



IMPRESA X INNOVAZIONE

La firma digitale:

un nuovo paradigma per aumentare la fiducia
e la sicurezza del business

Questa guida è stata realizzata
grazie al contributo di Eds Italia.

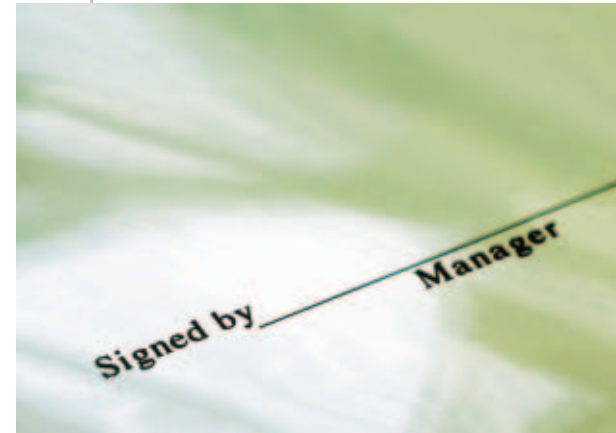
Le guide di questa collana
sono supervisionate da un gruppo di esperti
di imprese e associazioni del sistema Confindustria,
partner del Progetto Ixl:
Between Spa, Confindustria Servizi Innovativi, Gruppo Spee,
Hewlett Packard Italiana, Ibm Italia, Idc Italia,
Microsoft, Telecom Italia.

Suggerimenti per migliorare l'utilità
di queste guide e per indicare altri argomenti
da approfondire sono più che benvenuti:
toolkit@confindustria.it





LA FIRMA DIGITALE: un nuovo paradigma per aumentare la fiducia e la sicurezza del business



CHE COS'È LA FIRMA DIGITALE

La firma digitale è il risultato di una procedura informatica, che consente al sottoscrittore di rendere manifesta l'autenticità del documento informatico e al destinatario di verificarne la provenienza e l'integrità. La firma elettronica non deve essere confusa con la digitalizzazione della firma autografa, con la rappresentazione grafica dell'immagine della propria firma. Questo è il risultato di un procedimento di calcolo che, a partire da un oggetto che tipicamente è un documento e da informazioni associate ad una persona (coppia di chiavi asimmetriche), produce un nuovo oggetto, il documento firmato. Il documento firmato digitalmente ha lo stesso valore legale di un documento con

firma autografa. Il documento firmato digitalmente offre il vantaggio di non poter essere manomesso in alcun modo.

Documento e firma sono un tutt'uno, un unico archivio inscindibile. Il primo aspetto da considerare, il primo vantaggio della firma elettronica, è che nessuna parte del documento firmato può essere variata, manomessa, integrata, nemmeno in minima parte, pena l'invalidazione della firma. Non è necessario firmare tutte le pagine di un documento, per tutelarsi da sostituzioni, ma è sufficiente firmare il documento nella sua interezza.

La firma digitale è un sistema che consente:

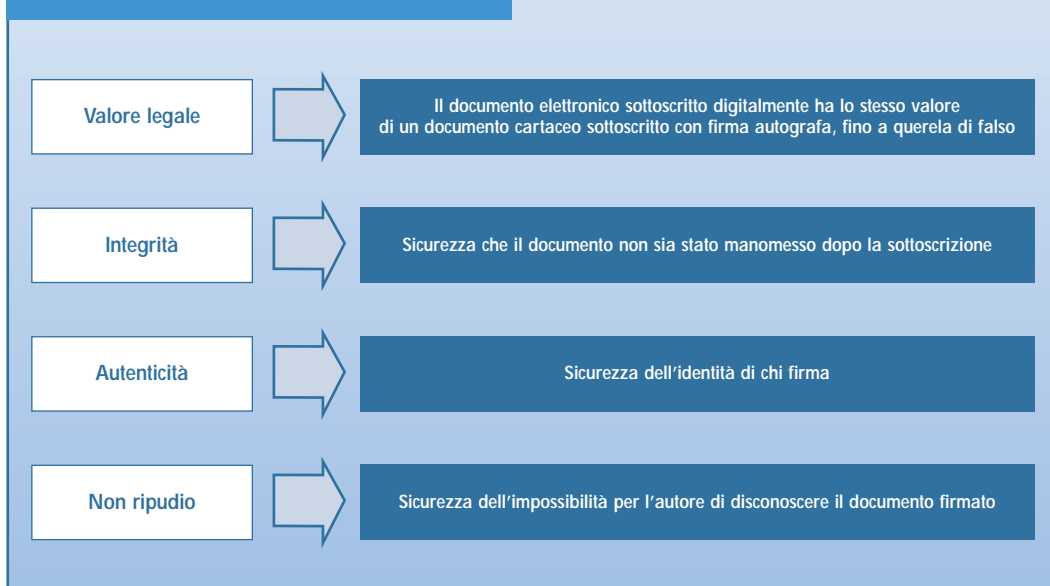
- all'autore di un documento informatico di renderne manifesta l'autenticità, analogamente a quanto avviene apponendo la firma autografa su un documento cartaceo;
- al destinatario del documento di verificarne la provenienza e l'integrità.

Così intesa la firma digitale diventa l'equivalente elettronico di una tradizionale firma apposta su carta, assumendone lo stesso valore legale.

In sostanza, la normativa vigente definisce la Firma Digitale come la possibilità, prevista e regolata dal punto di vista sia giuridico che tecnologico, di fare proprio, cioè di firmare legalmente, un documento informatico.



FIGURA 1 - LE CARATTERISCHE DELLA FIRMA DIGITALE



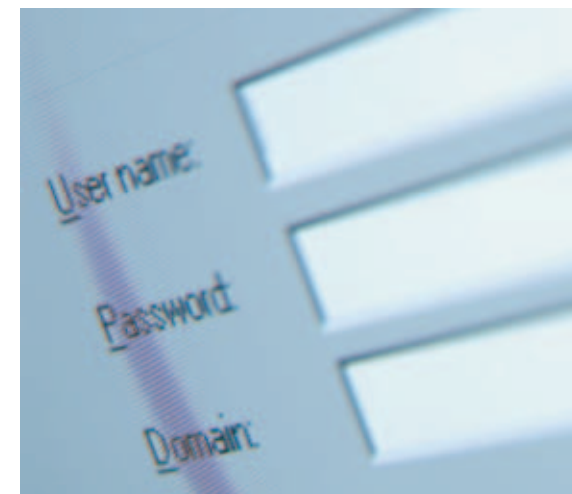
Le caratteristiche fondamentali della firma digitale sono elencate nella figura 1.

Tre sono dunque 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. È importante che le informazioni siano originali, non modificate durante la trasmissione, accidentalmente o intenzional-

mente. 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 lo-



greta, può decifrare il testo riportandolo alla forma originaria.

L'inconveniente di tali sistemi è che si basano su un'unica chiave, per cui è sufficiente che qualcuno la scopra per decifrare il messaggio, ed eventualmente anche alterarlo e cifrarlo di nuovo, senza che il destinatario se ne accorga. Inoltre, nel caso di documenti che vanno trasmessi a più destinatari, la chiave segreta deve essere portata a conoscenza di tutti, compromettendone la

ro 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.

La ricerca di un sistema che consentisse di "firmare", in maniera sicura, i documenti elettronici ha trovato una risposta nei sistemi di "crittografia", nati in origine per rendere un testo comprensibile solo al destinatario. I sistemi di crittografia tradizionali si basano su una chiave segreta: un algoritmo che trasforma i caratteri del testo in altri caratteri non comprensibili (testo "cifrato"). In base a tali sistemi il destinatario, utilizzando la medesima chiave se-





sicurezza al crescere del numero di soggetti che ne vengono a conoscenza (a meno che non si crei una chiave diversa per ogni coppia di interlocutori!).

Altri sistemi di crittografia più “evoluti” consentono di superare tali problemi, essendo basati su una coppia di chiavi asimmetriche, cioè una coppia di chiavi aventi, tra le altre, due caratteristiche:

- un documento cifrato dalla prima chiave della coppia può essere decifrato esclusivamente utilizzando la seconda;
- la conoscenza di una delle due chiavi non concede alcuna informazione utile alla ricostruzione dell'altra.

Le peculiarità della crittografia basata su chiavi asimmetriche sono state sfruttate per creare i sistemi di firma digitale, nei quali le due chia-

vi sono attribuite univocamente a un titolare:

- **la chiave privata** è a disposizione esclusiva del titolare, custodita all'interno di una “Smart Card” (supporto informatico da collegare al PC) e protetta da un codice segreto conosciuto solo da lui;
- **la chiave pubblica**, anch'essa associata al titolare, è invece contenuta in un “Certificato Digitale” (documento informatico) reso accessibile a tutti su Internet da particolari soggetti - i Certificatori Accreditati.

CARATTERISTICHE E VANTAGGI

Nella figura 2 si riportano le principali caratteristiche della firma digitale e le differenze rispetto alla tradizionale firma autografa apposta su documento cartaceo.

FIGURA 2 - DIFFERENZE TRA FIRMA AUTOGRAFA E FIRMA DIGITALE

Documento cartaceo con firma autografa	Documento informatico con firma digitale
La provenienza è garantita dalla firma autografa	La provenienza e l'integrità sono garantite dalla firma digitale
L'integrità è garantita dal supporto cartaceo (assenza di cancellazioni o abrasioni)	Ha valore solo fino alla scadenza del certificato della chiave pubblica (a meno che non si utilizzi una marca temporale o altro accorgimento idoneo)
Vale per tutta la vita del supporto cartaceo	Non esiste il concetto di copia: il documento informatico (“file”) con firma digitale è sempre un originale e può essere duplicato in un numero indefinito di file indistinguibili gli uni dagli altri
Il documento originale è sempre distinto dalla copia	

Le caratteristiche della firma digitale garantiscono al documento su cui è apposta:

- certezza di autenticità (provenienza dal firmatario) e integrità (assenza di alterazioni dopo la sottoscrizione);
- pieno valore legale – ha lo stesso valore legale di un documento cartaceo con firma autografa.

Inoltre, il suo utilizzo consente:

- eliminazione di documenti cartacei – grazie all'archiviazione su supporti informatici, anche dei documenti firmati da conservare in originale;
- tempestività - rende possibile la stipulazione, giuridicamente vincolante, di rapporti contrattuali anche a grandi distanze, senza necessità di spostamenti di persone o di spedizioni di materiale;

- eliminazione di timbri e simili – nei casi in cui hanno valore di firma, integra e sostituisce l'apposizione di sigilli, punzoni, timbri, contrassegni e marchi di qualsiasi genere.

COME FUNZIONA LA PROCEDURA

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'im-



pronta 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.

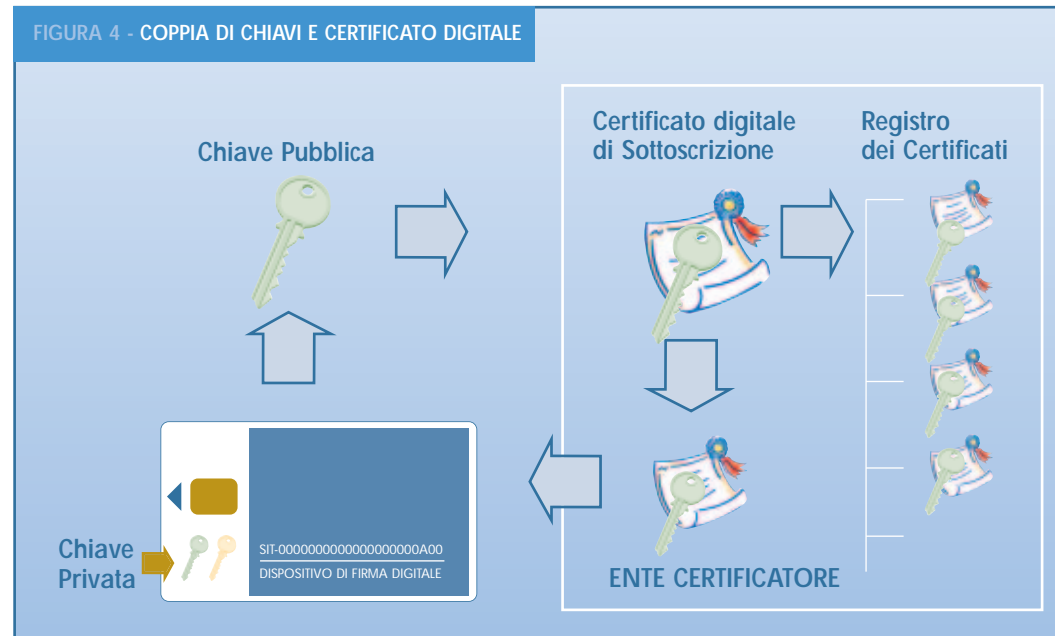
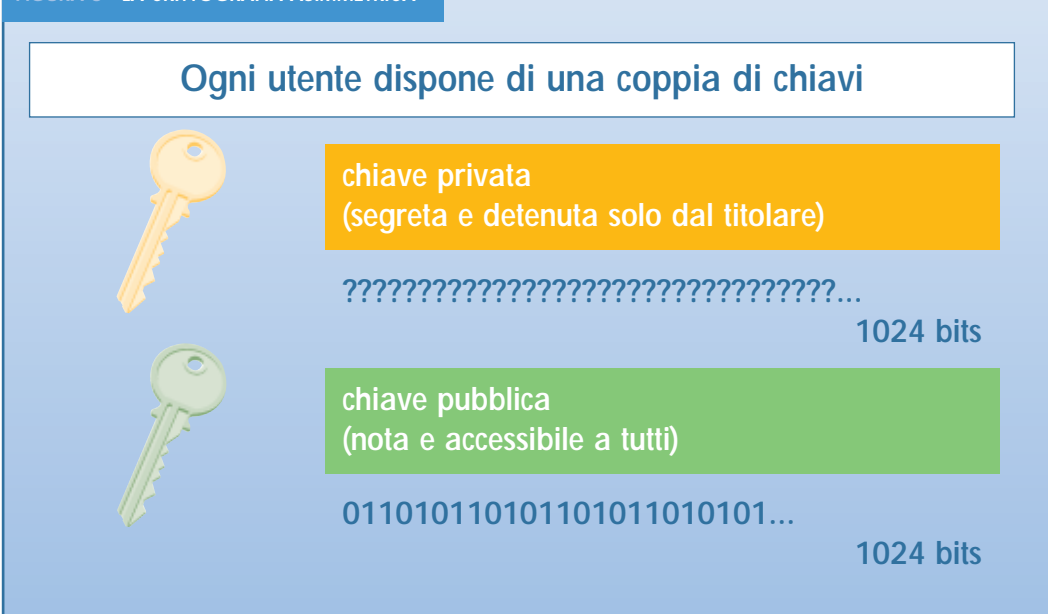
Analogamente ad una firma autografa manuale, la firma digitale è univoca, non può non appartenere al firmatario, essendo prodotta dal suo codice privato, che solo lui può usare. Anche se prodotta dalla stessa chiave privata, ogni firma digitale è diversa, perché deriva da un'impronta diversa, ottenuta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

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.

Da quanto esposto è evidente che la funzione della firma digitale non è più quella di rendere il testo comprensibile solo al destinatario (la chiave pubblica è accessibile a tutti!), bensì quella di verificarne la provenienza dal titolare della chiave privata (Figura 3).

FIGURA 3 - LA CRITTOGRAFIA ASIMMETRICA



Per tale motivo, anziché cifrare l'intero documento, è possibile utilizzare l'impronta del documento: una sorta di "riassunto" costruito in modo da risultare diverso anche a seguito di variazioni in uno solo dei caratteri digitati nel documento di partenza, ma molto più leggero e veloce da cifrare e de-cifrare.

Verifica dell'ID del mittente
Durante la fase descritta sopra, effettuata durante un collegamento Internet, l'applicazione si connette automaticamente alla Autorità di Certificazione e verifica che il certificato del mittente non sia scaduto, revocato, bloccato (Figura 4).

È importante sottolineare, ancora una volta, quanto segue:

- Ogni coppia di chiavi è unica.
- Non è possibile ricavare la chiave privata dalla corrispondente chiave pubblica.
- Solo ogni chiave della coppia consente di sbloccare il codice dell'altra, cioè di effettuare l'operazione inversa a quella ottenuta con l'altra.

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 conva-

lida 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.

IL RUOLO DEL CERTIFICATORE

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, contenente 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)
- Un 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) impongono di utilizzare dispositivi sicuri, cioè un token, per registrarvi l'ID atto a generare una firma digitale.

Per ottenere un ID ci 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.

Coloro che intendono dotarsi di quanto necessario per poter sottoscrivere, con firma digitale, documenti informatici possono rivolgersi ad uno dei soggetti autorizzati: i Certificatori.



I sistemi di firma digitale, di per sé, non garantirebbero in alcun modo la reale provenienza del messaggio dalla persona che asserisce di esserne l'autore: chiunque, in teoria, potrebbe generare una coppia di chiavi ed associarla al nome di un'altra persona anziché al proprio. D'altronde, la possibilità di verificare integrità e paternità di un documento è subordinata al fatto che una delle due chiavi venga resa pubblica.

Il Legislatore ha, quindi, introdotto la figura del Certificatore, che ha proprio il compito di accertare l'identità personale del richiedente e di aggiornare apposite liste dei certificati emessi e di quelli sospesi o revocati, cosicché:

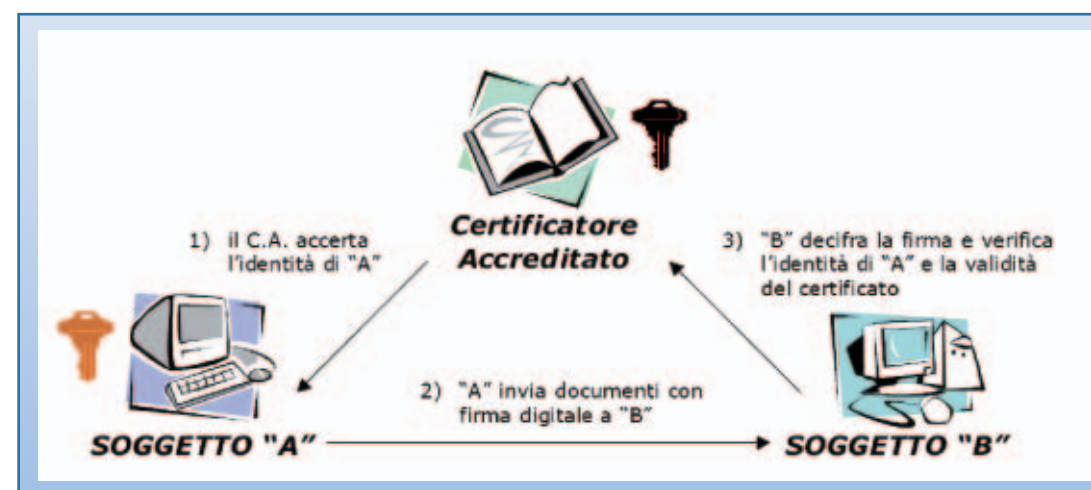
- chi abbia firmato un messaggio con una



chiave non sospesa né revocata non possa in alcun modo disconoscere il contenuto e la paternità;

- chiunque riceva un documento con firma digitale possa verificare l'identità del firmatario e la validità del relativo certificato.

L'identificazione certa del titolare della firma digitale è la fase più delicata, perché se un soggetto riesce a farsi passare per un altro tut-





ti i successivi passaggi sono viziati dall'inganno iniziale: per tale motivo, chi richiede il rilascio della firma digitale deve recarsi di persona presso uno dei punti di registrazione del Certificatore con un documento di

identità valido. Inoltre, il Legislatore richiede ai Certificatori accreditati (Figura 5), oltre agli stessi requisiti previsti per l'esercizio dell'attività bancaria, il rispetto di ulteriori condizioni atte a dimostrare la loro affidabilità.

FIGURA 5 - CERTIFICATORI ACCREDITATI

I Certificatori accreditati sono iscritti in un apposito elenco, consultabile sul sito Internet dell'AIPA - Autorità per l'informatica nella Pubblica Amministrazione:

S.I.A. S.p.A. (dal 27/01/2000)

(cessata attività dal 01/01/2003 - certificatore sostitutivo Actalis)

SSB S.p.A. (dal 24/02/2000)

(cessata attività dal 01/01/2003 - certificatore sostitutivo Actalis)

BNL Multiservizi S.p.A. (dal 30/03/2000)

(cessata attività dal 30/11/2003 - certificatore sostitutivo Actalis)

Infocamere SC.p.A. (dal 06/04/2000)

Finalis S.p.A. (dal 13/04/2000)

(cessata attività dal 31/12/2003 - certificatore sostitutivo: nessuno)

Saritel S.p.A. (dal 20/04/2000)

(società fusa per incorporazione nella I.T. Telecom S.p.A.)

Postecom S.p.A. (dal 20/04/2000)

Seceti S.p.A. (dal 06/07/2000)

(cessata attività dal 31/07/2003 - certificatore sostitutivo Actalis)

Centro Tecnico per la RUPA (dal 15/03/2001 - confluito nel CNIPA in data 01/01/2004)

In.Te.S.A. S.p.A. (dal 22/03/2001)

ENEL.IT S.p.A. (dal 17/05/2001)

(cessata attività dal 31/12/2004 - certificatore sostitutivo: nessuno)

Trust Italia S.p.A. (dal 07/06/2001)

Cedacrinord S.p.A. (dal 15/11/2001 - ora Cedacri S.p.A.)

Cedacri S.p.A. (dal 15/11/2001 - Nuova denominazione sociale della Cedacrinord S.p.A.)

Actalis S.p.A. (dal 28/03/2002)

Consiglio Nazionale del Notariato (dal 12/09/2002)

I.T. Telecom S.p.A. (dal 06/02/2003 - già Saritel S.p.A.)
(cessata attività dal 31/12/2004 - certificatore sostitutivo I.T. Telecom S.r.l.)

Comando C4 - IEW (dal 10/04/2003 - Nuova denominazione Comando Trasmissioni e Informazioni Esercito)

Consiglio Nazionale Forense (dal 11/12/2003)

SOGEI S.p.A. (dal 26/02/2004)

Sanpaolo IMI S.p.A. (dal 08/04/2004)

Banca Monte dei Paschi di Siena S.p.A. (dal 03/08/2004)

Lombardia Integrata S.p.A. (dal 17/08/2004)

Banca Intesa S.p.A. (dal 09/09/2004)

Banca di Roma S.p.A. (dal 09/09/2004)

CNIPA (dal 15/03/2001)

I.T. Telecom S.r.l. (dal 13/01/2005)

Comando Trasmissioni e Informazioni Esercito (dal 10/04/2003 - già Comando C4 - IEW)

Consorzio Certicomm (dal 23/06/2005)

Comando C4 Difesa - Stato Maggiore della Difesa (dal 21/09/2006)

COME OTTENERLA

Qualunque persona fisica dotata di capacità giuridica può richiedere la firma digitale ad uno dei Certificatori accreditati iscritti nell'elenco dell'AIPA (www.aipa.it).

Generalmente, l'iter per il rilascio segue i seguenti passi:

1. Il soggetto interessato sceglie il Certificatore al quale presentare richiesta (le P.A. che aderiscono alla RUPA/RUPAR possono rivolgersi al Centro Tecnico per la RUPA per ottenere gratuitamente il kit di firma).
2. Il Certificatore accerta l'identità del richiedente (che deve recarsi di persona presso il punto di registrazione indicato) e fornisce il kit contenente:
 - *Smart Card* (supporto simile a una carta di credito, in cui si conservano la chiave privata e copia del certificato digitale contenente la chiave pubblica);
 - *Lettores di Smart Card* (da collegare al PC per procedere all'apposizione della firma su di un file);
 - *Software* per l'apposizione della firma (da installare sul PC).
3. Il Certificatore provvede a pubblicare il certificato nell'apposito registro consultabile su Internet.
4. Il richiedente collega il lettore di Smart Card al proprio Personal Computer, attraverso l'apposita porta USB o seriale (per i PC portatili, anche PCMCIA), installa il software sul PC, inserisce la Smart Card nel lettore (digitando il codi-

ce PIN) ed esegue i comandi suggeriti dal software per procedere all'apposizione della firma.

In prossimità della scadenza (o a seguito di eventi particolari), il titolare dovrà richiedere un nuovo certificato.

Su richiesta, e con il consenso di eventuali terzi interessati, nel certificato è possibile specificare anche la sussistenza di poteri di rappresentanza o di altri titoli relativi all'attività professionale o a cariche rivestite.

ALTRI TIPI DI FIRMA ELETTRONICA

Nel 1999, la Direttiva CE n. 93 "Relativa ad un quadro comunitario per le firme elettroniche" ha introdotto la distinzione tra diverse tipologie di firma elettronica.

In base a tale distinzione, recepita con D.Lgs. 10/2002 e DPR 137/2003, la cosiddetta "firma digitale" disciplinata dai precedenti atti normativi rappresenta la versione più evolu-





ta, l'unica tipologia di firma elettronica idonea ad essere utilizzata per l'invio telematico alla Pubblica Amministrazione di istanze e dichiarazioni. Parallelamente, nei documenti informatici delle Pubbliche Amministrazioni la firma autografa è sostituita unicamente dalla firma digitale. Di seguito si riporta un quadro sintetico (Figura 6) dei diversi tipi di firma elettronica previsti, nel quale la firma di-

gitale si configura come un particolare tipo di firma elettronica qualificata con certificato rilasciato da Certificatore accreditato.

ALCUNI ESEMPI D'USO DELLA FIRMA DIGITALE

E-mail e comunicazioni sicure

Quante e-mail escono dalla vostra azien-

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

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? È un collaboratore autorizzato o qualche altro? È un'azienda partner o un concorrente? Vi serve una identificazione elettronica se volete controllare l'accesso alle informazioni aziendali, selezionandolo secondo livelli di autorizzazione.

zione 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.

CASI REALI

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.

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

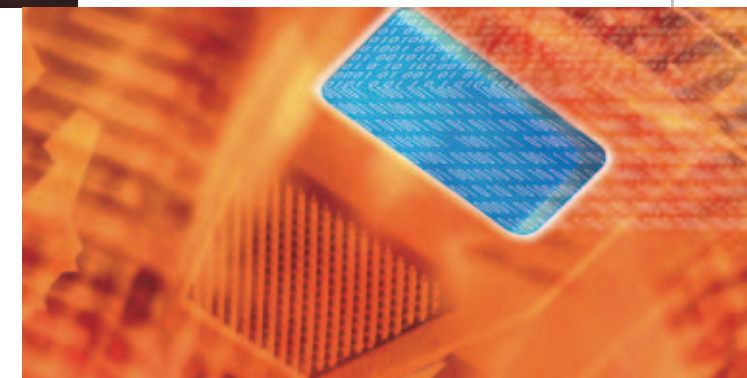


Commercio elettronico e pagamenti sicuri

Troppo spesso non siamo sicuri dell'identità di un cliente. Spediamo merce, iniziamo processi di produ-

FIGURA 6 - TIPI DI FIRMA ELETTRONICA

Tipo di firma	Descrizione	Requisiti del Certificatore	Funzione dei certificati	Effetti
ELETTRONICA	Dati elettronici, allegati o connessi a documenti informatici, utilizzati come metodo di autenticazione.	I legali rappresentanti e i soggetti preposti all'amministrazione devono possedere i requisiti di onorabilità ex T.U. sull'attività bancaria e creditizia. L'attività è libera e non necessita di autorizzazione preventiva.	Collegano la firma elettronica al titolare e ne confermano l'identità.	Sul piano probatorio, i documenti con tale firma sono liberamente valutabili in base alle loro caratteristiche di qualità e sicurezza.
ELETTRONICA AVANZATA	Firma elettronica che garantisce anche l'integrità del documento e creata con mezzi sui quali il firmatario può conservare un controllo esclusivo.			
ELETTRONICA QUALIFICATA	Firma elettronica avanzata creata mediante un dispositivo sicuro, con certificato rilasciato da Certificatore qualificato.	Come sopra, più altri requisiti di affidabilità (organizzativa, tecnica, finanziaria, dei sistemi utilizzati, ...). È richiesta una comunicazione di inizio attività al M.I.T.	Contengono i dati previsti dalla normativa, firmati digitalmente dal Certificatore che li ha rilasciati. L'emissione, revoca e sospensione sono oggetto di pubblicazione.	Sul piano probatorio, i documenti con tale firma fanno piena prova di autenticità fino a querela di falso.
DIGITALE	Firma elettronica qualificata con certificato rilasciato da Certificatore accreditato.	Come sopra, più forma di società di capitali e capitale sociale non inferiore a quello necessario per l'attività bancaria. È richiesto l'accreditamento presso il M.I.T. e l'iscrizione in apposito elenco pubblico.		





LIK TID IIFMR AIDIGATELE D IOCTS

ieP ropet regenarerf riemd gitila i èenecssraoie ssre eodatid inud siopisitovs ciru oep ralq nerezaoiend leelf riem(octstiiuotd anu amsractra d oadu notek nSU)B ,nul teoterd imsractra dn(lec sa onic iun nos itulizizi il token USB), un software in grado di interagire con il dispositivo per la generazione di firme digitali e per la gestione del dispositivo stesso (es. per il cambio del PIN che ne consente l'uso).

I costi del kit completo è variabile da certificatore a certificatore; a titolo orientativo è comunque possibile ottenere il kit completo ad un prezzo di circa 100€. Il certificato ha una scadenza e deve essere, quindi, rinnovato periodicamente. In genere, hanno una validità di uno o due anni, il rinnovo ha un costo orientativo di 10/15 € per anno. È bene evidenziare che tutti i certificatori prevedono delle condizioni economiche specifiche per forniture di particolare rilievo.

Le imprese

Quando un'impresa decide di dotare un numero considerevole dei propri dipendenti del kit di firma digitale, contatta i vari certificatori per scegliere, sulla base del numero dei kit necessari, del costo complessivo dell'operazione e dei servizi accessori offerti, quello che meglio soddisfa le proprie esigenze. Inoltre, è piuttosto frequente che vi siano accordi al fine di demandare all'impresa stessa l'attività di registrazione e di verifica dell'identità del titolare del certificato. Questa pratica viene spesso utilizzata in quanto comporta diversi benefici per tutti i soggetti coinvolti (dipendente, impresa e certificatore). Il dipendente non deve recarsi fisicamente presso l'autorità di registrazione del certificatore, l'impresa ha un risparmio notevole in termini di ore lavoro spese dai dipendenti per recarsi presso il certificatore, oltre al controllo diretto dei certificati emessi per i propri dipendenti con procedure snelle e rapide che consentono di richiedere sospensioni e revocche dei certificati stessi. Il certificatore trae vantaggio dal fatto che non deve impegnare risorse umane per il riconoscimento dei titolari, la verifica dei titoli e di eventuali incarichi o ruoli svolti per l'impresa richiedente.

online. Alcune banche o gruppi bancari appaiono tra i certificatori accreditati, presenti nella lista AIPA.

E-mail sicure

È 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 e-mail 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 e-mail che passano attraverso un server di posta aziendale, eventualmente respingendo e-mail non firmate ed automaticamente cifrando e decifrando quelle destinate a certi indirizzi.

RIFERIMENTI NORMATIVI

L.59/1997 (L. Bassanini)

Delega al Governo per il conferimento di funzioni e compiti alle regioni ed enti locali, per la riforma della Pubblica Amministrazione e per la semplificazione amministrativa. In previsione della realizzazione della RUPA (Rete Unitaria della Pubblica Amministrazione) e dello scambio di dati che questa consentirà tra Uffici pubblici, e tra questi e i cittadini, ha sancito che:

Art.15, comma 2 - "Gli atti, dati e documenti formati dalla Pubblica Amministrazione e dai privati con strumenti informatici o telematici, i contratti stipulati nelle medesime forme, nonché la loro archiviazione e trasmissione con strumenti informatici, sono validi e rilevanti a tutti gli effetti di legge. (...)”

DPCM 8/2/1999

Regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici.

CE 93/1999

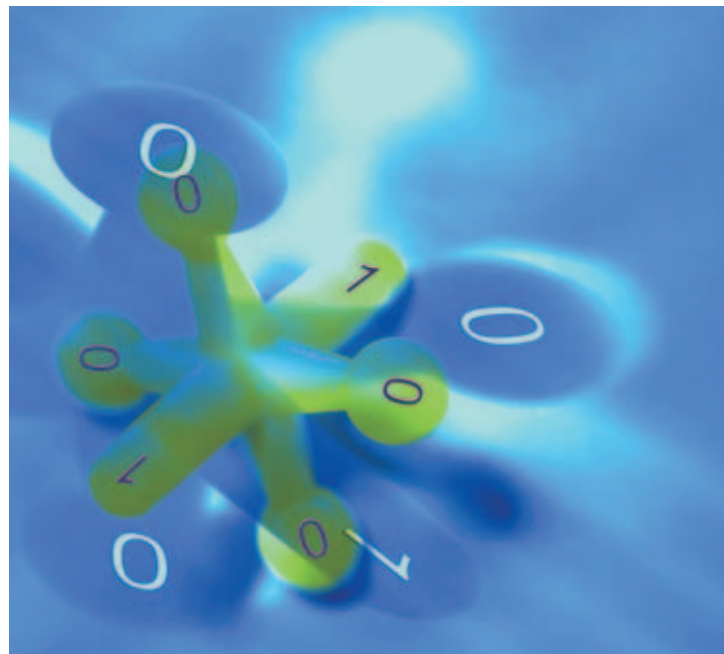
Direttiva CE relativa ad un quadro comunitario per le firme elettroniche.

Introduce la distinzione tra diverse tipologie di firma elettronica, in base alla quale la firma "digitale", di cui ai precedenti atti normativi, si configura come la versione più evoluta (firma elettronica qualificata con certificato rilasciato da Certificatore accreditato).

DPR 445/2000

Testo Unico delle disposizioni legislative e regolamentari in materia di documenta-





anche per fax e via telematica.”

Comma 2: “Le istanze e le dichiarazioni inviate per via telematica sono valide se sottoscritte mediante la firma digitale (...).”

D.Lgs. 10/2002

Recepimento della Direttiva 1999/93/CE sulla firma elettronica.

DPR 137/2003

Regolamento recante disposizioni di coordinamento in materia di firme

zione amministrativa. Ha stabilito che, per le istanze e le dichiarazioni inviate per via telematica alla Pubblica Amministrazione, dovrà essere utilizzata la firma digitale (non, quindi, una qualsiasi firma elettronica) e che nei documenti informatici delle Pubbliche Amministrazioni la firma autografa è sostituita unicamente dalla firma digitale.

Art.25, comma 1: “In tutti i documenti informatici delle pubbliche amministrazioni la firma autografa o la firma, comunque prevista, è sostituita dalla firma digitale (...).”

Art.38, comma 1: “ Tutte le istanze e le dichiarazioni da presentare alla Pubblica Amministrazione o ai gestori o esercenti di pubblici servizi possono essere inviate

elettroniche a norma dell’articolo 13 del decreto legislativo 23 gennaio 2002, n. 10. Hanno modificato ed integrato il T.U. assicurando, tra l’altro, una speciale efficacia probatoria al documento informatico sottoscritto con firma digitale o con un altro tipo di firma elettronica avanzata.

DPR 445/2000, Art.10, comma 3 – “Il documento informatico, quando è sottoscritto con firma digitale o con un 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 di una firma sicura, fa inoltre piena prova, fino a querela di falso, della provenienza delle dichiarazioni da chi l’ha sottoscritto.”