed integrità del contenuto. Ovviamente per le operazioni di verifica dei documenti devono essere utilizzati gli stessi programmi usati in precedenza per le operazioni di firma.

La firma elettronica non è quindi una firma vera e propria, come potrebbe essere la firma autografa, bensì è un'elaborazione software del documento. È quindi necessario definire standard tali da garantire l'interscambio dei documenti firmati tra il maggior numero di persone possibile.

Questi ed altri vincoli sull'utilizzo dei programmi di firma porteranno inevitabilmente alla necessità di avere più di una firma elettronica a seconda dell'utilizzo che si desidera farne; questo concetto sarà chiarito in seguito.

Per dare un'idea di come si può presentare un documento firmato elettronicamente si allega un breve esempio di un testo firmato con PGP (programma disponibile gratuitamente su Internet) dall'autore. In neretto viene evidenziato il testo originale del documento, tutte le altre informazioni sono state aggiunte dal programma PGP per gestire la firma. La firma vera e propria è costituita dall'ultima riga che contiene una sequenza di caratteri apparentemente senza senso ad una semplice lettura ma che contengono tutto ciò che serve a PGP per verificare a posteriori il documento.

La firma elettronica consente quindi di attribuire paternità certa al messaggio e certezza dei contenuti. Non aggiunge necessariamente segretezza infatti il testo del messaggio resta in chiaro visibile a tutti.

Nell'esempio sotto riportato sono evidenziati in neretto il testo vero e proprio del messaggio e la firma digitale. Come si può vedere la firma digitale consiste semplicemente in una lunga serie di caratteri ASCII apparentemente senza senso. In questi caratteri vengono salvate e crittografate delle informazioni circa l'identità di chi ha firmato, la data del documento ed dei codici di controllo che permettono di verificare le eventuali alterazioni dei contenuti. **Le firme elettroniche di una stessa persona non sono quindi tutte uguali** ma differiscono volta per volta se non per altro perché cambia l'ora. Contrariamente alla firma autografa che garantisce solo la paternità, la firma elettronica aggiunge anche l'informazione temporale.

```

-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1
Esempio di testo firmato

Con i migliori saluti
andrea sommaruga
-----BEGIN PGP SIGNATURE-----
Version: PGPfreeware 5.5.3i for non-commercial use <http://www.pgp.com>
iQA/AwUBNo/X8j8XHmMEbbChEQLNHgCfXuXSE/+r8QE5Lbj5qQxK4NcAKkEAOIsFKxQR/jVDfqNR6sGerHOYP2Ce=t0Hn
-----END PGP SIGNATURE-----

```

Quello che segue è invece un messaggio firmato e crittografato, ovvero un messaggio a cui oltre alla certezza del contenuto e la paternità è stata anche aggiunta la segretezza. Oltre alla paternità aggiunta applicando la firma elettronica come nell'esempio precedente, si è aggiunta la segretezza ovvero il messaggio è stato crittografato con la chiave pubblica del destinatario, in questo caso il messaggio non risulterà più leggibile ma sarà completamente codificato. Attenzione: per tornare ad avere il messaggio in chiaro è necessario disporre della chiave privata del destinatario.

```

-----BEGIN PGP MESSAGE-----
Version: PGPfreeware 6.5.3 for non-commercial use <http://www.pgp.com>

qANQR1DBwU4DbXohFGAnz4sQCADNZCVXI6fSYhf2zifIk1m3OC1mzpZq/014FcPY
CV0tfxSypSRv7fec4RfakFPemrklgK/3eXLXtG5M9psWBkW0vBaYuPGDRP7ARfyS
ANJYuPDrrIKRoFYlplrQUIfBmZKf4yAG3Yh0YBACLf4j5RtgByVmpE0LAJW/k+p
Meb1OCP1YQ1d2oozhmf7G8FxFu+RD9l/EOqnD2pxbfTjXPg8b/1RZwzeXp3fWiiCc
gGr420I41vOWr+v9g7jCewW7m+j6Kp1+o7Gup8nuNb0Fi/4D/3HpTt5lmXvESvPA
5R/3DLdfqc2713USqU21Ss0lNZ/iQFXyS4khEqFFvwk/zyhWB/4oulm3tw47H0p6
FY3sPeI9xU+FKoOgd3hrPgNxxhoilIRJea/qvUiZzMo+cdZb5eLSSp3Easfn8Xxn
Bp1lvyjjWLD6GduKSWMq43eV/bmmajMIYfxRnfwlsczcaEW+3ojZDk4SXSwQVhJK
kxbBlLeq/qxgul3biHLfL7TQAKJqEt3VuyoPwDShAYqyYvUVTPyV29wu0IWuvB
Tp/Ne/pf5a4otoKyzP2/uWfAiUTGi9YAZR2Fr40N/oScvGr1uMd5605bRwbv0vtq
Uicvv6bVOAJ3NtrPs2afe4FF39LFOEuiURU3xvblBcW9aL59oSdg/HlgR2SJJV23
nl/8gLLpyYtEgqZKRvJ10qLDv2PcqOG7RQfLRR9yM0xD/Xf0LFOpLzeof/nA2Oig
AkB+SX3tGWQNsPtgnUKHKCD1KTc1KREOUbLS29YjQ2R+4o3sswsqPAFlxQ1JqR37
tkJALdu2zaA9EmRVV//jRuv/lfySoutAGAxiltWRSeCDXWbw0IGUS0+mnGo2h6bH
8Eex
=XFHR
-----END PGP MESSAGE-----

```

Sempre basandomi su PGP riporto per completezza un esempio di verifica di una firma. Il programma riporta le informazioni sulla firma e sull'integrità del documento. In questo caso è andato tutto bene quindi segnala quando e da chi è stato firmato e dice che il documento non è alterato “**PGP Signature Status: good**”

```

*** Signer: Sommaruga Andrea Guido <sommaa@stnet.net>
*** PGP Signature Status: good
*** Signed: 12/06/02 12.26.03
*** Verified: 12/06/02 12.26.10
*** BEGIN PGP VERIFIED MESSAGE ***

```

Quello che segue è invece un messaggio firmato e crittografato. Oltre alla paternità aggiunta applicando la firma elettronica come nell'esempio precedente, si è aggiunta la segretezza ovvero il messaggio è stato crittografato con la chiave pubblica del destinatario.

```

*** END PGP VERIFIED MESSAGE ***

```

Riportiamo un secondo esempio in cui il documento firmato il documento è stato alterato falsificandolo. La verifica della firma riporterà il nome corretto di chi ha firmato il messaggio, quindi la paternità, ma fallisce nella verifica del contenuto: viene quindi smascherata la falsificazione: **PGP Signature Status: bad.**

```
*** Signer: Sommaruga Andrea Guido <sommaa@stnet.net>
```

```
*** PGP Signature Status: bad
```

```
*** Signed: 12/06/02 12.30.38
```

```
*** Verified: 12/06/02 12.31.17
```

```
*** BEGIN PGP VERIFIED MESSAGE ***
```

Quello che segue è invece un messaggio firmato e crittografato. Oltre alla paternità aggiunta applicando la firma elettronica come nell'esempio precedente, si è aggiunta la segretezza ovvero il messaggio è stato crittografato con la chiave pubblica del destinatario.

QUESTA RIGA E' STATA AGGIUNTO DI PROPOSITO!

```
*** END PGP VERIFIED MESSAGE ***
```

Gli esempi riportati in questa sezione in realtà non hanno senso, stampati non vogliono dire nulla. Sono stati inseriti solo per darvi un'idea di come viene modificato il testo applicando le firme digitali.

La firma digitale: non è la firma autografa presa con uno scanner !

3.1 Chiavi pubbliche e chiavi private

La firma elettronica si basa esclusivamente su algoritmi matematici che elaborano

Le tecnologie attualmente disponibili si basano su algoritmi di crittografia a chiave asimmetrica e cioè basate su due chiavi: pubblica e privata. Le chiavi vengono definite asimmetriche perché la conoscenza di una delle due chiavi non svela nulla a riguardo dell'altra chiave.

In questo caso i programmi di firma si basano sulle informazioni associate alla chiave privata per “firmare” il documento. La verifica della correttezza della firma avviene solo mediante la chiave “pubblica” associata.

Questo è il punto: **con la chiave privata firmo e con la chiave pubblica verifico la firma!** La **chiave privata è e DEVE essere mantenuta segreta** mentre **la chiave pubblica è e DEVE essere resa pubblica** e cioè nota a tutti.

Una caratteristica importantissima del meccanismo delle firme elettroniche è che lo stesso documento può essere firmato da più persone e può di conseguenza essere verificato per tutte le firme. Il processo di verifica è assolutamente insensibile all'ordine con cui sono stati firmati i documenti. Per la verifica occorrerà ovviamente fornire le chiavi pubbliche di tutti i soggetti che hanno firmato.

Analogo discorso nel caso di un documento crittografato: il processo è lo stesso. Anche in questo caso il documento può essere crittografato con più chiavi pubbliche, per poterlo leggere sarà quindi necessario decifrarlo con le varie chiavi private. Anche in questo caso non è importante l'ordine con cui vengono applicate le chiavi private per la decifrazione. Ovviamente il documento cifrato è illeggibile e sarà leggibile solo dopo avere applicato tutte le chiavi private!

Risulta ora evidente il primo ostacolo da superare: la gestione delle chiavi. Affinché sia possibile realizzare un sistema di firma elettronica di uso generale è necessario, oltre ovviamente definire il programma da usare per le firme, anche definire chi si prende carico di generare le chiavi per gli utenti. Entrano in gioco a questo punto delle nuove figure che vengono definite **enti certificatori**, il cui compito è quello di fornire agli utenti le coppie di

chiavi e di mantenere un database (in realtà un server su Internet o una generica rete dati) in cui memorizzare le chiavi pubbliche accessibile in consultazione da chiunque. Questi enti svolgono il fondamentale ruolo di certificazione di identità' delle persone; devono fornire le chiavi solo dopo essersi accertati della reale identità del richiedente. In tutto il processo di firma elettronica questo è il punto più critico: dalla serietà degli enti certificatori dipende la sicurezza del sistema!

Che senso avrebbe un documento firmato digitalmente da una persona mediante certificato (firma digitale) emesso da un ente certificatore non affidabile?

La necessita' di doversi fidare degli enti certificatori porta inevitabilmente a non fidarsi di certificati emesse da enti ignoti, nasceranno quindi vari certificatori per i vari servizi che si renderanno disponibili in via telematica. Dal punto di vista del singolo questo vuole dire avere più certificati a seconda del servizio a cui vuole accedere.

Avere più certificati vuole semplicemente dire avere più chiavi private da memorizzare sul disco rigido del proprio PC sotto forma di files o da memorizzare su altri dispositivi come ad esempio le smart card (tessere formato carta di credito) a seconda della modalità di emissione da parte dell'ente certificatore.

Ovviamente il sistema di firma elettronica ideale prevede l'utilizzo di un solo programma con certificati emessi da un solo ente universale, in questo modo è possibile avere un unico certificato per accedere a tutti i servizi ma questo, almeno allo stato attuale, è pura utopia.

Esiste un ulteriore problema pratico per quanto riguarda la gestione dei certificati da parte degli enti certificatori; non è sufficiente accertarsi della reale identità della persona per fornirla di certificato ma ci si deve in qualche modo attrezzare per dare al certificato una validità temporale limitata o in qualche modo limitabile. È necessario gestire un meccanismo di revoca del certificato che consenta di segnalare all'utente che il documento risulta firmato con un determinato certificato ma che il medesimo risulta scaduto o bloccato.

A parte vari problemi pratici il processo di firma di un documento da parte dell'utente è semplicissimo; il programma esegue un'elaborazione del documento stesso per aggiungere il certificato dell'utente, questo processo non richiede nulla altro che il documento, la chiave privata ed i programmi installati sul PC.

Il processo di verifica del certificato di un documento firmato da altri richiede un passaggio in più e cioè una connessione telefonica (Internet) per accedere all'elenco delle chiavi pubbliche dell'ente certificatore da cui leggere la chiave pubblica per la verifica del certificato. Ovviamente questa fase di ricerca della chiave pubblica e di verifica del certificato è svolta automaticamente dal programma di gestione della firma elettronica.

Il passaggio dalla carta all'elettronica sarà ovviamente una specie di rivoluzione nelle nostre abitudini. Coinvolgerà tutti i tipi di professioni, vedi ad esempio i Notai che si troveranno a dovere gestire nuove tipologie di documenti, ed ovviamente anche i singoli cittadini che dovranno utilizzare nuovi strumenti molto diversi da quelli a cui sono abituati.

Affinché la firma elettronica prenda realmente piede occorre un notevole sforzo legislativo per la regolamentazione dei servizi telefonici e per la definizione di criteri universali da adottare per la validazione dei documenti elettronici.

3.2 La legislazione in materia

Sul fronte legislativo si notano dei notevoli passi avanti verso il riconoscimento, a tutti gli effetti di legge, dei documenti in altra forma rispetto ai tradizionali documenti cartacei. I vari stati si stanno muovendo per dare ufficialità ai documenti elettronici. Anche l'Italia cerca di adattarsi al profondo cambiamento in atto e, con la Legge del 15 marzo 1997 n° 59 articolo 15 comma 2, apre le porte all'era dell'informatica gettando le basi per un utilizzo sempre maggiore dell'informatica e della telematica nella generazione, nell'invio e nell'archiviazione dei documenti in forma elettronica.

Dal testo di legge: **Gli atti, dati e documenti formati dalla pubblica amministrazione e dai privati con strumenti informatici o telematici, i contratti stipulati nelle medesime forme, nonché la loro archiviazione e trasmissione con strumenti informatici sono validi e rilevanti a tutti gli effetti di Legge.**

E' quindi chiara l'intenzione di equiparare i documenti in forma elettronica ai tradizionali documenti cartacei. Nel testo di legge e' specificato un piano di interventi per arrivare, nel giro di 5 anni, a potere gestire i documenti completamente in forma elettronica e prevedere un progressivo abbandono del supporto cartaceo. Ovviamente la Legge, o meglio il regolamento di attuazione, specifica anche i requisiti che un "**documento**" deve avere per potersi definire "**documento ai sensi di legge**". Anche nel caso italiano si e' deciso di affidarsi ad un algoritmo di crittografia a chiavi asimmetriche. La Legge prevede che vengano istituiti degli enti certificatori che avranno il compito di attribuire le chiavi private e di gestire le chiavi pubbliche.

Il giorno 8/2/99 sono state emanate le prime regole tecniche per con i requisiti minimi che le società che desiderano proporsi come "certification authority" devono soddisfare, ovviamente tali regole saranno sicuramente soggette a future revisioni data la vastità e la delicatezza della materia. Questo è il primo passo per avviare la complessa gestione delle firme digitali che dovrà garantire dei requisiti di assoluta sicurezza. In termini di investimenti le società che desiderano proporsi come enti certificatori, dovranno sostenere dei costi altissimi soprattutto per quanto riguarda le infrastrutture. Oltre a determinati calcolatori dotati dei più sofisticati sistemi software di protezione dalle intrusioni, dovranno essere costruiti gli edifici rispettando determinati requisiti di sicurezza per evitare il rischio di sottrazioni di dati da parte di malintenzionati.

Ad oggi (anno 2005) esistono vari enti certificatori che emettono apparecchiature per la gestione della firma elettronica, tra queste possiamo sicuramente citare le Poste Italiane e le Camere di Commercio oltre al sistema Bancario.

Questi enti hanno ovviamente adottato sistemi proprietari per la gestione delle firme elettroniche. In linea di massima i vari sistemi sono simili e si compongono di un programma di firma e di un dispositivo per leggere le smart card su cui vengono memorizzate le firme elettroniche. I vari programmi hanno dei funzionamenti simili tra loro. Si aspettano di ricevere come input dei testi da firmare in formati standard. Ad esempio il software delle Camere di Commercio accetta i documenti in formato solo testo ed i documenti in formato Acrobat (PDF).

I vari sistemi di firma richiedono tutti una connessione internet attiva. Questo si giustifica con la necessità di avere una fonte certa per l'ora (marca temporale) ed utilizzare il database delle firme/revoche aggiornato in tempo reale. Uno dei problemi maggiori della gestione dei

database delle firme elettroniche è costituito dalla gestione delle revoche o delle durate delle firme. Le firme elettroniche possono avere una valenza temporale ben definita ad esempio possono essere valide per un determinato anno solare. In questo caso è possibile firmare digitalmente nel solo periodo di validità della firma. Superato il periodo di validità temporale la firma deve essere ovviamente mantenuta in linea dai sistemi anche se non è più attiva. Serve sempre potere verificare un documento scritto in un periodo in cui la firma era ancora valida ed il software deve dire ovviamente che la firma è autentica e che il documento non è stato contraffatto.

Oltre alla scadenza naturale delle firme devo anche predisporre i meccanismi di revoca, ad esempio in caso di perdita o furto della smart-card. In questo caso la firma deve potere essere bloccata in un qualsiasi istante. Ovviamente i database devono tenere conto anche di questa possibilità.

3.3 nota sui formati di file

Occorre fare una breve considerazione sui formati dei file. Come illustrato in precedenza la crittografia applicata per firmare elettronicamente un messaggio, consente di attribuire paternità e certezza del contenuto di un qualsiasi file. Negli esempi sopra esposti si trattava di semplici file ASCII in solo testo quindi le informazioni relative alla firma sono state inserite all'interno dello stesso file. Il file firmato in questi esempi è stato modificato.

Qualora desideri invece firmare un file che non può essere alterato, ad esempio un documento di un programma di videoscrittura, le informazioni di firma elettronica devono obbligatoriamente essere memorizzate esternamente in un file ASCII, non potendo in nessun modo alterare il file originario. La verifica della firma in questo caso richiede i due file e controlla che il file originale non risulti alterato rispetto alle informazioni contenute nel file di firma. La firma elettronica è quindi in grado di assicurarmi che il documento non è stato contraffatto.

Esiste però un piccolo punto debole della catena: in questo caso il file per essere visualizzato ha bisogno di un interprete ovvero di un programma di videoscrittura, come OpenOffice, che estrae il contenuto analizza i comandi di formattazione e compone a video il documento. Per assurdo, nel caso di un calcolatore seriamente compromesso, ci potrebbe essere il programma di videoscrittura che si comporta in modo diverso dalla copia usata per scrivere l'originale documento e quindi il documento potrebbe risultare visualizzato in modo diverso.

Questo può capitare perché ad esempio un word processor, mescola nei file dati e comandi di formattazione che verranno interpretati dal programma di visualizzazione.

Per avere la massima sicurezza con i documenti firmati elettronicamente si dovrebbe utilizzare il formato solo il classico formato ASCII solo testo. In questo caso la visualizzazione del contenuto, dopo avere verificato la correttezza della firma, è nativa senza dovere passare da nessun programma di visualizzazione quindi non è possibile vederlo diverso dal testo originale scritto.

Un'alternativa al formato solo testo consiste nell'appoggiarsi a formati standard aperti ovvero a formati basati su specifiche rese disponibili pubblicamente. Tra questi standard troviamo il formato PDF di Adobe oppure il formato PS sempre di Adobe. Acrobat ed il Postscript sono due standard veri e sono di pubblico dominio. Le specifiche per il formato PS e per il formato PDF sono pubbliche disponibili per chiunque desideri implementarle.

Nel caso dei normali programmi di elaborazione testi, tra cui il diffusissimo **Word di Microsoft**, **il formato di salvataggio dei file non è un vero e proprio standard** perché non si basa su delle precise specifiche rese pubbliche. E' solo uno formato proprietario di un determinato programma ma **ripeto è solo un formato proprietario** non uno standard aperto vero. Non è quindi consigliabile adottare questo formato per accettare dei documenti firmati digitalmente. Non considero accettabile il formato di word in quanto, per quanto detto all'introduzione, un documento firmato digitalmente nasce e vive solo in formato digitale, deve quindi sempre essere gestito e verificato mediante l'applicazione con cui è stato firmato e mediante il programma con cui è stato generato. Dato il vizio congenito di Microsoft di continuare a modificare le versioni di office, ci si potrebbe trovare tra qualche anno nella spiacevole situazione di non riuscire più a gestire i documenti creati con vecchie versioni di office e firmati digitalmente perché magari le ultimissime versioni di Office non supportano più il formato. Non è uno scenario impossibile: i commerciali di Microsoft sono sempre allenati nel trovare soluzioni che spingano gli utenti a forzati e costosi aggiornamenti.

Altri programmi di videoscrittura come openoffice, la nota applicazione della Sun Microsystems, si basano su formati aperti e si prestano alle applicazioni della firma digitale.

4 Come funziona il meccanismo delle firme elettroniche

Vediamo una breve sintesi dei processi di firma supponendo due diversi scenari. Il primo la tipica gestione di una compra vendita con tre figure in gioco ed il secondo il tipico scambio di documenti segreti con più persone in gioco.

4.1 firma di più persone

Schematizziamo il funzionamento di un processo di firma elettronica di un documento. Supponiamo di fare un caso pratico in cui un documento di compravendita di un immobile deve essere firmato dai tre soggetti venditore, acquirente e notaio. Devono quindi essere apposte al documento:

- firma del venditore
- firma del compratore
- firma del Notaio
- data dell'atto apposta dal Notaio

ovvero il documento dovrà essere firmato dai tre soggetti e dovrà inoltre ricevere la marca temporale che darà la data certa. Con la firma elettronica il processo è semplicissimo.

Il documento viene composto ovviamente elettronicamente, le varie persone firmano il documento con i loro programmi di firma elettronica, che ovviamente devono essere compatibili e basarsi sulle firme emesse o riconosciute dal medesimo ente certificatore. La marca temporale e' una firma elettronica come le altre posta dal programma che ad esempio chiede l'ora via Internet ad uno dei servizi che forniscono l'ora esatta tipo il Gallileo Ferraris di Torino per l'Italia.

Per la verifica dell'autenticità del documento sarà sufficiente chiedere al programma di firma di verificare la validità delle firme dei tre soggetti. Il programma sarà quindi in grado di dire se il documento è inalterato o se è stato falsificato e di verificarne l'autenticità della firma e quindi la paternità.

Con questo semplice giro si associa paternità, certezza dei contenuti e data certa al documento: ha quindi tutte le carte in regola per essere un vero e **proprio documento digitale con validità legale digitale**.

Attenzione ho enfatizzato volutamente il termine digitale perché deve essere chiara una cosa: la firma elettronica è un artificio sui dati e quindi è verificabile solo per i documenti in formato digitale. Non si può assolutamente parlare di verifica della firma elettronica su documenti stampati su carta. Se il documento è su carta posso solo ricorrere alle tradizionali firme autografe, bolli, timbri ecc. Se il documento è digitale posso firmarlo elettronicamente! **Non facciamo confusione: non esiste la firma elettronica su carta.**

Il meccanismo della firma elettronica è semplicissimo, quello che lo rende una cosa leggermente più complicata è tutta l'infrastruttura necessaria per il corretto funzionamento del sistema. E' necessario che il sistema sia relativamente comodo da usare, che abbia una gran diffusione, che abbia particolari doti di sicurezza insomma l'infrastruttura che controlla il gioco delle firme è un'infrastruttura seria e complessa!

4.2 documento segreto

Con le stesse tecnologie applicate per firmare digitalmente i documenti è anche possibile proteggere i documenti da occhi indiscreti e cioè crittografarli.

Supponiamo di avere un documento che contiene le istruzioni per attivare o disattivare un determinato allarme e che può essere utilizzato solo se tre persone sono concordi nell'utilizzarlo. In questo caso il documento è generato in automatico da un programma che lo crittografa con le chiavi pubbliche delle tre persone autorizzate a leggerlo. Essendo crittografato il documento sarà illeggibile. Per estrarre le informazioni è necessario decrittografare il documento.

- generazione automatica del codice (il documento sarebbe leggibile ma è solo all'interno del software quindi inaccessibile)
- cifratura con chiave pubblica del primo soggetto (il documento diventa illeggibile anche per colui che lo ha cifrato)
- cifratura con chiave pubblica del secondo soggetto (il documento resta illeggibile anche per colui che lo ha cifrato)
- cifratura con chiave pubblica del terzo soggetto (il documento resta illeggibile anche per colui che lo ha cifrato)
- il documento reso segreto viene rilasciato

Il processo di estrazione del codice segreto (decrittografia) deve ovviamente seguire il processo inverso. Le tre persone devono essere d'accordo sull'estrazione del codice. A questo punto devono decifrare il documento con le loro chiavi private. Per quanto detto prima non è importante l'ordine di applicazione delle chiavi ma **il documento resterà ovviamente illeggibile fino a quando tutti e tre i soggetti non avranno applicato le loro chiavi per decifrarlo.**

- decifratura con chiave privata del secondo soggetto (il documento resta illeggibile)
- decifratura con chiave privata del primo soggetto (il documento resta illeggibile)
- decifratura con chiave privata del terzo soggetto (il documento diventa leggibile)
- è finalmente possibile leggere il documento: è tornato leggibile

5 Breve glossario sulla crittografia

La crittografia, per quanto già detto sopra è il cardine della firma elettronica ma può anche essere usata come tecnologia per proteggere un messaggio o più in generale un documento da occhi indiscreti. Con i moderni algoritmi di cifratura a chiavi asimmetriche è possibile proteggere un messaggio in modo che solo il destinatario di quel messaggio sia in grado di leggerlo.

La cifratura e' una tecnica di protezione per i testi in modo che non sia possibile, o almeno sia molto difficile, leggere il contenuto senza conoscere l'algoritmo di cifratura utilizzato. Il processo inverso prende il nome di decifratura.

Le prime applicazioni di tecniche di cifratura dei testi risalgono ad applicazioni militari per lo scambio dei messaggi.

Con i calcolatori sono stati adottati algoritmi di cifratura sempre più complessi e sicuri. Si e' arrivati a scrivere dei programmi che, mediante "chiavi elettroniche" consentono di cifrare i documenti proteggendoli da occhi indiscreti.

Chiavi Elettroniche: simmetriche

Un sistema di cifratura a chiave simmetrica è un sistema basato su di un'unica chiave che viene utilizzata indistintamente per cifrare e per decifrare il documento. Naturalmente per potere leggere il documento si deve conoscere la chiave di cifratura. Questo metodo presenta lo svantaggio di richiedere un canale sicuro per l'invio della chiave di cifratura al destinatario del messaggio e di non fornire nessun metodo sicuro per attribuire una paternità certa al messaggio.

Chiavi Elettroniche: asimmetriche

Il concetto di chiave asimmetrica è nuovo rispetto alla crittografia tradizionale.

Un sistema di cifratura mediante chiave asimmetrica si basa su una coppia di chiavi utilizzate una per cifrare il documento e la seconda per decifrare il documento. La sostanziale novità è quindi che la chiave di cifratura non può essere utilizzata per la decifratura del documento inoltre la conoscenza di una delle due chiavi non fornisce alcuna indicazione utile per determinare la seconda chiave.

Si introduce quindi il concetto di chiave pubblica e chiave privata. La chiave pubblica è nota a tutti e la chiave privata è personale.

In questo modo posso garantire ai documenti autenticità e segretezza.

Immaginiamoci due diversi scenari:

- Invio di un messaggio da A a B leggibile solo da B
- Invio di un messaggio da A a B leggibile solo da B ma con la certezza che sia stato scritto da A

Nel primo caso e' sufficiente cifrare il messaggio con la chiave pubblica di B. In questo modo per leggere il messaggio sarà necessaria la chiave privata di B quindi solo B potrà leggere il messaggio. Il mittente, dopo avere cifrato il messaggio con la chiave pubblica del destinatario, non sarà più in grado di decifrarlo.

Nel secondo caso prima occorrerà effettuare una cifratura con la chiave privata di A quindi una seconda cifratura con la chiave pubblica di B. Il processo di decifratura seguirà l'iter inverso; prima richiederà una decifratura con la chiave privata di B quindi una seconda decifratura con la chiave pubblica di A. Questo secondo passo garantisce l'autenticità del messaggio: essendo stato cifrato con la chiave privata di A e' stato scritto da A!

Algoritmo RSA di cifratura

Brevettato da tre ricercatori del Mit (Rivest, Shamir e Adleman) dalle cui iniziali deriva la sigla. Si basa sulla possibilità di creare dei cifrari a chiave asimmetrica utilizzando particolari proprietà formali dei numeri primi. Oggi l'algoritmo RSA è ritenuto di massima affidabilità anche se in realtà non è sicuro in termini puramente matematici, dato che esiste la possibilità teorica, seppure molto improbabile, che nuove scoperte matematiche possano portare a delle falle negli schemi.

5.1 Programmi per Firmare e Crittografare

A questo punto è interessante inserire una breve sezione che illustri dei programmi con cui è possibile sperimentare le applicazioni della crittografia.

Questa non vuole assolutamente essere una rassegna dei programmi di crittografia disponibili sul mercato ma cito solo i due più noti disponibili liberamente ed un'applicazione commerciale che non ha avuto un brillante futuro e che NAI ha smesso di supportare dal 2002.

PGP

Il PGP Pretty Good (tm)Privacy e' un programma di cifratura basato sul algoritmo RSA a chiavi asimmetriche. E' abbastanza diffuso in Internet. Al fine di ottimizzare le prestazioni utilizza una cifratura a chiave simmetrica (algoritmo più veloce) per il corpo del messaggio al quale viene aggiunta come intestazione la chiave simmetrica di decifratura a sua volta cifrata con un algoritmo a chiave asimmetrica (più lento).

Per maggiori informazioni: <http://www.gnupg.org>

GNUPGP

Il progetto GNUPGP si propone di fornire uno strumento di crittografia basato su software open source. Attualmente (giugno 2002) è disponibile la versione 1.0.7 per il download dal sito del gruppo <http://www.gnupg.org>

In questa nuova versione sono stati corretti dei buchi delle precedenti versioni ed è stata migliorata la compatibilità con le chiavi generate dal PGP.

In questa versione le chiavi private vengono memorizzate ed esportate in nuovo formato che utilizza l'algoritmo SHA-1 per la verifica dell'integrità dei dati. Il nuovo algoritmo di default per la cifratura è il CAST5, per l'hash è l'SHA-1. E' è stato aggiunto il supporto per le firme non revocabili.

E' stato inoltre aggiunto il supporto RSA per la generazione delle chiavi.

Per maggiori informazioni: <http://www.gnupg.org>

PGP Desktop Security

Il progetto PGP Desktop Security, ossia il software commerciale basato sul programma di crittografia più famoso del mondo il PGP di Phil Zimmermann, è stato creato e gestito dalla NAI, attualmente purtroppo è stato abbandonato

La società ha affermato che il progetto PGP Desktop non era più valido commercialmente e che la tecnologia del PGP verrà utilizzata in altri prodotti della McAfee come l'e-business server, il personal firewall ed i client VPN.

Questa applicazione è stata citata solo come motivo di riflessione. Se si deve implementare qualche cosa di serio con la crittografia si devono prendere misure tali da scongiurare il pericolo di adottare un programma di una società che lo abbandona magari dopo qualche anno. NAI è una società seria e grossa, sicuramente non si pensava che la sorte di PGP Desktop Security potesse essere questa ma è stato abbandonato.

Gli esempi di queste pagine sono stati tutti realizzati con la versione freeware del prodotto di NAI

FIGURA 1 - FINESTA DI GESTIONE DELLE CHIAVI PUBBLICHE E PRIVATE.

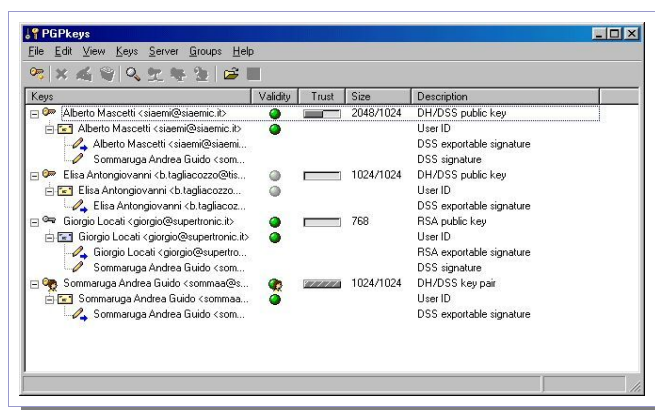


FIGURA 2 - FINESTA DI VERIFICA DI UNA FIRMA CON SUCCESSO

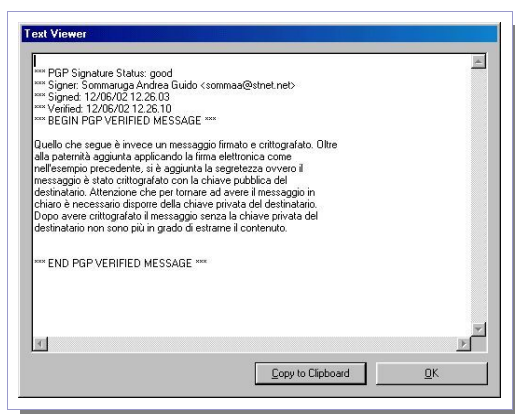
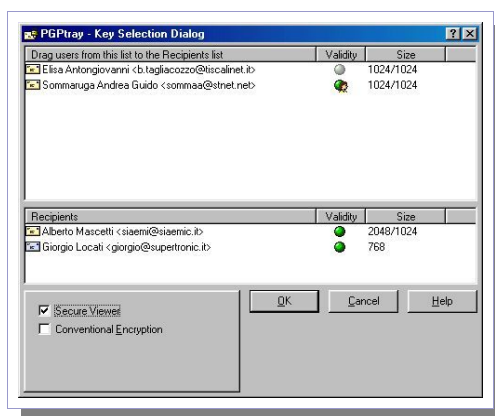


FIGURA 3 - FINESTRA SEGNALAZIONE MANCANZA DELLA CHIAVE PRIVATA PER DECODIFICARE IL MESSAGGIO**FIGURA 4 - FINESTRA IN CUI POSSE SCEGLIERE LE CHIAVI PUBBLICHE PER CIFRARE UN MESSAGGIO**

Purtroppo come ho già detto questo progetto non è più supportato e sviluppato da NAI, resta comunque un valido programma per fare degli esperimenti in proposito. La versione personale è gratuita ed è semplice da usare. In qualsiasi caso le firme digitali generate da questo programma sono poi utilizzabili anche da GNUPGP ed altri software analoghi.

Per maggiori informazioni: <http://www.nai.com>

6 Crediti, Ringraziamenti, Licenza

6.1 Crediti

6.2 Ringraziamenti

A tutti i volontari che ogni giorno dedicano parte del loro tempo per realizzare le migliaia di applicazioni Open Source e a tutti gli utenti che accettano di impegnarsi nella migrazione dalle applicazioni commerciali a cui sono abituati, alle nuove applicazioni Open Source.

In particolare per gli spunti sull'impaginazione grafica del modello ringrazio Mirto Silvio Busico e Gianluca Turconi.

6.3 Licenza

È garantito il permesso di copiare, distribuire e/o modificare questo documento seguendo i termini della GNU Free Documentation License, Versione 1.1 o ogni versione successiva pubblicata dalla Free Software Foundation; mantenendo:

- Il Testo Copertina con il riferimento all'autore
- Senza Sezioni non Modificabili
- Il testo deve essere ridistribuito con la stessa licenza

Una copia della licenza può essere ottenuta presso Free Software Foundation, Inc. 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA.

Copyright © 2004 Andrea Guido Sommaruga
Viale tunisia, 25
20124 Milano

7 Impaginazione di questo documento

In questo modello sono stati introdotti vari stili di paragrafo personalizzati :

Text body 1,2 e 3 rispettivamente per il corpo del testo seguente le intestazioni Heading 1,2 e 3 (Intestazione 1,2,3,4 nella versione localizzata). L'impostazione di questi stili avviene automaticamente ogni volta che si va a capo dopo una delle intestazioni citate. Utilizzano il carattere Times.

Titolo Copertina, Times 32pt.

Testo riportato. E' utile per riportare brevi testi contenenti esempi ecc. Utilizza il carattere Courier 12pt.

Nel caso non vengano automaticamente attivati, questi stili si possono applicare manualmente, selezionandoli tra gli stili personalizzati (Modelli Utente) contenuti nello Stilista (premere il tasto F11 per visualizzarlo/nascondere)

Sono stati modificati anche 3 degli stili standard e cioè Heading 1,2,3 (Intestazione 1,2,3 nella versione localizzata), con uno sfondo giallo, ombreggiato con riquadro grigio-azzurro, esattamente come i titoli riportati in queste pagine.

Nelle righe d'intestazione della pagina sono riportati automaticamente i titoli dei capitoli modificati con lo stile Heading 1 (Intestazione 1) più il numero di versione che deve essere modificato manualmente dalla pagina di copertina. Il numero di versione è inserito come variabile utente ed è riportato nelle intestazioni automaticamente.

Nel piè di pagina è indicata la data corrente e il numero di pagina. Dal momento che questo documento è stato pensato per la stampa, i due campi sono alternativamente posizionati a destra e a sinistra, utilizzando due stili di pagina diversi, in modo da rispecchiare l'andamento delle pagine stampate. Per lo stesso motivo è stata introdotta una pagina di retro-copertina.

L'indice è modificabile in automatico a patto che si siano utilizzati gli stili contenuti nello Stilista. E' sufficiente posizionare il cursore lampeggiante al suo interno (1 click sinistro) e poi cliccare col tasto destro su di esso, scegliendo Aggiorna Indice.

Il grassetto è ottenuto con lo stile **Enfasi Forte**.

Lo stile *Enfasi* serve invece per *evidenziare il testo con il corsivo*.

C'è inoltre lo stile per le cornici delle immagini.