I programmi per la firma digitale

di Nicola Bortolotti

Siamo infine giunti al termine di questa prima serie di articoli dedicati alla firma digitale. Prima serie perché l'argomento, sebbene consolidato da anni sotto l'aspetto matematico sia teorico che applicativo (comunque sempre in fermento), non lo è affatto per quanto concerne le implicazioni legali e i suoi riflessi sulla vita sociale ed economica: si può anzi senz'altro affermare che, da quest'ultimo punto di vista, la storia del documento elettronico "firmato" sia solo all'inizio del proprio (presumibilmente lungo e fulgido) cammino. Un cammino che "Nuova Antigone" seguirà assiduamente, perché destinato - almeno negli intenti - a rivoluzionare la burocrazia e le procedure amministrative del mondo intero.

Come promesso, quindi, fisseremo alcuni concetti fondamentali presentando nel contempo alcuni programmi disponibili sul mercato e di libero utilizzo - perlomeno privatamente - che consentono di apporre la propria firma digitale, ricordando tuttavia i limiti dell'attuale normativa sotto il profilo del riconoscimento "ufficiale" della "signature" apposta.

La firma digitale è un'arma?

Questa domanda, che potrebbe sembrare astrusa provocazione, in realtà ha risposta sorprendentemente affermativa e, come corollario, ha indotto conseguenze che vanno dal drammatico al curioso (si veda nel seguito l'accenno alla storia del software PGP).

Ma perché una firma va trattata - seppure indirettamente - alla stregua di un'arma? La giustificazione risiede in un aspetto squisitamente tecnico: la possibilità di apporre una firma digitale, infatti, discende da una tecnica di cifratura dei documenti detta "Crittografia a chiave pubblica" (Nuova Antigone 98/1). Crittografia e firma, dunque, sono indissolubilmente legate, in quanto l'algoritmo matematico che le rende possibili è sostanzialmente lo stesso, seppure applicato in maniera diversa.

Il grado di "sicurezza" di una firma è dunque direttamente proporzionale alla "impenetrabilità" di un documento cifrato.

La possibilità di firmare in maniera sicura consente pertanto, all'occorrenza, di rendere illeggibili i propri documenti in modo altrettanto sicuro.

I pericoli della crittografia

Questa "sicurezza", seppur gradita e senza effetti collaterali sotto il profilo della firma, rappresenta una potenziale fonte di pericolo per quanto concerne l'aspetto crittografico.

Coprire un documento allo sguardo di occhi indiscreti è, infatti, tradizionalmente uno strumento militare e dunque soggetto a vincoli di segretezza; parallelamente, il valore strategico di poter decifrare i messaggi del "nemico" può essere immenso (si pensi al famoso caso della macchina "Enigma").

La crittografia a chiave pubblica conferisce a chiunque sia in possesso di un banale personal computer la possibilità di rendere indecifrabili i propri documenti anche ai più potenti supercalcolatori delle forze armate mondiali; passando in campo civile, permette di rendere impenetrabili le proprie comunicazioni (anche illecite) persino alle più sofisticate task-force dell'FBI.

Per questa ragione, i programmi che rendono possibili la - apparentemente innocua - firma digitale, erano - fino a pochi anni or sono - soggetti negli USA alle regole internazionali sul traffico d'armi! Ora, invece, esistono nove categorie di prodotti (dalle smart card personalizzate alle applicazioni specificatamente finanziarie, dai software di protezione dai virus all'autenticazione) soggette alle meno restrittive regole del dipartimento del commercio per quanto concerne l'esportazione dagli States. Il problema è costituito dal fatto che - tipicamente - un software che consente di apporre la firma digitale permette anche la cifratura del documento...

Pretty Good Privacy

Tutto questo per introdurre la storia (dagli aspetti quasi romanzeschi) di una pietra miliare della firma digitale ossia "PGP", il programma che - fin dagli albori della telematica personale - ha rappresentato il punto di riferimento per quanti volessero contrassegnare (e, all'occorrenza, proteggere) i propri documenti elettronici.

Innanzitutto una precisazione che potrebbe sembrare scontata: perché è necessario utilizzare dei programmi per apporre la propria firma digitale?

Semplicemente perché, come è stato ampiamente illustrato anche in

Nuova Antigone 98/1 e 98/2, una firma digitale non è una semplice sequenza di bit sempre uguali a loro stessi bensì il risultato di un complesso procedimento che non è possibile eseguire senza l'ausilio di un personal computer.

I problemi sono iniziati proprio qui: sebbene la base matematica della crittografia a chiave pubblica sia di dominio della comunità scientifica internazionale, l'esportazione di un software crittografico "forte" è considerato negli Stati Uniti alla stregua dell'esportazione di munizioni e dunque illegale, qualora non sia concessa una specifica licenza.

La scappatoia

Dopo anni trascorsi sul filo del rasoio nei quali PGP veniva tacitamente - e in maniera sostanzialmente illegale - "scaricato" via modem anche da non residenti negli Stati Uniti (in violazione dunque ai regolamenti: fatto, questo, che ha provocato non pochi grattacapi al geniale creatore del programma, Philip Zimmermann) è stato scoperto un "bug" nei severi regolamenti USA: una "backdoor", una vera e propria scappatoia - il cui rinvenimento è degno di un italico azzeccagarbugli - che ha reso legalmente possibile l'utilizzo di PGP anche al di fuori degli States.

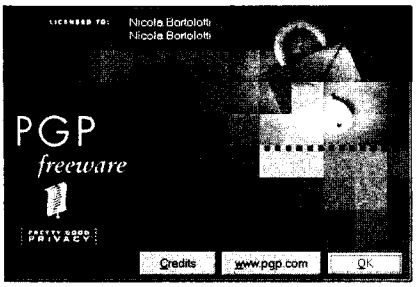

Figura 1 - La finestra "about" con la quale si presenta una delle ultime versioni internazionali di PGP freeware, il software di libero utilizzo personale per la firma digitale e la cifratura dei documenti.

Le restrizioni all'esportazione, infatti, riguardano solamente software in forma *elettronica*, materiale o immateriale (dischi, download da BBS e da Internet, e così via). Ciò detto, il codice sorgente di PGP è stato *legalmente* esportato dagli USA in forma cartacea: 12 volumi, pari a più di 6000 pagine, che sono poi stati scannerizzati e riportati in forma elettronica consentendo la ricompilazione e la lecita distribuzione internazionale del programma, che per uso privato è gratuito. A questo lavoro hanno partecipato oltre 70 volontari sparsi per l'Europa per un totale di oltre 1000 ore di lavoro. E' nata dunque la versione "internazionale" di PGP (caratterizzata da una "i" minuscola che segue il numero di versione). A partire dalla 5.0i, ne sono state rilasciate altre versioni (ad esempio la 5.5.3i per Windows 95 alla quale si riferisce la figura 1). Per ogni ulteriore informazione al riguardo, è possibile consultare la pagina Internet www.pgpi.com, spartana ma completa (figura 2).

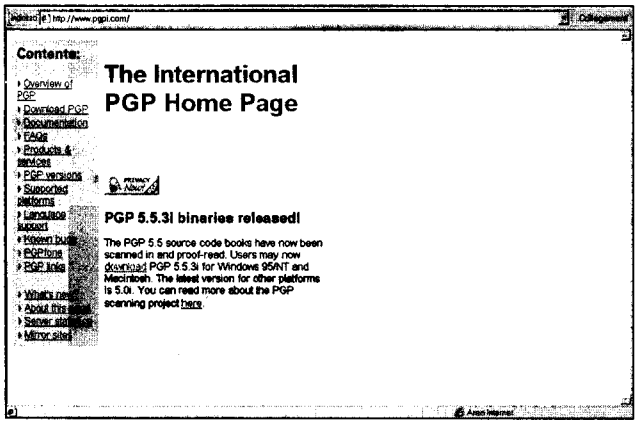

Figura 2 - Anche se sulla finestra "about" appare l'indirizzo Internet ufficiale del programma PGP (Pretty Good Privacy, una creazione di Philip Zimmermann che ha fatto storia), al di fuori degli Stati Uniti - per ragioni ampiamente discusse nell'articolo - è necessario far riferimento ad un'altra pagina, www.pgpi.com, spartana ma completa e di agevole consultazione. Da notare la voce "Download PGP" che consente di scaricare tramite Internet il software (un altro URL fondamentale è www.csd.uu.se/~d95mno/PGP.html).

Utilizzo di PGP

Dopo lo scaricamento e la rapida installazione del programma, il primo e fondamentale passo da seguire (una volta per tutte) è quello della generazione della coppia di chiavi: vengono richiesti nome e indirizzo di posta elettronica da associare ad esse (figura 3).

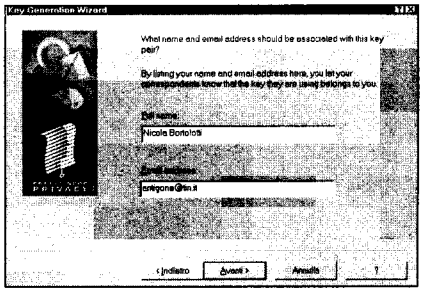

Figura 3 - La prima e fondamentale fase propedeutica all'utilizzo di PGP consiste nella generazione della coppia di chiavi (pubblica e privata): una fase delicata che PGP assolve nel miglior modo possibile, anche se un po' criptico per i "non iniziati". Qui viene richiesto il nome completo dell'utilizzatore e il suo corrispondente indirizzo di posta elettronica.

Sebbene l'idea sottesa alla crittografia a chiave pubblica sia sostanzialmente unica, le possibili realizzazioni e algoritmi da essa derivanti sono molteplici, con numerose varianti. Questa pluralità si è riflessa anche sulle versioni di PGP che si sono succedute nel tempo, creando purtroppo alcune incompatibilità.

Come si può vedere dalla figura

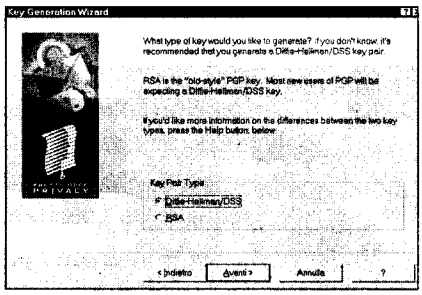

Figura 4 - Anche se i principi della crittografia a chiave pubblica, ampiamente discussi nei numeri precedenti di "Nuova Antigone", sono sostanzialmente gli stessi, vari autori hanno contribuito con algoritmi diversi. Di fatto, quindi, i sistemi sono diventati sempre più sicuri (persino "troppo", secondo gli organismi governativi di buona parte del mondo) ma anche incompatibili fra di loro. La scelta può quindi essere imbarazzante; ad esempio, nella figura - sempre relativa alla generazione della coppia di chiavi - viene chiesto di decidere fra due tipi di coppie: il più moderno "Diffie-Hellmann/DSS" e il consolidato "RSA", tuttavia indispensabile per scambiare messaggi con coloro che utilizzano vecchie versioni di PGP. Quale preferire?

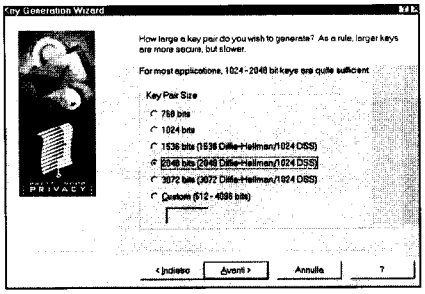

Figura 5 - Anche la scelta della dimensione della coppia di chiavi è lasciata all'utente. Tipicamente la lunghezza è direttamente proporzionale alla sicurezza. Conformemente ai suggerimenti dei matematici della stessa RSA, PGP offre solo cifratura "forte".

4, l'attuale versione di PGP permette di scegliere tra una coppia di chiavi generate con l'algoritmo di Diffie-Hellman/DSS (più recente) o il tradizionale RSA (preferibile solo qualora si preveda di scambiare posta con coloro che utilizzano versioni di PGP vetuste). Si noti che alcune versioni "internazionali" freeware (ossia di utilizzo gratuito) di PGP non prevedono l'opzione RSA.

Altra scelta fondamentale è costituita dalla lunghezza della coppia di chiavi (figura 5); in linea di principio, maggiore è la lunghezza della chiave minore è la probabilità (comunque marginale) che essa possa venire contraffatta. Ma, a questo punto, è opportuno aprire una parentesi necessaria per capire perché la diffusione di PGP faccia - ancora oggi - paura.

La questione della "strong" encryption

Ciò che impensierisce il governo USA, in realtà, non è la cifratura tout-court bensì la cosiddetta cifratura "forte", ossia con chiavi di lunghezza tale da rendere impossibile la decifratura da parte di FBI e simili anche in caso di necessità.

A tal proposito, allo stato attuale le agenzie governative statunitensi considerano cifratura "forte" algoritmi asimmetrici con lunghezza della chiave superiore a 512 bit. Come si può notare, PGP offre chiavi con lunghezza comunque superiore alla fatidica soglia. In ultima analisi, PGP offre solo cifratura "forte".

E' altresì significativo notare (e lo ricorderemo nel seguito parlando di Outlook Express) il fatto che i matematici dell'RSA per diversi anni hanno considerato "inadeguate dal punto di vista commerciale" chiavi da 512 bit e consigliano agli utilizzatori domestici chiavi di almeno 768 bit.

Un gioco ad incastro

Si può poi optare per una durata delle chiavi limitata nel tempo (figura 6) e giungere ad un'altra decisiva finestra di dialogo (figura 7), quella ove si richiede la scelta di una password a protezione della propria chiave privata. Questa richiesta, a prima vista, potrebbe disorientare: negli articoli precedenti, infatti, è emerso con chiarezza che la chiave privata non verrà mai distribuita e dovrà rimanere - gelosamente custodita - nel personal computer del legittimo proprietario. Che bisogno ci sarebbe, allora, di una password a protezione di una chiave che comunque rimarrà nei meandri del proprio PC?

La risposta è semplice e può apparire evidente a tutti quanti siano avvezzi all'utilizzo di computer in ambiente d'ufficio. Pensate infatti cosa potrebbe accadere se, in assenza del legittimo proprietario, qualcuno si sedesse al PC e digitasse sotto... mentite spoglie: se non ci fosse la barriera di questa password, il sedersi ad una determinata postazione di lavoro equivarrebbe ad assumere l'identità dell'utilizzatore abituale. In aggiunta, una semplice copia su dischetto di una chiave privata - qualora fosse "in chiaro" e utilizzabile senza password - sarebbe un modo oltremodo facile di rubare l'identità del legittimo possessore. Ecco quindi che si rende necessario un gioco ad incastro di cifrature e password anche se si lavora sul proprio computer e anche se ciò non ha ovviamente nulla a che fare con l'essenza della firma digitale.

Una password "locale" ben scelta, in definitiva, rende de facto inattuabili simili disegni fraudolenti di rilevanza penale: con PGP, infatti, ogniqualvolta si desideri firmare digitalmente un proprio documento, occorrerà immettere questa pas-

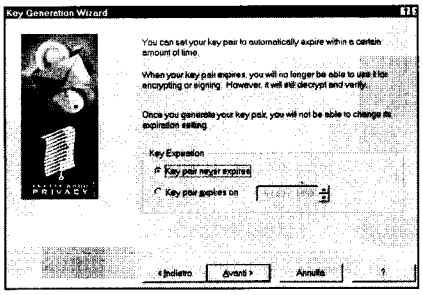

Figura 6 - E' anche possibile fissare un limite temporale di utilizzo delle chiavi per la firma e la cifratura, come appare dall'immagine, sempre relativa alla fase di generazione delle chiavi che va eseguita una volta per tutte. Da notare che l'"expiration setting", una volta create le chiavi, non è più modificabile.

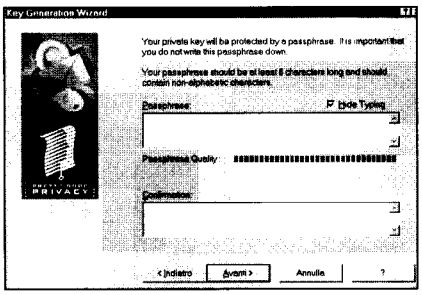

Figura 7 - Per evitare che malintenzionati possano utilizzare la vostra chiave semplicemente per il fatto di trovarsi a lavorare sul vostro Personal Computer, PGP ne protegge sempre l'uso con una password che va scelta all'atto della generazione della coppia di chiavi ed è fondamentale ricordare o conservare in un luogo sicuro e distinto dal PC stesso.

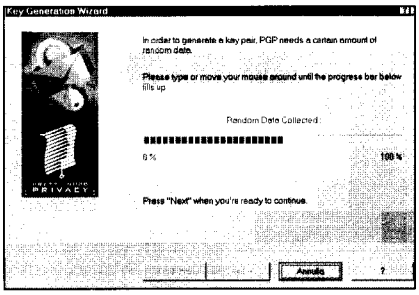

Figura 8 - Può apparire bizzarra questa fase della creazione della coppia di chiavi, nella quale PGP chiede di muovere il mouse per collezionare una sequenza di numeri casuali indispensabile all'algoritmo di generazione; in realtà si tratta di un'ulteriore conferma del grado di maturità, affidabilità e sicurezza raggiunto dal programma ideato da Zimmermann.

sword. Ciò potrà apparire irritante, ma è in realtà una misura di sicurezza inevitabile a garanzia dell'intero procedimento. Man mano che si digita la password, che non deve essere breve e va tassativamente ricordata, una barra di misurazione indica la "bontà" della parola d'ordine scelta. Segue una finestra apparentemente bizzarra (figura 8) nella quale si richiede di muovere il mouse al fine di creare una sequenza di numeri casuali che verranno utilizzati dall'algoritmo di generazione della coppia di chiavi.

Il grande momento

Ed ecco il grande momento. Le chiavi (figura 9) sono state generate. La parte pubblica, a questo punto, andrebbe trasmessa (via Internet) ad un apposito "key server", ossia ad un sito che la renda visibile a tutti quanti ne abbiano bisogno. I lettori attenti riconosceranno subito in questo "server" una parte delle funzioni che deve svolgere la autorità di certificazione discussa diffusamente nel numero passato. In realtà i "key server" proposti da PGP si limitano a mettere a disposizione un archivio di chiavi pubbliche e dunque non sono certificatori accreditabili presso la legge italiana. Dal DPR 513 si evince infatti, oltre alla penalizzante e discutibile condizione che prescrive per l'autorità di certificazione "forma di società per azioni e capitale sociale non inferiore a quello

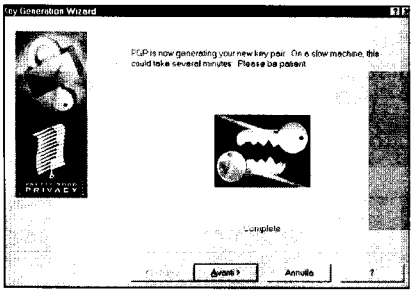

Figura 9 - Finalmente PGP può ora generare la coppia di chiavi: una fase che l'utilizzo dei moderni processori ha reso estremamente rapida; l'avvertimento in figura è dunque destinato a Personal Computer obsoleti: bisogna infatti ricordare che la storia di PGP affonda le sue radici nel 1991, quando le macchine basate sull'8088 erano ancora significativamente diffuse e utilizzate.

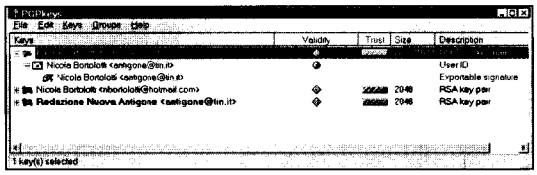

Figura 10 - La coppia di chiavi è stata creata ed è ora utilizzabile per firmare i propri documenti; la parte pubblica può essere distribuita in modo da permettere a terzi la validazione (e, all'occorrenza, consentire la cifratura di testi e files a noi diretti). Da notare che, come si può desumere dalla figura, è possibile creare firme per diversi account di posta elettronica.

necessario ai fini dell'autorizzazione all'attività bancaria, se soggetti privati", anche che - come è invece assai logico - "il certificatore è tenuto a: identificare con certezza la persona che fa richiesta della certificazione".

Quest'ultima azione - peraltro di fondamentale importanza - non è compiuta dai "key servers".

E' prevedibile nell'immediato futuro una armonizzazione e globalizzazione a livello mondiale dell'attività di certificazione, con struttura gerarchica. Tale struttura, però, a tutt'oggi latita anche se esistono diversi metodi ibridi (che possono coinvolgere anche l'utilizzo del telefono!) per accertarsi dell'identità dello scrivente senza bisogno di un'autorità.

Come utilizzare le chiavi

Generate le chiavi, che possono essere anche più di una coppia (si veda al proposito la figura 10), rimane il problema di come usarle. Una volta installato, PGP rimane tacitamente "disponibile" in vari modi: ad esempio il PGPtray nella barra delle applicazioni di Windows 95 (terza icona da sinistra nella figura 11). Una volta attivato si presenta il menu di figura 12: la voce di interesse per apporre la firma digitale è "Sign Clipboard"; per la verifica "Decrypt/Verify Clipboard".

Il metodo più generale per utilizzare PGP consiste nel copiare negli appunti il testo da firmare e invocare "Sign Clipboard"; verrà richiesta la password relativa a quella chiave e, al termine, negli appunti (figura 13) sarà presente il testo originario

Figura 11 - D'ora in avanti, supponendo utilizziate Windows 95, l'icona del PGPtray (la terza dalla sinistra) sarà sempre presente sulla vostra barra degli strumenti.

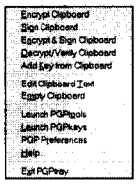

Figura 12 - Cliccando sul PGPtray è possibile accedere immediatamente a tutte le funzionalità offerte dal PGP, come mostra l'immagine.

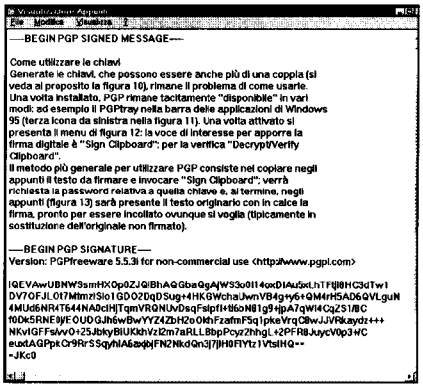

Figura 13 - Il metodo più generale per utilizzare PGP consiste nel copiare negli appunti il testo da firmare e invocare "Sign Clipboard"; verrà richiesta la password relativa a quella chiave e, al termine, negli appunti sarà presente il testo originario con in calce la firma, pronto per essere incollato ovunque si voglia (tipicamente in sostituzione dell'originale non firmato).

con in calce la firma, pronto per essere incollato ovunque si voglia (tipicamente in sostituzione dell'originale non firmato). Per validare un documento ricevuto, invece, dopo aver prelevato la chiave pubblica del mittente da un "key server", si copierà negli appunti l'intero messaggio firmato e si richiamerà la funzione "Decrypt/Ve-rify Clipboard". In caso di messaggio alterato o non originale comparirà un apposito avviso; qualora, invece, la validazione avvenga con successo comparirà il testo "pulito" e un log (figura 14) nel quale viene riportata anche la data e l'ora in cui il documento è stato firmato (la validazione di data e ora costituisce infatti

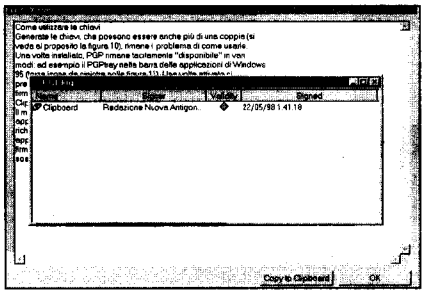

Figura 14 - Per validare un documento ricevuto - dopo aver prelevato la chiave pubblica del mittente (ad esempio dal suo sito o da un "key server") - si copierà negli appunti l'intero messaggio firmato e si richiamerà la funzione "Decrypt/Verify Clipboard". In caso di messaggio alterato o non originale comparirà un apposito avviso; qualora, invece, la validazione avvenga con successo comparirà il testo "pulito" e un log nel quale viene riportata anche la data e l'ora in cui il documento è stato firmato (la validazione di data e ora costituisce infatti un'ulteriore possibilità offerta dalla firma digitale e disponibile con PGP).

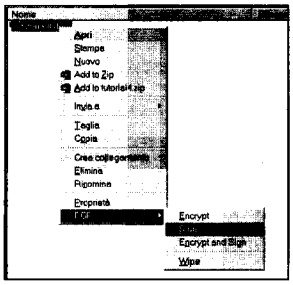

Figura 15 - Per "firmare" un file qualsiasi, non di testo, si dovrà invece ricorrere in Windows 95 a "Gestione risorse", selezionare il file e premere il tasto destro del mouse: nel menu contestuale che apparirà, scegliendo la voce PGP si dovrà cliccare su "sign".

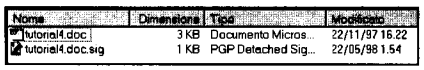

Figura 16 - In tal modo (digitata la password corretta) verrà creato un secondo file associato con estensione "sig" (signature, ossia firma). Cliccando su di esso verrà automaticamente verificata (qualora sia già stata memorizzata la chiave pubblica del proprietario) la genuinità del file originario.

un'ulteriore possibilità offerta dalla firma digitale e disponibile con PGP).

Per "firmare" un file qualsiasi, non di testo, si dovrà invece ricorrere in Windows 95 a "Gestione risorse", selezionare il file e premere il tasto destro del mouse: nel menu contestuale che apparirà, scegliendo la voce PGP si dovrà cliccare su "sign" (figura 15). In tal modo (digitata la password corretta) verrà creato un secondo file associato (figura 16) con estensione "sig" (signature,

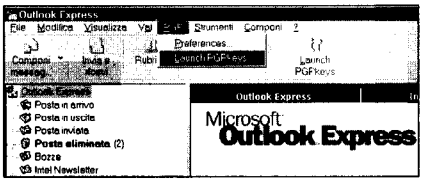

Figura 17 - L'integrazione di PGP con i più diffusi applicativi è affidata ad appositi plug-in, realizzati dai programmatori di tutto il mondo e messi gratuitamente a disposizione tramite Internet. Nella figura vediamo come appare il programma di posta elettronica Microsoft Outlook Express (distribuito con Internet Explorer 4), dopo l'applicazione del plug-in appropriato. Da notare che, cliccando su "Preferences... EMail" è possibile attivare l'opzione "Use PGP/MIME when sending email" che rende facilissime, quasi "invisibili", le operazioni di firma e cifratura dei documenti.

ossia firma). Cliccando su di esso verrà automaticamente verificata (qualora sia già stata memorizzata la chiave pubblica del proprietario) la genuinità del file originario.

PGP è anche integrabile con diffusissimi applicativi di posta elettronica tra i quali Eudora, Microsoft Exchange, Outlook e Outlook Express (figura 17).

L'esigenza di una forte integrazione

L'importanza strategica di firma digitale e crittografia (per convalidare transazioni nonché proteggerne alcune da occhi indiscreti) è destinata ad aumentare esponenzialmente nei prossimi anni e questo fatto, ovviamente, ha fatto sì che i più importanti produttori di software studino costantemente nuove soluzioni integrate che consentano la "signature" di messaggi e documenti in maniera estremamente agevole per l'utente.

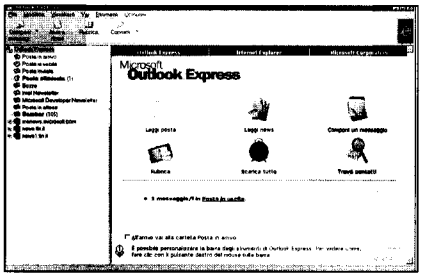

Figura 18 - Microsoft Outlook Express offre, a prescindere dal PGP plug-in, alcune interessanti opzioni di firma digitale e cifratura a chiave pubblica conformi allo standard S/MIME.

Si è visto infatti che PGP - vera pietra miliare - ha, nel suo essere un programma "indipendente" (anche se integrabile in alcuni applicativi), ad un tempo il suo punto di forza e il suo tallone di Achille. L'utilizzatore medio, infatti, non gradisce operazioni di seleziona-copia-firma-incolla o seleziona-copia-verifica. Per non parlare di interazioni basate sul web (ad esempio la compilazione di form di ordine direttamente su browser), pressoché impossibili da gestire tramite PGP o simili.

Outlook Express

I "big" del software, Microsoft in testa, per sviluppare il commercio in rete (e, indirettamente, i loro proventi) hanno quindi integrato algoritmi a chiave pubblica di firma e cifratura nei loro programmi di navigazione e gestione di posta elettronica Internet.

L'esempio che illustriamo in queste pagine è quello di Microsoft Outlook Express (figura 18), software associato ad Internet Explorer 4 e utilizzabile gratuitamente da chi già detenga la licenza d'uso dei sistemi operativi Microsoft.

Outlook Express contiene al suo interno interessanti strumenti di cifratura/decifratura e firma/validazione che utilizzano algoritmi asimmetrici con chiave a 512 bit (dunque non "strong", il che ne rende possibile la facile esportazione ma pone anche qualche limite alla effettiva sicurezza ottenibile).

Una volta associato un "certificato" ad un "account" di posta elet-

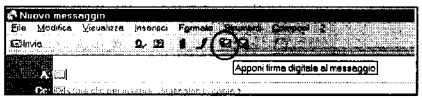

Figura 19 - Come appare nel particolare della finestra di composizione di un nuovo messaggio, la firma di un documento (dopo la procedura di assegnazione di un "certificato") è infatti possibile con un semplice "clic" con facilità persino eccessiva (la firma di un documento dovrebbe sempre implicare un atto fortemente volontario ancorché noioso, come la digitazione di una password).

tronica (si vedrà tra poco come fare), sarà possibile firmare digitalmente qualsiasi messaggio semplicemente cliccando (figura 19) sull'icona riportante una busta con timbro a ceralacca stilizzato (particolare in figura 20).

Fra i certificatori operanti a livello internazionale (e comunque ancora non riconosciuti legalmente in Italia ai sensi del DPR 513), Microsoft si appoggia a Verisign (in figura 21 la pagina con l'offerta commerciale di un ID digitale a meno di 10 dollari all'anno compresa un'assicurazione), dando la possibilità agli utilizzatori di Outlook Express di vedersi assegnata una firma di prova gratuita per due mesi.

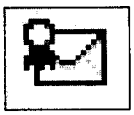

Figura 20 - L'icona della "firma digitale" di Outlook Express.

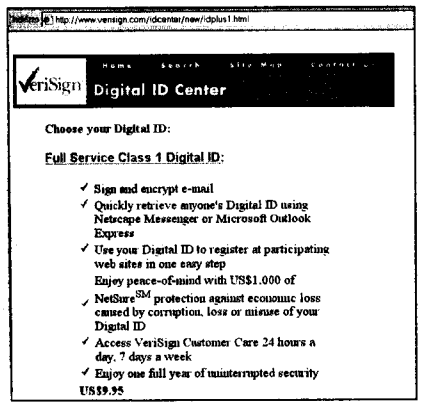

Figura 21 - Fra i certificatori operanti a livello internazionale (e comunque ancora non riconoscibili legalmente in Italia ai sensi del DPR 513), Microsoft si appoggia preferibilmente a Verisign di cui si può vedere la pagina web con l'offerta commerciale di un ID digitale a meno di 10 dollari all'anno compresa un'assicurazione. Per gli utilizzatori di Outlook Express è prevista l'assegnazione di una firma di prova gratuita per due mesi.

Procedura semplice ed immediata

La procedura da seguire è semplice e può essere svolta partendo da Outlook Express, che automaticamente apre Internet Explorer quando necessario. C'è ovviamente un modulo assai essenziale da compilare (visibile in parte in figura 22), un invito a controllare la posta (figura 23), un primo messaggio di conferma (figura 24), e infine le congratulazioni finali (figura 25). Se il livello di sicurezza offerto da PGP nella generazione e conservazione delle chiavi sembra rasentare la paranoia, viceversa il procedimento qui esposto può senz'altro destare qualche ben riposta perplessità: si tratta tuttavia di chiavi non "strong", per giunta assicurate nell'utilizzo (anche se è lecito dubitare che una simile sequenza, sebbene gradita per l'utente, possa mai essere avallata ai sensi del DPR 513) e, in definitiva, ben venga l'easy-to-use.

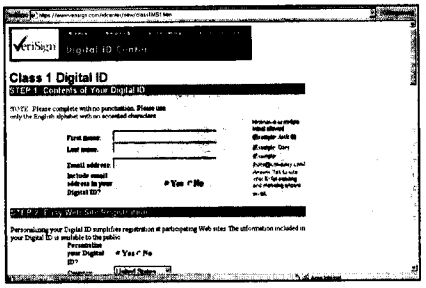

Figura 22 - La procedura di assegnazione di un ID digitale è semplice e può essere completata senza uscire dall'accoppiata Internet Explorer 4 - Outlook Express. Bisogna ovviamente compilare un ridotto questionario, parzialmente mostrato in figura.

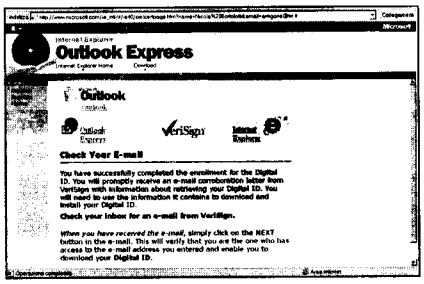

Figura 23 - Nel corso della procedura verrete invitati a controllare la vostra casella di posta elettronica...

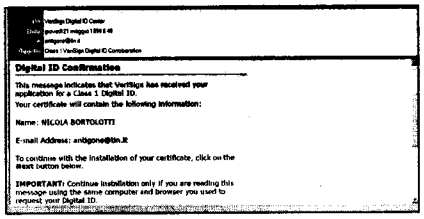

Figura 24 - ...dove troverete un primo messaggio di conferma e, continuando...

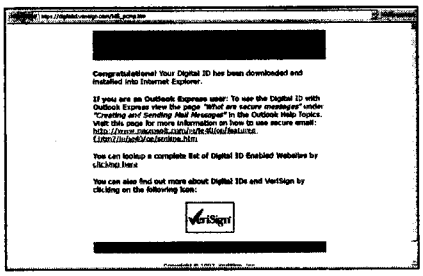

Figura 25 - ... sul browser apparirà infine la conferma dell'avvenuto scaricamento ed installazione dell'ID digitale. Una procedura rapida ma non scevra dal destare ben riposte perplessità sotto il profilo della sicurezza pressoché assoluta (che invece assicura PGP).

Si noti però che, contrariamente al caso di PGP, per l'utilizzo della firma - una volta associata all'account di posta elettronica - non è richiesta alcuna password; massima attenzione, quindi, alle mani indiscrete che operano sul vostro PC!

Facilità estrema con S/MIME

Outlook Express utilizza il comodissimo e universalmente accettato standard S/MIME (Secure Multipurpose Internet Mail Extensions) per lo scambio della posta, in pratica un'estensione del MIME (ben noto a tutti quanti abbiano almeno una volta allegato a un messaggio di posta un file: nessun bisogno di codifica/decodifica manuale, il messaggio viene allegato ed estratto in maniera del tutto automatica e trasparente per l'utente) dedicata alla validazione e cifratura.

Niente copia-incolla: tutto viene gestito cliccando l'icona di figura 20 in fase di preparazione del messaggio. Quando invece si riceve un messaggio "firmato" compare un pre-messaggio di avviso - che si potrà comunque escludere nel futuro (figura 26). Continuando, si perverrà infine al messaggio originale, che si intenderà "validato" in assenza di "Messaggi sulla protezione" indicanti eventuali problemi.

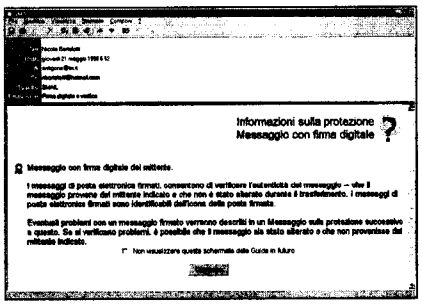

Figura 26 - Quando si riceve un messaggio "firmato" compare un pre-messaggio di avviso - che si potrà comunque escludere nel futuro. Continuando, si perverrà infine al messaggio originale, che si intenderà "validato" in assenza di "Messaggi sulla protezione" indicanti eventuali problemi.

verrà infine al messaggio originale, che si intenderà "validato" in assenza di "Messaggi sulla protezione" indicanti eventuali problemi.

Conclusioni

Da questa - necessariamente superficiale - carrellata in tre numeri, si può forse intuire un potenziale pericolo: quello, cioè, che ci si avvii ad un'autentica Babele della firma digitale e della cifratura.

E' ancora ben vivo nella memoria il ricordo di un presidente degli Stati Uniti che, in tempi recenti, diede l'ordine di un attacco "in chiaro" (ordine che fu intercettato da un radioamatore, al quale i grandi networks non diedero però credito) perché l'aereo in cui si trovava utilizzava un sistema crittografico diverso da quello dei militari che dovevano ricevere l'ordine...

Anche limitando la nostra analisi a due programmi, abbiamo visto come filosofia, modo d'uso, sicurezza ottenibile, potenzialità, generazione delle chiavi siano diversissime e profondamente incompatibili.

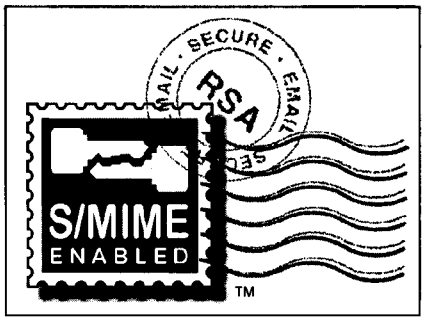

Figura 27 - Il logo di S/MIME, che si avvia a diventare lo standard per la posta elettronica "sicura" in ambiente Internet.

In realtà gli interessi economici legati alla "identità digitale" sono enormi e porteranno a una rapida convergenza della quale lo standard S/MIME dovrebbe (o potrebbe) essere uno dei punti cardine (nella figura 27 il "logo" ufficiale) in quanto in predicato di diventare uno standard Internet.

Nell'attesa, la situazione permarrà un po' disorientante per l'utente medio, stretto fra tecnologie perennemente *in fieri* e ambiziosi obiettivi di legge nazionali e linee guida europee: il DPR 513 prescrive infatti che "entro il 31 dicembre 1998, le pubbliche amministrazioni valutano in termini di rapporto tra costi e benefici il recupero su supporto informatico dei documenti e degli atti cartacei dei quali sia opportuna od obbligatoria la conservazione e provvedono alla predisposizione dei conseguenti piani di sostituzione degli archivi cartacei con archivi informatici" ma, soprattutto, "entro il 31 dicembre 1998 le pubbliche amministrazioni provvedono a definire e a rendere disponibili per via telematica moduli e formulari elettronici validi ad ogni effetto di legge per l'interscambio dei dati nell'ambito della rete unitaria e con i soggetti privati".