INDICE

INDICE DELLE FIGURE

a cura di:
ing andrea guido sommaruga

LA FIRMA DIGITALE O 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 attribuiscano "***valore legale***".

Per firmare elettronicamente un documento è necessario potergli attribuire una paternità certa e garantire l'inalterabilità del contenuto, ciò è reso possibile dall'utilizzo dei ***programmi di firma elettronica***.

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 le 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 necessita' 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 allego 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 mi 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.

```
-----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.pgpi.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. Dopo avere crittografato il messaggio senza la chiave privata del destinatario non sono più in grado di estrarne il contenuto.

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

```
qANQR1DBwU4DbXOhFGAnz4sQCADNZCVXI6fSYhf2zifIk1m3OClmzpZq/014FcPY
CVOtfXSyPSRv7fec4RfakFPEMrk1gK/3eXLXtG5M9psWBkW0vBaYuPGDRP7ARfyS
ANJYuPDrriIKRoFYlplrQUIfBmZKf4yAG3Yh0YBACLf4j5RtgByVmpE0LAJW/k+p
Meb1OCP1YQ1d2oozhmf7G8FxU+RD9l/EOqnD2pxbfTjXPg8b/1RZWzeXp3fWiiCc
gGr420I41vOWr+v9g7jCewW7m+j6Kp1+o7Gup8nuNb0Fi/4D/3HpTt5lmXvESvPA
5R/3DLdfqc27l3USqU21SsOlNZ/iQFXyS4khEqFFvwk/zyhWB/4ou1m3tw47H0p6
FY3sPeI9xU+FKoOqd3hrPgNxkhoi1iRJea/qvUiZZmO+cdZb5eLSSp3Easfn8Xxn
Bp11vyjjWLD6GduKSWMq43eV/bmmajMIYfxRnfwlsczcaEW+3ojZDk4SXSwQVhJK
kxbBlLeq/qxgu1s3biHLFfL7TQAkJqEt3VuyoPWDShAYqyYvUVTpyV29wu0IWuvB
Tp/Ne/pf5a4otoKyzP2/uWfAiUTGi9YAZR2Fr40N/oScvGr1uMd56O5bRwbv0vtq
UIcvv6bVOAJ3NtrPs2afe4FF39LFOEuiURU3xvbLBcW9aL59oSdg/HlgR2SJJV23
nl/8gLlpyYtEgqZKRvJ10qLDv2PcqOG7RQfLRR9yM0xD/Xf0LFOpLzeof/nA2Oig
AkB+SX3tGWQNsPTgnUKHKCD1KTc1KREOUb1S29YjQ2R+4o3sswsqpAFIxQ1JqR37
tkJALdu2zaA9EmRVV//jRuv/lfySoutAGAxiltWRSeCDXWbw0IGUS0+mnGo2h6bH
8Eex
=XFHR
-----END PGP MESSAGE-----
```

Vediamo anche 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. Attenzione che per
tornare ad avere il messaggio in chiaro è necessario disporre della chiave privata del
destinatario. Dopo avere crittografato il messaggio senza la chiave privata del destinatario non
sono più in grado di estrarne il contenuto.


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

Riportiamo un secondo esempio in cui, dopo avere firmato il documento ho volutamente aggiunto una riga in più al testo falsificandolo. Dal controllo della firma risulta che è stato firmato da me e quando (quindi la paternità) ma fallisce la verifica del contenuto: viene quindi smascherata la mia falsificazione: ***PGP Signature Status: bad.***

Attenzione il programma non è in grado di dirmi che modifiche ho fatto ma mi dice semplicemente che il testo è stato alterato.

```
*** 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 ***

Vediamo quindi di illustrare i principi di funzionamento della firma
elettronica. 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
QUESTA RIGA E' STATA AGGIUNTO DI PROPOSITO!


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

Vediamo quindi di illustrare i principi di funzionamento della firma elettronica. 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.

L'operazione di firma in questo caso aggiunge delle informazioni crittografate (la riga strana aggiunta al testo) mediante la chiave privata, che possono essere lette e correttamente decrittografate solo con 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 decifratura. 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 di cui non posso fidarmi?

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.

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 autority 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 2002) 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).

Le Camere di Commercio hanno dotato il loro sistema per la firma digitale di una interessantissima applicazione chiamata "***Legal Mail***" che consente di implementare per la posta elettronica un meccanismo simile alle ricevute di ritorno delle raccomandate.

Attualmente la scomodità dei vari sistemi di firma che ho avuto occasione di vedere è la necessità di effettuare tutte le operazioni on-line ovvero connessi ad internet. Questo si giustifica con il fatto di potere disporre on-line della marca temporale e del database delle firme 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.

NOTA SUI FORMATI DI FILE

Occorre fare una breve considerazione sui formati dei file. Abbiamo detto che 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 ho potuto inserire all'interno dello stesso file il contenuto vero e proprio del messaggio e le informazioni di firma elettronica.

Qualora desideri invece firmare un file che non può essere alterato, ad esempio un documento di word, le informazioni di firma elettronica devono obbligatoriamente essere memorizzare 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 file di word 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 come word che estrae il contenuto analizza i comandi di formattazione e compone a video il documento. Potrei trovarmi con il programma di visualizzazione, ovvero word per l'esempio, che si comporta in modo diverso dalla copia usata per scrivere l'originale documento e quindi il mio 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.

Potrei per esempio realizzare facilmente un programma alterato che riconosce il comando di grassetto ed invece di evidenziare il testo in grassetto omette il testo in esame, in questo caso mi troverei di fronte ad un ***file regolarmente verificato*** dalla firma elettronica ma ***visualizzato in modo diverso*** per un vizio del programma.

Il punto a cui volevo arrivare è che se desidero la maggiore sicurezza possibile con i documenti firmati elettronicamente o crittografati, dovrei basarmi soltanto sul 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 e' 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 possibile decidere di adottare questo formato per accettare dei documenti firmati digitalmente.

COME FUNZIONA IL MECCANISMO DELLE FIRME ELETTRONICHE

FIRMA DI PIÙ PERSONE

Provo a questo punto a schematizzare il funzionamento di un processo di firma elettronica di un documento. Supponiamo di fare un caso pratico in cui ho un documento di compravendita di un immobile. Il documento deve essere vistato da una certa serie di figure:

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

In questo caso ho previsto quattro figure ovvero tre persone ed una marca temporale. 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.

Per la verifica dell'autenticità del documento sarà sufficiente chiedere al programma di firma di verificare la validità delle firme dei tre soggetti e della marca temporale. 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 riesco quindi ad associare paternità, certezza dei contenuti e data certa al mio 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***.

Gli esempi che ho riportato all'inizio di 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 mio testo applicando le firme. Per vedere di che cosa si tratta ***quando si parla di firma digitale: non è la firma autografa presa con uno scanner***!

Nell'esempio 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!

DOCUMENTO SEGRETO

Nell'esempio fatto ho parlato di firma elettronica analogamente potrei fare l'esempio del documento crittografato che contiene una combinazione. Supponiamo di avere un codice che serve ad esempio per attivare o disattivare un determinato allarme e che può essere utilizzato solo se tre persone sono concordi nell'utilizzarlo. In questo caso il codice è generato da un programma che cifra il risultato con le chiavi pubbliche delle tre persone autorizzate a leggerlo.

- 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 deve ovviamente seguire il processo inverso. Le tre persone devono ovviamente 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

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.

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.gnupgp.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 SEQUENZA FIGURA - FINESTA DI GESTIONE DELLE CHIAVI PUBBLICHE E PRIVATE.

FIGURA SEQUENZA FIGURA - FINESTRA DI VERIFICA DI UNA FIRMA CON SUCCESSO

FIGURA SEQUENZA FIGURA - FINESTRA SEGNALAZIONE MANCANZA DELLA CHIAVE PRIVATA PER DECODIFICARE IL MESSAGGIO

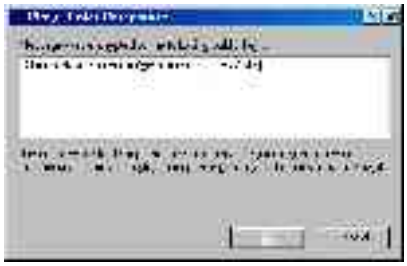

FIGURA SEQUENZA FIGURA - FINESTRA IN CUI POSSE SCEGLIERE LE CHIAVI PUBBLICHE PER CIFRARE UN MESSAGGIO

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