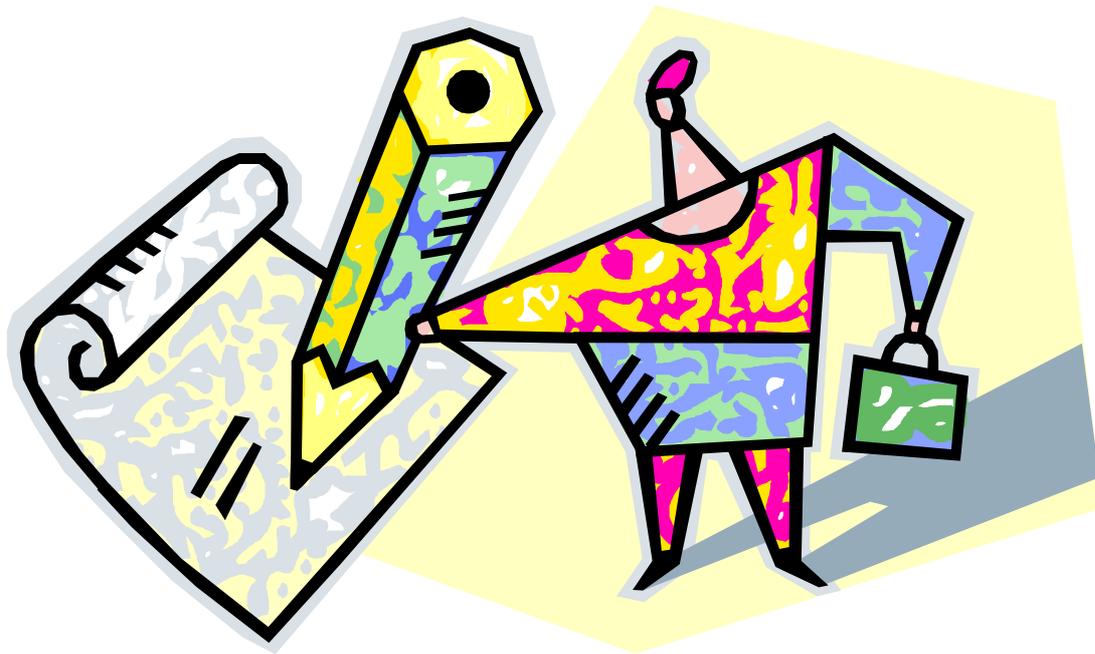


Guida Alla Firma Digitale



Per fare affari meglio e in sicurezza

partner data s.r.l.
Servizi e Prodotti Informatici

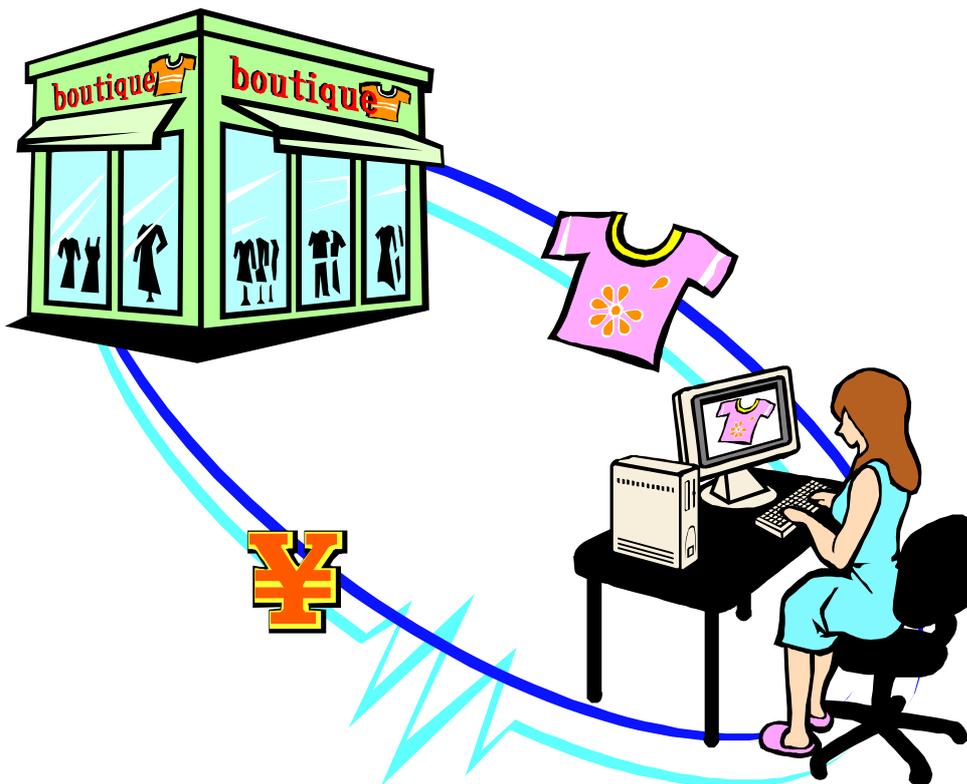
partner data – Via P. Marocco, 11- 20127 Milano - Tel 02.2614 7380-Fax 02.2682 1589
info@partnerdata.it – www.partnerdata.it

1 Introduzione

Internet sta offrendo a tutti noi nuove opportunità. Siamo ancora agli albori di questa era e ci sono possibilità ancora inesplorate o inutilizzate per incrementare e migliorare l'uso di questo mezzo.

Uno dei grandi vantaggi di Internet sta nel suo essere "un sistema aperto"; ma proprio questa peculiarità rappresenta la sua maggior debolezza. Noi non sappiamo mai con certezza con chi stiamo comunicando, chi sta dall'altra parte, dietro la sua tastiera, chi ci sta ordinando beni o servizi, mandando email o provvedendo ai pagamenti. Inoltre non sappiamo mai se le nostre email raggiungono le persone giuste e se non vengono modificate strada facendo.

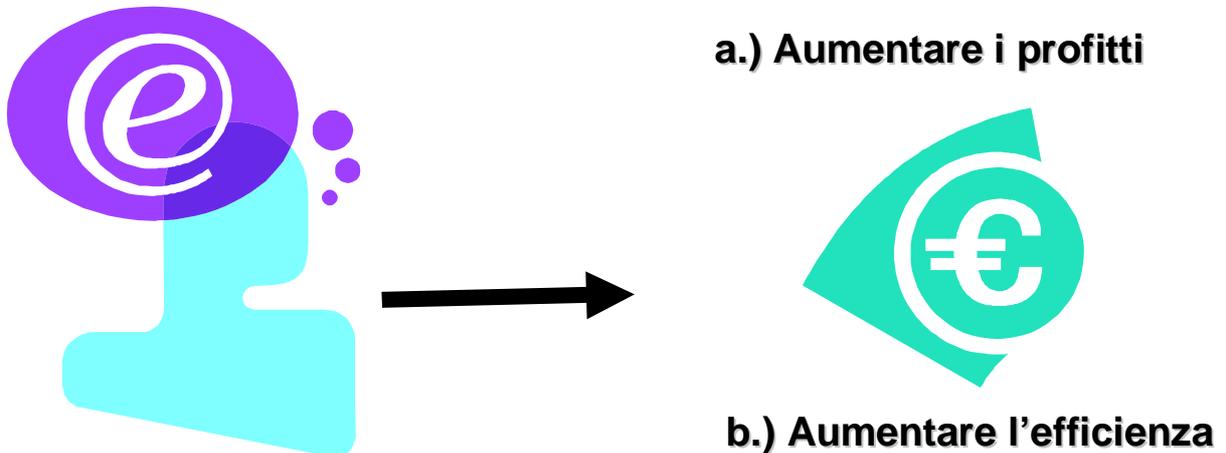
Malgrado tutto ciò l'era digitale ha introdotto nuovi convenienti modi di fare gli affari. Il cosiddetto eBusiness permette alle aziende di competere in un mercato mondiale fornendo loro un veloce ed illimitato accesso a prodotti ed informazioni.



Le aziende, ovunque nel mondo, sono in grado di usare il canale dell'eBusiness per raggiungere tanti clienti quanti prima era impensabile. Questo aumenta l'efficienza.

Le principali ragioni che portano le aziende ed i professionisti ad adottare l'eBusiness sono:

- aumentare i profitti aumentando il numero dei clienti, o
- aumentare l'efficienza e quindi ridurre i costi



Tuttavia, perché l'eBusiness possa crescere ai ritmi pronosticati, bisogna che la fiducia nella sicurezza delle informazioni digitali sia almeno non inferiore a quella data alle informazioni cartacee.

1.1 Perché serve questa guida?

Questa **Guida alla Firma Digitale** può essere utile perché il modo tradizionale di fare affari si basa su secoli di tradizione e noi abbiamo imparato come farlo e come affrontare i relativi rischi e cavilli legali. Per entrare nel mondo del commercio elettronico ci vogliono nuovi strumenti e diverse competenze. Ecco quindi la necessità della identificazione elettronica e della firma digitale per poter fare transazioni on-line più efficienti e contemporaneamente ridurre i rischi. Questa Guida risponde quindi alle seguenti domande:

- Perché serve l'identificazione elettronica e la firma digitale?
- Cosa sono l'identificazione elettronica e la firma digitale?
- Come si usano l'identificazione elettronica e la firma digitale?
- Quali sono gli aspetti legali, i rischi e le responsabilità insite nell'utilizzo della firma digitale?

1.2 Struttura della Guida

Questa Guida è strutturata in modo da renderne facile la lettura, chiarificando e semplificando i passi necessari ad assicurare un corretto uso dell'eBusiness, col fine di incoraggiare l'uso generalizzato della firma digitale da parte delle piccole e medie industrie (PMI) e dei professionisti.

Questi i capitoli della guida:

1 Introduzione

2 La fiducia nell'eBusiness

Questo capitolo spiega perché è necessario disporre di soluzioni sicure e degne di fiducia. Internet è un buon mezzo di comunicazione, ma la sua *apertura* può portare a scarsa fiducia nella sua sicurezza da parte degli utenti. Qui si evidenzia come la firma digitale giochi un ruolo importante nel fornire fiducia nelle transazioni on-line.

3 Identificazione e firma elettronica

Questo capitolo descrive le firme digitali e la loro funzione di identificazione. Si esamina la tecnologia impiegata ma ad un livello tale da permetterne la comprensione a non esperti. Si descrive la crittografia a chiave pubblica, una delle metodologie usate nelle firme elettroniche. Si vedrà il ruolo che assumono nella verifica elettronica dell'identità delle entità di certificazione normalmente note come Autorità di Certificazione (CA).

4 Validità legale della Firma Digitale

Il maggior dubbio negli affari è se alla firma digitale si debba dare lo stesso peso e livello di validità della tradizionale firma grafica. Qui si evidenzia come l'Italia per prima (e la maggior parte degli Stati membri della C.E. poi) ha promulgato leggi in proposito e quindi recepito la Direttiva comunitaria sulla Firma Elettronica. Queste leggi danno lo stesso livello di validità alla firma digitale ed a quella manuale.

5 Responsabilità e Rischi

L'affidabilità di una firma digitale dipende, in larga misura, dalla sicurezza dai codici usati per firmare. Questo capitolo enfatizza l'importanza di tenere la chiave privata in dispositivi sicuri per non comprometterne la validità. Anche si evidenziano i rischi nell'uso della firma digitale che possono scaturire da errori umani, per esempio nella fase di verifica. Si consiglia qui l'uso di alcuni accorgimenti per effettuare firme sicure, evitando alcuni noti rischi.

6 Esempi

Qui si presenta alle PMI come vengono normalmente usate le firme digitali nelle comunicazioni tra aziende ed organizzazioni governative (e-government), tra azienda e aziende ed all'interno della stessa azienda.

7 Appendici

Breve Glossario dei termini e riferimenti al contesto normativo italiano.

2 La fiducia è una necessità – come dare fiducia all'eBusiness

Malgrado il gran parlare di eBusiness è chiaro che il commercio elettronico è ancora poca cosa. E' comunemente accettato che una delle principali ragioni di ciò sia la mancanza di fiducia al mercato elettronico.

Per raggiungere il potenziale commerciale offerto da Internet, i consumatori devono sapere che i beni e servizi offerti sono descritti correttamente, che avranno quello per cui hanno pagato, e che se ciò non avviene potranno ricorrere con opportuni strumenti e garanzie. Dal momento che la fiducia è una delle maggiori aspettative degli utenti di Internet, il fornire un valido mezzo di autenticazione è un importante passo verso l'affidabilità delle transazioni online.

Prima dell'avvento di Internet tre erano i principali mezzi di comunicazione nelle transazioni commerciali:

- vis a vis, nei negozi e centri commerciali
- per posta/fax, grazie agli ordini tramite catalogo
- per telefono

Internet è il quarto mezzo. Questo nuovo mezzo ha alcuni notevoli vantaggi sui primi tre:

- Vendere on-line costa meno di ogni altro canale di vendita. E' questo il vantaggio più importante per il mondo degli affari, proteso alla riduzione dei costi ed al giusto profitto.
- E' molto più facile acquistare per i clienti anche in zone di difficile accesso. Permette infatti di trovare numerosi fornitori di prodotti simili, facilitando le scelte al compratore. Grazie a portali di *procurement* o ai cosiddetti *market place* il compratore ha rapidamente informazioni sui prodotti, sulle modalità di acquisizione, sui tempi di spedizione e trasporto.
- Il mercato si espande dalla dimensione nazionale a quella internazionale. In questa era elettronica le aziende possono muoversi rapidamente, attirare più clienti grazie alla pubblicità on-line, stringere accordi commerciali con partner di nazioni lontane.
- D'altro lato, dà modo ai compratori di scegliere accuratamente i migliori prodotti e servizi: e ciò grazie alla disponibilità di informazioni 24 ore al giorno e 365 giorni all'anno.



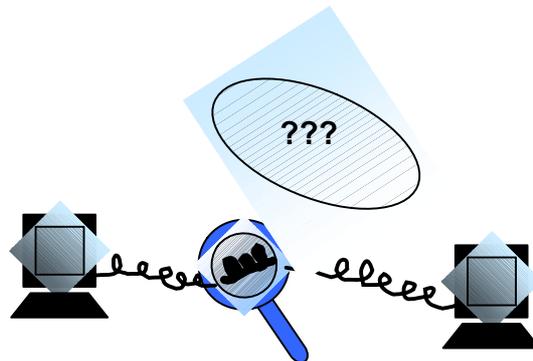
- Riduce i tempi morti tra gli investimenti ed gli introiti ottenuti da prodotti e servizi. Ciò migliora il servizio ai clienti e, unitamente a quanto riportato nei punti precedenti, facilita la concorrenza che a sua volta riduce i prezzi per i consumatori.

La domanda allora è come mai, stante tutti questi vantaggi, il commercio tramite Internet è ancora così relativamente limitato? E' accertato che perché l'eBusiness possa raggiungere le dimensioni pronosticate, deve esserci fiducia in questo nuovo modo di fare gli affari. Fiducia nell'eBusiness vuol dire credere che le persone e le organizzazioni coinvolte siano solide, affidabili, autentiche.

3 Identificazione e firma elettronica

Tre sono le funzioni insite in un processo di firma elettronica:

l'**identificazione**: indica con certezza chi è il mittente di un messaggio elettronico. In molte occasioni è indispensabile che le due parti in comunicazione conoscano la controparte remota. L'identificazione elettronica rende possibile identificare un utente, un cliente, un partner grazie a strumenti elettronici.



la **firma**: garantisce che il documento non è stato modificato dopo la sua sottoscrizione e gli dà uno status legale. E' importante che le informazioni siano originali, non modificate durante la trasmissione, accidentalmente o intenzionalmente. La firma elettronica permette al mittente di firmare il messaggio cosicché il destinatario possa sapere con certezza chi l'ha spedito e che l'informazione non è stata alterata. Ciò tra l'altro impedisce che il mittente possa in seguito disconoscere la paternità del documento (non-ripudiabilità).



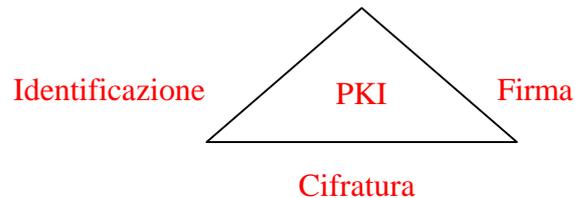
la **cifratura** (funzione facoltativa): viene usata per proteggere le informazioni da occhi diversi dal destinatario, sia quando vengono registrate che trasmesse. Il rendere informazioni riservate disponibili solo a un certo numero di ben definite persone è stato praticato per millenni. Gli imperatori romani proteggevano con cifratura i messaggi che inviavano o che venivano scambiati tra le truppe. Nel loro caso, il mezzo di trasporto era un corriere, che portava il messaggio scritto su una pergamena; e la cifratura consisteva nel famoso codice Romano, che sostituiva le lettere del messaggio con altre, precedentemente concordate. Oggi fortunatamente disponiamo di strumenti ben più sofisticati



Ci sono varie metodologie per realizzare queste 3 basilari funzioni. Qui ci soffermiamo su una di esse, in quanto la legge italiana e quella della C.E. e degli Stati Membri si basano su questa: **Public Key Infrastructure** (PKI-Infrastruttura a Chiave Pubblica)

Non è abituale che le legislazioni specifichino particolari metodologie o tecniche. Invece la legislazione europea e anche quella italiana sulla firma digitale prescrive la PKI, senza alternative.

PKI riguarda tutte e tre le funzioni base, identificazione, firma e cifratura.



PKI è sia una tecnologia che un procedimento metodologico.

La *tecnologia* si basa su 2 chiavi di cifratura, dette **chiave privata** e **chiave pubblica**, che vengono usate per le tre diverse funzioni. Un documento può essere cifrato con una delle due chiavi; se cifrato con la chiave pubblica potrà essere decifrato solo utilizzando la corrispondente chiave privata, e viceversa. La conoscenza di una chiave non permette di arrivare alla conoscenza dell'altra.

La *metodologia* definisce le regole di generazione, di utilizzo e di gestione delle chiavi. Ci sono infatti diversi modi di usare la PKI, con diverse conseguenze sui livelli di sicurezza.

3.1 Identità Elettronica (ID)

Un utente, perché possa firmare e quindi essere identificato deve avere una sua identità elettronica. Una identità elettronica, o ID, è composta, in ambiente **PKI**, da un certificato elettronico e dalle due chiavi di cifratura (pubblica e privata). Il certificato è un documento digitale, contenete tra l'altro i dati anagrafici dell'individuo, firmato dalla Autorità di Certificazione (**CA**) che è l'entità garante che assegna l'identità elettronica (certificati e chiavi).

Un ID può assumere diverse forme, dato che chiavi e certificati possono essere registrati in diversi supporti:

- Un file di dati (software)
- Una dispositivo hw (token)

Esempi di token sono le smartcard (in forma di carta di credito); le SIM card (i chip usati nei telefonini GSM), i token USB (le chiavette dotate di chip direttamente inseribili in una porta USB).

La legge Italiana e quella europea (**Direttive sulla Firma Elettronica**), impone di utilizzare dispositivi sicuri, cioè un token, per registrarvi l'ID atto a generare una firma digitale.

3.1.1. Come ottenere un ID

Il cittadino si deve recare presso un ente delegato da una Autorità di Certificazione (CA) per ottenere il suo dispositivo di firma; la CA si accerta della identità del richiedente e quindi rilascia il dispositivo, personalizzato con il suo certificato e chiavi. Per esempio le Camere di Commercio rilasciano il certificato emesso da Infocamere; l'elenco delle CA italiane qualificate si trova nel sito dell'AIPA (Autorità per l'Informatica nella Pubblica Amministrazione): <http://www.aipa.it>

Si possono anche ottenere ID via Internet, da certificatori non qualificati.

3.1.2. Come usare e preservare la propria ID

L'uso dell'ID è sempre protetto da una password personale che solo voi conoscete. Ciò garantisce che non possa essere usato da altri. La password è nota come **PIN (Personal Identification Code)**, e può essere sostituita da identificazioni biometriche, come l'impronta digitale.

E' anche possibile bloccare l'ID, analogamente a quanto oggi si fa con una carta di credito persa o rubata. Bisognerà per questo notificare a chi l'ha rilasciato l'ordine di inibirne l'uso.

3.1.3. Carta di Identità Elettronica (CIE) / Carta Nazionale dei Servizi (CNS)

La ID può essere inserita nella carta d'identità elettronica o nella carta nazionale dei servizi, quando questi documenti saranno disponibili. Questo è un eccellente modo di unificare due funzioni ed esemplifica l'importanza di maneggiare con cura il vostro documento d'identità. Noi sappiamo come aver cura della nostra carta di identità o del nostro passaporto, e la stessa attenzione dovremo riservarlo alla nostra ID card, per evitare che cada in mani sbagliate.



3.2 Come si usa la ID? Come si fa a firmare?

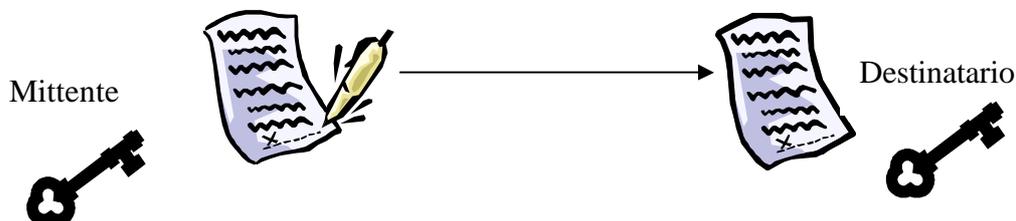
Per la firma e l'identificazione elettronica ci si avvale di programmi applicativi e di servizi prestati dalla Autorità di Certificazione. Queste sono le fasi da eseguire:

- attivare il programma atto a firmare il documento da voi già realizzato
- selezionare il documento da firmare
- inserire il dispositivo di firma (smartcard) nell'apposito lettore
- firmare il documento attivando la relativa procedura, avendo precedentemente inserito il vostro PIN
- inviare il documento firmato
- il destinatario provvederà a verificare la validità sia del documento tramite un opportuno programma sia del vostro certificato tramite la CA.

Di seguito spieghiamo come funziona la procedura.

3.2.1. Uso della chiave privata

Il programma di firma, per firmare un documento, esegue per prima cosa la funzione di hash, cioè, tramite un apposito algoritmo, ottiene dal documento stesso un codice univoco detto impronta o hash: una seppur minima modifica del documento produrrebbe un'impronta completamente diversa e non è possibile il processo inverso, cioè dall'impronta risalire al documento che l'ha originato. Il programma di firma a questo punto cifra con la chiave privata del firmatario il codice impronta ottenuto: questa è la firma digitale del documento. Nel documento spedito al destinatario verrà quindi inclusa la firma ed il certificato del mittente, che comprende la sua chiave pubblica.



Analogamente ad una firma autografa manuale, la firma digitale è univoca, non può non appartenere al firmatario, essendo prodotta dal suo codice privato, che solo lui può usare. Anche se prodotto dalla stessa chiave privata, ogni firma digitale è diversa, perché deriva da un'impronta diversa, ottenuta dal processo di calcolo (hash) effettuato sul singolo documento.

3.2.2. Uso della chiave pubblica

Il destinatario del documento firmato riceve insieme al documento stesso la sua firma ed il certificato del mittente con la sua chiave pubblica; il programma di verifica ricalcola l'impronta del documento, confronta quella calcolata con quella ricevuta, decifrata con la chiave pubblica del mittente: se sono uguali il documento è convalidato.

3.2.3. Verifica dell'ID del mittente

Durante la fase descritta sopra, effettuata durante un collegamento Internet, l'applicazione si connette automaticamente alla CA e verifica che il certificato del mittente non sia scaduto, revocato, bloccato.

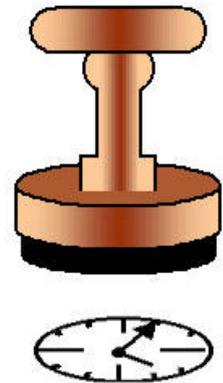
3.2.4. Cifratura

Una firma digitale non procura riservatezza ad un documento se il documento stesso è in chiaro. Per ottenere ciò, il mittente dovrà, dopo aver apposto la firma, cifrare il messaggio prima della sua spedizione, utilizzando la chiave pubblica del destinatario; solo quest'ultimo potrà decifrare il documento perché solo lui può disporre della chiave privata adatta ad *aprire* il documento solo a lui destinato.

3.2.5. Marca Temporale

Un'altro dei fattori che fanno sicura ed affidabile la firma digitale è la marca temporale. Una marca temporale digitale associa ora e data ad un documento elettronico. Nell'ambiente digitale è importante assegnare una data certa ad un documento per mostrare quando è stato scritto e firmato (pensate ad esempio la partecipazione a gare e concorsi).

La marca temporale convalida il documento, anche certificando che l'ID del suo firmatario era valido al momento della firma.



L'uso della marca temporale non tocca il contenuto del documento né modifica la sua firma.

4 Validità legale della firma digitale in Italia

L'Italia, insieme alla Germania, è stata la prima nazione a dotarsi di una legge relativa alla firma digitale (vedere in appendice i riferimenti normativi), prima che la C.E. promulgasse le sue raccomandazioni in proposito.

Il legislatore ha quindi dovuto in un secondo tempo recepire le norme europee e ciò ha creato alcuni problemi di interpretazione che nuove norme di prossima pubblicazione dovrebbero chiarire.

Oggi infatti hanno valore legale sia le *firme digitali avanzate* o *qualificate* o *forti*, come dalla legge iniziale, sia le *firme elettroniche*, come previste dalle direttive europee.

La differenza principale risiede nel fatto che le firme forti si basano su *certificati qualificati* rilasciati da Certificatori accreditati, quelli per intenderci elencati nella lista AIPA di cui al punto 3.1.1; inoltre sono generate solo da dispositivi sicuri, quali le smartcard, e non ad esempio da chiavi private salvate in un file su disco del PC.

Un documento che riporti una firma forte è equiparabile ad un documento cartaceo con firma certificata da notaio o pubblico ufficiale.

Il DPR 445/00 del 28/12/2000 afferma infatti: "il documento informatico, quando è sottoscritto con firma digitale o con altro tipo di firma elettronica avanzata, e la firma è basata su di un certificato qualificato ed è generata mediante un dispositivo per la creazione della firma sicura, **fa piena prova fino a querela di falso della provenienza delle dichiarazioni da chi l'ha sottoscritto**".

Il documento firmato con semplice *firma elettronica* ha pur sempre in giudizio lo stesso valore di una scrittura redatta e sottoscritta sul foglio cartaceo. Non ci addentriamo in ulteriori dettagli anche perchè si attendono a breve decreti chiarificatori.

5 Rischi e responsabilità

5.1 Rischi

L'attendibilità di una firma digitale è basilare e dipende da vari fattori:

- La certezza dell'identità, verificata dalla CA all'atto della concessione dell'ID
- La generazione della chiave privata e la sua gestione; per avere una ID *qualificata* la chiave privata deve essere generata all'interno del dispositivo sicuro (smartcard) e da lì non deve poter uscire né essere accessibile da alcuno.
- La riservatezza del PIN, in modo che l'ID possa essere utilizzato solo dal suo proprietario.
- La verifica dell'ID, della firma, della sua data, da parte del destinatario di un messaggio firmato

5.2 Responsabilità

Ogni attore nel processo di firma ha le sue specifiche responsabilità per garantire la sicurezza dell'intera operazione.



5.2.1. Responsabilità e compiti del firmatario

I sottoscrittori di firme digitali devono avere molta cura della loro ID e della loro chiave privata per evitare che possano essere utilizzate abusivamente, se cadute in mani sbagliate.

Uno dei problemi più comuni in questa nostra era digitale è quello del ladro di identità.

Per questo la chiave privata, per la legge italiana, nasce nel dispositivo sicuro e da lì non esce. Ma tutto è inutile se vi carpiscono il PIN di accesso. Alcuni consigli sul come gestire il proprio PIN:

- attenzione quando digitate il PIN, che nessuno vi guardi;
- cambiate spesso il PIN;
- non tenetelo scritto in foglietti vicini al dispositivo di firma;
- non usate la data di nascita, il nome del figlio, ecc.. ma codici non facilmente riportabili a voi;
- installate nel vostro PC validi antivirus, sempre aggiornati, per evitare che i dati digitati possano venir intercettati da eventuali hacker.

Se pensate che il vostro ID è compromesso, se la vostra smartcard è stata persa o sottratta, è responsabilità vostra revocare l'ID, comunicandolo immediatamente alla CA, che generalmente accetta comunicazioni 24 ore su 24.

Un altro rischio è insito nel documento che andate a firmare: documenti prodotti da applicazioni quali ad esempio Word o Excel possono contenere le cosiddette *macro* che in realtà sono dei programmi che potrebbero in un secondo tempo modificare quanto apparentemente avete firmato, e ciò senza invalidare la firma.

E' quindi bene firmare documenti redatti con programmi che non prevedano l'uso di macro linguaggi, come ad esempio i formati testo (.TXT).

E' bene chiarire un ulteriore punto non sempre noto: l'uso di certificati di firma rilasciati da un certo certificatore non è limitato al suo ambito di competenza ma ha valore legale generale come descritto al punto 4.

Per esemplificare: la smartcard ricevuta gratuitamente dalla Camera di Commercio, spesso affidata al commercialista, non serve solo per firmare documenti destinati al Registro delle Imprese ma per firmare qualsiasi documento a chiunque diretto, mantenendo ovviamente la sua validità legale completa. Analogamente un ID rilasciato da un istituto bancario non serve solo per firmare documenti ad esso diretti od entrare nel suo sito protetto: è un documento di identità elettronica di uso generale. Conclusione: mantenete in luoghi sicuri i vostri dispositivi di firma e il relativo PIN.

5.2.2. Responsabilità e compiti del destinatario

Il programma che *apre* un documento firmato ne verifica la sua validità (integrità) e verifica inoltre che il certificato del firmatario non sia scaduto (per legge non può durare più di due anni); è necessario però anche verificare la validità dell'ID del firmatario, collegandosi alla CA che ha emesso l'ID o scaricandone le liste di revoca: il certificato potrebbe essere stato bloccato (perché smarrito) o revocato.

5.2.3. Responsabilità e compiti del certificatore (CA)

I compiti dell'Autorità di Certificazione sono:

- Il processo di assegnazione dell'ID
- Il servizio di revoca
- Il servizio di validazione

La CA deve assicurarsi della reale identità del soggetto a cui rilascia un ID. I certificatori, per poter rilasciare *certificati qualificati* devono essere accreditati a ciò; come già detto sono elencati nel sito AIPA.

La CA potrà revocare o sospendere la ID di un soggetto, senza chiederne il suo consenso se:

- Un dato riportato nel certificato risulta falso
- Un prerequisito al rilascio dell'ID è stato disatteso
- La chiave privata dell'ID è stata in qualche modo compromessa, inficiando l'affidabilità dell'ID

La CA deve mantenere le liste di revoca pubbliche e sempre disponibili ai cittadini. Questa è l'importante funzione di validazione attuata dalla CA.

La CA stessa, od altre organizzazioni a questo preposte, dovranno fornire la marca temporale, qualora richiesta dal firmatario. Anche il servizio di fornitura della marca temporale contribuisce alla sicura validazione del documento da parte della CA.

6 Alcuni esempi d'uso della firma digitale

6.1 Per il singolo cittadino

6.1.1. Email sicure

Oggi chiunque può leggere ed anche modificare il testo di una vostra email. Spesso ci si chiede se è sufficientemente sicuro inviare informazioni confidenziali in Internet (per esempio i codici delle carte di credito preferiamo inviarli via fax). E siamo sicuri che arrivino alla persona giusta? E che non vengano modificate strada facendo?

Le email possono essere protette dalla firma digitale ed eventualmente dalla cifratura del testo.

6.1.2. Uso sicuro di Internet

Spesso dobbiamo usare nome e password per entrare in certi siti. Avete mai pensato che altri potrebbero registrarsi usando i vostri dati, lasciando credere che siate voi? Che altri possano usare il vostro nome e la vostra password? L'utilizzo del vostro ID, rilasciato da una CA, vi identifica con sicurezza per entrare in siti particolarmente riservati, quale ad esempio il vostro conto bancario.

6.1.3. Pagamenti sicuri

Il fornire, via internet, dati relativi a conti correnti, carte di credito, ecc. presenta evidenti rischi. Perché fornire tutte queste informazioni ogni volta che facciamo un acquisto? Sarebbe molto meglio fornire una tantum le coordinate di pagamento e poi farsi riconoscere dal fornitore grazie a comunicazioni firmate digitalmente, che gli garantiscono l'identità del cliente e la non ripudiabilità dell'ordine da parte dello stesso.

6.2 Per le aziende

6.2.1. Email e comunicazioni sicure

Quante email escono dalla vostra azienda giornalmente, spedite da voi e dai vostri colleghi? Siete sicuri che le informazioni scambiate non arrivino sul tavolo di concorrenti poco scrupolosi? Le email firmate possono essere cifrate, leggibili quindi solo dal giusto destinatario.

6.2.2. Accesso sicuro ai sistemi informativi

Normalmente usiamo nome e password per accedere ai vari moduli dei nostri sistemi informativi aziendali, locali o remoti che siano. Volete controllarne l'accesso? Volete sapere chi ha utilizzato certi programmi? E' un collaboratore autorizzato o qualche altro? E' un'azienda partner o un concorrente? Vi serve una identificazione elettronica se volete controllare l'accesso alle informazioni aziendali, selezionandolo secondo livelli di autorizzazione.

6.2.3. Commercio elettronico e pagamenti sicuri

Troppo spesso non siamo sicuri dell'identità di un cliente. Spediamo merce, iniziamo processi di produzione basandoci su ordini ricevuti elettronicamente (e i fax non sono più sicuri). Ma l'ordine è reale? Ce lo pagheranno? Non verrà disconosciuto? Un ordine firmato digitalmente non è stato modificato da alcuno, è sicuramente di quel cliente che non potrà in alcun modo ripudiarlo.

6.3 Per la pubblica amministrazione

6.3.1. Servizio al pubblico

Obiettivo di ogni amministrazione pubblica è quello di migliorare il servizio ai suoi utenti. Oggi molte di esse rendono disponibili in Internet alcune notizie utili ai cittadini; ma ci sono moltissime altre informazioni e moltissimi servizi non ancora disponibili.

E' inoltre importante in molti servizi pubblici che le informazioni raggiungano solo le persone giuste e non altri; pensate ai servizi sociali e sanitari, per esempio. La firma digitale e relativa identificazione elettronica rispondono a queste esigenze, sempre più sentite delle pubbliche amministrazioni.

6.3.2. Offerte/Acquisti

Partecipare a gare pubbliche è un tipico esempio dei benefici che la firma digitale può dare alle aziende. Le offerte a contratti governativi sono state sempre fatte manualmente; con l'introduzione delle gare elettroniche i tempi si riducono drasticamente, sia nella fase di offerta che in quelle successive di contrattazione e di ordine. Ovviamente la sicurezza nella individuazione degli offerenti, nella non modificabilità dei documenti e nella loro non ripudiabilità, nella riservatezza degli stessi sono caratteristiche indispensabili e che solo la firma digitale rende attuabili.

6.4 Casi Reali

6.4.1. Registro Delle Imprese

Il 9 dicembre 2002 è entrato in vigore l'art. 31 secondo comma, della legge n. 340/2000 che, in poche righe, introduce una vera e propria rivoluzione e un nuovo modo di concepire, organizzare e gestire documenti informatici con piena validità legale. Le imprese, le associazioni di categoria, i professionisti, devono utilizzare la firma digitale come unico strumento per "comporre la pratica societaria" da inviare all'ufficio del Registro delle Imprese tenuto presso le Camere di Commercio.

Le Camere di Commercio su indicazione del Ministero delle Attività Produttive distribuiscono gratuitamente a tutte le società una smart card contenente l'ID del suo rappresentante legale, avvalendosi dei servizi di InfoCamere, la loro società di informatica. La smart card può essere ritirata presso gli uffici delle Camere di Commercio o presso i soggetti autorizzati dalle stesse Camere di Commercio o dal certificatore.

6.4.2. Procedure telematiche di acquisto per l'approvvigionamento di beni e servizi da parte di amministrazioni pubbliche

Il DPR 4 Aprile 2002 definisce le regole per le amministrazioni pubbliche per bandire gare ed effettuare acquisti telematici di beni e servizi. Ovviamente il regolamento prevede l'uso della firma digitale. Nel sito www.acquistinretepa.it sono elencate le gare aperte, quelle aggiudicate, i regolamenti di partecipazione e quant'altro.

6.4.3. Home Banking

Molte banche, per rendere disponibili ai propri clienti l'accesso a servizi remoti, consegnano agli stessi ID in smartcard o dischetti, necessari per entrare nella banca online. Alcune banche o gruppi bancari appaiono tra i certificatori accreditati, presenti nella lista AIPA.

6.4.4. Email sicure

E' ormai pratica corrente scambiare documenti cifrati e firmati tra diverse aziende o tra diversi operatori nell'ambito della stessa azienda.

Gli usuali prodotti disponibili nel mercato permettono oggi di firmare e cifrare email e allegati, utilizzando dispositivi di firma digitale forte o di firme elettroniche. Inoltre sono disponibili, spesso gratuitamente, applicazioni di firma digitale distribuite da alcune CA od acquistabili per pochi euro in Internet o presso i negozi specializzati.

Esistono anche programmi più completi che per esempio filtrano tutte le email che passano attraverso un server di posta aziendale, eventualmente respingendo email non firmate ed automaticamente cifrando e decifrando quelle destinate a certi indirizzi.

7 Appendici

7.1 Breve glossario di termini

Certificato / Certificato digitale

Garantisce l'identità di un firmatario. Contiene oltre ai dati anagrafici la sua chiave pubblica, la scadenza del certificato stesso ed a volte i limiti d'uso. Inoltre identifica l'Autorità di Certificazione che l'ha rilasciato e include la firma digitale della CA.

Chiave

Codici alfanumerici usati per cifrare e decifrare messaggi secondo certi algoritmi i più noti dei quali sono il DES o Triplo DES per la *cifratura simmetrica* ed RSA per quella *asimmetrica* (vedere più sotto).

Chiave pubblica

In una PKI è la chiave che viene resa pubblica (pubblicata dalla CA, allegata nel certificato che accompagna un documento firmato): viene usata per verificare la firma e per cifrare un messaggio (utilizzando quella del destinatario).

Chiave privata

Sta in modalità sicura nel dispositivo di firma; viene generate dal dispositivo stesso e nessuno la conosce; solo il suo proprietario può usarla per firmare i documenti.

Cifratura asimmetrica

Il messaggio viene cifrato con una chiave e decifrato con un'altra (e viceversa). Una delle due chiavi verrà definita privata, il cui uso è riservato al proprietario, e l'altra pubblica, nota a tutti. Metodologia nota anche come cifratura a chiave pubblica.

Cifratura simmetrica

Il procedimento che rende incomprensibile un messaggio ad una terza parte e dove le parti autorizzate usano la stessa chiave, precedentemente concordata, per cifrare e decifrare il messaggio.

Gestione delle chiavi

E' il processo che assicura che le chiavi utilizzate nelle fasi di autorizzazione ed autenticazione siano maneggiate in modo sicuro, secondo regole ben definite. Comprende le attività di generazione, distribuzione, certificazione, archiviazione e distruzione delle chiavi stesse. E' il compito affidato alle Autorità di Certificazione (CA).

Integrità

E' la qualità del documento che garantisce che sia:

- originale, non modificato, ne accidentalmente ne artatamente
- completo.

Marcatura Temporale

E' un file firmato dal certificatore ed allegato al documento originale che testimonia, con la garanzia data dal certificatore stesso, il momento in cui è stata apposta la firma.

Non-ripudiabilità

E' la garanzia che il mittente di un messaggio non possa in seguito disconoscerlo, completamente o parzialmente. Un messaggio firmato non può essere ripudiato dal suo firmatario; un messaggio arrivato, firmato dal destinatario e rispedito al mittente garantisce la ricezione del destinatario e da questi non potrà essere disconosciuto.

Public Key Infrastructure (PKI)

E' questo il complesso di programmi, procedure e servizi necessari per attivare un sistema di cifratura asimmetrica, firma digitale, certificati digitali in applicazioni di rete.

Procurement

Si intende il processo (solitamente elettronico) tramite il quale una organizzazione, generalmente pubblica, invita fornitori a offrire beni o servizi secondo certe condizioni.

7.2 Il contesto normativo italiano

- Decreto del Presidente della Repubblica **10 novembre 1997, n. 513** - Regolamento contenente i criteri e le modalità di applicazione dell'articolo 15, comma 2, della legge 15 marzo 1997, n. 59, in materia di formazione, archiviazione e trasmissione di documenti con strumenti informatici e telematici
- Decreto del Presidente del Consiglio dei Ministri **8 febbraio 1999** - Regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici ai sensi dell'articolo 3, comma 1, del Decreto del Presidente della Repubblica, 10 novembre 1997, n. 513
- Decreto del Presidente della Repubblica **28 dicembre 2000, n. 445** - Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa
- Circolare del **16 febbraio 2001**, n. AIPA/CR/27 - Art. 17 del decreto del Presidente della Repubblica 10 novembre 1997, n. 513: utilizzo della firma digitale nelle Pubbliche Amministrazioni
- Decreto legislativo **23 gennaio 2002, n. 10** - Attuazione della direttiva 1999/93/CE relativa ad un quadro comunitario per le firme elettroniche

8 Indice

1. Introduzione
 - 1.1. Perché questa guida
 - 1.2. struttura della guida
2. La fiducia nell'eBusiness
3. Identificazione e firma elettronica
 - 3.1. Identità elettronica
 - 3.2. Come si usa l?D? Come si fa a firmare?
 - 3.2.1. Uso della chiave privata
 - 3.2.2. Uso della chiave pubblica
 - 3.2.3. Verifica dell'ID del mittente
 - 3.2.4. Cifratura
 - 3.2.5. Marca temporale
4. Validità legale della firma digitale in Italia
5. Rischi e Responsabilità
 - 5.1. Rischi
 - 5.2. Responsabilità
 - 5.2.1. Rischi e compiti del firmatario
 - 5.2.2. Rischi e compiti del destinatario
 - 5.2.3. Rischi e compiti del certificatore
6. Alcuni esempi d'uso della firma digitale
 - 6.1. Per il singolo cittadino
 - 6.1.1. Email sicure
 - 6.1.2. Uso sicuro di Internet
 - 6.1.3. Pagamenti sicuri
 - 6.2. Per le aziende
 - 6.2.1. Email e comunicazioni sicure
 - 6.2.2. Accesso sicuro ai sistemi informativi
 - 6.2.3. Commercio elettronico e pagamenti sicuri
 - 6.3. Per la pubblica amministrazione
 - 6.3.1. Servizio al pubblico
 - 6.3.2. Offerte / Acquisti
 - 6.4. Casi reali
 - 6.4.1. Registro delle imprese
 - 6.4.2. Procedure telematiche di acquisto per l'approvvigionamento di beni e servizi da parte di amministrazioni pubbliche
 - 6.4.3. Home banking
 - 6.4.4. Email sicure
7. Appendici
 - 7.1. Breve glossario dei termini
 - 7.2. Il contesto normativo italiano

Ringraziamenti a Dr. Rita Esen e May-Lis Farnes del CEN (The European Committee for Standardization): partendo da una bozza da loro prodotta, liberamente tradotta, abbiamo realizzato la presente guida integrandola di riferimenti alla realtà italiana.