

Editoriale

Mercato e diritti umani

La nuova Grande Muraglia Cinese 3

Marcello Oddini

La posta dei lettori 4

a cura di Alessandro Longo

Attualità

Made in Internet 6

Luca De Leone

Grandi vendite, piccole vendite

Quelli della coda lunga 10

Giuseppe Granieri

Single sign on

Identità oggi fa rima con libertà 16

Fabio Metitieri

Digitale terrestre

Dtt, la televisione incinta della Rete 20

Lele Dainesi

Persone e aziende

Idee e profili

Altiris anche in Italia lavora per razionalizzare gli asset It 22**Sterling commerce: non solo Edi** 23**Per Storage Tek il mercato in Italia cresce, ma lentamente** 23

Fabio Metitieri

Web Agency World

Virgilio Web Services: «Ripartire dalle competenze acquisite» 25**News d'agenzia** 27

Pietro Izzo

Risorse

Idearium 28

P.I.

Speciale - Sondaggi online

Cati, Capi o Cawi?

Se non lo sai, chiedilo! 32

Roberto Ghislandi

Formazione

Master & Corsi 46

Katia Girini

Connessioni

Mercato e tendenze 48

Alessandro Longo

Marketing

e-metrics

Raccogliere, interpretare e utilizzare i dati di traffico 54

Miriam Bertoli

Web design

Mode di stagione

I nuovi trend estetici 56

Sofia Postai

Tecnologie

La natura duale del Web

Oltre la distinzione fra ipertesto e applicazione 60

Maurizio Boscarol

Cavalli di razza

Java 6.0 Nome in codice: Mustang 64

Massimiliano Bigatti

Architettura estendibile

ASP.NET 2.0 Custom Membership 68

Roberto Brunetti

CSS 3

La gestione dei testi 72

Dario de Judicibus

Sicurezza

Oltre l'hacker, il tracker

Sulle tracce degli spammer 76

Enrico Bottari

Voce senza rischi

I problemi di sicurezza dei sistemi VoIP 81

Jeffrey T. Hicks

Laboratorio

Sicurezza da Stonesoft

Stonegate – High Availability Firewall e Multi-Link Vpn Engine 82

Marco Cremonini, Michele Vettori

Firma digitale

GlobalTrust – Enigma Lite Desktop Edition 88

Marco Cremonini

Prodotti

Le novità del mese 92

Paolo Crespi

Libri

Letti per voi 96

FM

N° 5 – Anno XI – giugno 2005

Direzione, redazione, abbonamenti, amministrazione e pubblicità:

Casa Editrice Tecniche Nuove SpAVia Eritrea, 21 • 20157 Milano • Italia
Fax 023551472 • www.tecnichenuove.com**Direttore responsabile:**
Giuseppe Nardella**Direttore editoriale:**
Marcello Oddini • tel. 0239090352
marcello.oddini@tecnichenuove.com**Coordinamento scientifico:**
Ernesto Damiani e Pierangela Samarati
Università degli Studi di Milano,
Dipartimento di Tecnologie per l'Informazione
pierangela.samarati@tecnichenuove.com
ernesto.damiani@tecnichenuove.com**Redazione:**
fax 0239090302
internet-pro@tecnichenuove.com**Progetto grafico e copertina:**
Franco Beretta • tel. 0239090239
franco.beretta@tecnichenuove.com**Hanno collaborato a questo numero:**
Massimiliano Andreozzi, Miriam Bertoli,
Massimiliano Bigatti, Maurizio Boscarol, Enrico Bottari,
Roberto Brunetti, Marco Cremonini, Paolo Crespi,
Dario De Judicibus, Luca De Leone, Roberto Ghislandi,
Katia Girini, Giuseppe Granieri, Pietro Izzo,
Alessandro Longo, Fabio Metitieri, Graziano Panzera,
Sofia Postai, Michele Zambelli**Abbonamenti:**
Daniela Toloi (responsabile)
tel. 0239090260 • abbonamenti@tecnichenuove.com
Alessandra Caltagirone • tel. 0239090241
www.tecnichenuove.com/riviste/informatica/internetpro**Relazioni pubbliche:** Sergio Savona**Vendita spazi pubblicitari:**
Giovanni Cerutti • tel. 0239090229 • 3357186848
giovanni.cerutti@tecnichenuove.com**Coordinamento stampa e pubblicità:**
Fabrizio Lubner (responsabile)
Tiziana Bartolini • tel. 0239090298
tiziana.bartolini@tecnichenuove.com**Pubblicità:**
Via Eritrea, 21 • 20157 Milano • tel. 02390901**Stampa:** Rotolito Lombarda
Via Brescia 53, Cernusco sul Naviglio MI**Responsabilità**
La casa editrice non assume alcuna responsabilità nel caso di eventuali errori contenuti negli articoli pubblicati o di errori in cui fosse incorsa nella loro riproduzione sulla rivista. Tutte le pubblicazioni su internet.pro avvengono senza eventuali protezioni di brevetti d'invenzione; inoltre, i nomi delle merci coperti da eventuale marchio registrato vengono utilizzati senza tenerne conto.

© 2005 Tecniche Nuove SpA

La riproduzione di illustrazioni e articoli pubblicati dalla rivista, nonché la loro traduzione, è riservata e non può avvenire senza espressa autorizzazione della casa editrice. I manoscritti e le illustrazioni inviati alla redazione non saranno restituiti anche se non pubblicati e la casa editrice non si assume responsabilità per il caso che si tratti di esemplari unici.

Associato a: **ANES** ASSOCIAZIONE NAZIONALE EDITORIA PERIODICA SPECIALIZZATA **ADERENTE A CONFINDUSTRIA****Tariffe degli abbonamenti:**Annuale 30 € - Biennale 50 €
Annuale Europa 60 € - Annuale Extra-Europa 100 €**Gli abbonamenti decorrono dal mese successivo al ricevimento del pagamento.**Costo copia singola 3,90 € (presso l'editore, fiere e manifestazioni)
Copia arretrata (se disponibile) 7,80 € + spese di spedizione

ISSN 1824-8403

Poste Italiane Spa - Spedizione in abbonamento postale
D.L. 353/2003 (convertito in Legge 27/02/2004 n° 46)
art. 1 comma 1 - DCB Milano.

Registrazione presso il Tribunale di Milano N° 117/90 del 23/2/90

Tecniche Nuove è iscritta al ROC - Registro degli Operatori della Comunicazione con il n° 6419 (delibera 236/01/Cons del 30/6/2001 dell'Autore per le Garanzie nelle Comunicazioni).

GlobalTrust – Enigma Lite Desktop Edition

Enigma Lite Desktop Edition è prodotto dall'italiana GlobalTrust Inc., la quale è affiliata della nota società canadese Entrust Inc., pioniere delle tecnologie basate su Pki, ed è l'unica Registration Authority in Europa dalla nascita dell'**Entrust International Affiliate System** nei paesi asiatici [www.entrust.com/certificate_services/affiliates.htm]. GlobalTrust è specializzata in soluzioni e prodotti di sicurezza basati su tecnologie crittografiche e Pki.

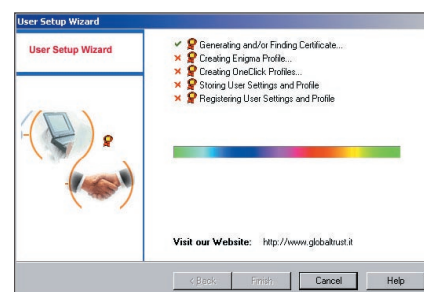
Documentazione

La documentazione di Enigma Desktop è sufficientemente completa dal punto di vista tecnico ma purtroppo per ora è disponibile solo in inglese. GlobalTrust ha comunque già annunciato il rilascio a breve di una versione completamente in italiano. Esiste però un altro aspetto sul quale la documentazione è insufficiente: il soddisfacimento dei requisiti imposti da normative nazionali e internazionali. Uno dei punti forti di Enigma Desktop è costituito proprio dalla dichiarata compatibilità con il decreto legislativo 196 del 30 giugno 2003 «Codice in materia di protezione dei dati personali», e con la direttiva europea sulla firma digitale dell'ottobre 2001, oltre a molte normative statunitensi. Come Enigma Desktop soddisfa i requisiti imposti da tali normative non viene descritto in nessun modo. Curioso come la compatibilità con la normativa italiana sia dichiarata nello User Reference Manual in inglese ma scompaia dalle brochure e dai comunicati stampa in italiano. Certo, considerando lo stato confusionale nel quale è caduta

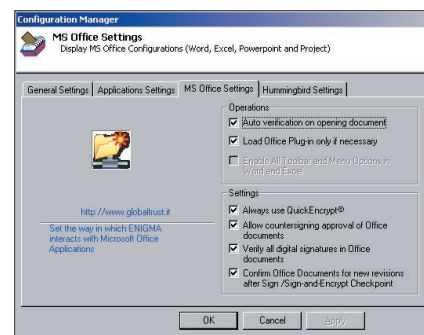
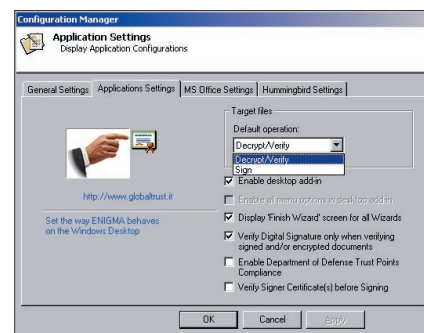
ultimamente la nostra normativa in merito a documenti elettronici e protezione dei dati personali, non si può biasimare GlobalTrust se preferisce glissare su questo punto. In ogni caso, se tutto ciò può apparire un dettaglio, non lo è in realtà, perché lasciare agli addetti ai lavori l'esclusiva della piena comprensione della normativa e di come gli strumenti la recepiscono, svuota di significato l'intreccio tra norme e tecnologia agli occhi del grande pubblico. Di conseguenza, le norme possono apparire come i soliti bizantinismi della burocrazia che non necessitano di comprensione ma solo di formale soddisfacimento. Questo è un errore da non fare, la commistione tra norme e tecnologia è il motivo dell'esistenza di un tool come Enigma Desktop, la difficoltà di definire in maniera chiara tale relazione è una delle cause sia della scarsa diffusione di tool come quello trattato sia del parziale fallimento fino a oggi subito da parte delle tecnologie basate su Pki.

Installazione e configurazione

La procedura d'installazione è adatta al target di riferimento, semplice e guidata da un wizard. La configurazione, gestita dal Configuration Manager, è anch'essa semplice da impostare e nella maggior parte dei casi i default sono appropriati. Nella versione attualmente disponibile, Enigma Desktop è compatibile solo con piattaforme Microsoft non meglio specificate, ma da quanto riportato da un comunicato stampa di GlobalTrust, sono attese a breve versioni compatibili con altri sistemi operativi.



Wizard per il setup di Enigma Desktop.



Il Configuration Manager di Enigma Desktop.

Parte fondamentale della configurazione del tool è la definizione del certificato dell'utente (naturalmente ne sono ammessi anche più di uno). Il certificato può essere semplicemente importato, se salvato in uno dei formati standard, per esempio PKCS#12, oppure deve essere generato attraverso il Certificate Generation Wizard. Il Certificate Generation Wizard supporta tre tipi di operazioni: generazione di certificato self-signed, generazione di certificato rilasciato da GlobalTrust, oppure generazione di una richiesta di certificato secondo lo standard PKCS#10. La prima tipologia è riservata soprattutto a un uso personale dei certificati importando il proprio certificato self-signed tra le CA Root. È in pratica un modo per utilizzare la tecnologia Pki per operazioni personali di firma e di crittazione,



Scheda tecnica

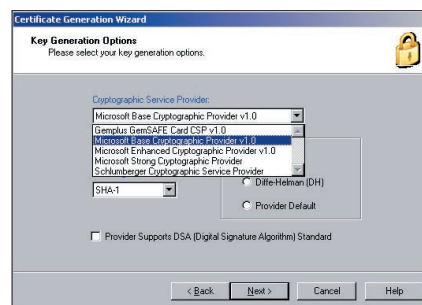
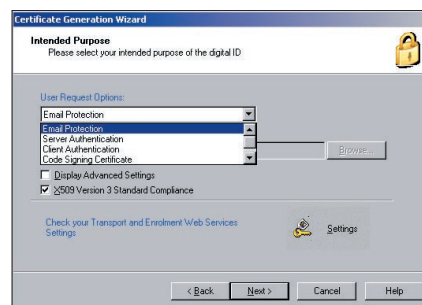
Tipologia	Suite per firma digitale e crittazione
Produttore	GlobalTrust Inc. Piazza San Pietro 2 05100 Terni www.globaltrust.it www.entrust.it info@globaltrust.it
Prezzo	500 €
Caratteristiche	Gestione time stamping, archiviazione e cancellazione documenti sicura, integrazione con Ldap e Crl online, posta elettronica Microsoft Outlook, supporto per Smartcard, token Usb, dispositivi biometrici. Conformità a normative nazionali e internazionali.
Giudizio	

limitate al più a una ristretta comunità di partner. Chi cerca semplicemente una funzionalità del genere ha a disposizione PGP e i corrispondenti tool freeware che lo implementano. Ricorrere a tecnologie basate su Pki non offre alcun beneficio reale in questo caso. Il target di Enigma Desktop è invece da cercare tra le organizzazioni che effettivamente implementano infrastrutture Pki, nelle quali quindi normalmente i certificati si richiedono in formato PKCS#10 o attraverso procedure offline e successivamente importati. Enigma supporta le diverse tipologie d'uso di un certificato – protezione della posta elettronica, autenticazione server o client, oppure firma di codice – e si integra con i più diffusi motori crittografici, presenti sia in smartcard sia in browser e mailer.

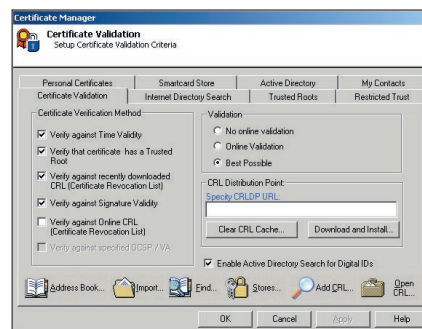
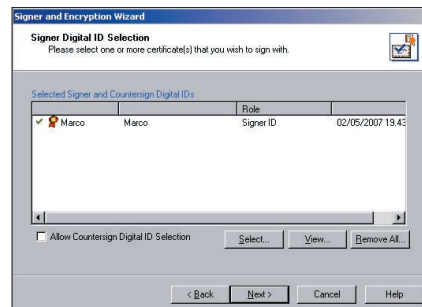
Funzionalità

Le funzionalità messe a disposizione da Enigma Desktop comprendono le tradizionali operazioni crittografiche di firma e cifratura di file offrendo un buon ventaglio di opzioni tra le quali la possibilità di apporre firme multiple utilizzando certificati diversi, la generazione di *timestamp* e l'inclusione di

loghi o immagini per una verifica visuale in aggiunta all'operazione di verifica crittografica. Enigma Desktop è integrato inoltre con Microsoft Office e Outlook; in tal modo l'utente ha a disposizione alcune icone e il menu OfficeGuard con le operazioni di Firma e Cifratura o la combinazione Firma&Cifratura delle due. Altre funzionalità importanti implementate da Enigma Desktop sono l'integrazione con le tradizionali Certificate Revocation List e le più recenti Online Crl, l'integrazione con Directory Server Ldap o con l'Active Directory di Microsoft. Tutte le funzionalità sono accedibili dalla Gui. Un aspetto decisamente negativo è dato dal fatto che le finestre non sono ridimensionabili, una dimenticanza che rende talvolta l'accesso alle informazioni poco agevole, soprattutto se tabellari. Per quel che concerne la possibilità di includere loghi o immagini nella procedura di firma digitale di un documento elettronico, si tratta di un'opzione poco diffusa prevista sia dalla legislazione Usa sia da quella europea. In generale, è consentito utilizzare un'immagine di 240x150 pixel come parte del contenuto firmato digitalmente. L'esempio più comune, ma anche quello



I passi salienti della generazione di un certificato attraverso il Certificate Generation Wizard: selezione dell'uso al quale il certificato è deputato (in alto), motore e algoritmi crittografici (in basso).

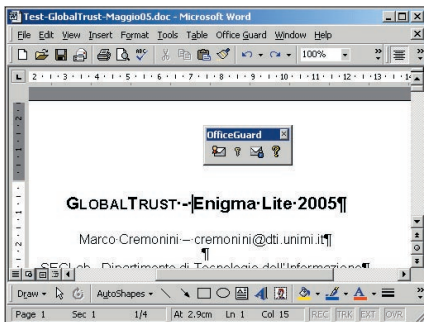


Selezione di un certificato per la firma (in alto) e il Certificate Manager per la gestione di tutte le opzioni legate ai certificati, alle operazioni crittografiche e alle autorità di certificazione riconosciute (in basso).

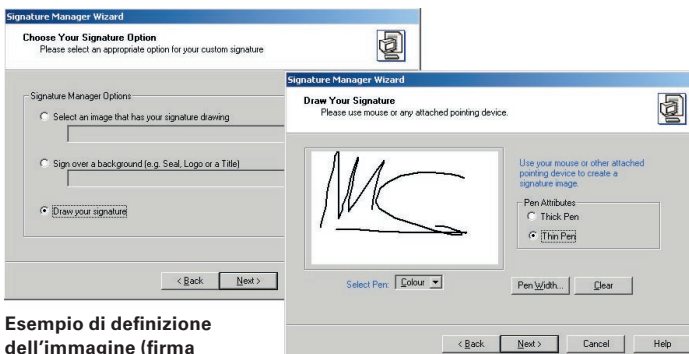
fonte di maggiori incomprensioni, è probabilmente l'uso della firma manoscritta acquisita via scanner. A scanso di equivoci, è bene precisare che tale opzione non sostituisce e non rappresenta in alcun modo un'alternativa alla firma digitale crittografica ma costituisce un'integrazione al contenuto del documento elettronico firmato. Può essere considerata in maniera simile al timestamp, ovvero un'informazione aggiuntiva firmata e crittata insieme al documento elettronico. Lo scopo dell'immagine firmata è quello di fornire, all'atto della verifica della firma digitale, un riscontro grafico dell'identità di chi ha apposto la firma digitale. È indispensabile tenere presente che, per quanto la resa finale di questa opzione sia di sicuro impatto sull'utente, essa rappresenta di gran lunga l'informazione meno certa di tutte e la forma di autenticazione più debole tra quelle esistenti. Un'altra funzionalità importante messa a disposizione da Enigma Desktop è la cancellazione sicura dei documenti (shredding). Il presupposto di tale funzionalità è che tutti i sistemi operativi gestiscono la cancellazione di file in

maniera logica, non fisica. In breve, i dati cancellati non vengono realmente distrutti dall'operazione di cancellazione ma semplicemente resi non più disponibili agli utenti. Questo fa sì che sia possibile implementare funzioni di recupero di dati cancellati, per esempio per errore. Allo stesso tempo però, è possibile che qualcuno non autorizzato possa recuperare quegli stessi dati che si intendevano cancellare in maniera definitiva. Per ovviare a questo esistono molti tool che offrono funzionalità di cancellazione sicura simile a quella offerta da Enigma Desktop. Tuttavia, GlobalTrust dimentica di specificare un dettaglio importante: anche la cancellazione sicura può essere poco sicura. Esistono diverse tecniche a questo proposito, tutte basate su algoritmi che forzano cicli di riscrittura delle locazioni di memoria nelle quali i dati da cancellare sono memorizzati. A seconda della complessità dell'algoritmo e del numero di riscritture le diverse soluzioni possiedono diversi gradi di sicurezza. Quanto più una tecnica di cancellazione sicura è realmente sicura, tanto più il tempo che tale operazione impiega è lungo. Quale di quelle disponibili, note e verificate GlobalTrust implementa? Non viene fornito alcun dettaglio e ciò non è affatto positivo. Le *One-Click Policy* sono un'altra funzionalità utile offerta da Enigma Desktop per semplificare il compito dell'utente. Si tratta di configurare un insieme di operazioni predefinite, per

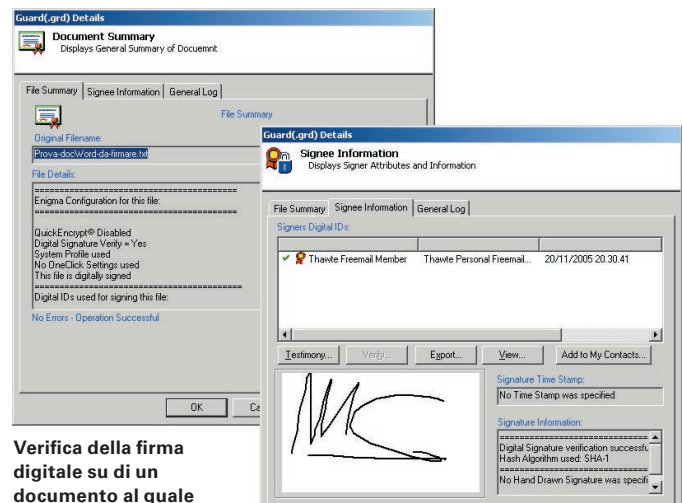
esempio di firma utilizzando un dato certificato, prevedendo l'inserimento di timestamp, seguita da cifratura con un ulteriore certificato e un certo algoritmo. Questo insieme di operazioni, che richiederebbero la selezione manuale attraverso svariate finestre, sono eseguite automaticamente richiamando la one-click policy corrispondente. L'ultimo aspetto del quale discutiamo è la Legal Signing Ceremony, ovvero una procedura che attira l'attenzione dell'utente sulle implicazioni legali dell'apposizione di una firma digitale oltre a fornirgli messaggi informativi di altro genere. La dicitura che attualmente appare recita: «I hereby declare that I have viewed and understood the contents of the selected file(s)». In poche parole, si dichiara di conoscere ciò che si sta firmando digitalmente. Questo passo, puramente formale, può venire richiesto in scenari ufficiali, pubbliche amministrazioni, per esempio. Tuttavia, nel provarlo sono stati riscontrati alcuni problemi. Il primo riguarda il pulsante Testimony Details che invariabilmente mostra una finestra completamente bianca. Dalla documentazione non è chiaro quali informazioni dovrebbe contenere, o viceversa cosa si dovrebbe fare affinché mostri qualcosa di significativo. Altri problemi sono stati riscontrati nell'uso delle icone e delle voci di menu OfficeGuard da Microsoft Word (MS Word 2000). Talvolta cliccando sulle icone non sono state invocate le



Le icone e il menu OfficeGuard in Microsoft Word.



Esempio di definizione dell'immagine (firma manoscritta) da associare al contenuto firmato.



Verifica della firma digitale su di un documento al quale era stata associata l'immagine (firma manoscritta).

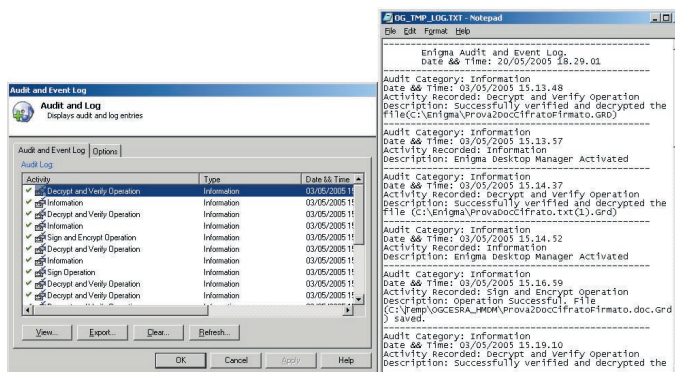
funzionalità di Firma o Crittazione, apparentemente a causa di qualche problema a livello di Gui. In un caso invece il problema riscontrato si è riprodotto costantemente: invocando l'operazione di Firma da Word 2000, giunti alla finestra della Legal Signing Ceremony, il pulsante View non mostra il documento che si sta firmando. Inoltre, se si decide di interrompere l'operazione attraverso il pulsante Cancel, il wizard non si chiude ma entra in uno stato inconsistente. Come prima l'impressione è che ci sia qualche piccolo errore nella gestione a livello di Gui. Nessun problema invece con PowerPoint ed Excel così come eseguendo l'operazione di firma del documento Word usando il Signer Wizard di Enigma anziché il menu di OfficeGuard integrato in Word. Infine, un'ultima nota, non particolarmente positiva, riguardo la funzionalità di Audit and Log. Le informazioni sono piuttosto scarse e la non ridimensionabilità delle finestre risulta particolarmente fastidiosa tanto da rendere diversi messaggi non interamente leggibili. Si può ricorrere al pulsante View, il quale semplicemente apre Notepad e mostra tutti i log in ordine sequenziale, non certo il meglio se si vogliono fare ricerche. Esiste anche il pulsante Export, di dubbia utilità visto che non fa nient'altro che salvare il file di testo contenente i log, operazione naturalmente disponibile da Notepad appena citato.

Conclusione

Il mercato dei prodotti centrati su tecnologie crittografiche e Pki sfrutta una delle più geniali intuizioni che non solo la crittografia ma probabilmente l'intera computer science abbia mai prodotto, gli algoritmi a chiave pubblica, e un'idea visionaria quanto affascinante, le Pki. Sono noti a tutti i grandi entusiasmi che queste tecnologie hanno suscitato pochi anni fa inseguendo l'obiettivo del documento elettronico che avrebbe reso obsoleta la carta e della firma digitale che rendeva la firma manoscritta un'anticaglia. L'applicazione pratica ha riportato tutti a una dura realtà nella quale le difficoltà e i problemi tecnologici prima sottovalutati si sono



La finestra di Legal Signing Ceremony con un messaggio formale di presa visione del documento firmato e lo spazio per eventuali altre comunicazioni.



Esempio di log di Enigma, dalla Gui in forma tabellare (a sinistra) e testuale (a destra).

rivelati in tutto il loro peso, gli errori strategici nella scelta delle applicazioni e nel rapporto tanto indispensabile quanto confuso con la controparte normativa e legale hanno sfianato decine di progettisti, l'inerzia della burocrazia e la oscura psicologia individuale degli utenti ha demolito i disegni più ambiziosi. È quasi imbarazzante sapere che una delle conseguenze della diffusione della firma digitale per l'accesso alle procedure e i servizi di alcune istituzioni pubbliche è stato quello di riempire i cassetti di molti commercialisti di centinaia di smartcard di loro clienti. Insomma, il settore nel quale Enigma Desktop si colloca non è dei più semplici e tuttora le difficoltà che questi sistemi hanno vissuto non sembrano essere finite. Occorrerebbe forse un ripensamento radicale di come queste tecnologie devono essere usate e proposte agli utenti privi di background tecnico, o forse qualcosa di ancor più radicale. Enigma Desktop non tenta nessuna strada innovativa ma svolge abbastanza bene il suo compito senza però brillare particolarmente. È positivo lo sforzo di integrazione di molte funzionalità, anche se talvolta la necessità di conformarsi a una

messe di legislazioni differenti tende a confondere gli utenti, soprattutto quelli italiani già alle prese con difficoltà di interpretazione delle normative nazionali. Più grave invece che in diversi aspetti sia apparsa un'attenzione insufficiente nei confronti degli utenti – la documentazione poco esplicita, alcuni difetti nella Gui anch'essa talvolta poco intuitiva per esempio – perché da più parti proprio l'interfacciamento con gli utenti è accusato di avere una parte rilevante nell'esito non felice delle Pki. I progettisti di un tool di questo genere dovrebbero, in mancanza di proposte innovative, essere maniacali nella cura di questi dettagli. Considerando il prezzo unitario da listino, l'offerta non sembra delle più economiche, anche se sui grandi volumi è ipotizzabile che gli sconti siano significativi. In definitiva quindi, pur senza impressionare particolarmente, è un tool onesto, per il quale è stato profuso uno sforzo rilevante sul lato delle normative ma che riprende un'impostazione già vista spesso nell'uso di queste tecnologie, la quale in passato non ha però riscosso il successo che si sperava. Rimaniamo in attesa di idee nuove capaci di dare nuovo slancio a questi sistemi. ●