a cura di Corrado Giustozzi

Firma digitale, identificazione del mittente, e-mail cifrata....

Un argomento che per essere sviluppato a fondo probabilmente avrebbe bisogno di un anno di articoli, ed il primo della serie sarebbe abbondantemente superato dopo aver scritto il quarto. Argomenti che stanno diventando sempre più attuali anche al di fuori delle aziende e degli atti ufficiali, che hanno bisogno, per definizione, di sicurezza sull'identità dello scrivente. Corrado ed io abbiamo pensato che comunque è arrivato il momento di dare un panorama, iniziale, non certo conclusivo, di quello che sta succedendo in questo settore, dei costi e dei possibili vantaggi.

di Sergio Pillon

Nel concorso di Miss Italia di qualche anno fa una notizia curiosa fece il giro dei giornali italiani, ed il titolo che fece La Repubblica suonava all'incirca: "Miss Italia scalda i cuori della spedizione italiana in Antartide". In quel periodo io ero proprio il responsabile del sistema di posta elettronica della spedizione Italiana in Antartide nonché il Postmaster (il responsabile tecnico) del dominio PNRA.IT, (Programma Nazionale di Ricerche in Antartide, appunto).

Naturalmente l'articolo si basava su un messaggio di posta elettronica ricevuto dai curatori del programma televisivo che quell'anno, grazie ad un accordo con Video On Line (riposi in pace, Amen...) inviava in "diretta" sulla Rete le immagini delle Miss.

Purtroppo, come scrissi nella lettera di smentita inviata ai giornali, l'unico cuore che Miss Italia poteva avere scaldato, e sì quello sarebbe stato un fatto da prima pagina mondiale, era di un VAX 3800 della Digital, unico abitante della Base a rimanere "vivo" nei mesi invernali! I lettori più attenti di MC si ricorderanno di un mio articolo del '93 sulla base robotizzata in Antartide, dove il suddetto (ed un po' sporcaccione evidentemente...) VAX 3800 provvedeva al controllo dei motori che gli fornivano la corrente, alla acquisizione dei dati e al mantenimento dei sottosistemi ingegneristici ed informatici (telefono satellitare, apparati di comunicazione, archiviazione dati) che fanno della base italiana al Polo Sud nei mesi invernali una capsula automatizzata "quasi viva". La prima cosa che ho fatto è stata di sgridare il VAX, che a spese dei contribuenti inviava della posta elettronica a Miss Italia... ma in realtà il poverino ha dimostrato che non c'entrava nulla. Semplicemente da uno dei computer di VOL era arrivato un messaggio "a firma" della spedizione Italiana in Antartide. Chissà chi aveva fatto in modo che arrivasse questa bella pubblicità gratuita all'uso di Internet attraverso Miss Italia?

Questo episodio ci ricorda come sia facile alterare la configurazione del proprio programma di posta elettronica per figurare come qualcun altro. In effetti le informazioni sul mittente che ricevete in un messaggio di posta elettronica hanno la stessa attendibilità di quelle scritte sul retro della busta di una lettera cartacea: sono da correlare alla buona fede di chi scrive. Non mi preoccuperei troppo di un messaggio

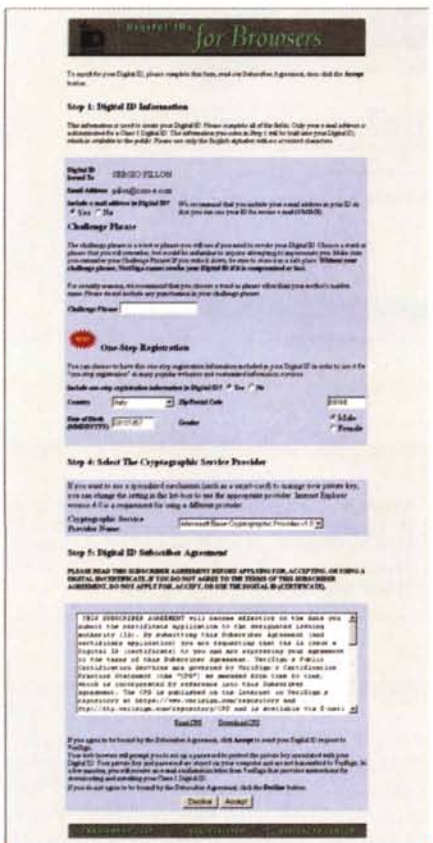
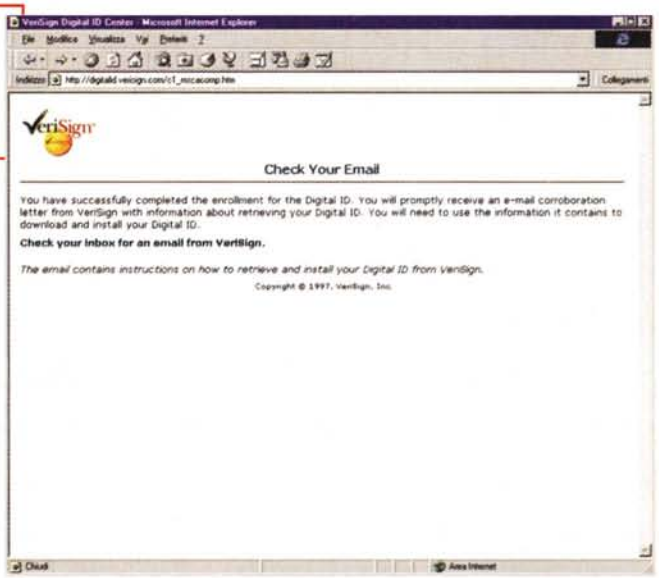


Figura 1 - Il modulo per la richiesta dell'ID digitale. Come potete vedere ho richiesto, con la procedura automatica, un ID digitale per i browser. Anche qui un po' di confusione, lo posso usare per la posta a patto di includere il mio e-mail nell'ID. Ma io proprio per Outlook Express lo avevo chiesto!!! Un contratto vero e proprio, con il quale ho ottenuto il mio ID da 9,95 dollari.

della nonna, ma se ricevessi un messaggio dalla presidenza del consiglio dei ministri non mi fiderei del mittente ma forse, ed anche poco, solo della carta intestata. Ed è questo il problema della posta "virtuale": non esiste la carta intestata e purtroppo molti tendono a considerare l'e-mail più attendibile della posta cartacea. Il conduttore della trasmissione, Fabrizio Frizzi, mi disse successivamente che non aveva affatto pensato che la lettera potesse essere falsa; ma certamente se l'avesse ricevuta per posta qualche dubbio in più lo avrebbe avuto...

Figura 2 - Se tutto è stato fatto correttamente riceverete immediatamente un messaggio nella vostra casella postale...



L'ID digitale

La soluzione ideale per evitare che qualcuno si spacci per voi nella posta elettronica è l'uso di un sistema ben collaudato (in Internet significa alcuni mesi...) di certificazione elettronica. Disponibile direttamente dal menu dei più usati programmi di posta elettronica, sicuramente ben integrato sia in Outlook Express di Microsoft che in Netscape Mail e News, l'uso dell'ID digitale (ossia di un identificativo non falsificabile che certifica l'identità del mittente) risolve in buona parte questi problemi. Certo non sono tutte rose e fiori, come sempre accade nel nostro mondo. Vediamo dunque assieme alcune rose ed alcune spine usando per questa "prova su strada" Verisign (http://www.verisign.com), uno dei maggiori fornitori del servizio.

Il primo passo da compiere è quello della richiesta di un proprio ID, e già qui le cose non sono chiarissime. Selezionando "opzioni" dal menu strumenti di Outlook Express, il programma di posta elettronica integrato in In-

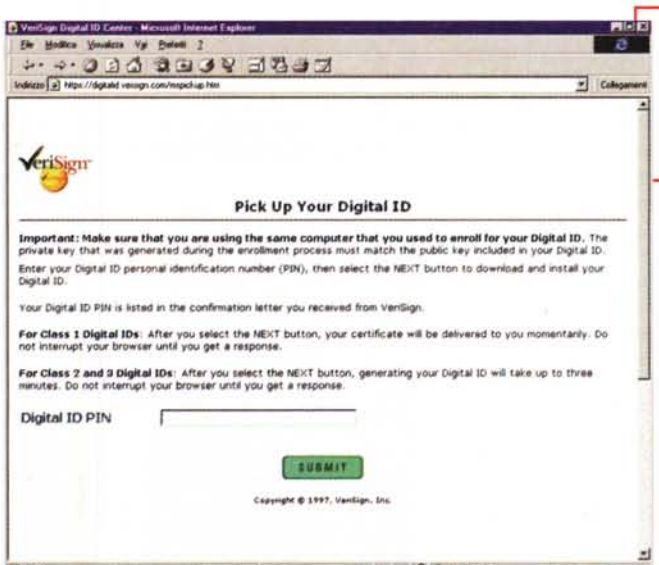


Figura 3 - Dopo aver ricevuto il messaggio con il proprio PIN ci si collega all'indirizzo indicato nel messaggio e si inserisce il codice, con copia & incolla.

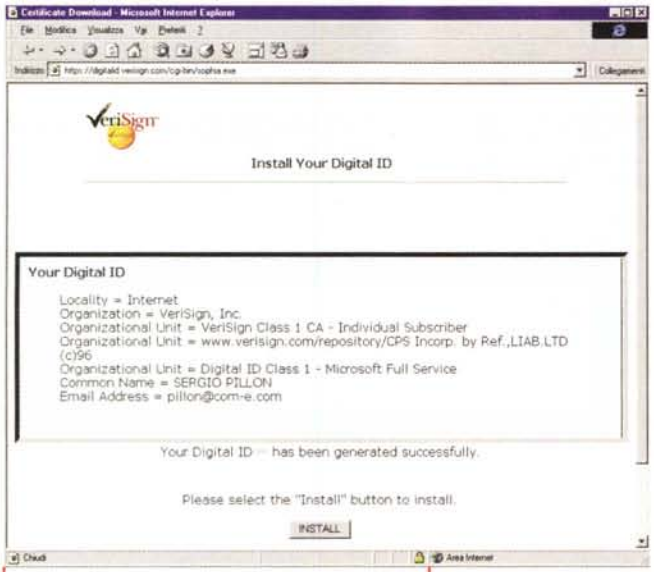


Figura 4 - Il quarto passo, l'ID viene generato e può essere installato sul proprio computer, il tutto direttamente dal sito. Come vedete dall'indirizzo, le transazioni sono fatte con il protocollo HTTPS, cioè il "secure http", cifrato per evitare possibili "catture" di codici.

Figura 5 - L'installazione è stata completata e da questo momento posso usare l'ID. Certo il tutto ha richiesto un po' di tempo ed una buona conoscenza dell'inglese, non mi risultano versioni in lingua nazionale... purtroppo.

ternet Explorer di Microsoft, appaiono le solite cartelle, in Protezione si trova il bottone Seleziona un ID digitale, pessima, traduzione del concetto OTTIENI un ID digitale!!!

In effetti continuo a sbagliarmi, ogni volta che accedo al menu, ora che di ID ne ho quattro, e voglio selezionarne uno finisco su questo bottone, che oltre tutto mi attiva il collegamento Internet per accedere ad una pagina, http://www.microsoft.com/ie_intl/it/ie40/oe/certpage.htm?name=Sergio%20Pillon&email=pillon@mclink.it dove prende le informazioni sul mio ID. E qui arriva la prima fonte di confusione *"Grazie a un'offerta speciale di VeriSign, gli utenti che utilizzano Microsoft Internet Explorer 4.0 possono ottenere gratuitamente un ID digitale personale, che altri utenti e provider di servizi in linea potranno utilizzare per verificare l'identità del mittente"* recita il sito Microsoft, ma non ho trovato nessuna traccia dell'offerta sul sito Verisign, per cui mi sono preso un ID a 9,95 dollari ed uno gratuito, con due diversi PC e due diversi indirizzi di posta elettronica. Vi farò sapere se dopo i 60 giorni di prova gratuiti che Verisign offre uno dei due verrà disattivato... Potrete anche scoprirlo da soli, anzi è molto meglio: dalla rubrica di Outlook Express, connessi alla rete, selezionate TROVA. Tra i servizi possibili scegliete Verisign, e cercate Sergio Pillon. Troverete i miei ID, con possibilità di inserire nell'agenda le mie informazioni pubbliche, e la parte "pubblica" del mio ID. Potremmo a quel punto, se avete anche voi un vostro ID scambiarci messaggi cifrati.

La firma elettronica dell'e-mail

Quello che abbiamo fatto in questo momento è ottenere da una "autorità di certificazione", in questo esempio Verisign, un identificativo digitale. Il procedimento in realtà va fatto proprio in linea, in modo che si riceva direttamente nella propria casella postale il messaggio di Verisign con il codice personale, con il quale dal sito WWW ottenere l'ID, che viene direttamente "Inserito" nel programma di posta elettronica ed anche nel Browser. Infatti ora quell'identificativo è disponibile anche mentre si naviga sulla Rete, per "autenticare" il nostro indirizzo elettronico.

Figura 6 - La prova del funzionamento per il browser. Se funziona, l'installazione è stata fatta con successo.

Ma attenzione: un messaggio con la firma digitale non identifica chi sta inviando il messaggio ma certifica solamente che la persona che scrive dall'indirizzo, ad esempio Pillon@mclink.it, è il legittimo proprietario dell'indirizzo! La responsabilità dell'identificazione del proprietario di un indirizzo di posta elettronica è un altro paio di maniche, si tratta quindi di una firma che certifica l'indirizzo, non la persona.

Le informazioni che si ottengono sui "proprietari" di identificativo digitale sono ad assoluta discrezione di chi ha richiesto l'ID. Per chiarire meglio il concetto, se all'indirizzo di

Pillon@mclink.it avessi assegnato Bruce Wayne, alias Batman, Gotham City, USA, esso sarebbe stato accettato lo stesso. Questo concetto va benissimo con la legislazione anglosassone, per cui non è quasi neppure un reato usare un altro nome tanto è la persona "fisica" che deve essere raggiunta dalla citazione (vi ricordate quelli che scappano inseguiti dall'ufficiale giudiziario che li deve toccare con il foglio perché sia valida la citazione?), ma assolutamente estraneo al nostro modo di pensare; in Italia è la nostra carta d'identità ad essere processata, non noi; noi "serviamo" solo dopo, alla fine, per pagare le multe o per andare in prigione.

Attenzione dunque, l'identificativo digitale della posta elettronica è un concetto di identificazione molto anglosassone e poco latino.

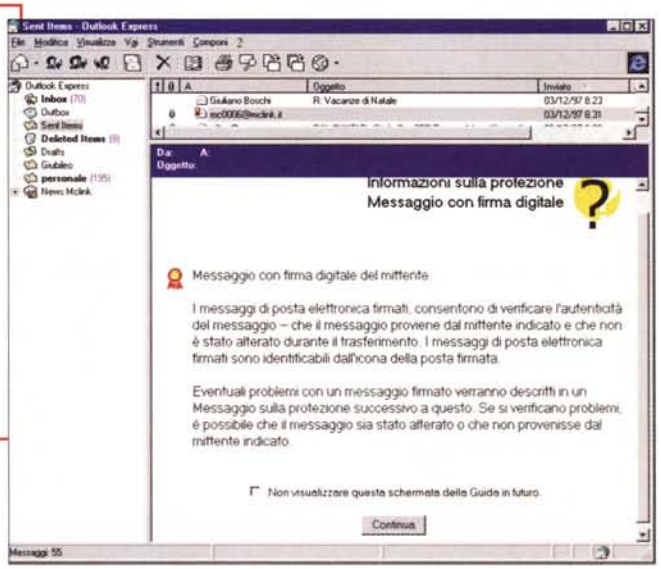


Figura 7 - Il primo messaggio di prova inviatevelo da soli: selezionate nel messaggio "inserisci firma digitale" e dovreste vedere questa pagina iniziale. Naturalmente si può richiedere di non vederla ogni volta. La coccarda nell'angolo permette di leggere le informazioni dell'ID ed anche di inserirlo nella rubrica personale. Un trucco: se non vi siete inseriti nella rubrica non potete inviare messaggi cifrati, perché il sistema non vi conosce...

La posta cifrata

Si sente dire spesso che la posta elettronica non è sicura, che i messaggi possono essere intercettati, che è più facile leggere un messaggio di posta elettronica che un messaggio cartaceo e via dicendo. Questo è probabilmente vero, ma bisogna vedere la cosa con un po' di ragionevolezza: dipende da cosa vogliamo fare con la posta elettronica!

Lo scherzo viene "stoppato" dalla firma digitale, ma l'invio di una strategia di marketing o semplicemente la posta elettronica in una rete aziendale possono essere molto appetitose anche per aziende concorrenti. Un uso "serio" di Internet anche in una piccola impresa deve iniziare a considerare l'ipotesi di scambiarsi messaggi cifrati.

I metodi usati sono molti, Corrado Giustozzi ne ha parlato in passato più volte e non mancherà di riparlarne in futuro, per ora assumiamo semplicemente un concetto: il messaggio cifrato è un messaggio che non può essere letto da altri che il legittimo destinatario, o da qualcuno che ha "rubato" la sua chiave. E' come mettere il messaggio in una cassaforte virtuale di cui esistono solo due chiavi, la nostra e quella del destinatario.

Ovviamente perché la cosa funzioni dobbiamo avere la nostra chiave privata e quella pubblica del destinatario, che si può ottenere semplicemente cercandola su una autorità di certificazione o richiedendola direttamente al nostro interlocutore.

Con Outlook Express ad esempio basta aver ricevuto un messaggio con firma digitale per poter aggiungere alla rubrica l'ID digitale del mittente e quindi poter cifrare i messaggi a lui diretti. Non avrebbe senso farlo senza disporre della sua firma, sarebbe come mettere i messaggi in una cassaforte che neppure noi potremmo riaprire!

La gestione dell'ID digitale

Non basta aver ottenuto un ID, digitale, occorre anche poterlo gestire. Già immagino le domande: *"io uso vari PC, posso portarlo su un altro computer?"* oppure *"Che succede se mi si rovina il file sul disco rigido?"* e via dicendo.

Innanzi tutto una prima caratteristica dell'ID digitale è la "esportabilità" del

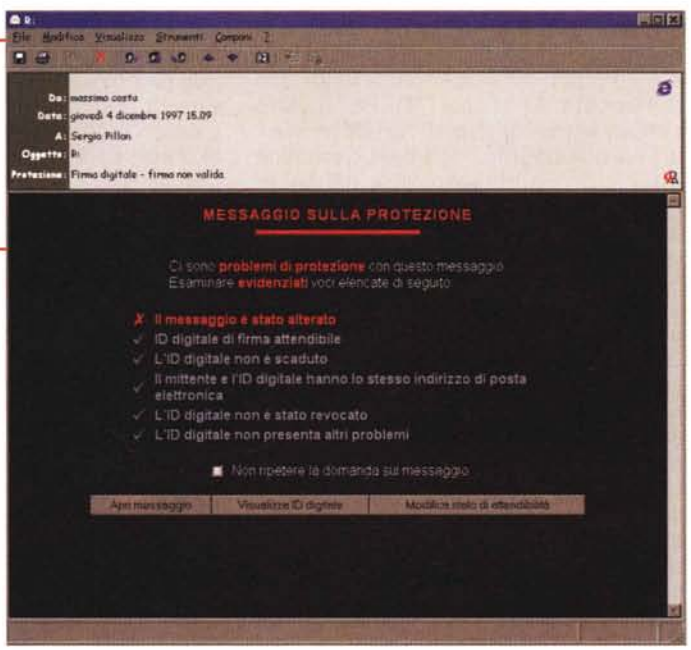


Figura 8 - Se non rifirmate un messaggio dopo averlo corretto succede questo! Vedete anche quanti controlli vengono fatti sul messaggio...

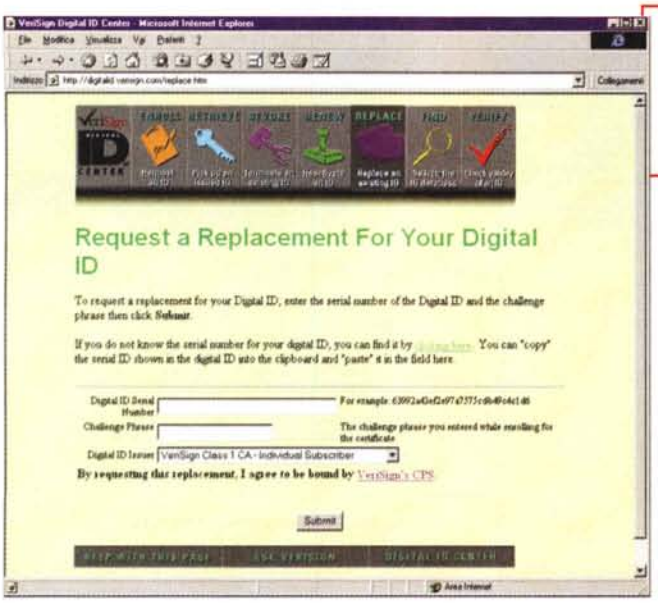


Figura 9 - Ecco il modulo per ottenere la sostituzione dell'ID digitale, semplice ed immediato. Magari fosse così con le carte di credito...

codice, nel senso che dal programma di posta elettronica o dal Browser si può selezionare "esporta ID digitale", per consentire di inviare l'ID ad altri utenti o ad altri programmi. Viene chiesto il nome di un file e la password per cifrarlo, e viene generato un file che può essere tranquillamente salvato su un dischetto ed usato su un altro computer con l'opzione inversa "importa ID digitale".

In effetti io ho vari account di posta elettronica che Outlook Express gestisce, e ad ognuno è assegnato un ID digitale. Lui (Outlook) per inviare la posta usa l'account "predefinito" ed è quindi di quello che mette l'indirizzo di risposta ed anche l'ID. Per inviare con un altro indirizzo si "predefinisce" un altro account... et voila! Semplice ma... non completamente efficace. Durate le varie prove qualcosa è successo, ed il programma non era più in grado di usare il mio vecchio identificativo: valido, esistente, ma non lo potevo importare perché esisteva già, non lo potevo esportare perché non valido e neppure eliminare (a proposito, non sono riuscito a trovare l'opzione "elimina ID digitale"!) Insomma sono stato costretto a revocare l'ID dal sito Verisign e farmene assegnare uno nuovo, come aver denunciato lo smarrimento della carta di credito chiedendone una nuova, con un altro numero. Il tutto per fortuna richiede pochi minuti, ed ora sul sito della Verisign trovate un mio ID revocato (viene mantenuto per motivi "storici") ed uno valido.

Il tutto è possibile farlo grazie ad una "challenge phrase", insomma una password un po' più lunga, che vi fa riconoscere sul sito Verisign come veri titolari dei diritti su quell'identificativo. Attenzione quindi, quando vi viene richiesta la passphrase usatene una che ricorderete nei secoli, potreste averne bisogno dopo mesi per operare sul vostro account. Quelle che vi vengono in mente al volo tipo "che noia le password" si dimenticano in fretta e rendono la vita complicata.

Insomma, come legittimi proprietari dell'ID possiamo revocarlo, chiederne una copia, il tutto in pochi minuti. L'unico problema è che ora ne ho due allo stesso indirizzo, uno revocato ed uno attivo... A proposito, mi dicono i bene informati che la versione attuale di Outlook Express non fa un controllo in linea se l'ID è valido quando riceve il messaggio, ma le nuove lo faranno. Debbo dire che non ho potuto controllare ma mi sembra abbastanza ovvio che lo debba fare: probabilmente se non lo fa ora lo farà la versione che sarà in giro quando leggerete l'articolo.

L'ID digitale nel browser

L'uso del sistema descritto per ottenere un ID lo inserisce anche nel browser, in questo caso in Internet Explorer. Il motivo è ovvio: spesso viene chiesta un'identificazione dell'indirizzo di posta elettronica quando si fanno delle transazioni, ma anche semplicemente per iscriversi nelle mailing list. È fin troppo facile iscrivere amici o nemici a mailing list, l'uso di un ID che certifichi l'indirizzo rende il processo molto più sicuro.

Ma anche nelle Intranet o in siti con "personalizzazioni" l'uso dell'ID digitale può semplificare la vita. Invece del solito (scomodo) uso di username e password, avere nel proprio browser un ID digitale "completo" permette di accedere ai propri dati in modo molto più semplice e sicuro. Attualmente questo metodo è poco diffuso sul Web e non sono molti i siti che lo supportano, ma probabilmente l'identificazione attraverso il browser diventerà sempre più richiesta, evitando la procedura di password eccetera.

Sicuramente un procedimento che semplifichi la navigazione sicura sulla Rete è auspicabile, ma alle volte non si vuole proprio essere identificati: ci mancherebbe solo che ogni volta che ci fermiamo a guardare la vetrina di un negozio qualcuno ci chiedesse i documenti! Ecco che quindi si tratta di una tecnologia "delicata", di cui è importante semplificare la gestione ma anche rendere difficile un uso improprio. Non ho approfondito l'argomento ma attualmente, disponendo di più di un ID digitale, quando sono andato in siti di prova che lo utilizzavano mi è stato sempre chiesto *"quale vuoi inviare?"*, mentre avrei preferito che mi si chiedesse *"Il sito ha richiesto il tuo ID digitale, vuoi inviarlo?"*.

Conclusioni

Quasi solo vantaggi: è economico (9,95 dollari), semplice, utile. Il possibile problema è forse proprio alla radice, l'autorità di certificazione. Chi la garantisce? Chi mi assicura che non userà i miei dati per inserirli in milioni di mailing list di ogni genere? Dove sarà tra un anno? Che diritti ho? Che valore ha un mio messaggio con la firma digitale con un certificato di Verisign o della Pizza e Fichi Corp.?

Una strada interessante, da esplorare e che sicuramente è nel futuro immediato. E soprattutto è ora che facciate qualche prova anche voi!

MC

AVM

I prodotti ISDN leader del mercato in Germania

ZyXEL

Router, Modem, TA: tutti i prodotti ISDN per il Personal Computing e le Reti Locali

SEDLBAUER AG

Adattatori ISDN per ogni necessità

Petra Internet Gateway

Gateway, Router, Firewall, software completo e versatile per internet ed intranet

Caldera OpenLinux

La più completa distribuzione Linux (anche in lingua italiana)

Max 128

La nuova scheda ISDN per Win 3.x, Win '95 e Win NT 4

VCON VIDEOCONFERENCING

I prodotti per videoconferenza con il migliore rapporto qualità/prezzo

ISDN point

...Benvenuti

..Welcome

fast-communication

la comunicazione veloce

is on line ...

e' in linea.....

CoFax TELEMATICA

http://www.cofax.it
Roma: 06/58201362
Milano: 02/29526100