Centro nazionale per l'informatica nella pubblica amministrazione

Guida

alla

Firma Digitale

Versione 1.3 – aprile 2009

SOMMARIO

1. Scopo e destinatari del documento

Questo breve documento ha lo scopo di chiarire le differenze sostanziali fra le varie tipologie di firme elettroniche, cosa è esattamente la firma digitale, le modalità con cui è possibile dotarsi di un dispositivo di firma digitale, come effettuare la verifica di una firma digitale e gli utilizzi pratici di questo strumento.
Il documento si rivolge ai cittadini, alle imprese ed alle pubbliche amministrazioni che intendono dotarsi dei dispositivi di firma necessari per sottoscrivere i documenti informatici.

2. Definizioni

Certificato qualificato	Insieme di informazioni che creano una stretta ed affidabile correlazione fra una chiave pubblica e i dati che identificano il Titolare. Sono certificati elettronici conformi ai requisiti di cui all'allegato I della direttiva n. 1999/93/CE, rilasciati da certificatori che rispondono ai requisiti di cui all'allegato II della medesima direttiva.
Chiave privata	La chiave della coppia utilizzata nel processo di sottoscrizione di un documento informatico L'elemento della coppia di chiavi asimmetriche, utilizzato dal soggetto titolare, mediante il quale si appone la firma digitale sul documento informatico
Chiave pubblica	La chiave della coppia utilizzata da chiunque esegua la verifica di una firma digitale l'elemento della coppia di chiavi asimmetriche destinato ad essere reso pubblico, con il quale si verifica la firma digitale apposta sul documento informatico dal titolare delle chiavi asimmetriche
Dispositivo di firma	Insieme di dispositivi hardware e software che consentono di sottoscrivere con firma digitale documenti informatici
Documento informatico	E' costituito da qualunque oggetto informatico (file) che contenga atti, fatti o dati giuridicamente rilevanti
Firma digitale	E' un particolare tipo di firma elettronica qualificata basata su un sistema di chiavi asimmetriche a coppia, una pubblica e una privata, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici
Firma elettronica	L'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di identificazione informatica
Firma elettronica qualificata	La firma elettronica ottenuta attraverso una procedura informatica che garantisce la connessione univoca al firmatario, creata con mezzi sui quali il firmatario può conservare un controllo esclusivo e collegata ai dati ai quali si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati, che sia basata su un certificato qualificato e realizzata mediante un dispositivo sicuro per la creazione della firma
Soggetto giuridico	Impresa, azienda, società; qualunque soggetto dotato di partita IVA
SSCD	Acronimo inglese (Secure Signature Creation Device) di "dispositivo sicuro per la creazione della firma". E' un dispositivo che soddisfa particolari requisiti di sicurezza. I più utilizzati sono costituiti da smartcard.
Titolare	Il soggetto cui sono attribuite le firme digitali generate attraverso una determinata chiave associata ad un determinato certificato

3. **Il quadro normativo**

Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445

Direttiva europea 1999/93/CE sulle firme elettroniche

Decreto legislativo 23 gennaio 2002, n. 10

Decreto del Presidente della Repubblica 7 aprile 2003, n. 137

Decreto del Presidente del Consiglio dei Ministri 13 gennaio 2004

Deliberazione CNIPA n.4 del 17 Febbraio 2005 "Regole per il riconoscimento e la verifica del documento informatico"

Decreto legislativo 7 Marzo 2005 n. 82 "Codice dell'amministrazione digitale"

Protocollo di intesa del 16 Febbraio 2006 per la disponibilità del formato di firma digitale definito nelle specifiche PDF proposto dalla società Adobe System Inc.

Decreto Legislativo 4 Aprile 2006 n.159 "Disposizioni integrative e correttive al decreto legislativo 7 marzo 2005, n.82 recante codice dell'amministrazione digitale"

Deliberazione CNIPA n.34 del 18 Maggio 2006 "Regole tecniche per la definizione del profilo di busta crittografica per la firma digitale in linguaggio XML"

Decreto del Presidente del Consiglio dei Ministri 30 marzo 2009

4. Struttura del documento

Il documento è strutturato per argomenti indipendenti. Lo scopo è quello di consentire anche la lettura delle sole sezioni di interesse. La seguente tabella ha lo scopo di indirizzare coloro che intendono leggere esclusivamente gli argomenti di loro interesse nell'individuazione degli stessi.
Per ogni argomento è quindi suggerito, dipendentemente dalla tipologia del lettore, il grado di attinenza alle esigenze informative peculiari.

Argomenti	Cittadini	Aziende	PA
IL QUADRO NORMATIVO	A	C	FC
INTRODUZIONE ALLE SOTTOSCRIZIONI INFORMATICHE	C	C	C
UTILIZZO DELLA FIRMA DIGITALE	C	C	C
LA FIRMA DIGITALE E LA DIRETTIVA EUROPEA SULLE FIRME ELETTRONICHE	A	C	C
LA DIFFUSIONE DELLA "FIRMA DIGITALE" IN EUROPA	A	A	A
IL VALORE LEGALE DELLA FIRMA DIGITALE IN ITALIA	FC	FC	FC
LA VALIDITÀ DELLA FIRMA DIGITALE NEL TEMPO	C	C	C
DOVE E COME DOTARSI DI FIRMA DIGITALE	FC	FC	C
I FORMATI DELLA FIRMA DIGITALE	FC	FC	FC
DOVE E COME DOTARSI DI FIRMA DIGITALE	FC	FC	FC
Firma digitale di un singolo documento in formato pkcs#7	FC	FC	FC
Firma digitale con procedure automatiche	A	C	C
LA PROCEDURA DI VERIFICA	FC	FC	FC
Esempio di verifica sul client	FC	FC	FC
Procedure automatiche di verifica	A	C	C
LA PROCEDURA DI FIRMA IN FORMATO pdf	FC	FC	FC

LE NUOVE REGOLE TECNICHE, IL DPCM 30 MARZO 2009	A	FC	FC
La FIRMA DIGITALE E L'EUROPA	C	FC	FC
LO STRUMENTO "FIRMA DIGITALE" INTEGRATO NEL PROCESSO DI E-GOVERNEMENT	A	FC	FC

FC = Lettura fortemente consigliata. **C** = Lettura consigliata. **A** = Lettura di approfondimento

5. Introduzione alle sottoscrizioni informatiche

A partire del 1997, una serie di provvedimenti legislativi hanno conferito valore giuridico al documento informatico e alla firma digitale. La pubblicazione della Direttiva Europea 1999/93/CE (Directive 1999/93/EC of the European Parliament and of the Council on a common framework for electronic signatures), nel gennaio del 2000, ha dato ulteriori impulsi al processo legislativo, imponendo un quadro comune agli Stati dell'Unione Europea. Il processo legislativo ha anche fornito delle indicazioni sulle tecnologie da impiegare per ottenere delle firme digitali che possano ritenersi equivalenti a quelle autografe. La struttura normativa dettata dal legislatore comunitario ha introdotto differenti sottoscrizioni o, più correttamente, differenti livelli di sottoscrizione. Nel linguaggio corrente, quindi, hanno iniziato a essere utilizzati i termini firma "debole" o "leggera" e firma "forte" o "pesante". Non è obiettivo di questa guida tecnica approfondire questi concetti, ma senz'altro è opportuno chiarire cosa sono queste firme e quale è la loro efficacia giuridica. Un breve approfondimento giuridico è sviluppato nel paragrafo 6 mentre nel seguito del paragrafo vengono presentati i principali aspetti tecnici.

Dal punto di vista tecnico e realizzativo è ben definita la firma "forte", ovvero quella che il legislatore definisce firma digitale. Essa è basata su un sistema a chiavi crittografiche asimmetriche, utilizza un certificato digitale con particolari caratteristiche, rilasciato da un soggetto con specifiche capacità professionali garantite dallo Stato e viene creata mediante un dispositivo con elevate caratteristiche di sicurezza che in genere è una smart card.

L'altra tipologia di firma è la parte complementare. Tutto ciò che non risponde anche in minima parte a quanto appena descritto, ma è compatibile con la definizione giuridica di firma elettronica presentata nella tabella delle definizioni, è un firma "leggera".
Ovviamente l'efficacia giuridica delle due firme è diversa. La firma digitale è equivalente a una sottoscrizione autografa. Le altre potrebbero non esserlo: vengono valutate in fase di giudizio in base a caratteristiche oggettive di qualità e sicurezza.

Come ulteriore garanzia per la pubblica amministrazione, che è obbligata ad accettare i documenti firmati digitalmente, i certificatori che intendono rilasciare certificati digitali validi per le sottoscrizioni di istanze e dichiarazioni inviate per via telematica alla pubblica amministrazione stessa, possono dimostrare di possedere particolari e comunque superiori caratteristiche di qualità e sicurezza e ottenere quindi la qualifica di "certificatore accreditato". Tale qualifica è sotto il controllo ed è garantita, in Italia, dallo Stato.

Concludendo, possiamo dire che nell'utilizzo del documento informatico, quando si ha la necessità di una sottoscrizione equivalente a quella autografa è indispensabile utilizzare la firma digitale.
Negli altri casi possiamo tranquillamente affermare che più che di un processo di firma si tratta di un processo di autenticazione con minori requisiti di sicurezza e quindi con una minore efficacia probatoria.

Da quanto esposto si può dedurre che nella pubblica amministrazione l'espressione del potere di firma nel documento informatico da parte del funzionario che ne ha titolarità, dovrà essere esercitata con la firma digitale.

6. Utilizzo della firma digitale

La firma digitale è uno strumento e come tale deve essere utilizzato nei modi e nei casi appropriati. Ricordiamo che non è corretto il suo utilizzo come sistema di identificazione in rete, per il quale esistono strumenti quali la carta d'identità elettronica e le carte di accesso ai servizi.
La firma digitale è utile nel momento in cui è necessario sottoscrivere una dichiarazione ottenendo la garanzia di **integrità** dei dati oggetto della sottoscrizione e di **autenticità** delle informazioni relative al sottoscrittore.
La garanzia che il documento informatico, dopo la sottoscrizione, non possa essere modificato in alcun modo in quanto, durante la procedura di verifica, eventuali modifiche sarebbero riscontrate, la certezza che solo il titolare del certificato possa aver sottoscritto il documento perché non solo possiede il dispositivo di firma (smartcard/tokenUSB) necessario, ma è anche l'unico a conoscere il PIN (Personal Identification Number) necessario per utilizzare il dispositivo stesso, unite al ruolo del certificatore che garantisce la veridicità e la correttezza delle informazioni riportate nel certificato (dati anagrafici del titolare), forniscono allo strumento "firma digitale" caratteristiche tali da non consentire al sottoscrittore di disconoscere la propria firma digitale (fatta salva la possibilità di querela di falso).
Esempi tipici dell'utilizzo della firma digitale possono essere ricercati in tutti gli adempimenti da effettuarsi verso le amministrazioni che richiedono appunto la sottoscrizione di una volontà: denunce, dichiarazioni di cambi di residenza, di domicilio, richieste di contributi, di esenzioni a pagamenti a causa del reddito o di altre condizioni particolari, ricorsi, ecc.
Fra privati può trovare un interessante impiego nella sottoscrizione di contratti, verbali di riunioni, ordini di acquisto, risposte a bandi di gara, ecc.
Ancora, la firma digitale trova già da tempo applicazione nel protocollo informatico, nella procedura di archiviazione documentale, nel mandato informatico di pagamento, nei servizi camerali, nelle procedure telematiche d'acquisto, ecc.
Alcuni Comuni che partecipano alla sperimentazione della Carta d'Identità Elettronica hanno dotato i propri cittadini di entrambi gli strumenti (CIE o CNS e Firma Digitale) e sviluppato dei servizi in rete tramite i quali i cittadini possono farsi identificare in rete (CIE/CNS), accedere quindi ai propri dati personali nel pieno rispetto delle norme sulla privacy, e sottoscrivere (firma digitale) dichiarazioni, denunce, ricorsi. Ecco quindi che si intravede l'obiettivo finale: dotarsi di un unico strumento con cui sarà possibile farsi riconoscere e sottoscrivere dichiarazioni, fruendo dei vantaggi derivanti dai servizi in rete.

7. La firma digitale e la direttiva europea sulle firme elettroniche

Come già detto sopra, la firma elettronica viene introdotta dalla Direttiva nell'ambito delle definizioni. Tale definizione è stata riportata nella tabella all'inizio della presente guida tecnica.
La lettura della definizione ne evidenzia la genericità, quindi essa si presta a interpretazioni differenti e, conseguentemente, risulta per certi versi ambigua e di difficile attuazione concreta. Essa è e rimane un principio giuridico.
Un piccolo passo in avanti lo consente, sempre nella Direttiva, la definizione di firma elettronica avanzata .
In base a tale definizione si comincia a comprendere che ci si deve confrontare con una molteplicità di tipologie di firma. Dal punto di vista pratico è sufficiente considerare:

a) la firma elettronica (generica) può essere realizzata con qualsiasi strumento (password, PIN, digitalizzazione della firma autografa, tecniche biometriche, ecc.) in grado di conferire un certo livello di autenticazione a dati elettronici;
b) la firma elettronica avanzata, più sofisticata, consente di identificare in modo univoco il firmatario garantendo anche l'evidenza di modifiche all'oggetto firmato, apportate dopo la sottoscrizione.

Allo stato dell'arte, solo il sistema a chiavi asimmetriche definito per la firma digitale nella legge italiana "pre-Direttiva", soddisfa i requisiti richiesti per la firma elettronica avanzata.
Nessuna delle due firme descritte soddisfano per la Direttiva il requisito di equivalenza con la firma autografa.
E' necessario quindi fare un ulteriore passo in avanti.

7.1 Firme "leggere" e firme "forti"

Anche se è correntemente utilizzato, all'interno della Direttiva non compare mai il concetto di firma "leggera", né quello di firma "forte". Queste definizioni sono state introdotte dagli addetti ai lavori per sopperire alla mancanza di una definizione esplicita di altre tipologie di firma.
Queste tipologie sono introdotte nell'articolo 5 della Direttiva. In particolare il primo comma di questo articolo introduce la tipologia di firma più importante dal punto di vista legale perché equivalente alla sottoscrizione autografa. Spesso ci si riferisce ad essa con il termine firma "forte", mentre fra gli addetti ai lavori, specialmente in campo internazionale, la si indica come "firma 5.1".
La firma "forte" è anch'essa nei termini presentati, un principio giuridico, ma vediamo come può essere realizzata praticamente.
Detta firma è una firma elettronica avanzata, perché così si deduce dalla definizione, che soddisfa specifiche caratteristiche derivanti dal certificatore. Quest'ultimo è il soggetto che certifica le chiavi mediante le quali la firma è stata generata. Infine la firma deve essere generata con strumenti che garantiscano un adeguato livello di sicurezza, come ad esempio un smart card.
Riassumendo, affinché la firma apposta possa essere considerata equivalente ad una autografa:

a) deve essere basata su un sistema a chiavi asimmetriche;
b) deve essere generata con chiavi certificate con le modalità previste nell'allegato I della Direttiva ;
c) deve essere riconducibile a un sistema di chiavi provenienti da un certificatore operante secondo l'allegato II della Direttiva e soggetto a vigilanza da parte del preposto organo istituzionale (il termine "vigilanza" è proprio del recepimento italiano della Direttiva che

utilizza "supervisione". L'organismo preposto a tale attività è il CNIPA, Centro nazionale per l'informatica nella pubblica amministrazione);

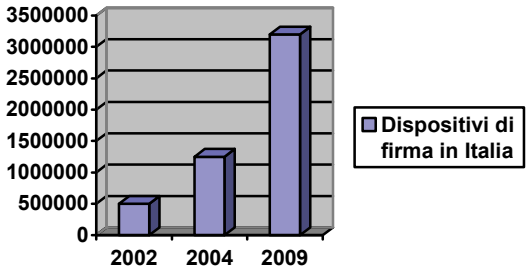
d) deve essere generata utilizzando un dispositivo sicuro che soddisfi i requisiti dell'allegato III della Direttiva.

Come si vede, a parte piccole differenze organizzative, la precedente normativa italiana "pre-Direttiva" soddisfa quanto appena riassunto.
I certificatori già iscritti nell'elenco pubblico dei certificatori hanno di fatto le caratteristiche per essere considerati "accreditati" secondo quanto previsto dall'articolo 3, comma 2 della Direttiva. Questo fatto, inoltre, è già stato riconosciuto nel primevo decreto di recepimento della Direttiva (art. 11, comma 2 del D.Lgs. 23 gennaio 2002, n. 10).
Il secondo comma dell'articolo 5 della Direttiva conferisce dignità giuridica alle altre tipologie di firma. Queste non sono definibili tecnologicamente a priori, possono essere generate senza vincoli sugli strumenti e sulle modalità operative. E' ovvio che non offrono garanzie di interoperabilità se non in particolari condizioni di utilizzo come, ad esempio, in gruppi chiusi di utenti. Infatti, in questo caso, la comunità di utenti condivide gli strumenti di firma e di verifica della stessa. Un giudice, come stabilito nel citato secondo comma dell'articolo 5 della Direttiva, non potrà rifiutare in giudizio queste firme "leggere", ma la loro ammissibilità nascerà dalla libera convinzione e non dall'obbligo di legge previsto per le firme cosiddette "forti". Le firme "deboli" ("5.2" in terminologia europea) assumono quindi un rilievo probante e non, come per le firme "forti" ("5.1" in terminologia europea) probatorio.
Infine, ricordiamo che la Direttiva europea prescrive che gli Stati membri notifichino alla Commissione l'organismo di vigilanza e accreditamento, l'organismo deputato a sovrintendere le certificazioni dei dispositivi di firma e l'elenco di tutti i soggetti che rilasciano sul territorio certificati qualificati.
Dette informazioni sono pubblicate sul sito della Commissione europea, a cura della Direzione Generale Information Society, ma a mero titolo informativo, difatti la pubblicazione non deriva da un obbligo normativo a carico della Commissione.

8. La diffusione della "firma digitale" in Europa

Nell'ambito del F.E.S.A. (Forum of European Supervisor Authority), il cui scopo è far incontrare rappresentanti dei vari organismi di vigilanza nazionali in Europa per l'armonizzazione dei principi e delle tecniche fondamentali che regolano la materia nei rispettivi Stati, si è proceduto più volte alla verifica della diffusione della firma digitale.

Da queste analisi è emerso che nel 2002 l'Italia era, con 500.000 certificati lo Stato con la maggiore diffusione di certificati, seguita dalla Norvegia con 32.000, e dalla Germania (26.000). Nel primo trimestre 2004 il numero dei dispositivi rilasciati in Italia per la firma digitale ha superato 1.250.000 unità e, ad oggi, abbiamo superato la soglia di 3.200.000 di unità. La firma digitale generata in qualunque Stato membro della Comunità deve, sulla base



dei trattati comunitari,essere riconosciuta dagli altri Stati. Al fine di rendere agevole tale mutuo riconoscimento è indispensabile che le norme nazionali di recepimento della Direttiva europea 1999/93/CE sulle firme elettroniche nei rispettivi Stati, forniscano un insieme comune di garanzie e certezze. Anche a tale fine diversi organismi fra cui l'EESSI, la Commissione sancita dall'articolo 9 della citata Direttiva europea, l'ETSI, il FESA, stanno lavorando per affinare la Direttiva stessa e realizzare nel contempo degli standard la cui applicazione consenta appunto di raggiungere un adeguato livello di fiducia in tutta la Comunità.

La diffusione della firma digitale in Europa e il suo utilizzo fra gli Stati è una sfida non da poco.

Basti pensare quanto è stato complicato raggiungere l'interoperabilità, perlomeno nel processo di verifica, in Italia, dove si aveva comunque il grande vantaggio derivante dal fatto che tutti i protagonisti (certificatori e titolari) dovevano sottostare alle medesime norme. Ciononostante è una sfida che la Commissione europea ha accettato cerando tutti i presupposti necessari per vincerla (vedi "La firma digitale europea").

9. Il valore legale della firma digitale in Italia

La firma digitale ha trovato l'impianto legislativo necessario per il proprio utilizzo con la pubblicazione, in data 15 aprile 1999, delle regole tecniche costituite dal DPCM 8 febbraio 1999 (abrogato e sostituito dal DPCM 13 gennaio 2004).
In data 27 gennaio 2000 veniva incluso, nell'elenco pubblico dei certificatori, il primo soggetto autorizzato a rilasciare dispositivi di firma digitale utilizzabili per poter sottoscrivere documenti informatici con la medesima validità giuridica della firma autografa.
La validità giuridica della firma digitale ha subito delle modifiche nel tempo, ad opera di decreti di diversa natura.

Provvedimento	Previsione normativa
DPR 513/97	*Il documento informatico, sottoscritto con firma digitale ai sensi dell'articolo 10, ha efficacia di scrittura privata ai sensi dell'articolo 2702 del codice civile.*
DPR 445/2000	*Il documento informatico, sottoscritto con firma digitale ai sensi dell'articolo 23, ha efficacia di scrittura privata ai sensi dell'articolo 2702 del codice civile.*
D.Lgs 10/2002	*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.*
C.A.D. D.Lgs 82/2005	*Il documento informatico, sottoscritto con firma digitale o con un altro tipo di firma elettronica qualificata, ha l'efficacia prevista dall'articolo 2702 del codice civile. L'utilizzo del dispositivo di firma si presume riconducibile al titolare, salvo **che sia data** prova contraria*
C.A.D. Modificato dal D.Lgs 159/2006	*Il documento informatico, sottoscritto con firma digitale o con un altro tipo di firma elettronica qualificata, ha l'efficacia prevista dall'articolo 2702 del codice civile. L'utilizzo del dispositivo di firma si presume riconducibile al titolare, salvo **che questi dia** prova contraria*

Cerchiamo di capire quindi il valore giuridico della firma digitale nel tempo.

Con i primi due decreti (DPR 513/97 e DPR 445/2000) la firma digitale era equiparata alla firma autografa: assolveva al requisito giuridico della forma scritta e, come la firma autografa, poteva essere disconosciuta dal presunto sottoscrittore. L'onere della prova ricadeva quindi in capo al terzo che, in caso di disconoscimento ad opera del presunto sottoscrittore, ne doveva dimostrare la paternità.

Il Decreto legislativo 23 gennaio 2002, n. 10, modificava profondamente il valore giuridico della firma digitale, ribaltando l'onere della prova: il presunto sottoscrittore, per annullare gli effetti giuridici della firma digitale, doveva intentare una querela di falso. Per chiarirne la portata si pensi che la querela di falso deve essere intentata dal sottoscrittore per vedere annullati gli effetti giuridici di una firma autografa autenticata.

Nel 2006, il CAD (Codice dell'Amministrazione Digitale – D.Lgs 7 marzo 2005, n.82) la firma digitale torna ad avere gli effetti della firma autografa (ex art. 2702 c.c.), ma soprattutto sono mitigati gli oneri in capo del presunto sottoscrittore per vedere disconosciuta la firma digitale: non deve più intentare una querela di falso, è sufficiente provare che altri abbiano potuto utilizzare il dispositivo di firma. Attenzione, non è cosa di poco conto tenendo in mente che i dispositivi non

sono violabili, che i codici segreti (PIN/PUK) utili per l'uso del dispositivo sono forniti in maniera sicura al legittimo titolare, che quest'ultimo sottostà ad obblighi inerenti la conservazione degli stessi che qualora fossero ignorati non libererebbero il titolare da colpa.

Per introdurre la successiva modifica, introdotta dal D.Lgs 4 aprile 2006, n. 159, si deve fare una riflessione sulla previsione all'epoca vigente e, in particolare al passo "*salvo **che sia data** prova contraria.*". Infatti si apriva la strada ad una condizione paradossale: si sarebbe potuto "dare prova" che altri avevano utilizzato il dispositivo di firma del titolare (atto vietato dalle norme), annullandone quindi gli effetti giuridici, sebbene il presunto sottoscrittore riconoscesse la paternità della propria firma e la volontà di sottoscrivere gli atti o fatti in parola.
Il D.Lgs 159/2006 è quindi intervenuto limitando detta facoltà al titolare medesimo.

10. La validità della firma digitale nel tempo

Esiste un altro aspetto degno di approfondimento che riguarda sempre il valore probatorio della firma digitale.
Ma prima è necessario ricordare che il certificato del titolare (l'elemento che consente di ricondurre le chiavi crittografiche usate ad una persona fisica) ha un periodo di validità, ma può anche essere revocato o sospeso([1]) prima della naturale scadenza. La revoca e la sospensione([2]) sopravviene in diversi casi, quali la sottrazione o lo smarrimento del dispositivo di firma, quando le informazioni contenute nel certificato non sono più corrette (Tizio dal certificato risulta amministratore unico di tale società, lasciando la società il certificato dovrà essere revocato) ([3]).

Ciò premesso, è evidente che potrebbero nascere delle problematiche legate alla necessità di poter fruire di un documento informatico sottoscritto con firma digitale in un momento temporale di molto posteriore a quello in cui la firma è stata prodotta, quando il relativo certificato è scaduto, revocato o sospeso.
In queste circostanze è quindi necessario riuscire a collocare nel tempo, in modo opponibile ai terzi, l'esistenza della firma del documento in questione in modo da poter dimostrare che la stessa è stata prodotta in un momento in cui il relativo certificato era ancora valido.

Per far ciò basta utilizzare il servizio di marcatura temporale([4]) tramite il quale si può associare - quando si ritiene necessario - ad un documento informatico una sorta di "etichetta elettronica" già sottoscritto, allo scopo di dimostrare che tale documento recante una data firma esisteva in un ben preciso momento. Il riferimento temporale opponibile ai terzi può altresì essere ottenuto attraverso l'utilizzo della posta elettronica certificata, della segnatura di protocollo e attraverso la procedura di conservazione documentale. L'utilizzo di tali modalità sono però ancora prerogativa esclusiva delle pubbliche amministrazioni (cfr. art. 39 del DPCM 13 gennaio 2004), e lo saranno almeno a tutto il mese di settembre 2009. Con l'entrata in vigore del DPCM 30 marzo 2009, la segnatura di protocollo e la posta elettronica certificata potranno essere fruite erga omnes.

---

[1] La revoca e sospensione del certificato hanno lo steso effetto giuridico: le firme digitali generate sulla base di un certificato scaduto, revocato o sospeso, non producono alcun effetto giuridico (equivalgono a mancata sottoscrizione).

[2] La revoca è irrevocabile, la sospensione è una condizione transitoria del certificato che può evolvere in revoca o "annullamento della sospensione". La sospensione è un istituto a tutela del titolare: il titolare non trova più il dispositivo di firma, ma non è certo se si trova a casa o se gli sia stato sottratto. In via cautelativa sospende il certificato per poi riattivarlo (annullamento della sospensione) o revocarlo a seconda del caso.

[3] Nel caso indicato è la società che, in qualità di "terzo interessato", avrà l'interesse e l'obbligo di richiedere al certificatore la revoca del certificato di firma digitale del'ex amministratore.

[4] Il Servizio di marcatura temporale deve essere reso disponibile ex lege a tutti i titolari dal certificatore di riferimento.

11. I formati della firma digitale

Attualmente il nostro ordinamento prevede l'utilizzo di tre formati per produrre file firmati digitalmente:

- firma digitale in formato pkcs#7
- firma digitale in formato PDF
- firma digitale in formato XML

11.1 Firma digitale in formato pkcs#7

Questo formato, meglio noto come *p7m*, come descritto più avanti nel Capitolo 11 è quello previsto dalla normativa vigente sull'interoperabilità della firma digitale ed è quello che le Pubbliche Amministrazioni sono obbligate ad accettare. E' il formato disponibile fin dagli arbori, il primo formato in uso fin dall'anno 1999.

11.2 Firma digitale in formato PDF

Sulla base dell'articolo 12 comma 9 della deliberazione CNIPA n. 4/2005 il 16 Febbraio 2006 è stato sottoscritto un protocollo d'intesa tra Adobe System Inc. e il CNIPA al fine di introdurre nel nostro ordinamento la possibilità di utilizzare il formato di firma definito nelle specifiche PDF, attraverso il RFC 3778. Sebbene sia ovvio associare il formato PDF a ben noti e largamente diffusi prodotti di mercato, si tratta di uno standard, la cui gestione in applicazioni sviluppate a tale scopo non obbliga al pagamento di alcuna "royalty" ad alcun soggetto.
Grazie a ciò la firma digitale ha fatto un enorme passo in avanti e oggi possiamo disporre di un formato che, da un lato è di larga diffusione e di immediata fruibilità (il software di lettura è scaricabile gratuitamente da Internet e di facile utilizzo) e, dall'altro, risponde ai requisiti tecnico e giuridici per poter trasportare firme digitali al suo interno.
Coloro che intendono sottoscrivere documenti con il formato PDF possono utilizzare il kit di firma digitale fornitogli dal proprio Certificatore di riferimento ed un qualsiasi prodotto di elaborazione PDF, purché esso generi file sottoscritti conformemente alle specifiche del formato stesso. Se il documento è stato predisposto adeguatamente, la sottoscrizione può avvenire anche con il prodotto freeware Acrobat reader.
Inoltre, a mese di marzo 2009, il formato pdf ha ottenuto dei riconoscimenti divenendo standard ISO (ISO 32000) ed ETSI TS 102778 .
Il suo utilizzo è descritto nei capitoli 13 e 14.

11.3 Firma digitale in formato XML

La deliberazione CNIPA n.34/2006 recante "Regole tecniche per la definizione del profilo di busta crittografica per la firma digitale in linguaggio XML" ha introdotto nel nostro ordinamento un ulteriore formato di firma basato sul linguaggio Xml.
Grazie a questo nuovo formato è possibile introdurre in maniera meno invasiva la firma digitale in settori come quello bancario e sanitario in cui il linguaggio in questione ha assunto notevole rilevanza nella gestione elettronica dei rispettivi flussi documentali .

Attenzione: contemporaneamente all'entrata in vigore delle nuove regole tecniche([5]), emanate con il DPCM 30 marzo 2009, il CNIPA emanerà una nuova deliberazione in merito.

[5] Sei mesi dopo la pubblicazione in Gazzetta Ufficiale.

12. Dove e come dotarsi di firma digitale

Coloro che intendono dotarsi di quanto necessario per poter sottoscrivere con firma digitale documenti informatici possono rivolgersi ad uno dei soggetti autorizzati: i Certificatori.
L'elenco pubblico dei certificatori è disponibile via Internet per la consultazione ([6]), dove sono anche disponibili i link ai siti web degli stessi sui quali sono indicate le modalità operative da seguire. E' bene precisare che vi sono alcuni soggetti che espletano questa attività esclusivamente per gruppi chiusi di utenti. E' il caso dello Stato Maggiore della Difesa, del Consiglio Nazionale Forense o del Consiglio Nazionale del Notariato, che svolgono detta attività solo per gli appartenenti alle proprie strutture e/o agli iscritti ai relativi ordini.
Esclusi questi soggetti vi sono, ad oggi, una dozzina di certificatori accreditati cui rivolgersi.
Di questi quelli con il maggior numero di autorità di registrazione ([7]) sono INFOCERT tramite le Camere di Commercio e POSTECOM tramite gli Uffici Postali([8]).
Ricordiamo che in nessun caso è possibile ottenere un dispositivo di firma digitale senza incontrarsi personalmente con il certificatore, o suo incaricato, che avrà l'obbligo di richiedere un documento di riconoscimento in corso di validità per verificare l'identità del richiedente.
Un tale evento costituirebbe una grave violazione dei requisiti operativi inerenti la sicurezza da segnalare rapidamente al CNIPA([9]) che, in qualità di ente governativo preposto alla vigilanza, potrà intraprendere le azioni del caso .

12.1 Il kit di firma digitale ed i costi

Per poter generare firme digitali è necessario essere dotati di un dispositivo sicuro per la generazione delle firme (costituito da una smartcard o da un token USB), un lettore di smartcard (nel caso in cui non si utilizzi 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 80€. Il certificato ha una scadenza, e deve essere quindi rinnovato periodicamente. In genere hanno validità da uno a tre anni, dipende dal certificatore, il rinnovo ha un costo orientativo di poche decine di Euro. E' bene evidenziare che tutti i certificatori prevedono delle condizioni economiche specifiche per forniture di particolare rilievo, come anche servizi aggiuntivi quali la fornitura di certificati di autenticazione e crittografia, caselle di posta elettronica certificata.

12.2 I Cittadini

I cittadini che intendono utilizzare la firma digitale dovranno recarsi **personalmente** presso l'autorità di registrazione (RA) del certificatore per l'identificazione, la sottoscrizione del contratto di servizio e fornitura, per consegnare eventuale documentazione comprovante il possesso di titoli

[6] L'elenco è disponibile sul sito CNIPA alla pagina http://www.cnipa.gov.it/qcsp
[7] Le autorità di registrazione, conosciute anche come Registration Authority, sono degli Uffici del Certificatore che espletano il compito di accertare l'identità dell'utente attraverso una serie di procedure definite nell'ambito di una precisa politica di sicurezza (come ad esempio, il controllo della carta di identità), riportata nel manuale operativo o disponibile nel sito web del Certificatore
[8] Generalmente i cosiddetti PT Business point .
[9] I contatti del CNIPA sono pubblicati in http://www.cnipa.gov.it/site/it-IT/Il_Centro_Nazionale/URP_-_Contatti/

qualora desideri che detti titoli siano riportati all'interno del certificato come previsto dall' art.4 comma 4 della Deliberazione CNIPA n.4/2005([10]).
Le procedure per richiedere il rilascio del certificato (e la fornitura del dispositivo di firma) sono peculiari di ogni certificatore anche se, nella sostanza, prevedono la medesima attività. Dette procedure sono riportate nel manuale operativo ([11]) di ogni certificatore ma anche nei rispettivi siti web. Nella scelta del certificatore è bene verificare quali servizi aggiuntivi sono forniti dagli stessi (es. certificato di autenticazione e crittografia, casella di posta elettronica certificata), la durata del periodo di validità del certificato ed i costi per il rinnovo. Per alcuni riferimenti si rimanda al paragrafo 12.5.

12.3 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 a 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 revoche 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.

12.4 Le pubbliche Amministrazioni

Le pubbliche Amministrazioni possono agire come descritto nel paragrafo precedente per le imprese o, in alternativa, possono richiedere di essere accreditate (iscritte quindi nell'elenco pubblico dei certificatori) utilizzando in realtà le infrastrutture tecnologiche di uno dei soggetti già iscritti nell'elenco pubblico dei certificatori. In questo caso, oltre ai vantaggi descritti nel paragrafo precedente, ottengono il vantaggio di risultare, nella fase di verifica di un documento informatico sottoscritto con firma digitale da un proprio dipendente, quali soggetti che emettono e garantiscono le informazioni inerenti il dipendente stesso e di esercitare un maggiore controllo sulle attività di certificazione.

12.5 Dove recarsi, chi contattare

Nella tabella che segue sono fornite informazioni inerenti tutti i certificatori che hanno risposto all'invito del CNIPA a voler fornire informazioni utili all'utente per scegliere il proprio certificatore.

---

[10] Tale articolo infatti prevede la possibilità di inserire all'interno del certificato la qualifica specifica posseduta dal richiedente. Questa informazione deve essere specificata al momento della registrazione attraverso la produzione della relativa documentazione richiesta dalla RA.

[11] Anch'essi disponibili presso i siti riportati in nota 6 oltre che presso il sito di ogni certificatore. Inoltre i certificatori sono soliti riportare chiaramente sui propri siti web le modalità per richiedere la fornitura del servizio.

La tabella che segue, aggiornata ad aprile 2009, potrà essere per sua natura oggetto di modifiche, si invita pertanto a visitare il sito del CNIPA all'indirizzo: www.cnipa.gov.it/tabellaQCSP .

CERTIFICATORE	SINGOLA EMISSIONE AL CITTADINO	SINGOLA EMISSIONE PERSONE GIURIDICHE (IMPRESE, ENTI…)	NOTE	LINK DELLA PROCEDURA PER LA RICHIESTA	DOVE RECARSI PER LA RICHIESTA (AUTORITA' DI REGISTRAZIONE)
ACTALIS	SI	SI		https://portal.actalis.it/Contact	Presso gli uffici Actalis di Milano (Via Torquato Taramelli, 26) e Roma (Via Di Casal Boccone, 188/190). Su richiesta, è possibile anche la registrazione presso il cliente.
ARUBAPEC	SI	SI		www.arubapec.it/FirmaDigitale.aspx	www.arubapec.it/CDRLaccreditati.aspx
BANCA MONTE DEI PASCHI DI SIENA	SI	SI	Esclusivamente ai clienti della Banca	http://infinita.mps.it/Prodotti/Firma+Digitale	Presso le filiali della Banca. http://infinita.mps.it/Filiali
CEDACRI	SI	SI		www.cedacricert.it/offerta/offerta_CA_consumatore.pdf	**Cedacri S.p.A.** Via del Conventino Collecchio - (PR) tel. 0521-807.367

CERTIFICATORE	SINGOLA EMISSIONE AL CITTADINO	SINGOLA EMISSIONE PERSONE GIURIDICHE (IMPRESE, ENTI…)	NOTE	LINK DELLA PROCEDURA PER LA RICHIESTA	DOVE RECARSI PER LA RICHIESTA (AUTORITA' DI REGISTRAZIONE)
CNDCEC	NO	NO	Esclusivamente agli iscritti agli albi tenuti dagli Ordini dei dottori commercialisti e degli esperti contabili	www.certicomm.it	- **Visura S.p.A**. Corso Vittorio Emanuele II, 326 - Roma visura@visura.it - **OPEN DOT COM S.p.A** Via Roma, 54 - Cuneo info@opendotcom.it - **ODCEC Roma** Via Flaminia 141 - Roma segreteria@odcec.roma.it
INFOCERT	SI	SI	E' disponibile anche una soluzione per non vedenti e ipovedenti	www.firma.infocert.it/rilascio	www.firma.infocert.it/rilascio/distribuzione Camere di Commercio ed altri Uffici di Registrazione Call center **199500130**
INTESA	NO	SI	Esclusivamente per clienti INTESA	Informazioni fornite a cura degli addetti alle vendite INTESA	Personale del certificatore si reca presso il cliente
INTESA SANPAOLO	NO	SI	Esclusivamente ai clienti della Banca	https://ca.intesasanpaolo.com	Presso le filiali del Gruppo Intesa Sanpaolo www.intesasanpaolo.com

CERTIFICATORE	SINGOLA EMISSIONE AL CITTADINO	SINGOLA EMISSIONE PERSONE GIURIDICHE (IMPRESE, ENTI…)	NOTE	LINK DELLA PROCEDURA PER LA RICHIESTA	DOVE RECARSI PER LA RICHIESTA (AUTORITA' DI REGISTRAZIONE)
IT TELECOM	NO	SI	Esclusivamente per clienti Telecom Italia, tramite il personale addetto alle vendite	Informazioni fornite a cura degli addetti alle vendite Telecom Italia.	Contattare gli addetti alle vendite Telecom Italia.
POSTECOM	SI	SI	E' necessario prima registrarsi all'indirizzo http://postecert.poste.it/firmadigitale/acquista.shtml	Cittadino: http://postecert.poste.it/firmadigitale/privati.shtml Persone giuridiche: http://postecert.poste.it/firmadigitale/business.shtml	Presso un ufficio postale abilitato. Elenco in: http://postecert.poste.it/firmadigitale/privati.shtml

13. La procedura di firma digitale

Generare una firma digitale richiede la disponibilità del kit di firma digitale che, ricordiamo, è composto dal dispositivo sicuro di generazione della firme (smartcard o token USB), eventuale lettore di smartcard, software di firma in grado di utilizzare lo specifico dispositivo di cui si è dotati. Difatti, mentre è vero che è possibile verificare firme digitali generate utilizzando dispositivi eterogenei, non è possibile (salvo essere dotati di software disegnati a tale scopo) utilizzare dispositivi di firma eterogenei nel processo di firma (dispositivo fornito dal certificatore A con il software di firma fornito dal certificatore B).
La procedura di firma è piuttosto banale: dopo aver reso disponibile il dispositivo, inserendo quindi la smartcard nell'apposito lettore o inserendo il Token USB nella porta specifica, l'applicazione di firma provvederà a richiedere l'inserimento del PIN di protezione, visualizzerà e richiederà di scegliere quale certificato si intende usare e procederà infine alla generazione della firma.
Ricordiamo infatti che un dispositivo sicuro di firma può contenere diversi certificati, e quindi diverse chiavi private, rilasciati per scopi diversi.
Tipico esempio potrebbe essere quello di un soggetto dotato di tre certificati di sottoscrizione: in qualità di cittadino, quale rappresentante legale di una società, quale componente di una commissione. Detto soggetto selezionerà, in fase di sottoscrizione, l'uno o l'altro certificato dipendentemente dalla natura dell'oggetto che si accinge a sottoscrivere.

13.1 Firma digitale di un singolo documento in formato pkcs#7

La firma digitale di un singolo documento è operativamente dipendente dal software di firma di cui si dispone. Tale software può essere fornito da un certificatore, ma sono disponibili anche numerosi prodotti sviluppati da altre aziende.
Indipendentemente dal prodotto però i passi per la sottoscrizione digitale di un singolo documento sono sempre gli stessi. Vediamo quali.
Ovviamente è necessario disporre di un personal computer al quale preventivamente abbiamo collegato il lettore/scrittore di smart card in base alle indicazioni del fornitore.
Dopo aver attivato il software di firma ci verrà richiesto di selezionare il documento da sottoscrivere e di inserire la smart card nel lettore se non lo si è ancora fatto. All'attivazione del processo di firma sarà chiesto l'inserimento del codice PIN della smart card (o token usb) e dopo qualche secondo potremo salvare un file sottoscritto e pronto per essere utilizzato.
In base alla legislazione vigente sull'interoperabilità della firma digitale il file sottoscritto conserva il suo nome originale, al quale viene aggiunta l'estensione "p7m". Ne risulta che il file *mensa.pdf*, dopo la sottoscrizione, diverrà *mensa.pdf.p7m* e come tale sarà fruito da altre applicazioni([12]).

13.2 Firma digitale con procedure automatiche

In numerose situazioni il procedimento di sottoscrizione può coinvolgere un elevato numero di documenti. Non è quindi efficiente in tali procedimenti l'utilizzo della sottoscrizione "documento per documento", quanto meno perché ogni sottoscrizione richiede la digitazione del PIN di sblocco della smart card di firma.
E' perfettamente legale l'utilizzo di procedure automatiche di sottoscrizione, purché ci si attenga a particolari cautele indicate anche dalla legislazione vigente che i Certificatori ben conoscono.

---

[12] Attenzione a non confondere la firma di un file pdf in formato pkcs#7con la firma pdf. Quest'ultima non modificherà l'estensione del nome del file che rimarrà sempre "pdf".

In particolare, è necessario che quando il titolare appone la sua firma mediante una procedura automatica utilizzi una coppia di chiavi diversa da tutte le altre in suo possesso. Questo per identificare immediatamente, in fase di verifica, il fatto che è stata utilizzata una procedura automatica. Per motivi analoghi, ogni dispositivo di firma utilizzato per procedure automatiche deve disporre di coppie di chiavi differenti, una per dispositivo, anche se il titolare è sempre lo stesso.
L'utilizzo di dispositivi di firma particolari denominati HSM (*Hardware Security Module*) garantisce migliori prestazioni rispetto alle smart card (o token usb). E' anche possibile utilizzare particolari applicazioni che consentono di digitare il PIN una sola volta a fronte della sottoscrizione di più documenti, garantendo comunque una chiara informativa circa la natura ed il numero dei documenti che verranno automaticamente sottoscritti.

14. La procedura di verifica

La procedura di verifica della firma digitale apposta ad un documento informatico consiste sostanzialmente nel verificare che:

1. il documento non sia stato modificato dopo la firma;
2. il certificato del sottoscrittore sia garantito da una Autorità di Certificazione (CA) inclusa nell'Elenco Pubblico dei Certificatori;
3. il certificato del sottoscrittore non sia scaduto;
4. il certificato del sottoscrittore non sia stato sospeso o revocato.

Per eseguire queste verifiche, oltre che per rendere leggibile il contenuto del documento, sono utilizzati specifici software. Detti software sono forniti dai certificatori ai titolari dei certificati; coloro che non sono dotati di un kit di firma digitale possono altresì utilizzare dei software disponibili per uso personale a titolo gratuito: attualmente ne sono stati segnalati otto. Detti software freeware sono stati resi disponibili dal CNIPA (FCMT) stesso e da altre società indicate sul sito del CNIPA .
Per eseguire la verifica non è necessario disporre di smartcard e lettore, in sintesi non si deve essere necessariamente dotati del kit di firma digitale.
Per eseguire le verifiche di cui ai punti 1, 2 e 3 è sufficiente essere dotati di un personal computer, di un prodotto utile per la verifica, piuttosto che del collegamento ad Internet per la verifica con prodotti *web based*. Per la verifica al punto 4 è necessario avere accesso ad Internet. Difatti, i software di verifica si collegano alla lista di revoca dove il certificatore che ha emesso il certificato qualificato renderà disponibili le eventuali informazioni relative alla sospensione o revoca del certificato.
Per la verifica al punto 2 è necessario che sui software installati sul client siano stati caricati i certificati di certificazione dei soggetti iscritti nell'elenco pubblico.
A tale scopo, nel caso in cui i software forniti non abbiano già i certificati delle CA caricati, è necessario scaricare dal sito preposto ([13]) l'elenco pubblico che contiene detti certificati e procedere alla loro installazione.
La procedura descritta è realizzata con il coinvolgimento dell'utente o in maniera completamente automatica dai software forniti dai certificatori, con la sola necessità di disporre di una connessione a *Internet* per la verifica della revoca, che deve necessariamente basarsi su informazioni molto aggiornate, e quindi disponibili esclusivamente in rete. E se la connessione ad *Internet* non è disponibile? Non implica che non possiamo effettuare la verifica, potremo sempre verificare l'integrità del documento, il tipo di firma, l'identità del sottoscrittore. Dobbiamo solo tener presente che non abbiamo potuto verificare una eventuale revoca a sospensione ed agire di conseguenza.

E' possibile vi siano altre verifiche non effettuabili in modalità automatica. In particolare, un certificato può avere dei limiti di validità dipendenti dalla natura del documento sottoscritto; a titolo di esempio, è possibile che un certificato qualificato garantisca la validità della firma a meno che essa non venga utilizzata per sottoscrivere contratti che coinvolgono transazioni monetarie che eccedono un limite stabilito dal certificatore. La firma di un contratto al di fuori di tali condizioni è considerata non valida, cioè corrisponde a mancata sottoscrizione. Limiti di questo tipo non sono verificabili in maniera automatica, e richiedono all'utente di porre attenzione ad eventuali note che, comunque, sono sempre incluse nel certificato relativo alla firma che si sta verificando.

[13] L'elenco è disponibile sul sito CNIPA all'indirizzo http://www.cnipa.gov.it/site/_files/lista%20dei%20certificati.html

14.1 Esempio di verifica sul client

Per rendere evidente che la procedura di verifica è in realtà molto più complessa da descrivere che da eseguire, in questo paragrafo viene riportato un processo di verifica effettuato con il prodotto FCMT.
Ipotizziamo quindi di aver ricevuto il documento "mensa.pdf.p7m" sottoscritto con firma digitale.

Puntando il documento con il mouse e premendo il tasto destro, si seleziona verifica (figura 13.1) o, in alternativa, si apre semplicemente il documento con un doppio click.

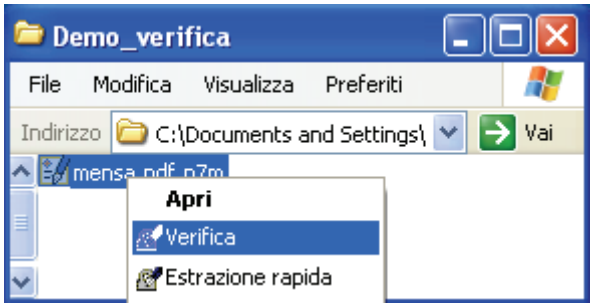


Figura 13.1 – Apertura del file in modalità verifica -

L'applicazione ci presenta subito una finestra dalla quale è possibile evincere che la firma è corretta: non è stato quindi modificato dopo essere stato firmato.
Abbiamo quindi assolto la verifica descritta al punto 1 del precedente paragrafo (figura 13.2).

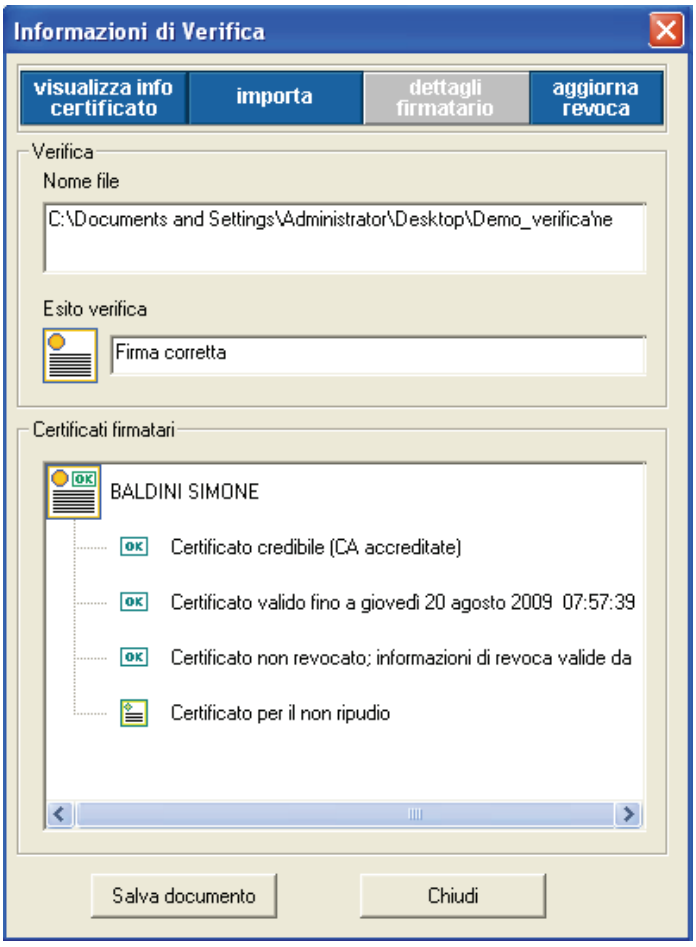


Figura 13.2 – Rapporto del software di verifica -

Per verificare che il certificato sia garantito da una CA autorizzata e non sia scaduto (verifiche 2 e 3) selezioniamo "visualizza info certificato".
Viene aperta la finestra mostrata in figura 13.3 dove si evince che il certificato del Titolare è valido in quanto tale periodo va dal 21 maggio 2007 al 20 agosto 2009, ed è credibile in quanto è stato verificato che lo stesso è sottoscritto, e quindi garantito, da una CA nota.

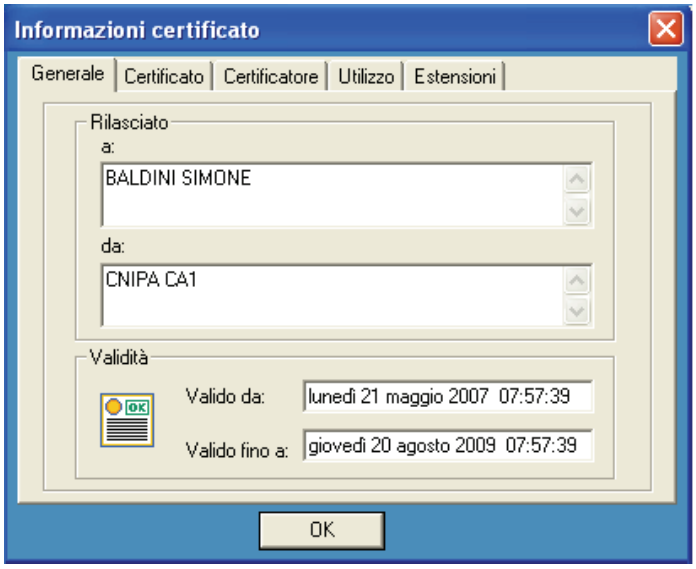


Figura 13.3 – Informazioni sul certificato del sottocrittore –

Cliccando, dalla finestra in figura 13.2, "aggiorna revoca", il prodotto di verifica si collega al certificatore per verificare lo stato del certificato del titolare.
Viene riproposta la finestra in figura 2 dove è evidente che alle ore 15:55:12 del 23 luglio 2007, il certificatore ha provveduto ad aggiornare le informazioni di revoca e che il certificato verificato non risulta essere revocato (o sospeso). Verifica al punto 4 eseguita!

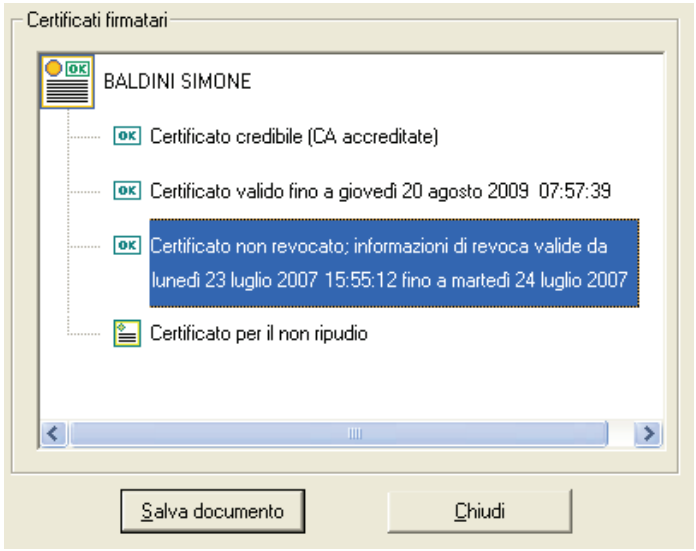


Figura 13.4 – Rapporto software di verifica: dettaglio revoca –

A questo punto sappiamo che la sottoscrizione del documento in questione è perfettamente valida, sappiamo chi ha sottoscritto il documento (vedi figura 13.2), e possiamo procedere a salvare copia del documento nel formato originale per la visualizzazione.
Selezionando quindi "Salva documento" dalla finestra principale (figura 13.2) ci viene chiesto (figura 13.5) dove salvare il documento a cui viene tolta la firma digitale.

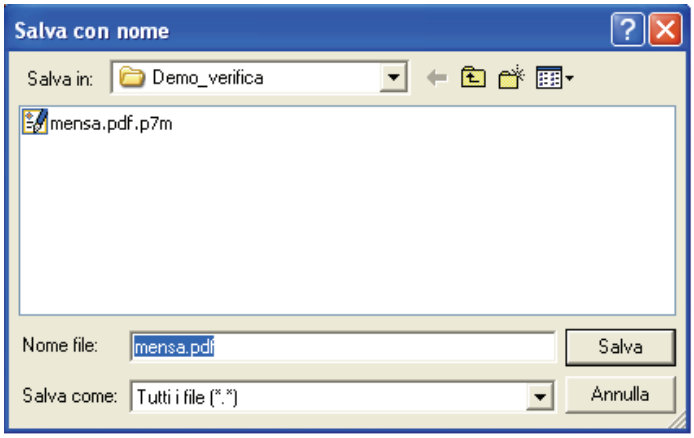


Figura 13.5 – Salvataggio del file estratto –

Sarà quindi necessario ricordare che il documento da conservare con le cure del caso è quello inizialmente ricevuto, quello che contiene la firma digitale, riconoscibile dall'estensione "p7m".

Altri prodotti possono ovviamente avere un'interfaccia grafica diversa, modalità operative peculiari, fermo restando che devono possedere funzionalità atte ad eseguire le verifiche descritte precedentemente.

14.2 Procedure automatiche di verifica

Nel caso in cui un soggetto realizzi un servizio in rete che prevede l'invio da parte degli utilizzatori di oggetti sottoscritti con firma digitale ovviamente non sarebbe consono utilizzare il processo di verifica manuale descritto precedentemente. Sarebbe quindi necessario realizzare una integrazione dell'applicativo destinato alla gestione di suddetto flusso informatico con funzioni di verifica delle rispettive firme digitali. Sono disponibili sul mercato diverse soluzioni che vanno da prodotti specifici le cui funzioni possono essere richiamate da altri applicativi, a librerie e macro specifiche da integrare direttamente nell'applicativo proprietario. Tanto i certificatori che *system integrator* possono essere d'aiuto per tali esigenze.

15. La procedura di firma in formato PDF

Per poter sottoscrivere digitalmente documenti in formato pdf anche in questo caso è necessario disporre del kit di firma digitale acquistabile presso uno dei certificatori accreditati iscritti nell'elenco pubblico, sebbene non si utilizzerà il software di firma. Ciò perché per rispettare la normativa vigente dovremo comunque utilizzare il dispositivo sicuro (smart card o token USB) ma, al posto del software fornito dal certificatore utilizzeremo un prodotto software in grado di processare e produrre file PDF contenenti firme digitali conformi alle specifiche (http://www.adobe.com/devnet/pdf/pdf_reference.html) ISO 32000 .

In considerazione della sua diffusione, nei seguenti paragrafi verrà spiegato come utilizzare i prodotti della famiglia Acrobat (versioni Professional e Reader) illustrando le procedure da seguire per l'apposizione e la verifica di firme digitali. Ciò non toglie che il cittadino è libero di scegliere di utilizzare prodotti diversi purché essi generino file conformi alla normativa di riferimento.

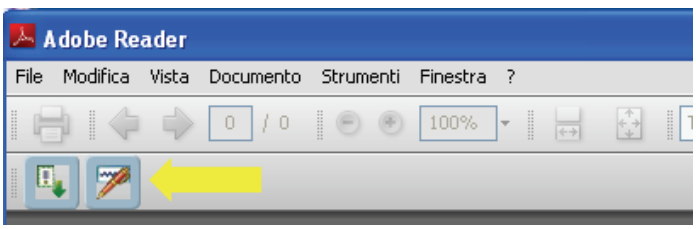
15.1 Firma digitale PDF: preparazione dell'ambiente

Prima di poter utilizzare l'Acrobat o il Reader per l'apposizione e la verifica di firme, è necessario impostare alcuni loro parametri([14]):

La prima operazione sarà quella di installare l'add-on (modulo) gratuito rilasciato da Adobe Systems Italia e scaricabile dal sito http://www.adobe.it/firmadigitale.
Questo strumento è indispensabile poiché consente di predisporre correttamente l'Adobe Reader e l'Adobe Acrobat per la fruizione delle firme digitali nel pieno rispetto della normativa vigente.
L'add-on è compatibile solo a partire dalla versione 7 del Reader e dell'Acrobat.

Figura 14.1 – Download del plug-in–

Dopo l'installazione del modulo potremmo notare l'aggiunta di due pulsanti alla barra degli strumenti del Reader e dell'Acrobat (figura 14.2).



[14] Quanto segue è stato realizzato usando la versione 8.

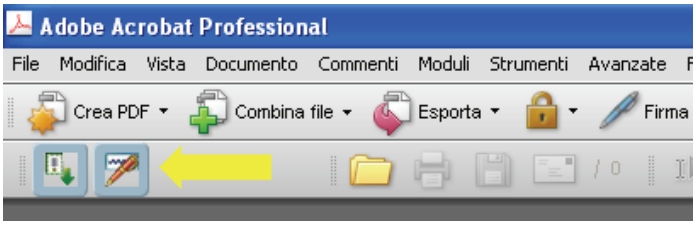


Figura 14.2 – Aggiunta del plug-in al Reader e al Professional –

Il primo dei due, evidenziato nella figura qui accanto, serve per installare nel Reader o nell'Acrobat l'Elenco Pubblico dei Certificatori Accreditati al CNIPA (figura 14.3). Dopo averlo cliccato ci verrà proposta una pagina che illustrerà passo dopo passo la procedura da seguire per l'installazione dell'Elenco Pubblico (in questa fase è necessaria la connessione Internet).
Il secondo pulsante invece è utilizzato solo in fase di verifica e quindi verrà trattato nel successivo capitolo.

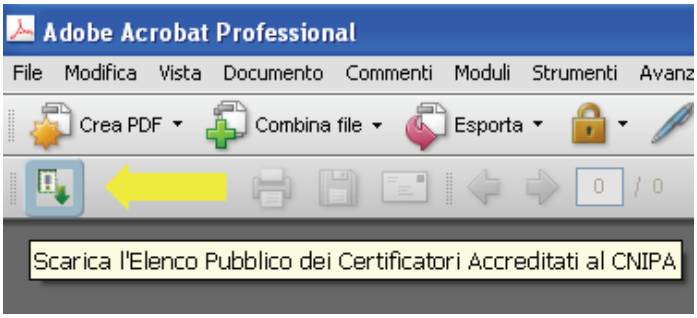


Figura 14.3 – Pulsante per l'istallazione dell'Elenco Pubblico –

La prossima operazione che eseguiremo ha lo scopo di consentire al software di Adobe di riconoscere ed utilizzare correttamente la smart card che utilizzeremo per firmare i documenti.
Per far ciò occorre aprire il gestore di certificati digitali del Reader o dell'Acrobat scegliendo dalla barra dei menù il menù Documento > quindi la voce Impostazioni di protezione oppure, alternativamente, il menù Avanzate > quindi la voce Impostazioni di protezione (figura 14.4)

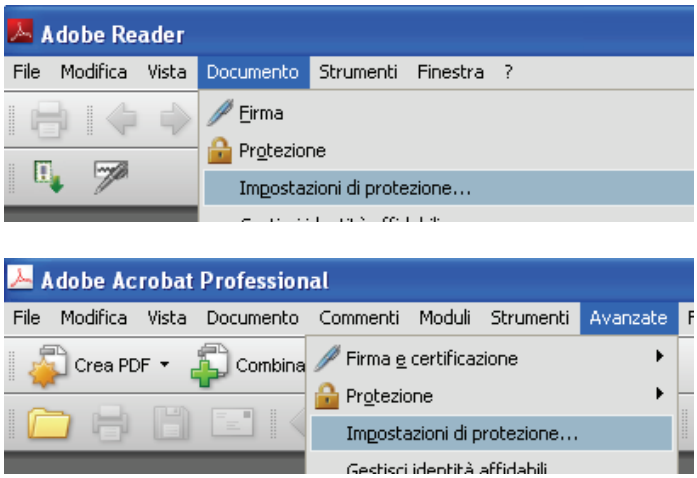
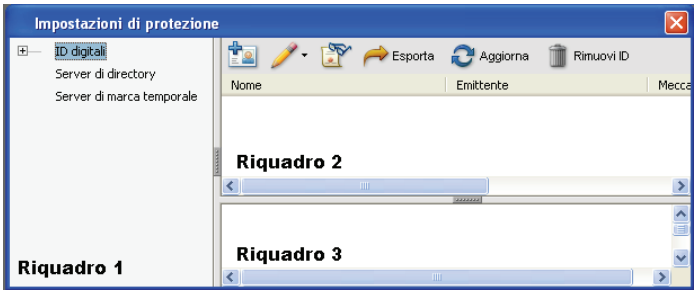


Figura 14.4 – Apertura del gestore dei certificati –

Ci verrà proposta una schermata come quella riportata qui accanto che per comodità da qui in poi considereremo suddivisa in 3 riquadri.
All'interno di essa andremo a scegliere ID digitali > Moduli e token PKCS#11 dopo di chè selezionando il pulsante Aggiungi modulo potremo navigare le nostre cartelle alla ricerca delle librerie della smart card caricate al momento dell'installazione del kit acquistato. Tali librerie si trovano normalmente nella cartella C:\WINDOWS\system32 e devono essere selezionate per indicare ad Acrobat o al



Reader il tipo di smart card che si sta utilizzando.

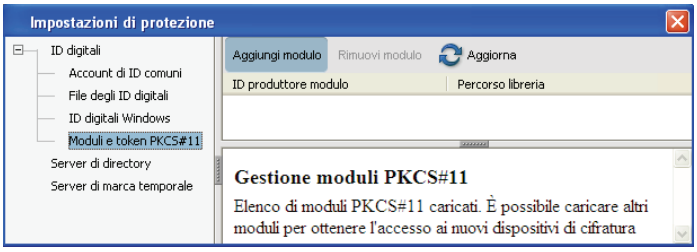
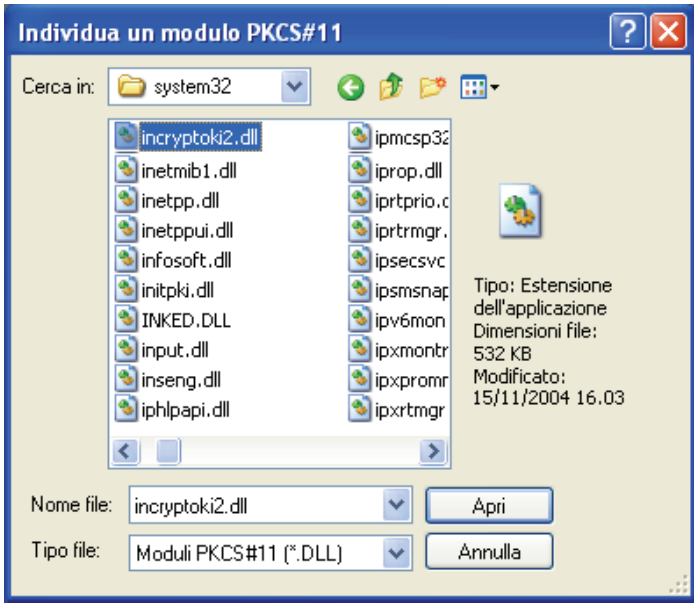


Figura 14.5 – Selezione del certificato di firma : Scelta della smart card –

Si tratta di file ".dll" i quali hanno un nome predeterminato che normalmente può essere recuperato richiedendolo al certificatore che ci ha fornito il kit.
Ad esempio nella figura accanto viene selezionato ed utilizzato il file **incryptoki2.dll.**
Dopo aver selezionato il file in questione, nel riquadro 2 di figura 14.5 comparirà un entry contenente il nome della smart card ed il percorso utilizzato per far riferimento alla libreria sopracitata (figura 14.6) .
Non ci resta ora che andare nel riquadro 1 e cliccare due volte sulla voce Moduli e token PKCS#11 per visualizzare il token nel quale sono memorizzate le nostre credenziali di firma (chiave privata e certificato) e selezionarlo.
Dopo aver effettuato doppio click sul token in questione ed inserito il PIN della smart card le nostre credenziali di firma verranno automaticamente ritrovate dal Reader o dall'Acrobat ed inserite nell'elenco degli ID digitali nel riquadro 2 (figura 14.8) . Saremo comunque obbligati al reinserimento del PIN ogni volta che tenteremo utilizzarle per apporre una firma.



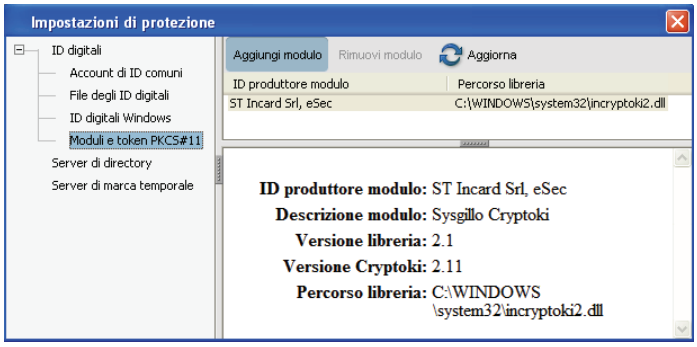


Figura 14.6 – Selezione del certificato di firma : Scelta del file *.dll* relativo alla smart card fornita –

Figura 14.7 – Selezione del certificato di firma : Scelta della smart card –

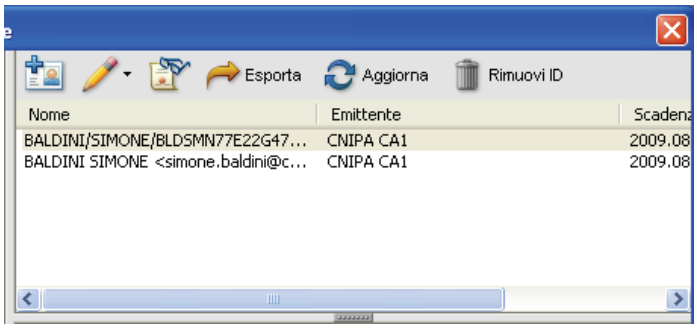


Figura 14.8 – Selezione del certificato di firma : Visualizzazione dei certificati della smart card –

Ora che abbiamo predisposto correttamente il nostro software Adobe per la verifica e la sottoscrizione di documenti pdf secondo la normativa vigente passiamo quindi vedere come apporre e verificare firme digitali.

15.2 Esempio di firma digitale in Adobe Acrobat

La sezione che segue spiega come utilizzare il software Adobe Acrobat per apporre firme digitali a documenti pdf.
Supponiamo di voler firmare il file denominato "mensa.pdf":

1. Apriamo il documento in questione con Acrobat e alla barra degli strumenti Firma selezioniamo la voce Apponi firma… (vedi figura).
2. Inseriamo la smart card nel lettore e dopo aver cliccato sul pulsante ok, nel messaggio che ci viene proposto, andiamo a tracciare nel documento il riquadro che conterrà la nostra firma.
3. Fatto ciò, ci verrà proposta una finestra come quella riportata qui a fianco. Qui selezioneremo il nostro certificato di firma all'interno del campo ID digitale ed inseriremo, all'interno del campo Password, il PIN necessario al suo utilizzo.
4. Per produrre file conformi alla normativa vigente è indispensabile che in questa fase venga selezionato il certificato di firma, recante la dicitura "Firma documento" (vedi figura).
   Una volta inserito il PIN e cliccato sul pulsante Firma il documento verrà firmato e salvato.

A questo punto la procedura di firma è completata.

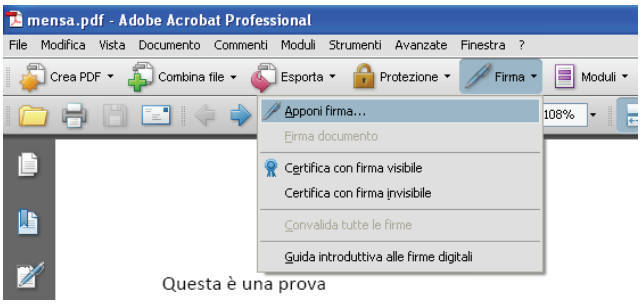


Figura 14.9 – Selezione voce : Apponi firma… –

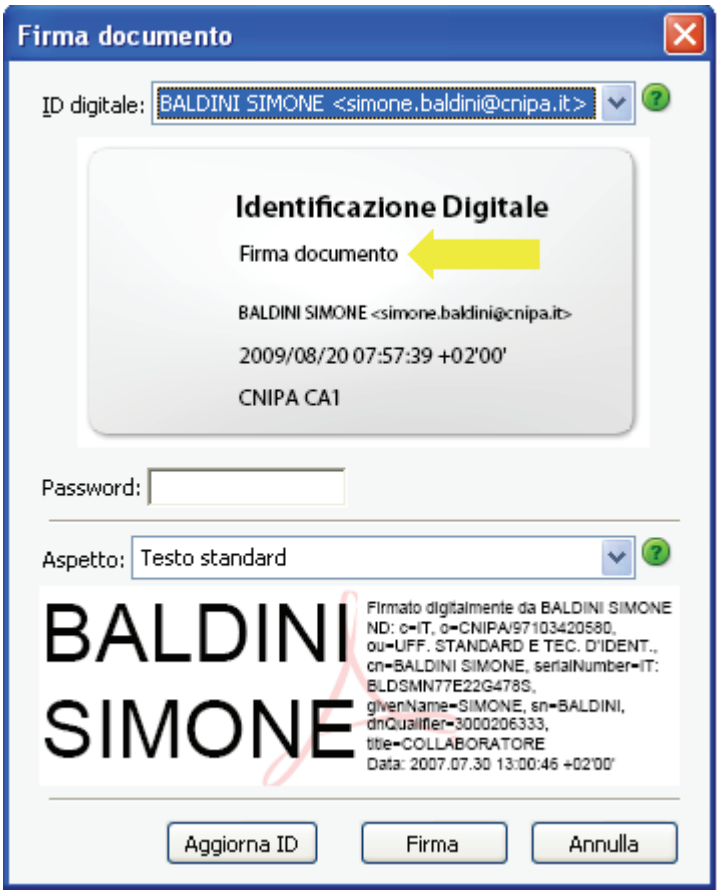


Figura 14.10 – Scelta del certificato di firma e immissione PIN –

15.3 Esempio di firma digitale in Adobe Reader

La procedura di firma di documenti pdf tramite Reader è simile a quella utilizzata con l'Acrobat

ma, rispetto a questa, presenta una differenza sostanziale rappresentata dal fatto che è possibile sottoscrivere solo documenti precedentemente abilitati.
Anche qui supponiamo di voler firmare il file "mensa.pdf"
Per capire se esso è stato abilitato o meno basta controllare che nella barra degli strumenti sia presente il pulsante Firma e che la voce Apponi firma... sia selezionabile (vedi figura seguente)

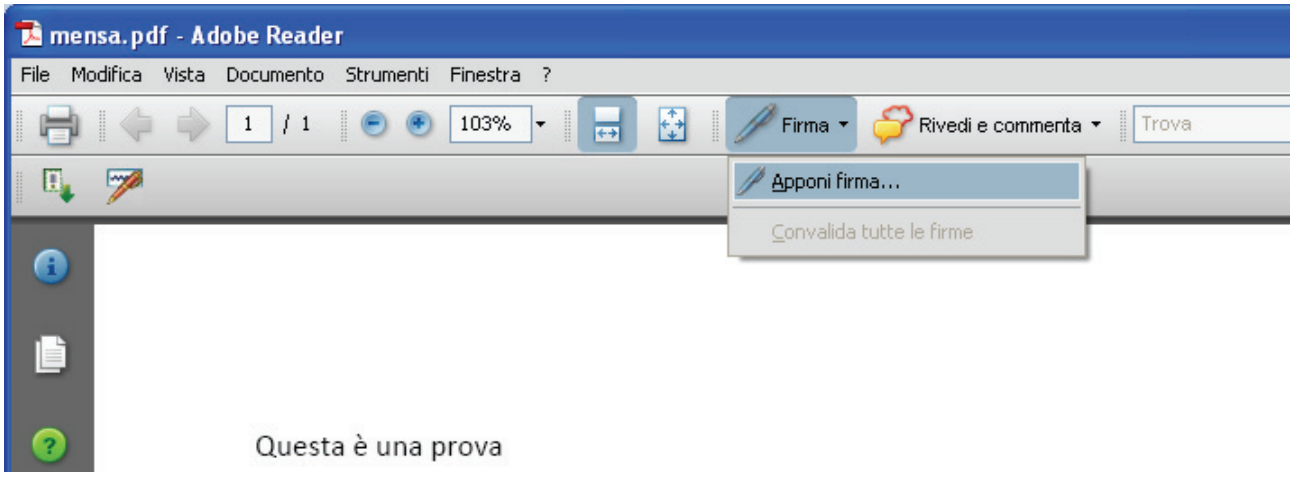


Figura 14.11 – Selezione voce : Apponi firma... –

A questo punto le alternative sono due:

1. Il documento contiene uno o più campi firma vuoti contraddistinti dal seguente simbolo .
   Inseriamo la smart card nel lettore e clicchiamo sul campo firma.
   Ci verrà quindi proposta la finestra per la scelta del certificato e da qui sarà sufficiente seguire le indicazioni riportate ai punti 3 e 4 del paragrafo precedente.
2. Il documento **non** presenta campi firma.
   In quest'ultimo caso non occorre replicare l'intera procedura di firma descritta al paragrafo precedente.

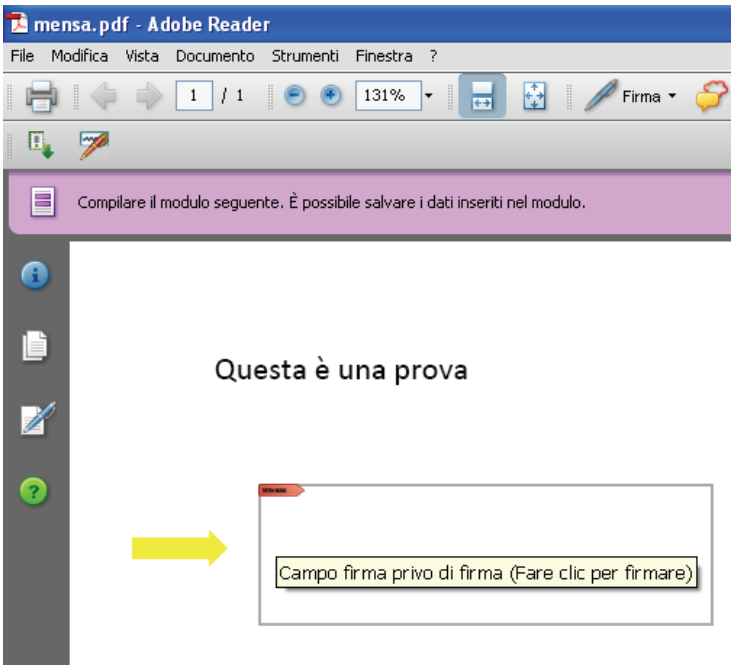


Figura 14.12 – Documento PDF con campo firma vuoto –

16. La procedura di verifica in formato PDF

La verifica della firma di documenti pdf è un operazione molto più difficile da descrivere che da eseguire
Supponiamo di voler verificare il file denominato "mensa_firmato.pdf".

Una volta aperto il documento la prima operazione da eseguire sarà quella di localizzare le sue firme.
Esse presentano un aspetto come quello riportato qui accanto e, normalmente, contengono al loro interno il nome del firmatario ed un simbolo rappresentante l'esito della verifica.

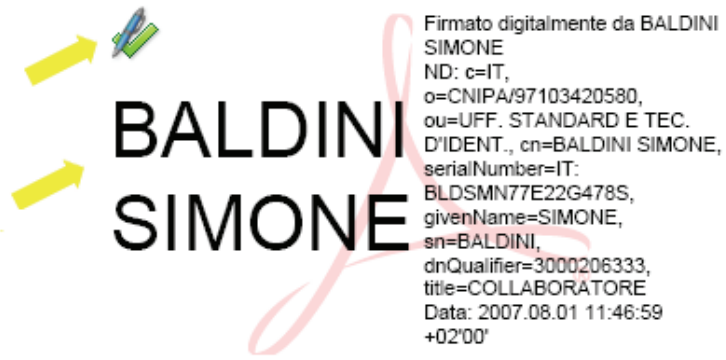


Figura 15.1 – Aspetto della firma –

Clicchiamo sopra la firma ed analizziamo la finestra che ci viene proposta.
Da essa possiamo ottenere informazioni riguardanti sia il firmatario e sia le eventuali modifiche occorse dopo l'apposizione della firma.

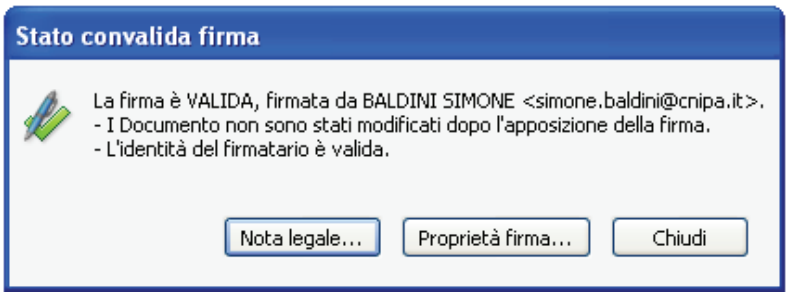


Figura 15.2 – Rapporto sintetico sulla verifica –

Proseguiamo cliccando il pulsante Proprietà firma... e prestiamo attenzione alla finestra successiva.
Attraverso essa andremo a verificare che:

1. il documento non sia stato modificato dopo la firma;
2. il certificato del sottoscrittore sia garantito da una Autorità di Certificazione (CA) inclusa nell'Elenco Pubblico dei Certificatori;
3. il certificato del sottoscrittore non sia scaduto;
4. il certificato del sottoscrittore non sia stato sospeso o revocato.

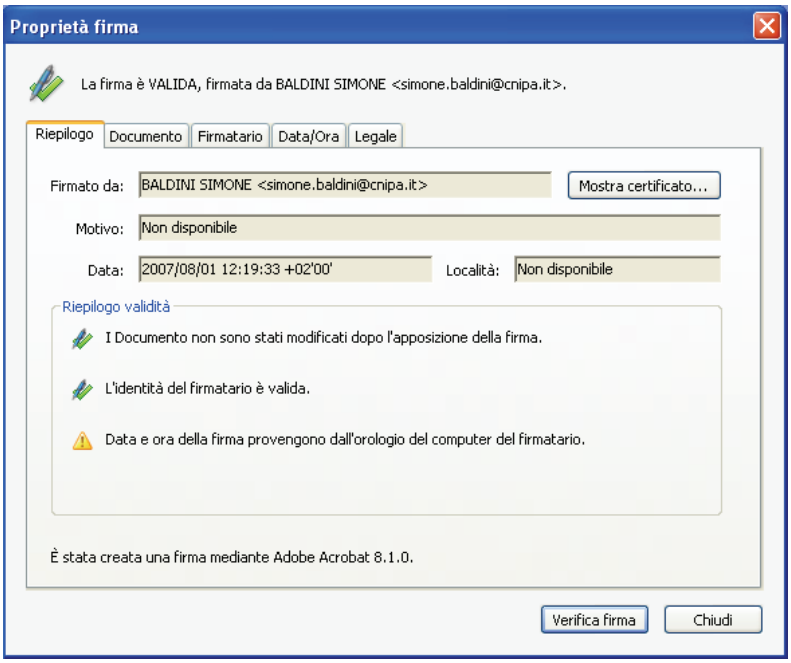


Figura 15.3 – Finestra di verifica : Riepilogo –

La finestra presenta 5 schede nelle quali possiamo recuperare tutte le info che ci servono per eseguire i controlli sopracitati.
Nella seconda delle cinque, quella denominata Documento, possiamo chiaramente vedere, come evidenziato, che il documento non ha subito modifiche dopo essere stato firmato.

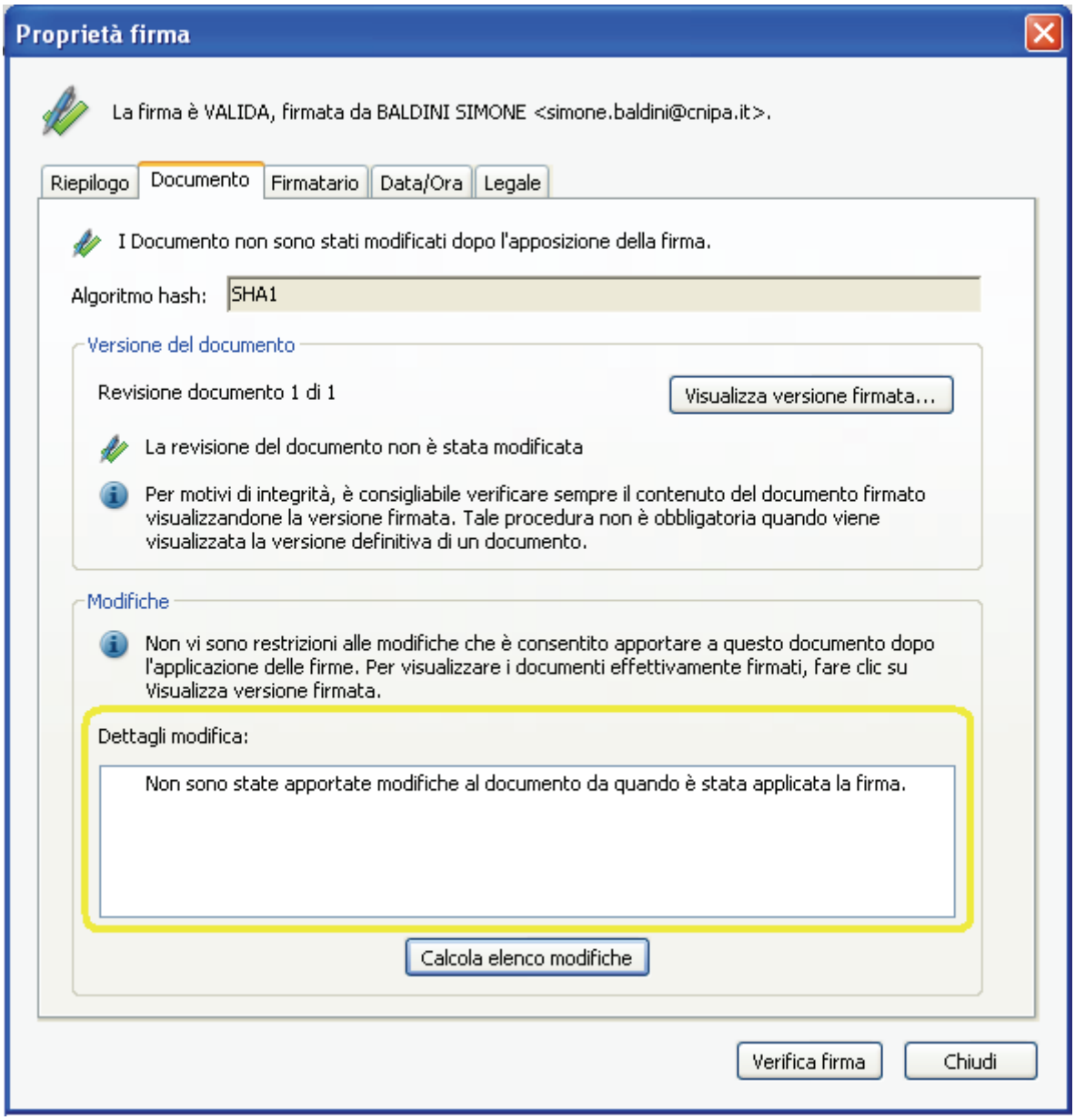


Figura 15.4 – Finestra di verifica : Verifica integrità del documento –

Abbiamo quindi assolto la verifica descritta al punto 1 del precedente elenco (figura 15d).
Procediamo quindi ad effettuare le rimanenti verifiche

Selezionando invece ora la scheda denominata Firmatario e concentrandoci sul riquadro Dettagli validità, possiamo effettuare il resto dei controlli.
In particolare possiamo verificare che:

1. Il certificato del sottoscrittore è emesso da una CA inclusa nell'elenco pubblico (primo punto)
2. Il certificato del sottoscrittore non è scaduto e non è stato neanche revocato (terzo terzo punto)

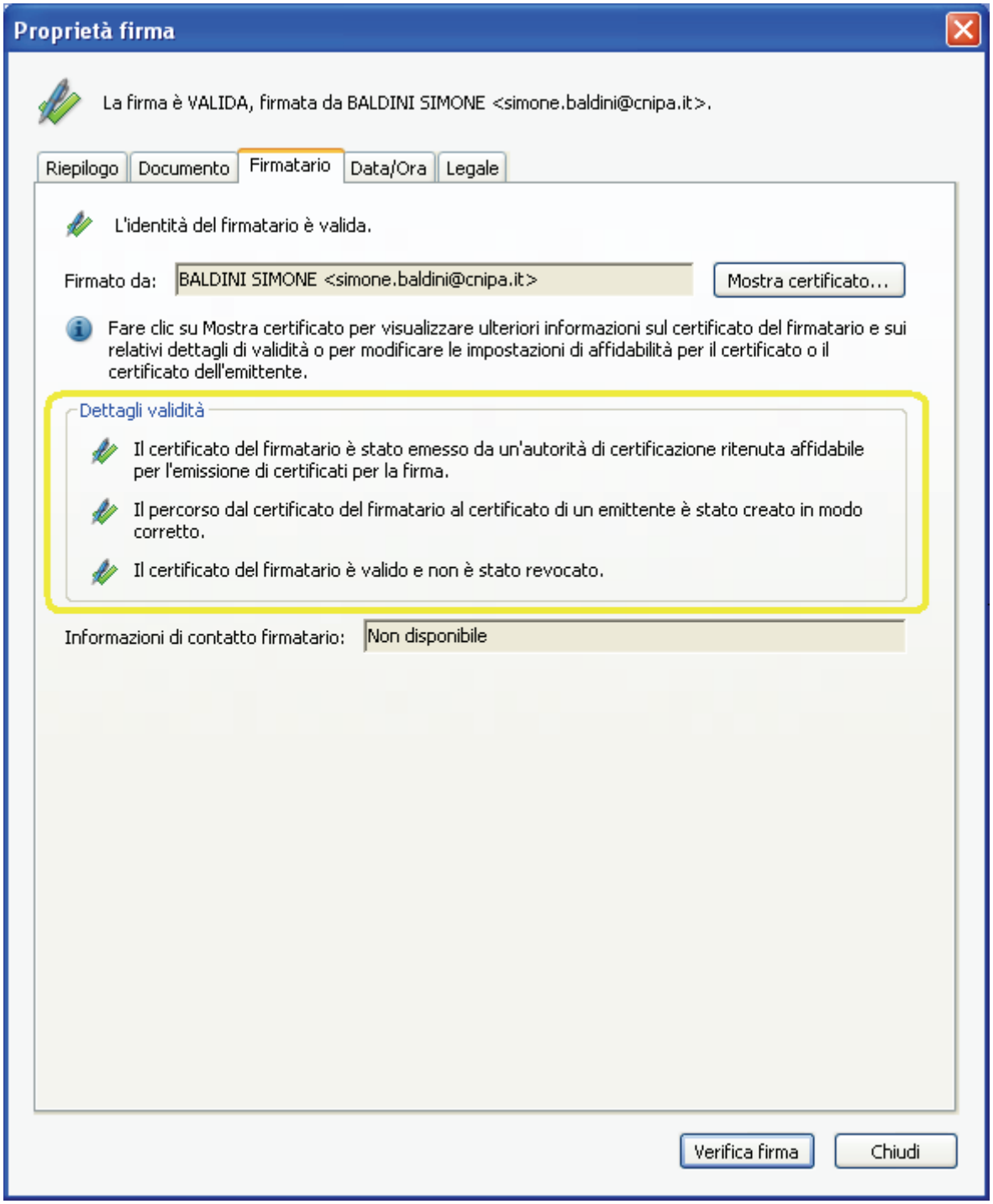


Figura 15.5 – Finestra di verifica : Verifica del certificato e della CA emittente –

A questo punto sono state effettuate anche le verifiche ai punti 2,3 e 4 e sappiamo quindi che la sottoscrizione è perfettamente valida.

17. Le nuove regole tecniche, il DPCM 30 marzo 2009

Il Decreto del Presidente del Consiglio dei Ministri 30 marzo 2009 abrogherà, sostituendolo, il DPCM 13 gennaio 2004. Il decreto contiene le regole tecniche inerenti l'intero impianto della firma digitale: algoritmi usati, requisiti dei certificatori, obblighi degli utenti, formati di firma, formato e semantica dei certificati, ecc.
Ma vediamo quali sono le modifiche più interessanti apportate con questo nuovo decreto([15]).

Articolo 1
Le definizioni sono state armonizzate con il CAD, eliminando quelle già presenti.
Da notare la definizione per "Dati per la creazione della firma" il cui obiettivo è quello di riferirsi, con tale locuzione, all'insieme degli elementi PIN e chiave privata.
Questa modifica concorre a raggiungere l'obiettivo descritto al seguente articolo 7.

Articolo 3
Stabilisce che le regole tecnologiche, che per loro natura debbono poter essere modificate rapidamente, saranno definite attraverso provvedimenti più rapidi, identificati in deliberazioni del CNIPA.
A titolo esemplificativo, pensiamo alla lunghezza delle chiavi di sottoscrizione, attualmente 1024 bit. Il giorno in cui queste chiavi non saranno più adeguatamente sicure si dovrà imporre un rapido cambiamento, incompatibile con i tempi necessari per l'emanazione di un nuovo decreto.
Per tale ragione tutti gli elementi tecnologici saranno emanati dal CNIPA con appositi provvedimenti che possono essere emanati in tempi rapidi.

Articolo 7
Con le modifiche apportate si vuole rendere possibile al certificatore qualificato di conservare le chiavi private dei titolari (quelle usate per l'operazione di generazione della firma digitale) su dispositivi sicuri per la generazione della firma particolari (gli HSM) situati presso di loro, all'interno di locali adeguatamente protetti. Nel contempo si garantisce che il certificatore, a seguito della generazione della firma, non possa venire a conoscenza degli atti o fatti oggetto della sottoscrizione, garantendo nel contempo che esclusivamente il titolare della chiave possa attivarne l'uso.
In questo modo si svincolerà l'uso della firma digitale alla disponibilità in locale di un apposito applicativo (potrà essere disponibile in rete) e di un apposito hardware (non sarà necessario disporre di un lettore). A tale scopo si agisce, oltre che sull'articolo 7, anche sull'articolo 1 comma 1 lettera e) ed articolo 9 comma 2 .
La ratio è che dipendentemente dalle caratteristiche del certificato([16]) sia possibile modulare i requisiti di sicurezza: se usiamo un certificato con forti limiti d'uso può essere sufficiente una connessione protetta con autenticazione con userid e password mentre, in assenza di limitazioni, sarà necessario mantenere inalterato il concetto di *possesso e conoscenza*, prevedendo oltre a userid e password, l'utilizzo di un sistema OTP([17]) (*possesso*) protetto da PIN (*conoscenza*). E' evidente

[15] Non sono analizzate tutte le modifiche apportate, ma solo quelle ritenute di maggior interesse generale.
[16] Ricordiamo che i certificati di sottoscrizione possono contenere limiti d'uso e/o di valore dei negozi. Possiamo avere quindi un certificato valido solo per la sottoscrizione degli atti derivanti dalla carica ricoperta all'interno dell'organizzazione (anch'esse riportate all'interno del certificato) od anche valido per la sottoscrizione di atti che non comportano oneri finanziari superiori ad un limite monetario prescelto.
[17] One Time Password

che vi dovrà essere un controllo sull'adeguatezza del sistema di autenticazione previsto per ogni singolo caso (vedi articolo 9).

Articolo 9
Con il nuovo comma 3 si stabilisce che il CNIPA, in fase di accreditamento e durante la vigilanza, dovrà verificare l'adeguatezza tecnologica delle modalità di autenticazione in relazione ai dispositivi di firma usati.

Articolo 10
La nuova formulazione consente di garantire un livello minimo di dati presentati obbligatoriamente durante il processo di verifica della firma digitale. Il CNIPA, verificando i prodotti di verifica forniti ai titolari dai certificatori, garantisce tale livello minimo omogeneizzando le caratteristiche di base dei prodotti di mercato.

Articolo 12
E' sancito, quale canale di comunicazione fra CNIPA e certificatore, l'uso della P.E.C., di fatto già utilizzata.

Articolo 14
E' stato inserito il nuovo comma 3 per evitare che si possa creare il paradosso di un certificato di sottoscrizione che ha validità superiore al certificato di certificazione utilizzato dal certificatore per sottoscriverlo.

Articolo 15
Si è inserita la previsione circa l'inserimento di qualifiche del titolare all'interno del certificato, già contenuta nella Deliberazione CNIPA 4/2005, in modo da dare alla stessa una maggiore valenza giuridica. E' formalizzato l'impegno assunto da parte dell'organizzazione che richiede o autorizza l'emissione di un certificato qualificato contenente informazioni quali l'organizzazione di appartenenza ed eventuali titoli posseduti dal titolare del certificato, di richiedere al certificatore la revoca del certificato al modificarsi delle stesse.

In altro comma si ribadisce che è facoltà del certificatore stabilire il periodo di validità del certificato, stabilendo nel contempo che spetta al CNIPA determinare il periodo massimo in considerazione della robustezza delle tecnologie in uso.

Articolo 17
Nell'articolo si ordina l'uso del "codice di emergenza", codice utilizzato dal titolare per farsi riconoscere dal certificatore in casi di particolare urgenza.

Articolo 18
Viene chiarito l'obbligo in capo al certificatore di comunicare l'avvenuta revoca del certificato al titolare dello stesso a prescindere dall'origine della richiesta di revoca.

Articolo 22
Sono state meglio chiarite le azioni da intraprendere e alcuni aspetti nella gestione della sospensione dei certificati qualificati. Si ricorda che la sospensione è uno stato temporaneo del certificato e che i naturali esiti sono o la riattivazione (leggi cessazione dello stato di sospensione) o la definitiva revoca del certificato.

Infine, al comma 6, è chiarito che in caso di cessazione dello stato di sospensione del certificato([18]) il certificato medesimo sarà considerato come mai sospeso. Tale previsione è necessaria in quanto, da un punto di vista tecnico, in tale evenienza le informazioni inerenti l'avvenuta sospensione non sono disponibili online.

Articolo 23
La sospensione effettuata nei casi previsti dalle norme su iniziativa del certificatore deve essere comunicata anche all'eventuale terzo interessato.

Articolo 26
Viene precisato il rapporto temporale tra certificato qualificato e certificato delle chiavi di certificazione.

Articolo 27
Si è provveduto ad armonizzare i commi e ad eliminare alcune previsioni di fatto inapplicabili.

Articolo 28
Stabilito che non è possibile prevedere la certificazione dei sistemi operativi in quanto un semplice innalzamento di release, piuttosto che l'installazione di una correzione, od altri elementi comportano la perdita della certificazione medesima, si richiede di intraprendere azioni atte a migliorare la sicurezza, effettuando il cosiddetto *hardening*([19]), dando al CNIPA, nell'ambito dell'attività di vigilanza (art. 31 CAD), il compito di verificarne l'idoneità.

Articolo 31
Sono stati meglio definiti alcuni degli argomenti contenuti nel piano della sicurezza e riformulata la modalità di consegna eliminando la doppia busta che non rendeva accessibili alcune informazioni che, fra l'altro, erano necessarie in fase di vigilanza.

Articolo 32
Viene chiarito che il "giornale di controllo" può essere costituito da registrazioni effettuate in diverse modalità anche, ma non esclusivamente, automaticamente da dispositivi specifici.
Viene inoltre armonizzato con il CAD il periodo di mantenimento delle stesse (20 anni).

Articolo 34
L'organizzazione del personale e la figura dei responsabili è stata rivista alla luce dell'esperienza maturata. Viene chiarito che in caso di outsourcing i responsabili di quali attività possano non essere dipendenti del certificatore.

Articolo 35
Si riformulano i requisiti di esperienza professionale necessari per assumere le cariche di "responsabili" previste dall'articolo 34.

Articolo 37
I riferimenti temporali opponibili ai terzi, già previsti dal precedente articolo 39, sono resi fruibili a chiunque: non si comprendeva infatti perché i riferimenti temporali ottenuti con la Posta Elettronica Certificata e derivanti dalla segnatura di Protocollo (ad opera della PA) e quelli derivanti dalla

[18] Avviene, su richiesta del titolare, quando non sussistono più dubbi circa eventuali problemi di sicurezza (furto, smarrimento, uso improprio, ecc.)
[19] Va precisato che tale attività era già svolta dai certificatori, come si è potuto verificare in fase di vigilanza.

procedura di conservazione documentale (ad opera di un pubblico ufficiale o di una PA) potessero essere utilizzati solo dalle pubbliche Amministrazioni. E' stato inoltre previsto, quale riferimento temporale opponibile ai terzi, il riferimento temporale ottenuto attraverso la "marca postale elettronica" in considerazione dell'avvenuta pubblicazione([20]) del DM 21 gennaio 2008.

Articolo 39
Si ridefinisce, alla luce dell'esperienza maturata, il contenuto dell'elenco pubblico dei certificatori.

Si da compito al CNIPA di definire in una propria deliberazione il formato dell'elenco pubblico([21]).

Si elimina la limitazione circa la sottoscrizione con firma digitale dell'elenco pubblico consentendo la sottoscrizione dello stesso anche con altre tipologie di firme elettroniche. Nulla cambia da un punto di vista di sicurezza in quanto trattasi di una firma particolare eseguita in ambiente protetto e con adeguati dispositivi hardware.

Articolo 41
Si indica, chiarendolo, il provvedimento con il quale sono indicate le modalità per inserire eventuali limiti d'uso o di valore nel certificato, difatti una loro rappresentazione libera sarebbe ingestibile in sede di verifica.

Articolo 43
Si chiarisce che è possibile apporre una marca temporale ad un documento informatico che contiene un'insieme di impronte. In pratica, avendo la necessità di apporre un riferimento temporale opponibile ai terzi a *N* documenti, anziché richiedere *N* marche (e pagare *N* marche) si può realizzare un documento contenente le impronte degli *N* documenti e quindi richiedere una sola marca temporale.

Articolo 49
Considerato che il Codice (CAD) prevede la conservazione degli elementi utili in sede processuale per un periodo di venti anni, si armonizza tale previsione stabilendo che anche le marche temporali debbano essere conservate dal certificatore per lo stesso periodo (prima erano 5 anni). Si ricorda che le marche temporali sono valide per l'intero periodo di conservazione a cura del certificatore.

Articolo 51
Questo articolo ribadisce che la firma digitale continua ad essere valida purché la sua esistenza sia collocabile, con un riferimento temporale opponibile ai terzi, in un determinato momento precedente alla sopravvenuta invalidità([22]) del certificato qualificato.

Articolo 52
Premesso che in caso di cessazione dell'attività da parte di un certificatore è necessario garantire la disponibilità e la conservazione della documentazione afferente detta attività, per il periodo previsto già nel CAD (20 anni), considerato che negli altri paesi europei tale attività è posta in capo all'organismo di vigilanza, l'articolo stabilisce che in tale situazione sia compito del CNIPA farsi carico di conservare detta documentazione.

---

[20] Pubblicato, per comunicato, nella Gazzetta Ufficiale 28 marzo 2009, n. 73.
[21] Si veda il capitolo 18. LA FIRMA DIGITALE E L'EUROPA per ulteriori informazioni.
[22] Scadenza, revoca e sospensione.

18. La firma digitale e l'Europa

La Direzione Generale Internal Market della Commissione europea ha costituito un "expert group" per l'implementazione della Direttiva europea 123/2006, comunemente nota come "Direttiva Servizi". Ricordiamo che, per quanto concerne questa guida, lo scopo della Direttiva Servizi è il libero scambio a livello comunitario di documenti sottoscritti con firma digitale.
Da tale precetto deriva la necessità di raggiungere l'interoperabilità nella verifica delle firme digitali.
Per il raggiungimento dell'obiettivo è necessario realizzare un sistema che consenta di:

1. condividere nella Comunità le informazioni inerenti i certificatori che emettono certificati qualificati;

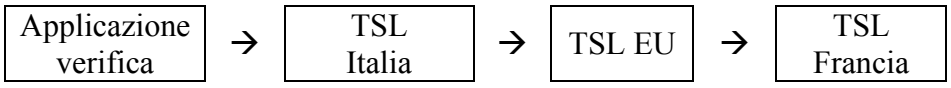
2. interpretare correttamente i certificati di sottoscrizione in modo da comprenderne la tipologia, comprendere se una determinata firma digitale presuppone l'utilizzo di un dispositivo sicuro per la generazione della firma;

3. stabilire quali formati di firma potranno essere utilizzati.

In questo modo sarà possibile il libero scambio (e la verifica) di documenti informatici sottoscritti con firma digitale.

Il termine posto dalla Commissione è il 20 dicembre 2009.

Al mese di marzo 2009 i 27 Stati membri anno raggiunto un accordo formale e tecnico sul primo punto. L'obiettivo sarà raggiunto con la realizzazione di una TSL (Trust Service Status List) nazionale che conterrà le informazioni inerenti i certificatori qualificati([23]) presenti nel proprio territorio. La TSL è stata realizzata sulla base dello standard ETSI TS 102 231 apportando le necessarie modifiche. L'ETSI è stato quindi coinvolto per la realizzazione di una nuova versione dello standard che recepisca le esigenze della Comunità.
La TSL conterrà anche l'indirizzo internet ove la Commissione manterrà la propria TSL. Questa conterrà esclusivamente gli indirizzi ove sono disponibili le TSL dei vari Stati membri.
In questo modo durante il processo di verifica di una firma basata su un certificato emesso in altro Stato si potrà raggiungere la corretta lista ove estrarre le informazioni inerenti lo specifico certificatore.



Anche per il secondo e terzo punto i lavori procedono a buon ritmo.
Essendo ancora in corso non si possono fornire indicazioni precise, tuttavia sui formati di firma sembra poter essere raggiungibile una accordo sui seguenti: CAdES, XAdES, e PAdES.

[23] Sono i certificatori che emettono certificati "qualificati". Possono essere soggetti accreditati o solo soggetti alla vigilanza. In Italia, come in numerosi altri stati membri, tali certificatori sono tutti accreditati.

19. Lo strumento "firma digitale" integrato nel processo di e-governement

Fin dalla sua nascita la firma digitale è stata una punta di diamante del Governo Italiano nell'ambito dei processi di semplificazione amministrativa. Infatti la firma digitale è indispensabile nell'automazione dei processi amministrativi, nella gestione informatizzata dei flussi documentali e in tutti quei procedimenti dove si vuole l'eliminazione del documento cartaceo (smaterializzazione del procedimento amministrativo).
Sono ormai numerose le applicazioni che utilizzano la firma digitale nell'ambito della pubblica amministrazione. Queste stanno coinvolgendo le imprese, con l'obbligo di trasmissione telematica dei bilanci alle Camere di Commercio, la pubblica amministrazione, con la piena smaterializzazione dei mandati di pagamento con tutti i flussi firmati digitalmente, i cittadini, con la possibilità già descritta precedentemente di inviare istanze e dichiarazioni alla pubblica amministrazione in modalità telematica.
I professionisti saranno sempre più coinvolti nell'utilizzo della firma digitale per gli atti notarili, gli atti giudiziari nell'ambito del processo telematico e per le dichiarazioni fiscali.

La diffusione della Carta d'Identità Elettronica e della Carta Nazionale dei Servizi non potrà che favorire ulteriormente lo sviluppo e il conseguente utilizzo della firma digitale da parte dei cittadini.

A livello internazionale c'è ancora da lavorare per garantire l'interoperabilità almeno a livello comunitario, ma dopo alcuni scetticismi da parte degli organismi comunitari il processo di regolamentazione è avviato anche in tal senso.

Al momento, in ogni caso ci si può dichiarare soddisfatti, visto che l'Italia, primo paese ad avere introdotto la firma digitale nella propria legislazione, è anche il primo paese a superare la soglia di 120 milioni di documenti sottoscritti l'anno con firma digitale.

Infine è corretto rendere noto che diversi certificatori fanno parte di Assocertificatori che "*ha lo scopo primario di promuovere la pratica della* ***firma digitale*** *e della* ***posta elettronica certificata*** *e, al contempo, di sviluppare la diffusione dei sistemi per l'archiviazione elettronica dei documenti e per la sicurezza informatica.*
L'associazione, a tal fine, garantisce la piena interoperabilità e la massima qualità e sicurezza dei servizi offerti dai propri associati e svolge un costante presidio normativo, a livello giuridico e tecnico, sia in sede nazionale che comunitaria."([24]).

[24] Estratto dal sito www.assocertificatori.org in data 14 aprile 2009.