Università Mediterranea di Reggio Calabria

Facoltà di Giurisprudenza
Corso di Laurea Magistrale in Giurisprudenza

RACCOLTA DI MATERIALE DIDATTICO PER IL CORSO DI DIRITTO DELL'INFORMATICA

Melchiorre Monaca

seminario tecnico

2013/2014

Testi di riferimento

- Alessio Plebe, Melchiorre Monaca
  Introduzione all'informatica delle conoscenze
  Editori Riuniti University Press 2010 - ISBN13: 9788864732152

- Andrew S. Tanenbaum, David J. Wetherall
  Reti di calcolatori - V edizione
  Pearson 2011 - ISBN13: 9788871926407

- DigIt PA - *Guida alla Firma Digitale* - 2009
  `http://www.digitpa.gov.it/sites/default/files/GuidaFirmaDigitale2009_a_0_0_0.pdf`

- DigIt PA - *Firme elettroniche*
  `http://www.digitpa.gov.it/firme-elettroniche-certificatori`

- DigIt PA - *Posta Elettronica Certificata*
  `http://www.digitpa.gov.it/pec`

Indice

Premessa

Con questa raccolta s'intende fornire allo studente una sorta di "traccia", un percorso che guidi lo studio attraverso le tematiche discusse a lezione, trasmettendo il "lessico minimo" indispensabile alla comprensione degli argomenti trattati nel modulo giuridico di questa stessa materia.

È stato evidentemente necessario semplificare - forse ai limiti del lecito - i contenuti qui riassunti: il lettore più interessato alla materia potrà approfondire gli argomenti di suo interesse sui testi di riferimento consigliati e sui lavori originali citati in bibliografia.

Capitolo 1

Reti di calcolatori

Una rete di telecomunicazioni è un sistema che fornisce servizi relativi al trasferimento di informazioni ad una popolazione di utenti distribuiti geograficamente. Le reti di telecomunicazioni sono vicine alla nostra esperienza quotidiana di uomini moderni: basti pensare alla rete telefonica, alla rete postale, alle reti per diffusione radio e TV, alle reti telematiche.

Alcune di queste reti sono di nuova concezione e quindi utilizzano tecnologie avanzate, tipicamente del settore elettronico (e in qualche caso anche della fotonica), mentre altre, come la rete postale, sono state in funzione per quasi due secoli e si basano su strumenti molto più tradizionali, quali i mezzi di trasporto.

Sappiamo inoltre che in tempi remoti sono esistite reti di telecomunicazioni basate su tecnologie diverse, come torri d'avvistamento e segnali luminosi o bandiere (i castelli della Valle d'Aosta, la Grande Muraglia Cinese), segnali di fumo (caratteristici degli indiani americani), o segnali acustici (i tam-tam della giungla). Inoltre, verso la fine del secolo scorso erano state attivate reti telegrafiche basate su segnalazioni ottiche, utilizzando tralicci su cui erano montati pannelli mobili azionabili dal basso e visibili da lontano.

È evidente una rilevante differenza tra le reti citate ad esempio: le reti per diffusione radio e TV, i segnali di fumo ed i tam-tam costituiscono reti a diffusione e unidirezionali: l'informazione viene distribuita da una sorgente

a chiunque disponga di un apparato ricevitore, quindi a ogni utente della rete, indipendentemente dalla sua identità. Non è inoltre possibile per la gran maggioranza degli utenti, che dispongono solo di un apparato ricevente, inviare informazioni ad altri. Le reti telematiche, la rete telefonica, il sistema postale, sono invece reti a selezione e bidirezionali: sono caratterizzate dalla possibilità per la sorgente dell'informazione di scegliere a quali interlocutori questa deve essere trasferita. In questo caso tutti gli utenti sono attrezzati sia per trasmettere sia per ricevere.

1.1 Dagli albori militari alla fisica delle alte energie

Internet, la rete delle reti che è divenuta il nostro principale strumento di ricerca, collaborazione ed interazione sociale, una realtà consolidata per il lettore oggi venticinquenne, ha radici lontane nella storia dell'Informatica. Riesaminare insieme i passi remoti della sua storia è un esercizio utile ed istruttivo su come stimoli storici e sociali, idee geniali e tecnologia possono essere fusi per creare qualcosa di unico e così influente da cambiare lo stile di vita di due terzi della popolazione mondiale.

Come spesso accade, il primo impulso alla realizzazione di un sistema d'interconnessione di calcolatori su scala geografica fu di origine militare. La "mamma" di Internet fu infatti ARPANET, una rete costruita negli anni '70 a scopo militare, pensata per condividere online il tempo di utilizzazione dei computer tra i diversi centri di elaborazione dati dell'ARPA (*Advanced Research Projects Agency*), che eseguivano ricerche scientifiche a lungo termine per conto del Dipartimento della Difesa degli Stati Uniti. Un'impresa non da poco, dato che all'epoca non esistevano standard per la costruzione di calcolatori ed i "supercomputer" erano isolati e basati su sistemi incompatibili tra loro.

Il progetto è principalmente dovuto alla caparbietà di Bob Taylor, direttore della divisione informatica dell'ARPA, alle idee rivoluzionarie di Joseph

Licklider, all'epoca coordinatore dell'IPTO (*Information Processing Techniques Office*) [1, 2, 3] ed alla teorizzazione delle reti a commutazione di pacchetto[1], proposta da Leonard Kleinrock [4] come argomento per la sua tesi di dottorato al Massachusetts Institute of Technology (MIT).

Tali e tanti sono gli eventi che si susseguono nel corso di un decennio, che si ritiene opportuno elencarne la sequenza:

1961 (luglio) Leonard Kleinrock del MIT pubblica *Information flow in large communication nets* [4] sulla teoria del *packet switching*

1962 (agosto) Licklider & Wesley Clark del MIT pubblicano *On-line man computer communication* [5] che forse può essere considerato il primo articolo sul concetto di internet

1962 (ottobre) J.C.R. Licklider diviene direttore dell'IPTO

1964 Leonard Kleinrock pubblica il libro *Communication net* [6], nel quale descrive rigorosamente il funzionamento di una rete basata sul *packet switching*

1964 (marzo) Paul Baran della RAND Corporation descrive, in una serie di memoranda per la USAF, una rete di comunicazione capace di resistere ad un attacco termonucleare basata sul packet switching [7]

1964 (settembre) Ivan Sutherland diviene il nuovo direttore dell'IPTO

1965 (ottobre) Lawrence Roberts (MIT) e Thomas Marrill (CCA) effettuano il primo collegamento con tecnologia packet switching fra il *TX-2* dei Lincoln Labs a Lexington e l'*AN/FSQ-32* della SDC a Santa Monica

1966 (agosto) Robert Taylor diventa il terzo direttore dell'IPTO ed assume Lawrence Roberts per coordinare il progetto

1967 (aprile) Wesley Clark suggerisce di utilizzare una sottorete di minicomputer, tutti uguali e compatibili tra di loro, dedicata esclusivamente alla ricezione e trasmissione dei dati. Suggerisce di chiamare questi computer IMP (*Interface Message Processors*). È la svolta concettuale che

[1] contrapposte alla commutazione di circuito, tipica dei sistemi di telefonia analogici

permetterà di superare i problemi legati all'eterogeneità dei computer dell'epoca

1967 (ottobre) Donald W. Davies, che lavora al National Physical Laboratory (UK), pubblica i risultati delle sul packet switching, svolte in modo del tutto indipendente dai ricercatori americani [8]

1967 (ottobre) Lawrence Roberts presenta il disegno della futura rete [9]

1968 (agosto) Lawrence Roberts invia a 140 società la "Request For Proposals" (RFP) per la realizzazione degli IMP della rete ARPANET; al bando rispondono la BBN e la Raytheon, ma non IBM e AT&T che giudicano il progetto improponibile: la fornitura è affidata alla BBN

1968 (ottobre) Leonard Kleinrock viene assunto al Network Measurement Center (UCLA)

1969 (aprile) restano ancora da definire le caratteristiche che deve avere l'interfaccia tra i singoli calolatori e gli IMP, che sono pubblicate da Bob Kahn

1969 (aprile) Steve Crocker scrive il primo *Request For Comment* (RFC) che tratta l'*host-to-host protocol* [10]: da questo momento tutti i protocolli di rete saranno formalizzati in documenti di questo tipo e gli RFC saranno il principale strumento di collaborazione e sviluppo della comunità di ricerca nell'ambito delle reti di calcolatori [11].

Finalmente, nell'ottobre 1969 viene stabilito il primo collegamento da computer a computer fra l'Università della California di Los Angeles e lo Stanford Research Institute: nasce il primo link ARPANET. I centri collegati si susseguono con ritmo incalzante ed alla fine del 1971 la rete conta già 15 nodi, che diventano 37 alla fine del 1972; da allora la crescita è esponenziale. È il periodo nel quale viene formalizzato da Crocker il protocollo NCP (*Network Control Program*) [12], che stabilisce le regole per la connettività alla base di ARPANET.

La svolta determinante avviene però nel 1974 con la pubblicazione dell'RFC 675, dal significativo titolo "Specification of Internet Transmission Control

Program" [13], dove appare per la prima volta il termine "Internet". Nel 1978 Cerf, Postel e Crocker aggiugono al TCP il protocollo IP (*Internet Protocol*) [14], mettendo a punto il definitivo modello su cui ancor oggi opera Internet, il TCP/IP [15].

Parallelamente nascono le prime applicazioni: Telnet, per la gestione remota di terminali, FTP per la trasmissione di file, E-Mail per la posta elettronica: sono tutte applicazioni basate sulla linea di comando, con un'interfaccia ostica e riservata al personale tecnico e ricercatore. Il primo tentativo di "interfaccia universale" alle risorse di rete è Gopher[2], ma la vera rivoluzione arriva con l'implementazione dell'interfaccia grafica e del mouse nei sistemi operativi.

Questi due elementi rendono possibile la nascita del World Wide Web (1990), un sistema per la condivisione di informazioni in ipertesto, sviluppato da Tim Berners-Lee [16] presso il CERN di Ginevra, pensato per facilitare la condivisione di informazioni scientifiche nella comunità dei fisici nucleari. Il sistema si basa sul protocollo HTTP [17] e sul linguaggio HTML: per standardizzare quest'ultimo, Berners-Lee fonda il World Wide Web Consortium (W3C), che tuttora si occupa di definire gli standard per il web[3].

Il resto è cronaca: l'avvento della "banda per tutti" (*broadband*) e, soprattutto, il DNS (Domain Name System), i motori di ricerca, i social network, la necessità di generare contenuti in modo collaborativo e semanticamente pregnante hanno portato alla nascita di quello che adesso è definito Web 2.0 [18].

1.2 Stipulare intese su come comunicare

Si vuole iniziare suggerendo una riflessione su cosa "si nasconde" dietro una semplice telefonata. Quando si solleva il microtelefono, prima di compiere

[2]la prima applicazione di rete basata su menu descrittivi a struttura gerarchica, realizzati mediante un'architettura di tipo client server

[3]una curiosità: il computer usato da Berners-Lee per realizzare il primo server web era basato sul sistema operativo NeXT, realizzato da Steve Jobs prima di rientrare alla Apple

qualsiasi azione, l'apparecchio telefonico controlla se è attivo il segnale di linea e restituisce un feedback sonoro: in modo totalmente trasparente per il chiamante, il telefono ha verificato l'esistenza di un collegamento fisico con la rete telefonica e la disponibilità di un canale per iniziare la comunicazione. Il passo successivo è la composizione del "numero di telefono", cioè dell'indirizzo del destinatario della telefonata. Val la pena notare che tale indirizzo è rigidamente codificato (infatti non può essere scelto dall'utente finale, ma viene assegnato dal provider dei servizi telefonici), è univoco (non possono esistere due utenti con lo stesso numero) ed ha una struttura gerarchica: un prefisso internazionale, un prefisso nazionale, un eventuale prefisso di centralino e, infine, l'identificativo del telefono chiamato.

Composto il numero, il segnale sarà instradato attraverso la rete telefonica mondiale e la richiesta di iniziare la comunicazione arriverà a destinazione: in altre parole, il telefono del destinatario squillerà e inizierà la conversazione...

...O no?

In realtà (pur supponendo che il telefono chiamato sia perfettamente funzionante) possono verificarsi almeno tre casi:

- l'essere umano che si vuole contattare non è in casa o non vuole rispondere
- l'apparecchio del destinatario è utilizzato per un'altra conversazione
- il destinatario risponde

Le tre situazioni saranno gestite in modo diverso. Nel primo caso, probabilmente, dopo un pò d'attesa, sarà chi chiama a chiudere la comunicazione; nel secondo caso si otterrà il tipico segnale di "occupato". Se invece si è fortunati, il destinatario, attivato il proprio microtelefono, risponderà col classico "...pronto..." o con un'altra frase convenzionale, a quel punto anche il chiamante, per iniziare la conversazione, userà un'espressione analoga. Durante tutta la telefonata, il sistema telefonico si occuperà di garantire che ciascun suono pronunziato giunga a destinazione velocemente, nella giusta sequenza e senza disturbi. Alla fine della telefonata sorge un problema, spesso causa

d'imbarazzo tra gli interlocutori: chi chiude per primo? Questa situazione capita, come si vedrà,anche nella gestione della connessione tra apparati fisici.

Infine, durante tutta la telefonata, non ci siamo minimamente preoccupati del tipo di telefono posseduto dal nostro interlocutore (fisso, cellulare, cordless, isdn, analogico): in realtà l'eterogeneità dei dispositivi da far comunicare aggiunge complessità e deve essere opportunamente gestita.

L'esempio precedente, sia pur semplicistico e limitato, evidenzia la complessità insita nel problema di mettere in comunicazione due entità remote (*end point*) variamente collegate.

Realizzare una rete di calcolatori richiede risorse e competenze in vari ambiti disciplinari, che vanno dalla progettazione e costruzione dei dispositivi fisici, al disegno e realizzazione del software che gestisce i servizi.

Pensare di codificare la materia in un blocco monolitico è dunque improponibile: è invece opportuno tentare di scomporre la problematica in una serie d'obiettivi specifici, il più possibile indipendenti l'uno dall'altro.

Il primo, ovviamente, è la connettività fisica tra gli apparati, necessaria affinché qualsiasi forma di comunicazione possa avvenire. Si noti, ancora una volta, la necessità di collegare alla stessa rete dispositivi di tipo diverso (per esempio PC e telefoni cellulari), su un ampio range di distanze (stampare un documento mediante la stampante dipartimentale è differente dal consultare un sito Web) e con esigenze di prestazioni diverse (lo *streaming* di un film richiede una "velocità" della rete molto maggiore rispetto alla trasmissione di un messaggio *e-mail*).

Un altro aspetto fondamentale è l'indirizzamento, cioè la necessità di poter identificare univocamente ciascun apparato (*host*) presente sulla rete. Come nel caso della telefonata, alla caratteristica d'univocità si deve associare la possibilità di conferire allo spazio d'indirizzamento una struttura gerarchica. Ancora, su una rete complessa, come, ad esempio, quella mondiale, è necessario poter determinare il percorso che i dati devono seguire per arrivare a destinazione nel modo più efficiente possibile: occorre cioè un

meccanismo di instradamento del traffico.

Tuttavia, il collegamento più veloce ed efficiente servirebbe a poco se i dati trasmessi non fossero correttamente interpretabili dal destinatario: occorre qualcosa che presieda al trasporto dei dati e che gestisca la connessione di modo che questi possano essere ricevuti in modo completo e senza errori da entrambe le parti. Infine occorre codificare le applicazioni che la rete deve erogare, i servizi, la loro interfaccia verso l'utente finale.

In sintesi (e semplificando) chi progetta reti di calcolatori dovrà tener conto di queste caratteristiche:

- Collegamento fisico
- Indirizzamento
- Instradamento
- Trasporto dei dati e gestione della connessione
- Applicazioni

Adesso si passerà a formalizzare quanto detto fin qui: per ridurre la complessità di progetto, le reti sono, in generale, organizzate a livelli, ciascuno costruito sopra il precedente. Lo scopo di un livello è offrire servizi ai livelli più alti, nascondendo i dettagli sull'implementazione. Le due macchine che devono comunicare prendono il nome di *host*: il livello n su un host "conversa" col livello n su un'altro host. Le regole e le convenzioni che governano la conversazione sono collettivamente indicate col termine protocollo di livello n. Si parla, in questo caso di "conversazione tra pari" e le entità (processi) che effettuano tale conversazione si chiamano *peer entity* (entità di pari livello).

In realtà non c'è un trasferimento diretto dal livello n di host A al livello n di host B. Ogni livello di host A passa i dati, assieme a delle informazioni di controllo, al livello sottostante; questo procedimento prende il nome di incapsulamento e ne discuteremo ampiamente più avanti. Questo meccanismo è evidenziato in Fig. 1.1. Al livello 1 c'è il mezzo fisico, attraverso il quale i dati vengono trasferiti da host A ad host B. Quando arrivano a host B, i

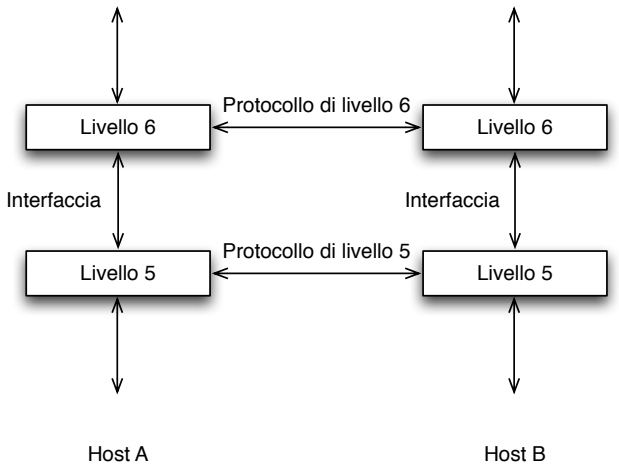


Figura 1.1: Comunicazione *peer to peer* tra livelli

dati sono trasmessi da ogni livello (a partire dal livello 1) a quello superiore, fino a raggiungere il livello n.

Fra ogni coppia di livelli adiacenti è definita un'interfaccia, che caratterizza le operazioni primitive che possono essere richieste *al* livello sottostante ed i servizi che possono essere offerti *dal* livello sottostante. Una buona progettazione delle interfacce tra i livelli consente di minimizzare la quantità e la complessità delle informazioni da trasferire e non preclude la possibilità di aggiornare l'implementazione del livello con l'evolversi della tecnologia.

Si noti che, in questo schema, un servizio definisce quali operazioni il livello è pronto ad eseguire per conto dei propri utenti (il livello superiore e quello inferiore), ma non dice nulla su come tali operazioni dovranno essere realizzate.

Di quest'ultimo aspetto si occupano i protocolli, cioè insiemi di regole che governano il formato ed il significato dei blocchi di informazione, dei pacchetti o dei messaggi che vengono scambiati dalle peer entity di un dato livello. Le entità utilizzano i protocolli per formalizzare le definizioni dei propri servizi. Esse sono libere di modificarli in futuro, purché non cambino i servizi erogati, implementando così la totale indipendenza della realizzazione di ciascun livello rispetto agli altri.

In questo modo si ottengono due vantaggi importanti: il primo è che possono dialogare fra loro anche host aventi caratteristiche (processore, sistema operativo, costruttore) diverse, il secondo è che ciascun livello si occuperà di un aspetto specifico in modo indipendente dall'implementazione dei livelli sottostanti; per esempio, una pagina web potrà essere interpretata correttamente dal *browser* indipendentemente dal fatto che il fruitore stia utilizzando un computer desktop collegato alla rete dell'Università o il suo portatile collegato via radio tramite un *hot spot* dell'aeroporto. L'insieme dei livelli e dei relativi protocolli di una specifica implementazione è detto architettura di rete.

1.2.1 Pensare a strati

Nelle pagine seguenti verranno esaminate in parallelo due formalizzazioni della struttura a strati fin qui presentata: un modello di riferimento, l'*ISO/OSI* ed un'architettura di rete, il *TCP/IP*. La sostanziale differenza tra i due è che il modello ISO/OSI si limita a specificare cosa dovrebbe fare ciascun livello, ma non specifica con precisione i servizi ed i protocolli che devono essere usati e, dunque, non può essere considerato un'architettura di rete. Tuttavia la sua rilevanza storica e concettuale lo rende il fulcro di ogni moderna implementazione di rete.

L'OSI (*Open Systems Interconnection*) Reference Model [19] è il frutto del lavoro della ISO (*International Standard Organization*), ed ha lo scopo di:

- fornire uno standard per la connessione di sistemi aperti, cioè in grado di colloquiare gli uni con gli altri;
- fornire una base comune per lo sviluppo di standard per l'interconnessione di sistemi;
- fornire un modello rispetto a cui confrontare le varie architetture di rete.

Esso non include la definizione di protocolli specifici (che sono stati definiti successivamente, in documenti separati). I principi di progetto che sono stati seguiti durante lo sviluppo del modello OSI schematizzano fedelmente quanto esposto nel paragrafo precedente:

- ogni livello deve avere un diverso strato di astrazione;
- ogni livello deve avere una funzione ben definita;
- i limiti dei livelli devono essere scelti in modo da minimizzare il passaggio delle informazioni attraverso le interfacce;
- il numero dei livelli deve essere abbastanza ampio per permettere a funzioni distinte di non essere inserite forzatamente nel medesimo livello senza che sia necessario e abbastanza piccolo per permettere che le architetture non diventino pesanti e poco maneggevoli.

Sono individuati e formalizzati sette livelli, numerati a partire dal basso: fisico, data link, network, trasporto, sessione, presentazione, applicazione (Fig. 1.2).

I livelli più bassi, da quello fisico a quello di trasporto, si occupano della consegna dei dati tra gli host, mentre quelli più alti si occupano della loro elaborazione e realizzano perciò le applicazioni di rete. Non si espliciterà adesso il significato ed il ruolo del singolo livello: essi diverranno più chiari nel seguito della trattazione.

Come avviene in pratica la comunicazione tra un livello e quello sottostante? Si supponga di dover spedire una lettera: redatto il messaggio su un foglio di carta, si metterà quest'ultimo in una busta, sulla quale viene scritto l'indirizzo del mittente e del destinatario. L'addetto della compagnia postale ritirerà la busta e la porterà al centro di smistamento della città di partenza, dove la lettera sarà messa in un sacco indirizzato alla città di destinazione. Il sacco sarà caricato via via sugli opportuni mezzi di trasporto (non importa quali e quanti) e giungerà al centro di smistamento della città di destinazione. Qui sarà aperto e la nostra busta sarà consegnata al postino per la consegna finale. Il postino leggerà l'indirizzo e consegnerà la lettera

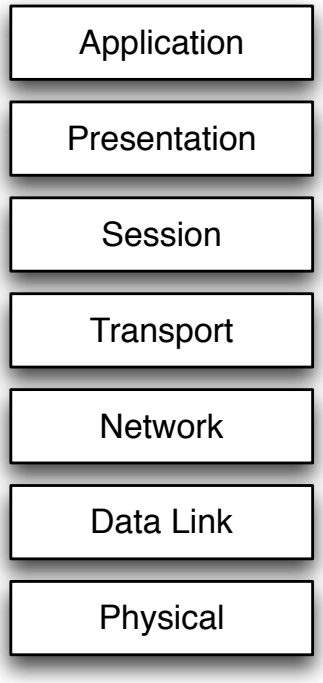


Figura 1.2: I livelli del modello di riferimento ISO/OSI

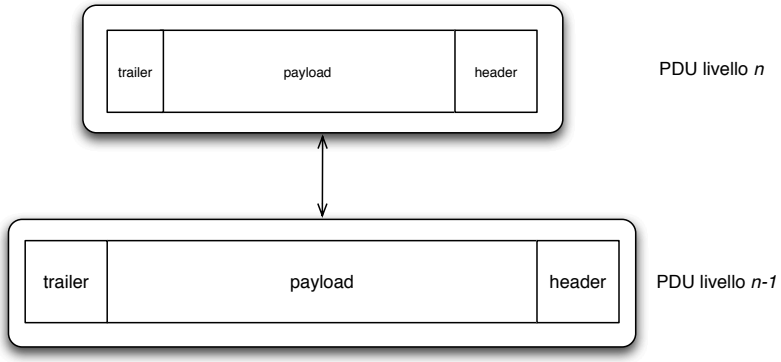


Figura 1.3: Incapsulamento dei dati nel livello sottostante

al destinatario. Il destinatario, letto l'indirizzo, aprirà la busta e leggerà il messaggio. É importante notare che soltanto il mittente ed il destinatario elaborano le informazioni contenute nella lettera, tutti gli altri protagonisti della consegna si limitano a leggere l'indirizzo sulla busta (o sul sacco) e reindirizzano la missiva alla tappa successiva.

Nelle reti di comunicazione avviene qualcosa d'analogo: i dati dell'applicazione vengono incapsulati nei livelli sottostanti fino ad arrivare al livello fisico; durante il percorso vengono "aperte" solo le "buste" relative ai livelli che si occupano dell'instradamento del messaggio e solo sull'host di destinazione i dati dell'applicazione vengono elaborati.

In altri termini, ciascun livello dell'host mittente incapsula i dati (*payload*) del livello superiore premettendo un'intestazione (*header*) ed, eventualmente, posponendo dei codici di controllo (*trailer*); a sua volta, il pacchetto così costruito diventa payload del livello sottostante (Fig. 1.3).

Lungo il percorso attraverso i nodi della rete vengono elaborati ed eventualmente modificati solo gli header dei livelli che si occupano della trasmissione. Soltanto sull'host di destinazione saranno elaborati gli header relativi ad ogni livello, fino alla consegna dei dati all'applicazione. Ad esempio, un *router*, che è un apparato che realizza l'instradamento dei dati, "aprirà" soltanto le "buste" fino al livello 3, che contiene le informazioni necessarie. Ciascun livello avrà una propria *Protocol Data Unit* (PDU), composta da

header, payload e trailer, che realizza l'incapsulamento. In particolare, è utile, per riferimento nel prosieguo della trattazione, conoscere i nomi delle PDU dei primi quattro livelli:

1. Livello fisico: *bit*
2. Livello data link: *frame*
3. Livello network: *pacchetto*
4. Livello trasporto: *TPDU* (*Transport Protocol Data Unit*)

1.3 Dalle intese ad Internet

Il TCP/IP (*Transmission Control Protocol / Internet Protocol*) [15] è l'architettura di rete che costituisce il fondamento della trasmissione dati in Internet.

Rispetto al modello ISO/OSI condensa i livelli fisico e data-link in un unico livello (*host-to-network*) ed i tre livelli applicativi in un più generico *application* (Fig. 1.4). Essendo nato principalmente per realizzare servizi Internet, formalizza in modo rigoroso i due livelli di networking (*Internet* e *transport*) definendone le funzionalità, lo spazio d'indirizzamento e le caratteristiche dei protocolli. Il livello più basso non è specificato nell'architettura, che prevede di utilizzare i protocolli disponibili per le varie piattaforme hardware e conformi agli standard, purché consentano agli host di inviare pacchetti IP sulla rete. Il livello applicativo è quello sul quale poggiano le applicazioni Internet che oggi tutti conoscono (posta elettronica, web, trasferimento file).

I protocolli che implementano le funzionalità del TCP/IP sono formalizzati in una serie di documenti denominati RFC (*Request For Comment*) [10, 11]: sono documenti aperti, nel senso che la descrizione di un protocollo esposta in ciascuno di essi potrà essere migliorata con la pubblicazione di un RFC successivo. Si descriverà di seguito sommariamente il ruolo di ciascun livello (usando la nomenclatura della pila ISO/OSI) evidenziando esempi d'implementazione nell'ambito del TCP/IP.

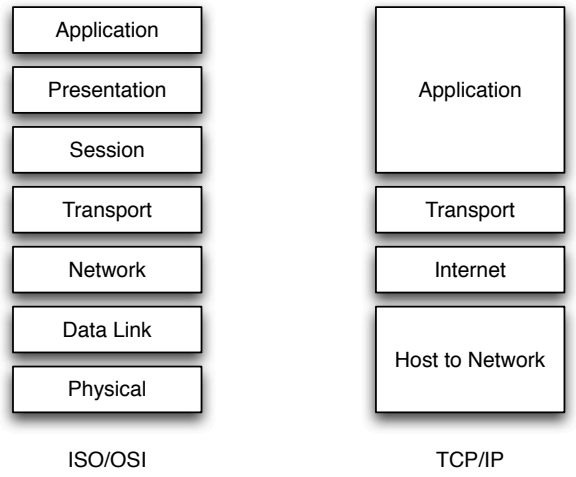


Figura 1.4: Lo stack TCP/IP

1.3.1 Consegnare i dati

Il livello fisico attiene la trasmissione di bit "grezzi" su un canale di comunicazione. Gli aspetti di progetto sono volti a garantire la congruenza dei bit ricevuti con quelli trasmessi; le specifiche sono, in massima parte, relative alle caratteristiche meccaniche, elettriche e procedurali delle interfacce di rete (componenti che connettono l'elaboratore al mezzo fisico) e alle caratteristiche del mezzo fisico stesso. La misura della "velocità" pura di una rete è data dalla quantità di dati che è possibile trasmettere nell'unità di tempo e spesso viene indicata con il nome di banda. L'unità di misura è il *bit/s* (attenzione, *bit* non *byte*), con i vari multipli: *kilo*, *Mega*, *Giga*. In teoria (ed in conformità col Sistema Metrico Internazionale) i multipli citati dovrebbero essere potenze di 10 (un kilo=1000), ma la matematica in base 2 e la tradizione portano spesso ad inpiegare come moltiplicatore $2^{10} = 1024$.

In realtà, fatto comunque salvo il principio "... più banda c'è meglio è...", spesso le prestazioni di una rete dipendono da altri fattori. Per esempio è auspicabile che una transazione bancaria vada, sia pur lentamente, a buon fine, piuttosto che precipitare rapidamente in uno stato impredicibile. Oppure, nel caso di trasmissione di voce in tempo reale (una telefonata su Internet),

non è fondamentale che la banda sia elevata: è molto più importante che la banda richiesta per la telefonata (piccola, dell'ordine dei $16Kb/s$) sia erogata con costanza nel tempo (*jitter* basso) di modo che le due parti possano percepire il parlato con fluidità. La destinazione d'uso della rete da realizzare e la sua estensione geografica giocano un ruolo fondamentale nei processi decisionali relativi alla progettazione; è allora utile suddividere le reti in categorie, ovviamente in modo del tutto indicativo. Una possibile classificazione è la seguente:

- PAN (*personal area network*): è una rete informatica utilizzata per permettere la comunicazione tra diversi dispositivi in ambito domestico; le tecnologie più utilizzate sono generalmente wireless (*WiFi*, *Bluetooth*), ma talvolta vengono usati anche cavi (*Ethernet*, *USB*, *FireWire*). Il classico esempio è costituito dal router WiFi, utilizzato per la connessione ad Internet.
- LAN(*local area network*): è costituita da computer collegati tra loro all'interno di un ambito fisico delimitato (un'azienda, un campus universitario); il cablaggio è costituito da un livello di distribuzione in fibra ottica e da punti d'accesso realizzati con cavo in rame. La banda tipica è dell'ordine del Gb/s.
- MAN (*metropolitan area network*): è un'infrastruttura in fibra ottica o, più raramente, wireless (*WiMax*) che realizza dorsali a larga banda che collegano i principali centri della vita sociale, politica e culturale della città.
- WAN (*wide area network*): realizza l'interconnessione tra le reti metropolitane, l'esempio tipico è Internet stessa.

La scelta del mezzo trasmissivo, cioè il supporto fisico che consente il collegamento degli host, è un elemento di fondamentale importanza nella realizzazione di una rete effettivamente funzionante; tale scelta è dettata sia da considerazioni tecniche (distanza massima tra due apparati, larghezza di banda, ostacoli di natura geografica), sia da motivazioni di carattere

economico-sociale (la diffusione del mezzo sul territorio, gli elevati costi e l'impatto sociale ed ambientale di alcune tecnologie).

Schematizzando, si usano mezzi fisici di quattro tipologie diverse: cavo elettrico, onde radio, fibra ottica, laser. Sulle classiche reti su doppino telefonico (dette anche POTS, *plain old telephone system*) è possibile realizzare reti con diverse tecnologie. Nel decennio scorso era frequente l'uso di *modem* per codificare segnali digitali sopra le comuni linee telefoniche analogiche: la connessione era *on-demand* e la velocità limitata a circa $56Kb/s$. Il grande vantaggio di questa tecnologia è che non richiede modifiche alla rete distributiva esistente. Una prima evoluzione furono le linee ISDN, costituite da due canali telefonici (in realtà ne serve un terzo, di controllo) in tecnologia digitale. La velocità massima di $128Kb/s$ veniva raggiunta sfruttando due connessioni in parallelo su canali da $64Kb/s$. Ma la tecnologia che ha consentito la diffusione di massa (*broadband*) della connettività domestica è, senza alcun dubbio, l'ADSL (*asymmetric digital subscriber line*): essa richiede l'installazione di nuovi apparati di commutazione nelle centrali telefoniche, chiamati DSLAM, e l'utilizzo di filtri negli impianti telefonici domestici per separare le frequenze utilizzate per la trasmissione dati da quelle per la comunicazione vocale. La banda erogata è asimmetrica, tipicamente $7Mb/s$ in *download* e $384Kb/s$ in *upload*, ma ormai tutti gli operatori telefonici offrono collegamenti a velocità maggiore.

Tra i candidati a sostituire il doppino per la distribuzione domestica dei servizi di telecomunicazioni, si possono citare le fibre ottiche e le infrastrutture della TV via cavo (diffusa soprattutto negli USA), il trasporto di dati sulla rete elettrica, le reti wireless e le reti satellitari (utili in aree disagiate). Per realizzare le LAN si usano in genere particolari cavi (UTP), costituiti da quattro doppini, ed interfacce di rete *Ethernet*: la particolare tecnica realizzativa li rende meno sensibili alle interferenze, consentendo di raggiungere velocità dell'ordine del Gb/s. Con tecnologie più costose, tipicamente utilizzate dai provider, si raggiungono velocità di $40Gb/s$ per il singolo link su fibra ottica.

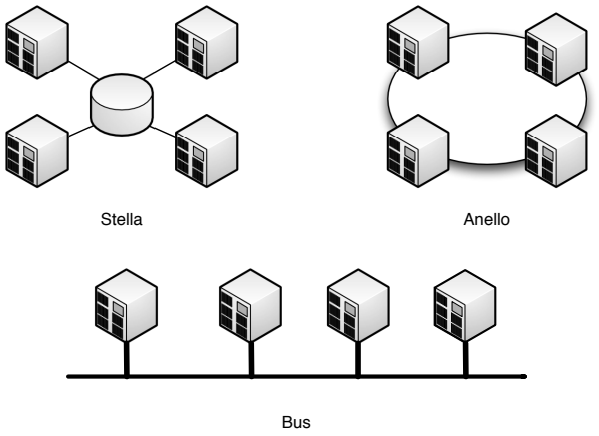


Figura 1.5: Topologia a stella, anello, bus

Il modo in cui i componenti di una rete sono collegati tra di loro, nel senso della disposizione ideale che questi hanno, viene definito generalmente attraverso quella che è nota come topologia di rete. Le reti punto a punto (*point-to-point*) consistono in un insieme di coppie di elaboratori connessi tra loro in vario modo (stella, anello, albero). Per passare da una sorgente ad una destinazione, l'informazione deve attraversare diversi elaboratori intermedi. Si ha una rete a stella quando tutti i componenti periferici sono connessi a un nodo principale in modo indipendente dagli altri; in tal modo tutte le comunicazioni passano per il nodo centrale e sono gestite completamente da questo. Si ha una rete ad anello quando tutti i nodi sono connessi tra loro in sequenza, in modo da formare un anello ideale, dove ognuno ha un contatto diretto solo con il precedente e il successivo; la comunicazione avviene (semplificando) a senso unico e ogni nodo ritrasmette i dati che non sono ad esso destinati al nodo successivo. Le reti *broadcast* (o *bus*) invece sono formate da un unico mezzo fisico, condiviso da più elaboratori, sul quale i messaggi inviati da un host vengono ricevuti da tutti gli altri. All'interno del messaggio vi è una parte relativa all'indirizzo del destinatario (elaborata a livello 2), in modo che tutte le altre macchine in ascolto possano scartare il messaggio in arrivo. Un esempio di una tale rete è la comune Ethernet [20].

Un problema tipico delle reti a bus è l'allocazione del canale trasmissivo.

Si pensi ad una normale conversazione tra esseri umani: capita talvolta che i due interlocutori inizino a parlare contemporaneamente. Di solito si genera una situazione d'imbarazzo che conduce ad un istante di silenzio, poi, dopo un intervallo casuale, uno dei due interlocutori riprende a parlare e la conversazione può aver luogo.

Analogamente, nel caso in cui il mezzo fisico è condiviso da più di due host, la trasmissione simultanea da parte di due di essi genera una sovrapposizione del segnale elettrico che inficia la trasmissione: è stata generata una collisione. Gli host che condividono il mezzo trasmissivo appartengono dunque allo stesso dominio di collisione: è evidente che maggiore è il numero di macchine appartenenti al dominio di collisione, più elevata è la probabilità che le collisioni abbiano luogo. Una buona regola nella progettazione delle reti è quindi far sì che i domini di collisione siano di dimensioni limitate.

Ciò non è possibile al mero livello fisico: occorre un protocollo, collocato nella parte bassa del livello 2, che consenta l'allocazione del canale trasmissivo all'host che vuole trasmettere. Si esamina ora il più diffuso, tipico delle reti ethernet: il CSMA/CD. CSMA/CD è l'acronimo inglese di *Carrier Sense Multiple Access with Collision Detection*, ovvero accesso multiplo tramite rilevamento della portante e delle collisioni. L'algoritmo è il seguente:

1. L'adattatore di rete sistema il messaggio in un buffer;
2. Se il canale è inattivo procede alla trasmissione, se è occupato attende prima di ritrasmettere;
3. Mentre trasmette, l'adattatore controlla la rete (è questo il vero e proprio collision detection), se non riceve segnali da altri adattatori considera il messaggio spedito, altrimenti è avvenuta una collisione, quindi va interrotta la trasmissione;
4. Se l'adattatore riceve, durante una trasmissione, un segnale da un altro adattatore, arresta la trasmissione e trasmette un segnale di disturbo (*jam*);

5. Dopo aver abortito la trasmissione attende un tempo casuale e ritrasmette.

Evidentemente un approccio di questo genere è poco efficiente perché comporta un elevato numero di ritrasmissioni, ma le reti a bus hanno il considerevole vantaggio dell'economicità e, per questo, sono ormai le più diffuse.

Quando si vogliono unire due o più reti (o anche degli elaboratori singoli) per formarne una sola più grande, occorre utilizzare dei nodi speciali connessi simultaneamente a tutte le reti da collegare. Il ripetitore è un componente che collega due reti fisiche intervenendo al primo livello ISO/OSI. In questo senso, il ripetitore non filtra in alcun caso i pacchetti dati, ma rappresenta semplicemente un modo per allungare un tratto di rete oltre il limite imposto dal singolo cavo passivo. Il ripetitore tipico è l'HUB, ovvero il concentratore di rete.

Da quanto detto risulta evidente che non può esistere un dispositivo di livello 1 in grado di interrompere un dominio di collisione; inoltre il lettore attento avrà notato che non è ancora emerso alcun tipo di meccanismo d'indirizzamento. Per ottenere questi risultati (ed altro ancora) occorre salire di livello.

Il *bridge* o *switch* è un dispositivo di livello 2 che mette in connessione due (o più) reti. Limitandosi a intervenire nei primi due livelli del modello ISO-OSI, il bridge è in grado di connettere tra loro solo reti fisiche dello stesso tipo. Il bridge più semplice duplica ogni frame nelle altre reti a cui è connesso; quello più sofisticato è in grado di determinare gli indirizzi dei nodi connessi nelle varie reti, ottimizzando il traffico. Nell'ottica dell'allocazione del canale trasmissivo, è interessante notare che l'inserimento di un bridge tra due segmenti di una rete a bus divide il dominio di collisione (Fig. 1.6).

Il livello data link ha il compito di offrire una comunicazione affidabile ed efficiente a due macchine adiacenti, cioé connesse fisicamente da un canale di comunicazione. Si occupa dunque di fare da tramite tra il livello 1 (fisico), che realizza la mera connettività ed il livello 3 (network), che instrada il

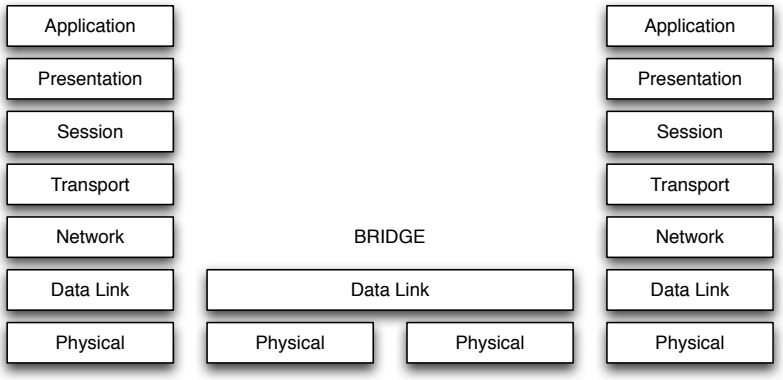


Figura 1.6: Collegamento a livello 2 mediante un bridge

traffico dati sulla rete geografica. È il livello sovrano delle LAN e attende alle seguenti incombenze principali:

- Frammentazione
- Controllo dell'errore
- Controllo di flusso
- Indirizzamento di livello 2

Un problema da non sottovalutare nella trasmissione dei dati a livello fisico è costituito dall'inaffidabilità del mezzo trasmissivo: per farsene un'idea basti pensare all'effetto che possono avere collisioni, interferenze e cadute di tensione sui collegamenti in rame. Per questo motivo è opportuno che il livello 2 si occupi di minimizzare il danno, organizzando i dati da trasmettere in piccoli "contenitori", i *frame*; in questo modo, un'eventuale problema comporterà la ritrasmissione di una piccola quantità d'informazione e non di tutto il contenuto della comunicazione. Questa operazione prende il nome di frammentazione.

Frammentati i dati, occorrerà prevedere un protocollo di controllo dell'errore, di solito basato sulla creazione di una *checksum*, una stringa generata con un opportuno algoritmo applicato al *payload* del frame. Questa sarà

calcolata dall'host trasmittente ed accodata al frame: l'host ricevente provvederà, ricevuto il frame, al ricalcolo della checksum, mediante il medesimo algoritmo, la confronterà con quella trasmessa e scarterà tutti i frame corrotti.

Per ogni frame correttamente ricevuto sarà inviata all'host trasmittente una "ricevuta di ritorno" (*acknowledgement* o, più semplicemente, *ack*): tutti i frame per i quali non arriverà, entro un tempo limite, un ack al mittente saranno ritrasmessi. Questo procedimento per il controllo del flusso è molto efficiente e consente, tra l'altro, di adeguare la velocità di trasmissione all'effettiva capacità di elaborazione del singolo host.

Infine, il livello 2 provvede a fornire una prima forma d'indirizzamento, in modo da evitare che host non coinvolti nella comunicazione siano comunque costretti ad elaborare a livelli più alti i dati ricevuti prima di scartarli.

Lo standard di livello 2 attualmente più diffuso è Ethernet. È una tecnologia nata molto presto, è più economica e facile da usare rispetto ai sistemi concorrenti, funziona bene e genera pochi problemi ed è adeguata all'utilizzo con TCP/IP; col passare del tempo lo standard si è aggiornato ed oggi consente velocità di trasmissione dell'ordine del Gb/s. Fornisce al livello di rete un servizio senza alcuna contrattazione iniziale ed il frame viene inviato nella LAN in modalità broadcast. Quando sarà ricevuto da tutti gli adattatori presenti sulla LAN, quello che vi riconoscerà il suo indirizzo di destinazione lo elaborerà (ed i dati saranno consegnati al livello 3), mentre tutti gli altri lo scarteranno. La gestione delle collisioni e dell'occupazione simultanea del canale di trasmissione viene gestita mediante il CSMA/CD.

Nelle reti più recenti si tende ad evitare completamente il problema delle collisioni, collegando ciascun host ad un bridge multiporta (*switch*) cosicché il dominio di collisione a cui appartiene ciascun host risulta essere popolato da due sole schede di rete: quella dell'host e la singola porta dello switch alla quale è collegato.

Gli indirizzi sono tutti a 6 byte in quanto Ethernet definisce uno schema d'indirizzamento a 48 bit [21]: ogni nodo collegato, quindi, ha un indirizzo Ethernet univoco di questa lunghezza. Esso corrisponde all'indirizzo fisico

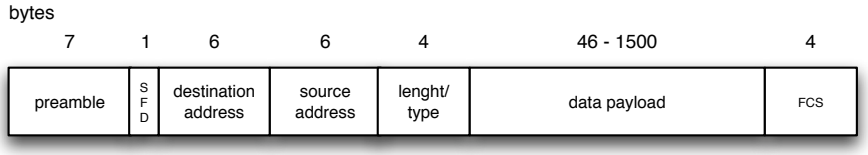


Figura 1.7: Struttura a blocchi di un *frame* Ethernet

della macchina ed è associato all'hardware (MAC *address*). Il MAC address viene, di solito, rappresentato in forma esadecimale: per esempio, il MAC address della scheda di rete del calcolatore col quale vengono redatte queste pagine è `00:0d:93:45:f4:22`.

In figura 1.7 è mostrata la struttura a blocchi di un frame Ethernet: si noti la presenza del MAC address sorgente e del MAC address destinazione. Inoltre il payload del frame ha dimensioni massime di 1500 Bytes, quindi il protocollo frammenterà i dati ricevuti dal livello 3 in blocchi di questa dimensione.

Per poter realizzare la consegna dei dati da un protocollo di livello 3, come nel caso del protocollo IP che viene descritto più avanti, ad un protocollo di livello 2, occorre un modo per definire un abbinamento tra gli indirizzi di questo protocollo superiore e gli indirizzi fisici delle interfacce utilizzate effettivamente, secondo le specifiche del livello inferiore.

Le interfacce Ethernet hanno un sistema di indirizzamento composto da 48 bit. Quando con un protocollo di livello network si vuole contattare un nodo, identificato quindi da un indirizzo di livello 3, se non si conosce l'indirizzo Ethernet, ma ammettendo che tale nodo si trovi nella rete fisica locale, viene inviata una richiesta circolare (broadcast di livello 2, indirizzo di destinazione `FF:FF:FF:FF:FF:FF`) secondo il protocollo ARP (*Address Resolution Protocol*). La richiesta ARP è ascoltata da tutte le interfacce connesse a quella rete fisica e ogni nodo passa tale richiesta al livello 3, che quindi leggerà il payload del frame, in modo da verificare se l'indirizzo richiesto corrisponde al proprio.

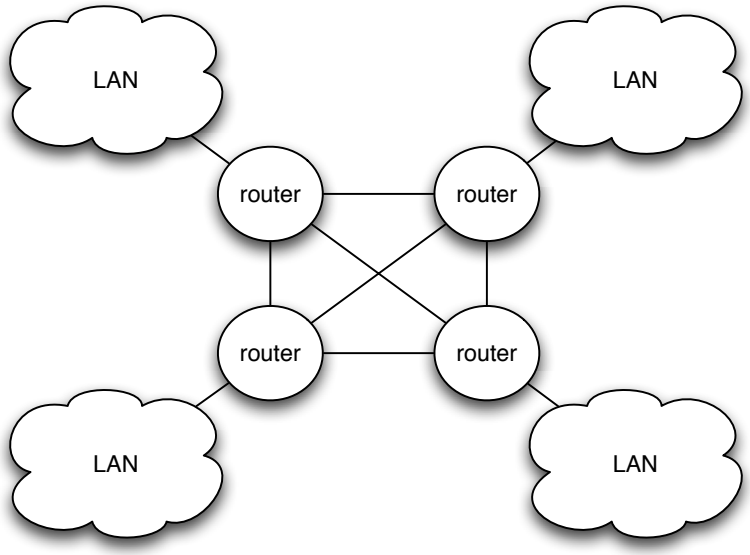


Figura 1.8: Internetworking a livello 3

In questo modo, soltanto il nodo associato all'indirizzo IP richiesto risponderà rivelando il proprio indirizzo Ethernet. Per praticità ogni nodo è in grado di conservare per un certo tempo le corrispondenze tra gli indirizzi di livello 2 e di livello 3, ottenute durante il funzionamento, mediante una tabella residente in memoria denominata ARP *table* o ARP *cache*.

Il livello network è incaricato di muovere i pacchetti dalla sorgente fino alla destinazione finale, attraversando tanti sistemi intermedi (*router*) della dorsale, anche su scala geografica: non a caso, nello stack TCP/IP questo livello prende il nome di *Internet* (Fig. 1.8). Ciò è molto diverso dal compito del livello data link, che è di muovere informazioni solo da un capo all'altro di un singolo canale di comunicazione.

Sintetizzando, il livello network si occupa di:

- gestire lo spazio di indirizzamento del livello 3
- conoscere la topologia della rete;
- scegliere di volta in volta il cammino migliore (*routing*);

- gestire le problematiche derivanti dalla presenza di più reti diverse (*internetworking*).

IP (*Inter-networking Protocol*) [14] è il protocollo di livello 3 della suite TCP/IP, nato per interconnettere reti eterogenee per tecnologia, prestazioni, gestione.

Gli indirizzi IP versione 4, cioè quelli tradizionali, sono composti da una sequenza di 32 bit, suddivisi convenzionalmente in quattro gruppetti di 8 bit, rappresentati in modo decimale e separati da un punto. Per esempio, l'indirizzo IP del computer (host) in cui risiede il file che contiene queste parole è il seguente:

`82.55.113.23`

ed è stato assegnato alla mia scheda ADSL dal provider di telecomunicazioni al quale sono connesso. Questo tipo di rappresentazione è definito come notazione decimale puntata. L'esempio seguente corrisponde all'indirizzo `1.2.3.4`:

`00000001.00000010.00000011.00000100`

All'interno di un indirizzo del genere si distinguono due parti: l'indirizzo di rete e l'indirizzo del nodo particolare. Il meccanismo è simile a quello del numero telefonico in cui la prima parte del numero, il prefisso, definisce la zona ovvero il distretto telefonico, mentre il resto identifica l'apparecchio telefonico specifico di quella zona. Come per i numeri telefonici, sulla rete mondiale l'indirizzo IP di ogni singolo host non può essere duplicato, cioè non possono esistere due apparati di rete con lo stesso indirizzo; per questo motivo esistono delle organizzazioni a livello mondiale (INTERNIC, RIPE) che si occupano di rilasciare gli IP ai provider che ne fanno richiesta. In pratica viene rilasciato un indirizzo di rete in funzione del numero di nodi da connettere. In questo indirizzo una certa quantità di bit nella parte finale sono azzerati: ciò significa che quella parte finale può essere utilizzata per gli indirizzi specifici dei nodi.

Considerando l'esempio precedente, un possibile indirizzo di rete potrebbe essere `1.2.3.0`, cioè:

`00000001.00000010.00000011.00000000`

In tal caso, si potrebbero utilizzare gli ultimi 8 bit (quindi $2^8 = 256$ indirizzi) per i vari nodi. Ma l'indirizzo di rete non può identificare un nodo in particolare, quindi il numero di indirizzi possibili per gli host diventa 255.

Inoltre, un indirizzo in cui i bit finali lasciati per identificare i nodi siano tutti a uno, identifica, per convenzione del protocollo, un indirizzo broadcast, cioè un indirizzo per la trasmissione a tutti i nodi di quella rete. Nell'esempio precedente, `1.2.3.255`

`00000001.00000010.00000011.11111111`

rappresenta simultaneamente tutti gli indirizzi che iniziano con

`00000001.00000010.00000011`

cioè che hanno lo stesso prefisso di rete.

In pratica, il livello 3 di tutti gli host della sottorete valuterà un pacchetto che ha come destinazione l'indirizzo di broadcast e passerà il payload di quel pacchetto al livello 4. Di conseguenza, un indirizzo broadcast non può essere utilizzato per identificare un singolo nodo ed il numero di indirizzi possibili per gli host dell'esempio scende a 254.

Il meccanismo utilizzato per distinguere la parte dell'indirizzo che identifica la rete è quello della maschera di rete o *netmask*. La maschera di rete è un numero di 32 bit, che viene abbinato all'indirizzo IP con l'operatore booleano AND[4]. La netmask sarà dunque costituita da tanti uno quanti sono i bit che si vuole dedicare alla parte di rete e da tutti zero per la parte host. Nell'esempio precedente, nel quale si sono usati 24 bit per la parte di rete, la netmask sarà:

`11111111.11111111.11111111.00000000`

[4]l'operatore AND fornisce in uscita 1 solo se i due valori in ingresso sono entrambi 1

cioè, in notazione decimale, `255.255.255.0` .

Il procedimento è il seguente: si definisce la netmask e la si applica all'indirizzo ip, il numero che si ottiene è l'indirizzo della rete: questa operazione non è soltanto una mera speculazione accademica, ma viene utilizzata in pratica dai router per calcolare la sottorete di destinazione dei singoli pacchetti al fine di instradare il traffico nel modo corretto. Nell'esempio precedente si ha:

`00000001.00000010.00000011.00000100`	`1.2.3.4`	(host)
`11111111.11111111.11111111.00000000`	`255.255.255.0`	(mask)
`00000001.00000010.00000011.00000000`	`1.2.3.0`	(net)

In base al valore dei primi bit, gli indirizzi IP vengono suddivisi in classi, ciascuna con una netmask convenzionale, per esempio la classe A è costituita da indirizzi il cui primo bit vale 0 e ha una netmask convenzionale di 8 bit, cioè `255.0.0.0`. In tabella 1.1 è riportata la classificazione completa.

Classe	Leading bits	Inizio intervallo	Fine intervallo
A	`0`	`0.0.0.0`	`127.255.255.255`
B	`10`	`128.0.0.0`	`191.255.255.255`
C	`110`	`192.0.0.0`	`223.255.255.255`
D	`1110`	`224.0.0.0`	`239.255.255.255`
E		`240.0.0.0`	`255.255.255.255`

Tabella 1.1: Classi d'indirizzamento IP

Si può notare che l'esempio scelto (net `1.2.3.0` con 24 bit di parte di rete) non è conforme alla tabella, infatti l'indirizzo `1.2.3.0`, convertito in cifre binarie, inizia con uno `0` e quindi appartiene alla classe A, che ha 8 bit dedicati alla rete. Non è un errore: estendendo la netmask si può suddividere una rete in sottoreti più piccole e ciò è molto utile, perché il numero di IP diversi ottenibili con 32 bit è grande, ma finito (2^{32}) e non avrebbe senso assegnare, per esempio, una intera classe C (254 indirizzi utili) ad una rete

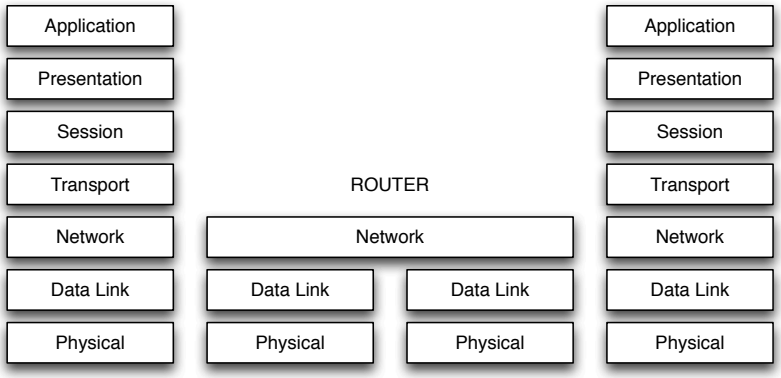


Figura 1.9: Instradamento a livello 3 mediante un router

di un piccolo ufficio con 4 computer[5]. L'operazione appena descritta prende il nome di *subnetting* e, purtroppo, non è supportata da tutti gli standard e protocolli. Gli ambienti in cui è possibile gestire il subnetting vengono definiti *classless*, mentre i contesti nei quali non si può derogare dalla rigida divisione in classi prendono il nome di *classfull*. In ambiente classless si può generalizzare la definizione di indirizzo di net e di broadcast di una sottorete: l'indirizzo della net sarà quello con tutti i bit della parte host posti a 0, mentre il broadcast avrà tutti i bit della parte host posti ad 1.

Un pacchetto IP avrà un header che conterrà l'indirizzo sorgente e l'indirizzo di destinazione, oltre a vari campi di controllo sui quali non ci soffermeremo. L'header sarà analizzato dal livello 3 dell'host: se il pacchetto ha un indirizzo di destinazione uguale quello del nodo che lo sta esaminando (oppure la destinazione è l'indirizzo di broadcast della sottorete) il payload del pacchetto verrà consegnato al livello 4 dell'host; in tutti gli altri casi il pacchetto sarà scartato. Per interconnettere due (o più) reti, intervenendo al terzo livello del modello ISO-OSI, è necessario un *router*; esso è in grado di *instradare* i pacchetti IP indipendentemente dal tipo di reti fisiche connesse effettivamente (Fig. 1.9).

[5]con una parte di rete di 29 bit si ottengono $2^3 - 2 = 6$ indirizzi utili, resta al lettore l'incombenza di calcolare il valore della netmask opportuna

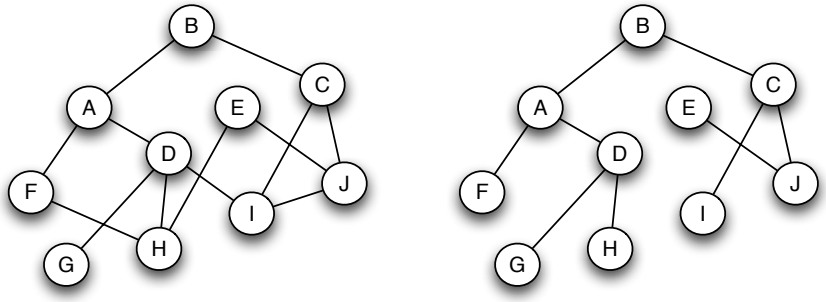


Figura 1.10: Costruzione del Sink Tree

L'instradamento dei pacchetti attraverso le reti connesse al router avviene in base a una tabella di instradamento che può anche essere determinata in modo dinamico, in presenza di connessioni ridondanti; questo procedimento prende il nome di *routing*. Un *algoritmo di routing* è quella parte del software di livello network che decide su quale linea d'uscita instradare un pacchetto che è arrivato al router. Da un algoritmo di routing desideriamo:

- correttezza (deve muovere il pacchetto nella giusta direzione);
- semplicità (l'implementazione non deve essere troppo complicata);
- robustezza (deve funzionare anche in caso di cadute di linee e/o guasti dei router e di riconfigurazioni della topologia);
- stabilità (deve convergere, e possibilmente in fretta);
- ottimalità (deve scegliere la soluzione globalmente migliore).

Esiste un cosiddetto principio di ottimalità per cui se il router j è nel cammino migliore fra i e k, allora anche il cammino ottimo fra j e k è sulla stessa strada. Se così non fosse, ci sarebbe un altro cammino fra j e k migliore di quello che è parte del cammino ottimo fra i e k, ma allora ci sarebbe anche un cammino migliore fra i e k. Una diretta conseguenza è che l'insieme dei cammini ottimi da tutti i router a uno specifico router di destinazione costituisce un albero, detto *sink tree* per quel router (Fig. 1.10).

```
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 172.31.255.253 to network 0.0.0.0

C    192.168.101.0/24 is directly connected, Vlan1
C    192.167.101.0/24 is directly connected, Vlan1
O    192.167.106.0/24 [110/5] via 172.31.200.22, 00:49:56, Vlan902
     192.167.107.0/24 is variably subnetted, 3 subnets, 3 masks
O       192.167.107.0/27 [110/6] via 172.31.200.86, 00:49:56, Vlan910
O       192.167.107.64/26 [110/18] via 172.31.200.86, 00:49:56, Vlan910
O       192.167.107.128/25 [110/5] via 172.31.200.38, 00:49:56, Vlan904
O    192.167.105.0/24 [110/3] via 172.31.200.70, 00:49:56, Vlan908
O    192.167.110.0/24 [110/5] via 172.31.200.13, 00:49:56, Vlan901
.....
```

Figura 1.11: Esempio di tabella di routing

In sostanza, gli algoritmi di routing calcolano i sink tree relativi a tutti i possibili router di destinazione, e quindi instradano i pacchetti esclusivamente lungo tali alberi. Ciascun router della rete conserverà una tabella di routing, generata a partire dal sink tree, che conterrà, per ogni sottorete di destinazione conosciuta dal router, l'indicazione della rotta (*route*) da far seguire ai pacchetti, cioè l'interfaccia tramite la quale instradare il traffico o l'IP del *next hop* (il salto successivo) sul percorso per raggiungere la sottorete di destinazione (Fig. 1.11). Eventualmente, se il protocollo è evoluto, la tabella di routing conterrà altre informazioni, come il peso della rotta (metrica), il protocollo di routing che l'ha comunicata al router, una marca temporale, etc.

Un'ultima osservazione: un router, specie se realizza un nodo di Internet, non può conoscere direttamente rotte per ogni destinazione possibile, perché la tabella di routing dovrebbe avere dimensioni (e quindi un'occupazione di RAM) enormi ed i tempi di aggiornamento sarebbero improponibili.

Il problema è di facile soluzione: alle rotte verso specifiche destinazioni si aggiunge anche la rotta verso la sottorete `0.0.0.0`, che, convenzionalmente, indica la destinazione "sconosciuta". Questa particolare rotta viene indicata come "*default route*" o "*last resort*": attraverso di essa il router instraderà tutto il traffico diretto a destinazioni non esplicitamente presenti nella tabella di routing.

Quando la rete cresce fino contenere decine di migliaia di nodi, diventa troppo gravoso mantenere in ogni router la completa topologia. Il routing va quindi impostato in modo gerarchico, come succede nei sistemi telefonici. La rete viene divisa in zone (spesso dette regioni): all'interno di una regione vale quanto visto finora, cioè i router (detti router interni) sanno come arrivare a tutti gli altri router della regione; viceversa, quando un router interno deve spedire qualcosa a un router di un'altra regione sa soltanto che deve farlo pervenire a un particolare router, detto router di confine (*border router*), che possiederà la rotta per il next hop verso la destinazione.

Il modo più semplice per implementare il routing è stabilire a priori i percorsi ottimali sulla rete e scrivere la tabella di routing direttamente nella configurazione dei router. Questo approccio, di tipo statico, ha il vantaggio della semplicità (non bisogna implementare sui router un software che calcoli le rotte, questo calcolo è gia stato fatto dall'amministratore di rete), ma richiede che l'amministratore conosca completamente la topologia della rete, in modo da poter calcolare i percorsi migliori. Inoltre l'amministratore dovrà materialmente scrivere la routing table d'ogni router e cambiarla esplicitamente ogni volta che è apportata una modifica alla topologia (un nuovo nodo, un guasto, la caduta di un circuito, un cambiamento negli indirizzi IP). Uno schema di questo tipo si adatta bene a piccole realtà, collegate a reti più grandi mediante un solo router di frontiera, che avrà anche il ruolo di last resort gateway. Nelle moderne reti si usano algoritmi dinamici, che si adattano automaticamente ai cambiamenti della rete. Questi algoritmi non sono eseguiti solo all'avvio della rete, ma rimangono in esecuzione sui router durante il normale funzionamento e aggiornano le rotte ad intervalli

temporali regolari o a seguito di variazioni di topologia.

Gli algoritmi di routing dinamico sono sostanzialmente di due tipi: *distance vector* e *link state*. Nel primo ogni router mantiene una tabella (*vector*) contenente un elemento per ogni altro router destinazione. Ogni elemento della tabella contiene la "distanza" (numero di hop, ritardo, ecc.) che lo separa dal router in oggetto e la linea in uscita da usare per arrivarci. Il protocollo distance vector più diffuso è il RIP. Per i suoi vicini immediati il router stima direttamente la distanza dei collegamenti corrispondenti, mandando speciali pacchetti ECHO e misurando quanto tempo ci mette la risposta a tornare. A intervalli regolari ogni router manda la sua tabella a tutti i vicini, e riceve quelle dei vicini. Quando un router riceve le nuove informazioni, calcola una nuova tabella scegliendo, fra tutte, la concatenazione migliore con quest'ordine: se stesso $\rightarrow$ vicino immediato $\rightarrow$ router remoto di destinazione.

Ovviamente, la migliore è la concatenazione che produce la minore somma di distanza fra il router stesso ed un suo vicino immediato (viene dalla misurazione diretta) e la distanza fra quel vicino immediato ed il router remoto di destinazione (viene dalla tabella ricevuta dal vicino immediato). L'algoritmo distance vector routing funziona piuttosto bene, ma è molto lento nel reagire alle cattive notizie, cioè quando un collegamento va giù. Ciò è legato al fatto che i router non conoscono la topologia della rete e basano le loro scelte solo sulle tabelle che vengono loro fornite dai router adiacenti.

Si è cercato di ovviare con un approccio diverso, che ha dato origine al link state routing. L'idea di base è che ogni router controlla lo stato dei collegamenti fra se stesso e i suoi vicini immediati (misurando il ritardo di ogni linea) e distribuisce tali informazioni a tutti gli altri; sulla base di tali informazioni, ogni router ricostruisce localmente la topologia completa dell'intera rete e calcola il cammino minimo verso tutti gli altri. I passi da seguire sono:

1. scoprire i vicini e identificarli;
2. misurare il costo (ritardo o altro) delle relative linee;

3. costruire un pacchetto con tali informazioni;
4. mandare il pacchetto a tutti gli altri router;
5. dopo aver ricevuto gli analoghi pacchetti che arrivano dagli altri router, costruire la topologia dell'intera rete;
6. calcolare il cammino più breve verso tutti gli altri router
7. redigere la tabella di routing e copiarla nella RAM.

Quando il router si avvia, invia un pacchetto HELLO su tutte le linee in uscita. In risposta riceve dai vicini i loro indirizzi (univoci in tutta la rete). Inviando vari pacchetti ECHO, misurando il tempo di arrivo della risposta (diviso 2) e mediando su vari pacchetti si deriva il ritardo della linea. Si costruisce un pacchetto con identità del mittente, numero di sequenza del pacchetto, età del pacchetto, lista dei vicini con i relativi ritardi. La costruzione e l'invio di tali pacchetti si verifica tipicamente a intervalli regolari o quando accade un evento significativo (es.: una linea va giù o torna su). La distribuzione dei pacchetti è la parte più delicata, perché errori in questa fase possono portare qualche router ad avere idee sbagliate sulla topologia, con conseguenti malfunzionamenti. Combinando tutte le informazioni arrivate, ogni router costruisce il sink tree della subnet e calcola il cammino minimo verso tutti gli altri router (l'algoritmo si chiama SPF, *Shortest Path First* [22]); con queste informazioni costruisce la propria tabella di routing.

Il vantaggio di questo approccio è che, all'occorrenza di una variazione dello stato della rete, è sufficiente che il router che la percepisce direttamente mandi una segnalazione a tutti gli altri, che, in modo autonomo, provvederanno a modificare le proprie tabelle di routing in conseguenza dell'evento segnalato. Il link state routing è molto usato attualmente su reti di grandi dimensioni: esempi di protocolli che implementano algoritmi di tipo link state sono: OSPF (*Open Shortest Path First*), che è il più usato, ed IS-IS (*Intermediate System-Intermediate System*), progettato per DECnet e poi adottato da OSI. La sua principale caratteristica è di poter gestire indirizzi

di diverse architetture (OSI, IP, IPX) per cui può essere usato in reti miste o multiprotocollo.

1.3.2 Comunicazione efficace

Fin qui si sono esaminati livelli, dispositivi e protocolli che, sinergicamente, ci consentono di realizzare la *connettività*, cioè la possibilità di scambiare dati tra due host, indipendentemente dalla loro distanza. Quel che ora occorre è uno strato che simuli la connessione diretta tra le due macchine, un cavo virtuale che nasconda al livello applicativo la complessità della rete fisica sottostante e che si occupi di organizzare e consegnare i dati affinchè siano fruibili dalle applicazioni. Il livello di Trasporto fa proprio questo, nello specifico sovrintende alle seguenti operazioni:

- offre servizi ai livelli applicativi;
- controlla la connessione;
- controlla il flusso dei dati;
- riordina le TPDU (Transport Protocol Data Unit).

La PDU di questo livello prende il nome di TPDU (Transport PDU) e l'indirizzamento, nel TCP/IP, è gestito mediante i numeri di porta.

Porta	Protocollo	Applicazione
21	FTP	File transfer
23	Telnet	Remote Login
25	SMTP	e-mail
80	HTTP	World Wide Web
110	POP3	Remote e-mail- access

Tabella 1.2: Indirizzi del livello di trasporto

Come si vede dalla tabella in Fig. 1.2, ciascun numero di porta identifica un servizio applicativo diverso: il *port number* è qundi il tramite con i

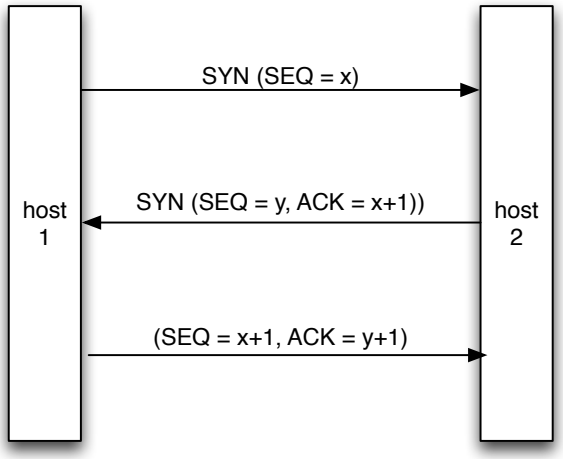


Figura 1.12: Three-way handshake

livelli applicativi superiori. Un servizio applicativo sarà quindi identificato dall'indirizzo IP dell'host che lo eroga e dal numero di porta che identifica il servizio stesso. Questa coppia di valori prende il nome di *socket*.

Un altro obiettivo del livello di trasporto è il riordino dei TPDU: il livello network si occupa, infatti, soltanto della consegna dei pacchetti, ma non garantisce che essi siano consegnati nell'ordine con il quale sono stati trasmessi. Ai fini della corretta ricostruzione dell'informazione è dunque necessario che il livello 4 si occupi di caricare il payload dei pacchetti ricevuti in un buffer e li consegni al livello 5 nell'ordine corretto. A questo livello è di fondamentale importanza la distinzione tra due tipologie di servizi: servizi affidabili orientati alla connessione (tipici di questo livello), servizi *datagram* senza gestione della connessione (poco usati in questo livello).

Il TCP [15] è il protocollo di livello 4 che si occupa di realizzare una connessione nell'ambito della suite TCP/IP. Il protocollo TCP è stato progettato per fornire un flusso di byte affidabile, da sorgente a destinazione, su una rete eterogenea e si occupa di:

- accettare dati dal livello application;

- spezzarli in segment, il nome usato per i TPDU (dimensione massima 64 Kbyte, tipicamente circa 1.500 byte);
- consegnarli al livello network, eventualmente ritrasmettendoli;
- ricevere segmenti dal livello network;
- rimetterli in ordine;
- consegnare i dati, in ordine, al livello application.

Esso realizza la connessione mediante un *three-way handshake*: l'host 1 invia all'host 2 un messaggio contenente la richiesta di iniziare la connessione ed un numero (sequence number) di sequenza; l'host 2 risponde con una "ricevuta di ritorno", contenente, a sua volta, un segnale di inizializzazione (SYN) con un proprio sequence number ed un segnale di acknowledgement (ACK) con il sequence number contenuto nel messaggio dell'host 1, aumentato di una unità. Come si vede dalla figura 1.12, il processo continua con una operazione analoga da parte dell'host 1, finché la connessione è attivata. Durante tutta la connessione i due host si scambieranno periodici messaggi di acknowledgement, in modo da effettuare il controllo della connessione. Il rilascio della connessione avviene mediante un messaggio di conclusione (FIN) al quale segue, normalmente, un messaggio di conferma della chiusura. Per evitare problemi alla disconnessione, spesso si stabilisce un tempo di timeout dopo il quale la connessione viene comunque considerata chiusa.

Il livello transport della suite TCP/IP fornisce anche UDP, un protocollo non connesso e non affidabile, utile per inviare dati senza stabilire connessioni (ad esempio per applicazioni client-server, streaming video). L'header di un segmento UDP è molto semplice e contiene essenzialmente la porta sorgente, la porta destinazione, la lunghezza del segmento ed una checksum, il calcolo della quale può essere disattivato, tipicamente nel caso di traffico in tempo reale (come voce e video) per il quale è in genere più importante mantenere un'elevato tasso di arrivo dei segmenti piuttosto che evitare i rari errori che possono accadere.

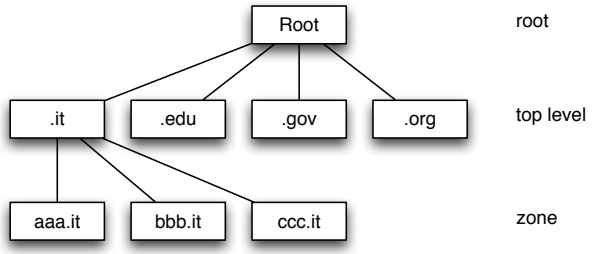


Figura 1.13: Gerarchia DNS

1.3.3 Le Applicazioni

In questo modello di architettura, sopra il livello transport c'è il livello application, nel quale viene effettivamente svolto il lavoro utile per l'utente. In questo livello si trovano diverse tipologie di oggetti:

- protocolli di supporto a tutte le applicazioni, come il DNS (*Domain Name System*, RFC 1034 e 1035);
- protocolli di supporto ad applicazioni di tipo standardizzato, come FTP (*File Transfer Protocol*, RFC 959) per il trasferimento di file, SMTP e POP3 (*Simple Mail Transfer Protocol*, RFC 821 e *Post Office Protocol*, RFC 1225) per la posta elettronica, HTTP (*HyperText Transfer Protocol*, RFC 1945) alla base del World Wide Web (WWW);
- applicazioni proprietarie.

DNS

Il DNS è un servizio di livello applicativo che mette in relazione gli indirizzi IP con delle stringhe di testo strutturate in modo gerarchico: i nomi di dominio (*domain name*), organizzati ad albero in *domini*, *sottodomini* (eventualmente altri sottodomini di livello inferiore...), fino ad arrivare a identificare il nodo desiderato[6] (Fig. 1.13).

[6]www.unime.it è l'host di nome www, appartenente al dominio unime.it

Il servizio, corrispondente alla porta 53 sia TCP (*zone tranfer*) che UDP (*request*), è erogato da nodi (*name server*) che si occupano di risolvere i nomi in indirizzi numerici IP e viceversa.

La gerarchia dei server rispecchia abbastanza fedelmente quella dei nomi di dominio, implementando almeno tre livelli: i *root server*, i *top level domain server*, i server di zona; una siffatta struttura permette di delegare al "proprietario" del dominio la gestione dei nomi degli host della propria zona (*hostname*), mantenendo comunque possibile la risoluzione del nome da ogni punto della rete mediante richieste ai nodi superiori dell'albero.

E-MAIL

La posta elettronica (*e-mail*) è uno dei servizi per i quali è nata la rete; è basata sul paradigma della posta tradizionale ed il suo utilizzo ne ripropone i passaggi, dalla composizione del messaggio, alla spedizione, all'iter di consegna, alla ricezione e lettura. Il servizio è realizzato mediante una serie di protocolli, ciascuno dedicato ad una particolare funzionalità; il cuore del sistema è il protocollo SMTP (*simple mail transfer protocol*, porta 25 TCP), che agisce da *mail transport agent* (MTA) e si occupa di ricevere i messaggi e trasportarli sulla rete fino al server (MTA) del destinatario.

La gestione delle *mailbox* moderne è demandata ai protocolli POP3 (*post office protocol*, porta 110 TCP) ed IMAP[7] (*Internet Message Access Protocol*, porta 143 TCP), che agiscono da *mail user agent*, consentendo all'utente finale di comporre, leggere, eliminare e spedire messaggi (via MTA).

Il singolo messaggio di posta elettronica ha un formato piuttosto semplice, che prevede un'intestazione (*header*) ed un corpo (*body*), separati da una linea vuota. Le linee che compongono l'header sono codificate in modo stringente, perché contengono i campi necessari al corretto instradamento del messaggio:

- *To*: indirizzo e-mail di uno o più destinatari, nella forma, a tutti nota, user@dominio.

[7] la gestione e-mail via web, alla quale siamo abituati, è realizzata tramite questo protocollo

- *From*: indirizzo e-mail del mittente
- *Cc*: indirizzo di uno o più destinatari per conoscenza;
- *Bcc*: come *Cc*, ma gli indirizzi non sono visibili al destinatario
- *Subject*: Argomento del messaggio

ed altri campi di gestione del messaggio, la cui descrizione non è qui essenziale.

Per ragioni storiche e di compatibilità, il formato previsto per i messaggi di posta elettronica è di "solo testo", costituito dai caratteri che compongono il codice ASCII; ciò renderebbe impossibile inviare allegati (immagini, filmati, documenti), in genere codificati in formato binario. Per superare questa limitazione viene utilizzato lo standard MIME (*Multipurpose Internet Mail Extension*, RFC 1341 e 1521), che si occupa di codificare (*encode*), allegare (*attach*) e decodificare (*decode*) gli allegati.

WORLD WIDE WEB

Il servizio, nato nel 1989 al CERN di Ginevra [17], è erogato dal protocollo HTTP (*hypertext transfer protocol*, porta 80 TCP) e prevede un'architettura basata su client (i *browser*) che interrogano *pagine*, scritte in linguaggio HTML, rese disponibili da server (*siti*) distribuiti su tutta la rete mondiale. L'architettura prevede uno spazio d'indirizzamento basato su URL (*Uniform Resource Locator*), sequenze di caratteri che identificano univocamente una risorsa, nella forma:

```
protocol://<user:pass@>host<:port></path><?query>
```

In tabella 1.3 sono riportati alcuni esempi.

Gli unici elementi indispensabili sono il protocollo e l'*hostname* del server da raggiungere; i campi opzionali *user* e *password* servono all'autenticazione per la consultazione di risorse private, il campo *port* è la porta del TCP (eventualmente diversa dalla 80 standard), il *path* è il percorso diretto tramite il quale è possibile raggiungere una risorsa senza passare dalla pagina iniziale

Nome	Uso	Esempio
http	Hypertext (html)	http://www.unime.it
ftp	FTP	ftp://files.unime.it
gopher	Gopher	gopher://gopher.unime.it/libs
mailto	e-mail	mailto:user@unime.it

Tabella 1.3: Esempi di URL

(*home page*) e, infine, il campo *query* è utile per passare parametri a pagine dinamiche, costruite a richiesta, mediante linguaggi di programmazione (per esempio il Python), basandosi sui dati presenti in un datatabase.

Questa forma di gestione degli indirizzi è molto potente e permette di collegare contenuti presenti su pagine e server diversi mediante *hyperlink*, basati sulla URL della risorsa da referenziare; ciò consente la "navigazione Internet" (*browsing*) con le modalità da tutti sperimentate nella vita quotidiana.

SEARCH ENGINES

Fin dagli inizi del Web un utente si trova più frequentemente a voler cercare informazioni di cui ignora la provenienza, piuttosto che accedere ad una pagina di cui possiede già la URI. Quest'ultimo è tutt'altro che un evento raro, ancora oggi la navigazione comprende sempre accedere a pagine usuali, in cui si ha interesse a verificare l'aggiornamento delle informazioni contenute, si pensi al sito di una Facoltà universitaria o ancor più alle versioni on-line di quotidiani. Purtuttavia il primo caso, in cui si ha in mente il genere di conoscenze desiderate ma non la loro fonte, perlomeno non sotto forma di URI, è di importanza prevalente nella fruizione della rete.

Una maniera inizialmente pratica di affrontare il sistema fu quella degli elenchi di risorse, pagine Web di per se scarse di contenuto, ma ricche di link ad altre pagine, selezionate manualmente ed eventualmente corredate singolarmente di un breve commento. è una soluzione che richiede un grande sforzo umano, ed è impiegata esclusivamente per settori ristretti, dove an-

cora oggi costituisce la forma più precisa e preziosa di ausilio alla ricerca. è evidentemente impraticabile come modo generalizzato di cercare nel Web. Il metodo che si è andato invece affermando è quello dei cosiddetti motori di ricerca, *search engine*, sistemi che l'utente interroga mediante una serie di parole, che reputa significative dei contenuti che cerca, e restituiscono elenchi di link a pagine selezionate automaticamente, sulla base di una semplice verifica del contenere quelle parole (dette *keywords*, parole chiave). Attualmente esiste un migliaio circa di diversi motori di ricerca, ma in questa sezione si prenderà in esame solo quello che da alcuni anni si è andato affermando come il più popolare dei motori di ricerca: Google. La sua fama è ben motivata risultando effettivamente il più efficiente sulla base di valutazioni oggettive [23].

Ci sono comunque degli elementi del sistema Google che sono comuni alla maggior parte degli altri motori di ricerca. Ciò che l'utente vede abitualmente, la pagina con la form per scrivere parole, è l'interfaccia del componente *searcher* del sistema, quello che effettua le ricerche per gli utenti. In realtà questo sottosistema non cerca proprio nulla su internet, ma funziona totalmente su database interni al motore di ricerca, generati dagli altri componenti. L'insieme degli archivi interni, denominato semplicemente *index*, è costruito dal software che si chiama appunto *indexer*, il quale pure lavora completamente off-line, su un altro enorme database, il *repository*, dove sono immagazzinate in formati compressi tutte le pagine Web conosciute dal motore di ricerca. Infine il *repository* è costruito dal *crawler*, il programma che effettivamente recupera copie delle pagine da internet.

Quest'ultima operazione è di gran lunga la più lenta, perché richiede l'effettiva navigazione attraverso la rete. è effettuata da tante copie dello stesso programma che lavorano in parallelo su computer distribuiti, raggiungendo velocità dell'ordine di migliaia di documenti scaricati al secondo. Pur con questo ritmo, se si tiene conto che attualmente il volume di documenti controllati da Google è di diversi miliardi, il tempo di attraversamento dell'intera rete è di decine di giorni. Mediamente uno stesso sito è rivisitato dai crawler

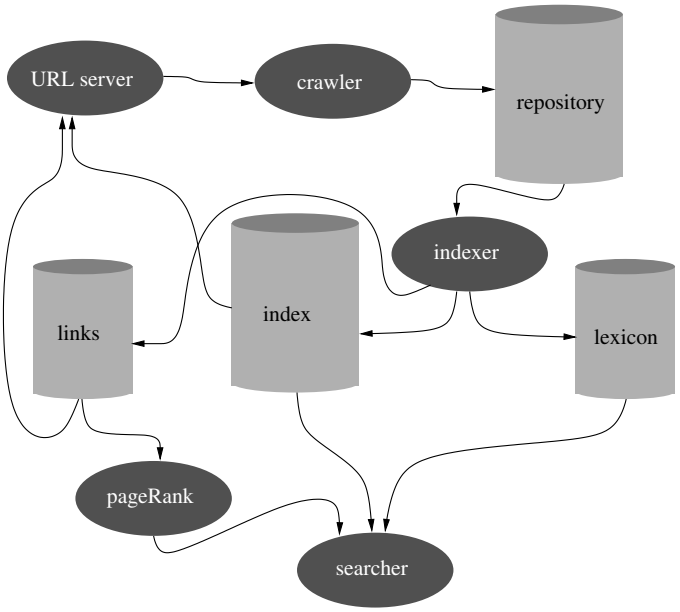


Figura 1.14: Uno schema generale dell'architettura di Google, o di un motore di ricerca analogo.

circa una volta al mese.

L'indexer passa in rassegna tutte le pagine archiviate nel repository e ne estrae diverse caratteristiche importanti per la ricerca. Anzitutto produce le liste dei cosiddetti *hits*, che sono parole con abbinato il numero di volte in cui compaiono nel documento, e la loro posizione. Inoltre riserva un trattamento particolare al testo contenuto nei tag `A`, che viene immagazzinato come parziale descrizione della pagina cui rimanda il link, e naturalmente viene inoltre archiviata la URI del link stesso. Queste informazioni sono quelle che poi, processate dal *URL Server*, andranno ad informare il crawler su dove reperire da internet le pagine. Ma un uso particolare in Google è quello che verrà spiegato al paragrafo successivo. Uno schema complessivo del sistema è in Fig. 1.14.

Il searcher tipicamente non effettua nulla di complesso, ma semplicemente cerca nell'index tutte le pagine che contengono le parole scritte dall'utente. Vi sono pochissimi accorgimenti opzionali che possono raffinare la ricerca, del tipo di imporre che le parole siano consecutive. Il risultato è che abitualmente

una ricerca sia esaudita da diverse migliaia di documenti. Aggiungere parole chiave non sempre migliora la situazione, e facilmente si passa da un numero molto elevato a nessun documento, quando le parole sono evidentemente poco compatibili. La strategia che può cambiare radicalmente la soddisfazione nella ricerca di conoscenze è nell'assegnare in qualche modo un punteggio alle pagine trovate, e presentarle nell'ordine corrispondente. Siccome chi naviga difficilmente si prende la briga di esaminare il contenuto di più di qualche decina di pagine recuperate, è evidente quanto sia essenziale che compaiano al primo posto quelle, tra molte migliaia, veramente rilevanti.

Le strategie dei primi motori di ricerca erano basate su semplici valutazioni rispetto alle parole cercate: per esempio aveva maggior punteggio una pagina che conteneva un numero maggiore di hit o un rapporto tra hit e numero complessivo di parole vantaggioso. Data l'importanza capitale per siti commerciali di comparire in cima agli elenchi dei motori di ricerca, criteri di questo genere hanno innescato rapidamente distorsioni aberranti, come pagine web ingigantite da parole invisibili (per es. scritte in colore bianco su sfondo bianco), ripetute migliaia di volte. Lo stesso fenomeno si potrebbe ripetere per qualunque criterio estratto dalla pagina stessa, è evidente che un'oggettività non poteva che scaturire da elementi esterni al documento, non controllabili da chi progetta la propria pagina.

Così come l'intero Web è derivato da un primo uso accademico, anche il metodo introdotto da Google, denominato *PageRank* [24], è preso in prestito dal modello di valutazione degli articoli scientifici in sede accademica: tramite le citazioni che riceve l'articolo stesso. Analogamente, il metodo PageRank assegna un punteggio ad ogni pagina Web in base a quante altre pagine hanno link a essa diretti, pesando il contributo di questi link mediante il punteggio di quelle altre pagine. In altre parole, un documento è ritenuto importante se ci sono altri documenti in cui compare come link, ma lo è ancor di più se questi documenti sono importanti.

Capitolo 2

Sicurezza

Per lo studio delle problematiche riguardanti la Sicurezza Informatica, la Firma digitale e la Posta Elettronica Certificata lo studente è invitato ad usare come traccia le slides del corso, approfondendo i contenuti mediante la lettura dei seguenti documenti:

- DigIt PA - *Guida alla Firma Digitale* - 2009

  `http://www.digitpa.gov.it/sites/default/files/GuidaFirmaDigitale2009_a_0_0_0.pdf`

- DigIt PA - *Firme elettroniche*

  `http://www.digitpa.gov.it/firme-elettroniche-certificatori`

- DigIt PA - *Posta Elettronica Certificata*

  `http://www.digitpa.gov.it/pec`

Bibliografia

[1] Joseph C.R. Licklider. Man-computer symbiosis. *IRE Transactions on Human Factors*, 1:4–11, 1960.

[2] J. C. R. Licklider. Man-computer partnership. *International Science and Technology*, May 1965.

[3] J. C. R. Licklider and Robert W. Taylor. The computer as a communication device. *Science and Technology*, April 1968.

[4] Leonard Kleinrock. *Information Flow in Large Communication Nets.* Proposal for a ph.d. thesis, MIT, May 1961.

[5] J. C. R. Licklider and Wesley Clark. On-line man-computer communication. In *Proceedings of the May 1-3, 1962, spring joint computer conference San Francisco, California*, AIEE-IRE '62 (Spring), pages 113–128, New York, NY, USA, May 1962. ACM.

[6] Leonard Kleinrock. *Communication Nets: Stochastic Message Flow and Design.* McGraw-Hill, New York, 1964.

[7] Paul Baran. On distributed communications. Memoranda for United States Air Force Project, RAND Corporation, Santa Monica (CA), august 1964.

[8] D. W. Davies, K. A. Bartlett, R. A. Scantlebury, and P. T. Wilkinson. A digital communication network for computers giving rapid response at remote terminals. In *Proceedings of the first ACM symposium on Operating System Principles*, SOSP '67, pages 2.1–2.17, New York, NY, USA, 1967. ACM.

[9] Lawrence G. Roberts. Multiple computer networks and intercomputer communication. In *Proceedings of the first ACM symposium on Operating System Principles*, SOSP '67, pages 3.1–3.6, New York, NY, USA, October 1967. ACM.

[10] S. D. Crocker. Host software, 1969.

[11] E. Krol. Hitchhikers guide to the internet, 1989.

[12] S. D. Crocker. New host-host protocol, 1970.

[13] V. Cerf, Y. Dalal, and C. Sunshine. Specification of internet transmission control program, 1974.

[14] J. Postel. Internet protocol, 1981.

[15] J. Postel. Internet message protocol, 1980.

[16] T. J. Berners-Lee, R. Cailliau, and J.-F. Groff. The World-Wide Web. *Computer Networks and ISDN Systems*, 25:454–459, 1992.

[17] T. Berners-Lee, R. Fielding, and H. Frystyk. Hypertext transfer protocol – http/1.0, 1996.

[18] D. DiNucci. Fragmented future. *Print*, 53(4):32, 1999.

[19] C. ISO. Information technology - open systems interconnection - basic reference model. International Standard 7498, ISO/IEC, United States, November 1994.

[20] A. G. Malis. Arpanet 1822l host access protocol, 1981.

[21] J. Postel and J. K. Reynolds. Standard for the transmission of ip datagrams over ieee 802 networks, 1988.

[22] Edsger W. Dijkstra. A note on two problems in connexion with graphs. *Numerische Mathematik*, 1(1):269–271, December 1959.

[23] Yi Shang and Longzhuang Li. Precision evaluation of search engines. *World Wide Web: Internet and Web Information Systems*, 5:159–173, 2002.

[24] Sergey Brin and Lawrence Page. The anatomy of a large-scale hypertextual Web search engine. *Computer Networks and ISDN Systems*, 30:107–117, 1998.

Appendice

- DigIt PA - *Guida alla Firma Digitale* - 2009

  http://www.digitpa.gov.it/sites/default/files/GuidaFirmaDigitale2009_a_0_0_0.pdf

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);

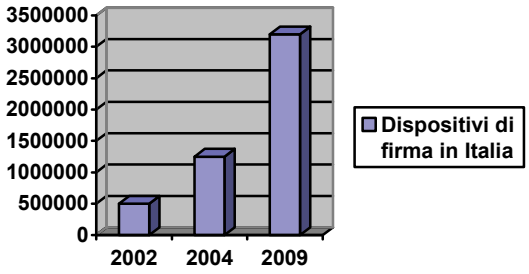
d) deve essere generata utilizzando un dispositivo sicuro che soddisfi i requisiti dell'allegato III della Direttiva.

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.

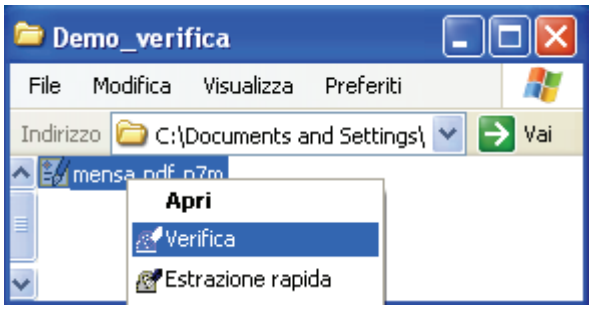


Figura 13.1 – Apertura del file in modalità verifica -

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).

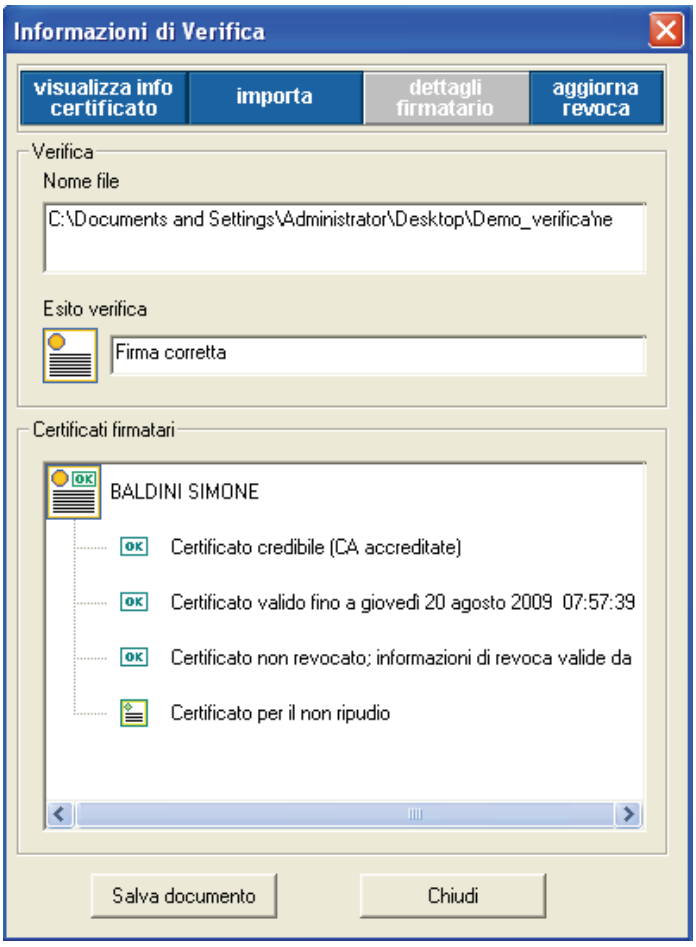


Figura 13.2 – Rapporto del software di verifica -

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.

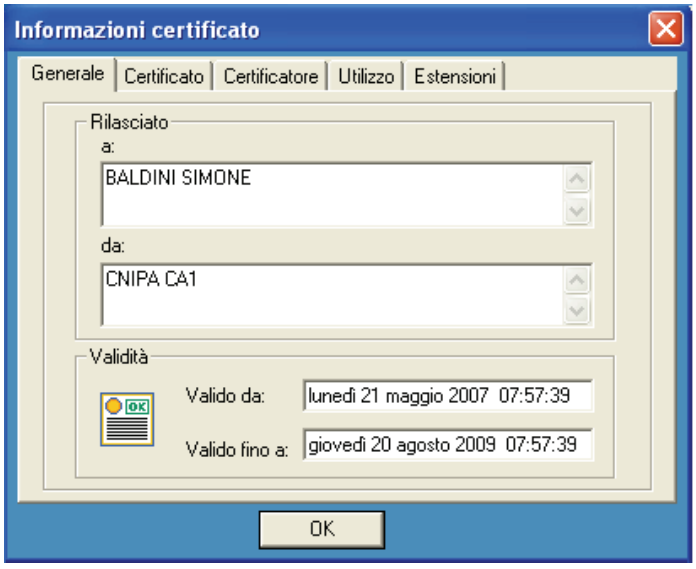


Figura 13.3 – Informazioni sul certificato del sottocrittore –

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!

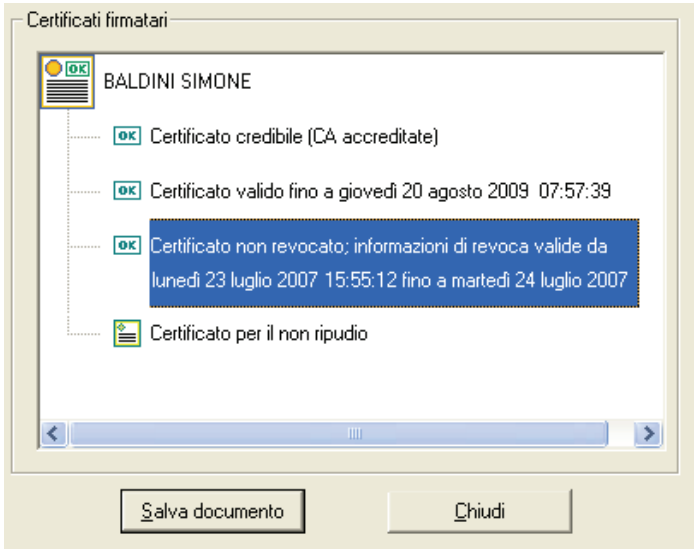


Figura 13.4 – Rapporto software di verifica: dettaglio revoca –

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.

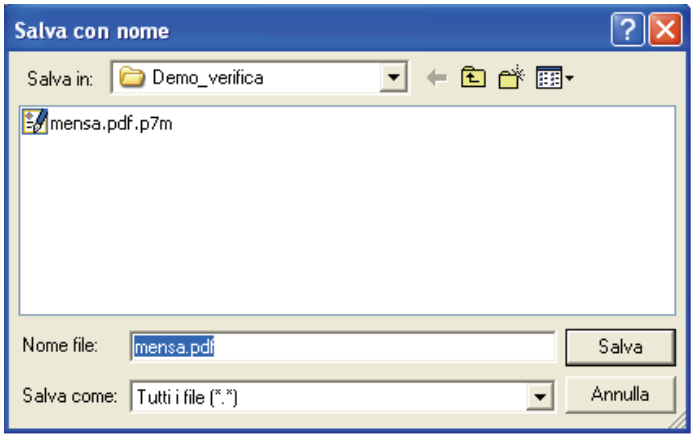


Figura 13.5 – Salvataggio del file estratto –

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.

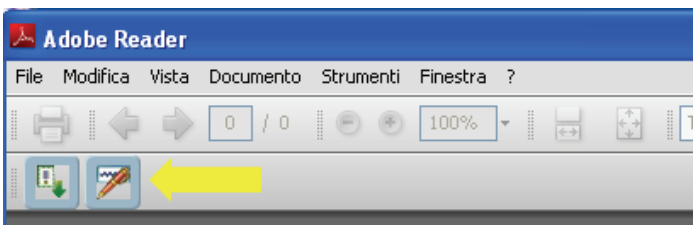
15.1 Firma digitale PDF: preparazione dell'ambiente

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.

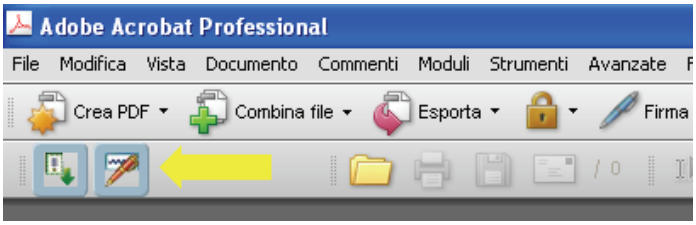


Figura 14.2 – Aggiunta del plug-in al Reader e al Professional –

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.

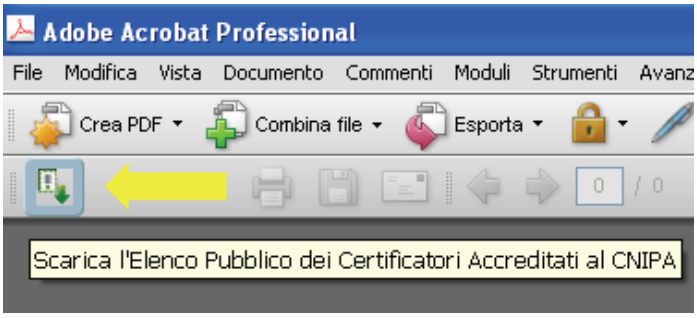


Figura 14.3 – Pulsante per l'istallazione dell'Elenco Pubblico –

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)

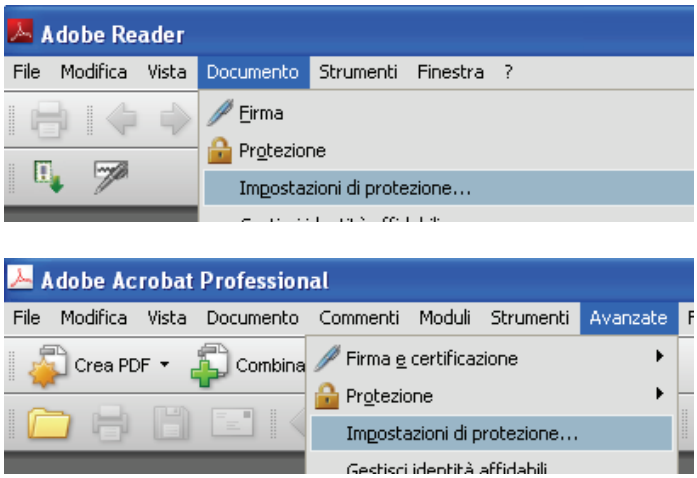
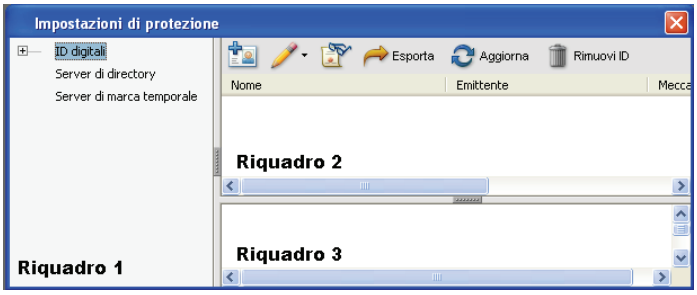


Figura 14.4 – Apertura del gestore dei certificati –

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.

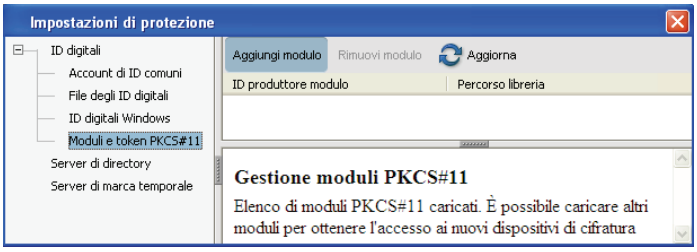
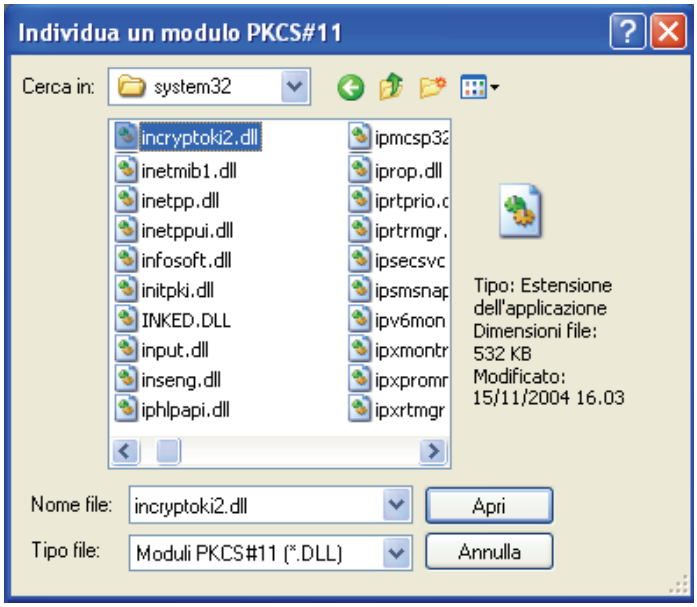


Figura 14.5 – Selezione del certificato di firma : Scelta della smart card –

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.



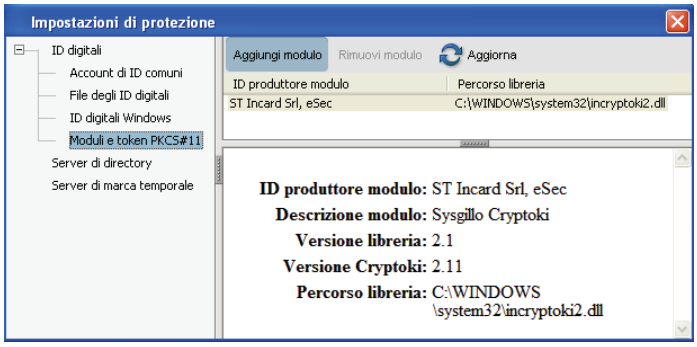


Figura 14.6 – Selezione del certificato di firma : Scelta del file *.dll* relativo alla smart card fornita –

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

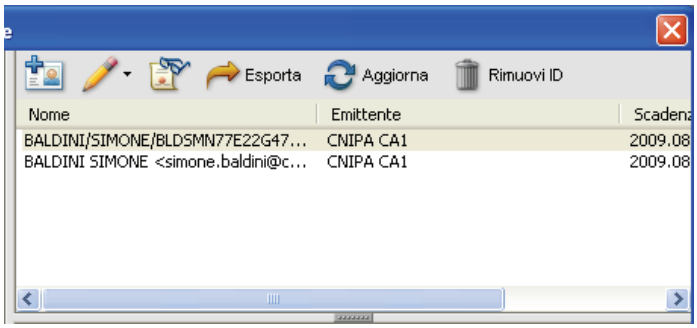


Figura 14.8 – Selezione del certificato di firma : Visualizzazione dei certificati della smart card –

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.

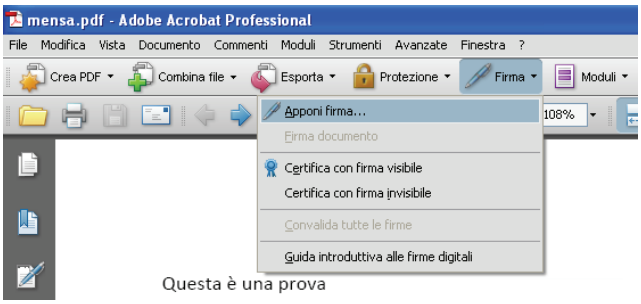


Figura 14.9 – Selezione voce : Apponi firma… –

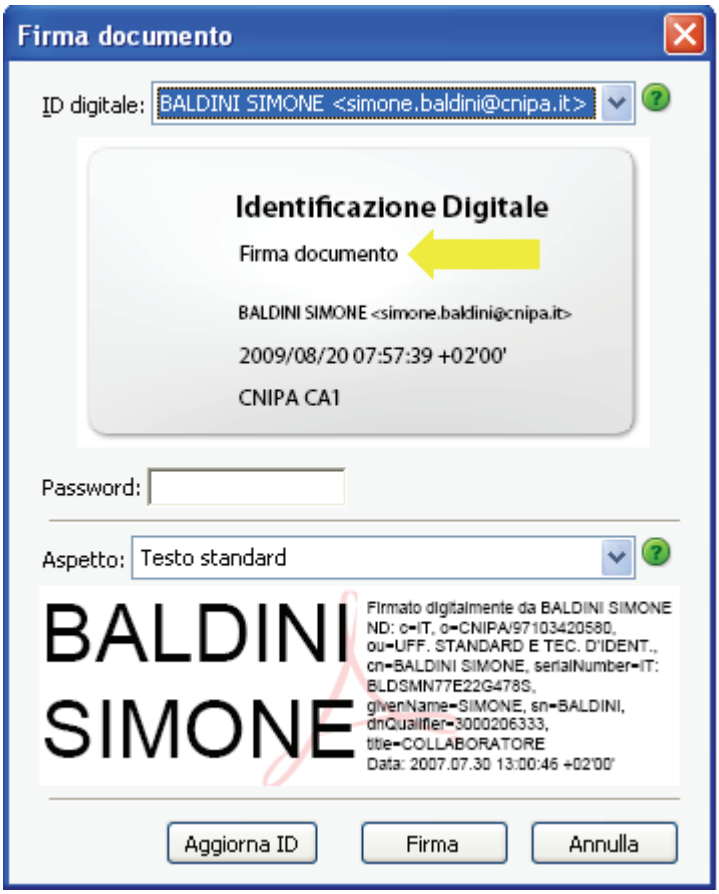


Figura 14.10 – Scelta del certificato di firma e immissione PIN –

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)

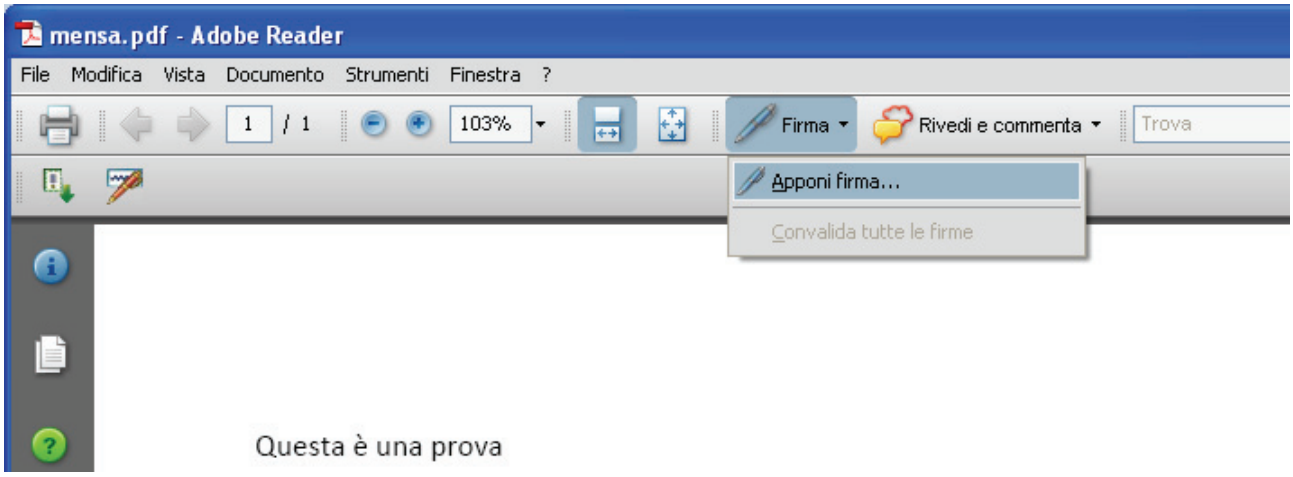


Figura 14.11 – Selezione voce : Apponi firma… –

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.

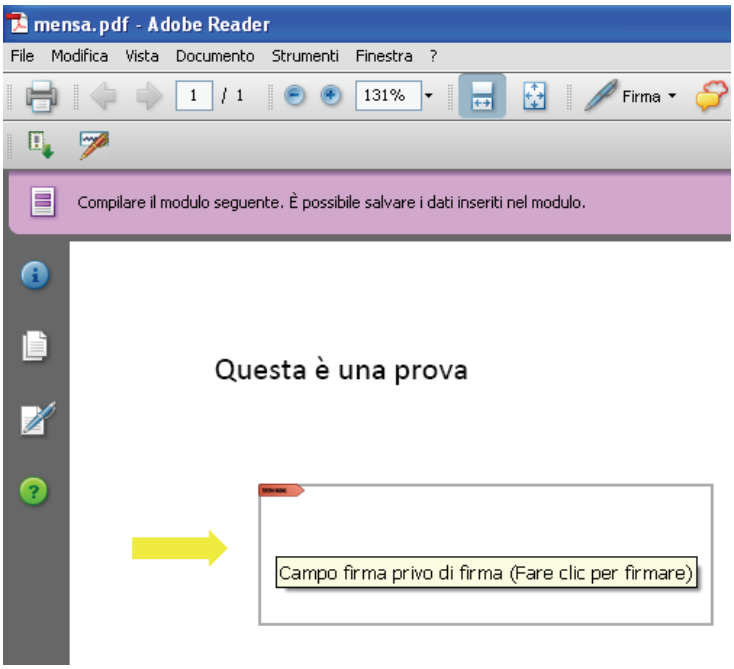


Figura 14.12 – Documento PDF con campo firma vuoto –

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.

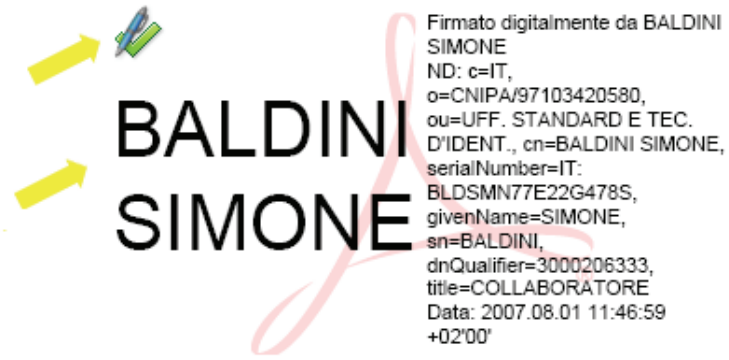


Figura 15.1 – Aspetto della firma –

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.

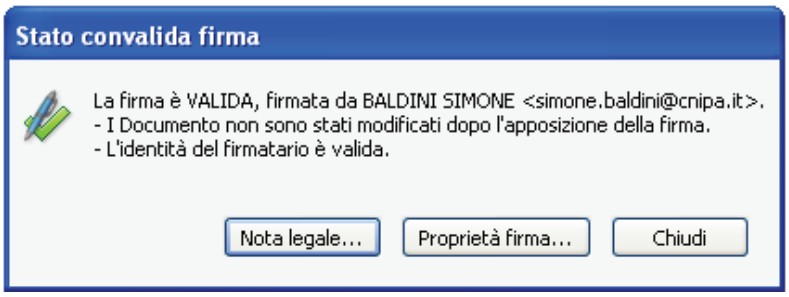


Figura 15.2 – Rapporto sintetico sulla verifica –

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.

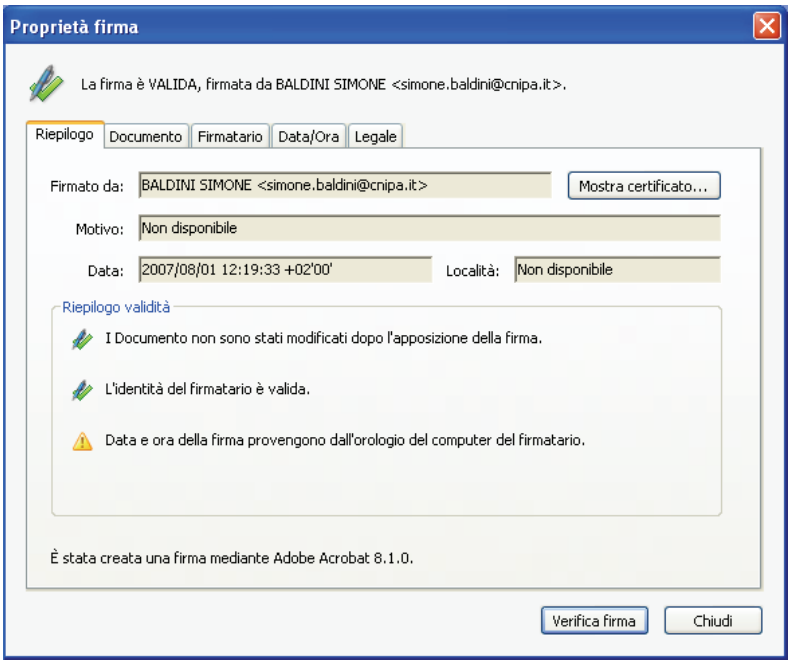


Figura 15.3 – Finestra di verifica : Riepilogo –

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.

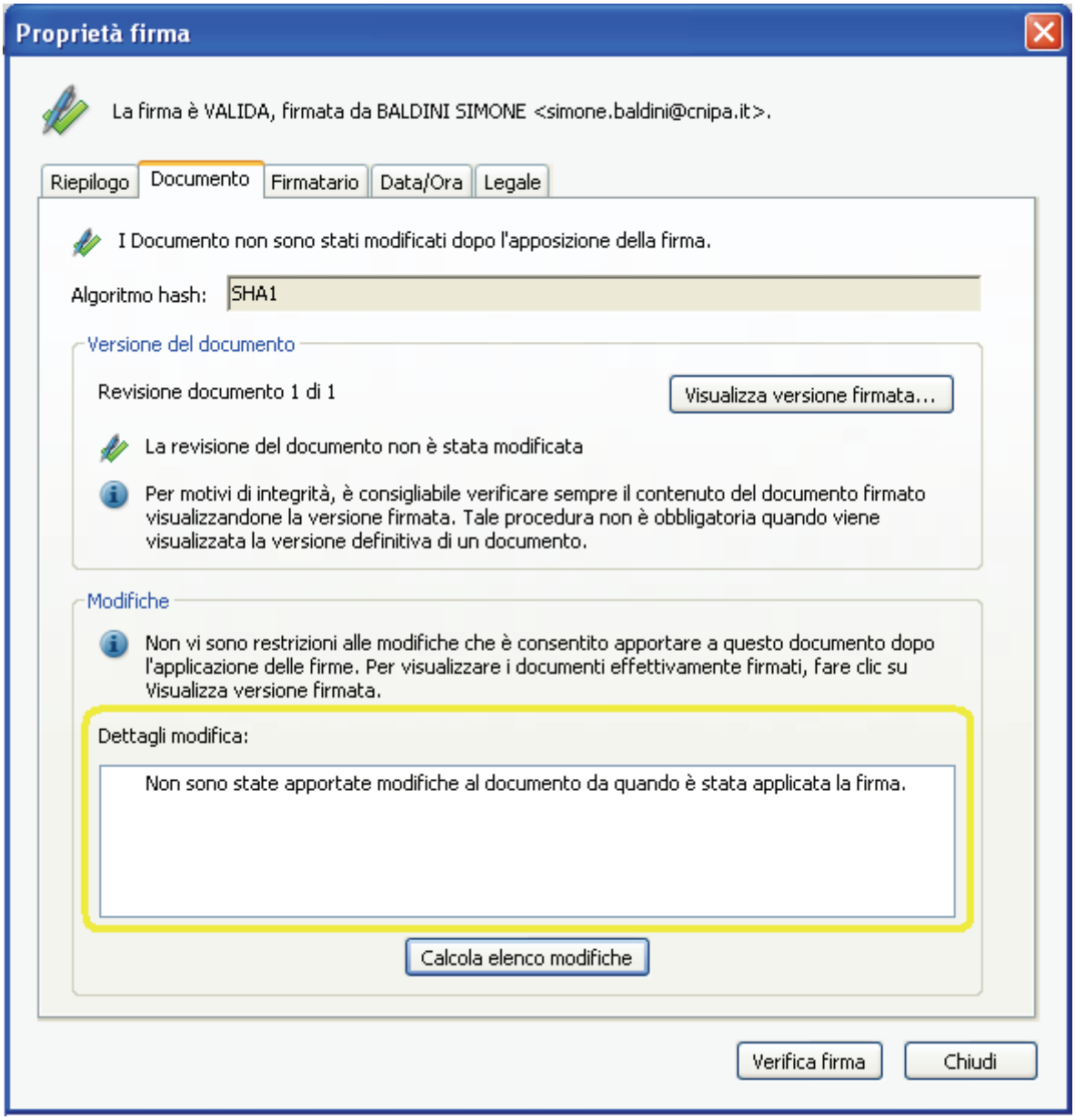


Figura 15.4 – Finestra di verifica : Verifica integrità del documento –

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)

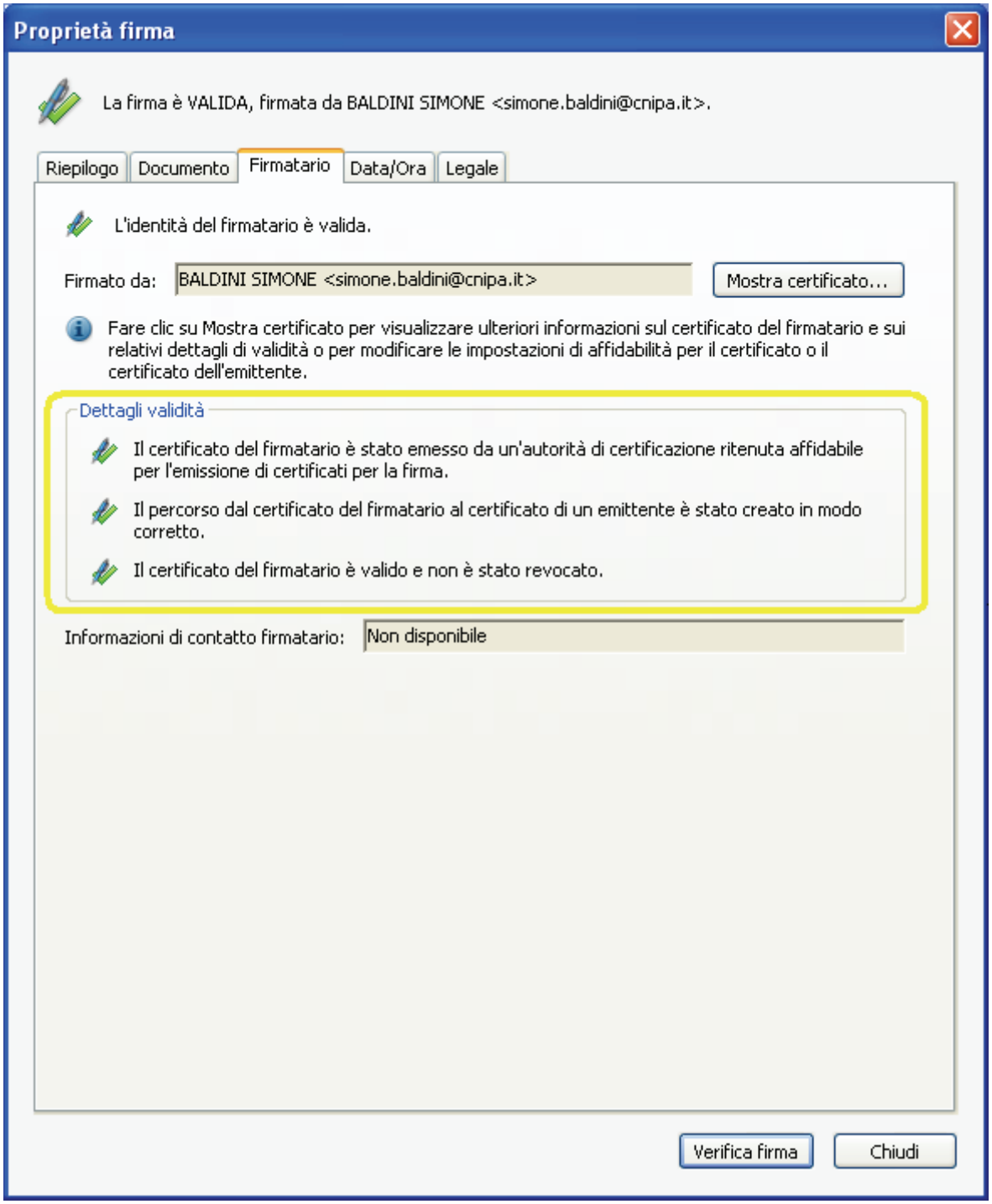


Figura 15.5 – Finestra di verifica : Verifica del certificato e della CA emittente –

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;

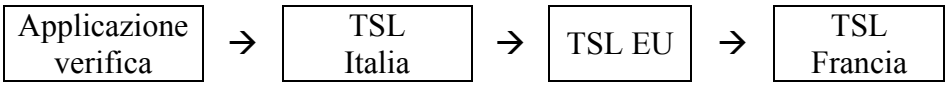
2. interpretare correttamente i certificati di sottoscrizione in modo da comprenderne la tipologia, comprendere se una determinata firma digitale presuppone l'utilizzo di un dispositivo sicuro per la generazione della firma;

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.

Typeset with LaTeX