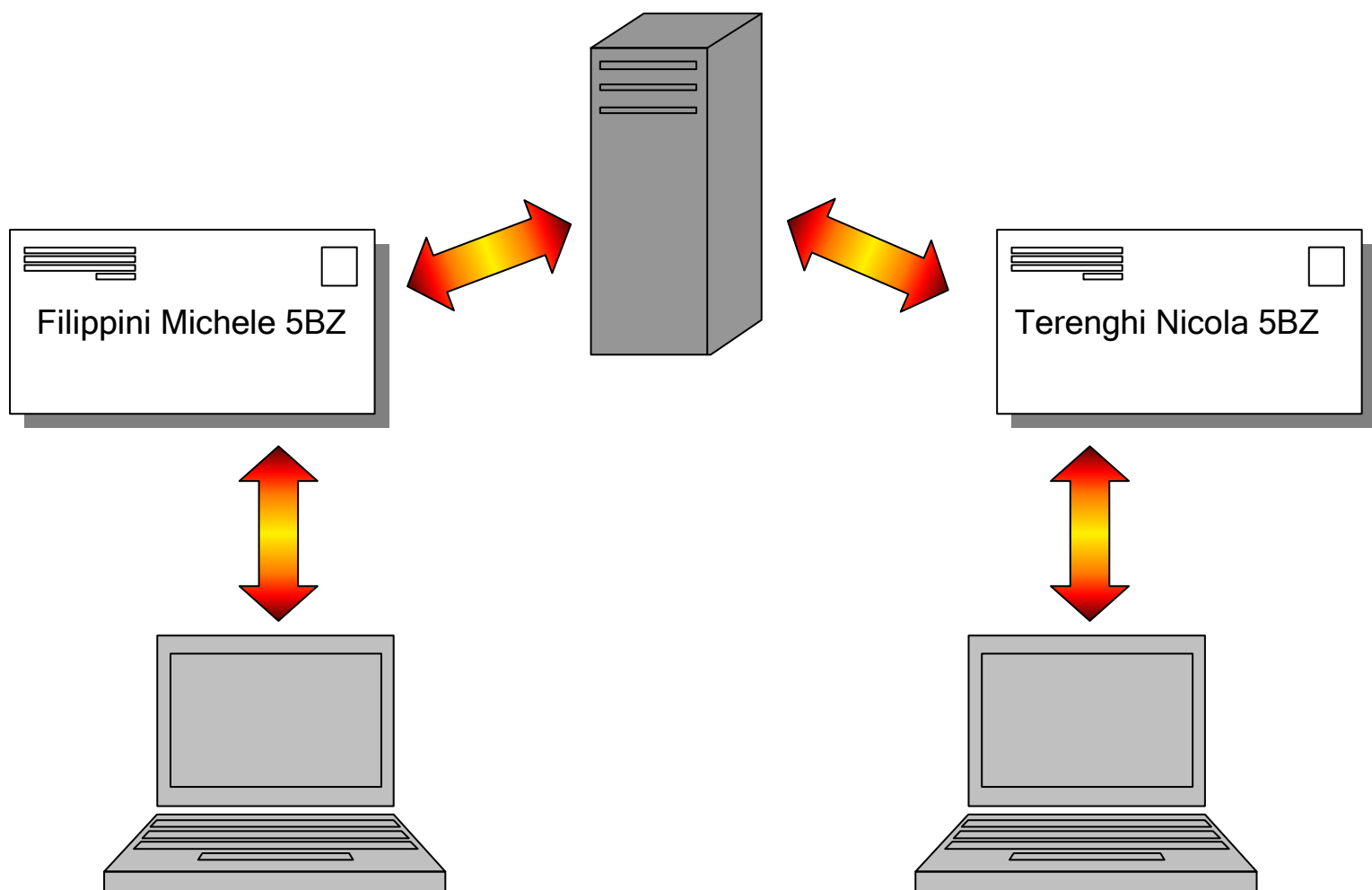


SERVER DI POSTA ELETTRONICA

INTRANET



Introduction

A protocol is a group of rules which control any data exchange activity among two entities.

In our case the two entities are the server, which provides the mail service, and the user, who receives the service.

POP3 (post office protocol) is the protocol needed for receiving the electronic mail messages (e-mail). In fact POP3 is used to read the mails contained in the server, through internet, in quick and simple way.

Since it is used only for receiving and for showing, it does not contain commands for sending messages. In these cases another protocol called SMTP is used.

In order to learn the function of this protocol, a search in the WEB has been made and thanks to the information given by the teacher, we started to design a client program and a server program which permits us the study of the protocol. The client and the server have been developed through Delphi (a visual programming mode for the rapid develop of general application and client-server application for Windows).

As far as the client program is concerned, we started from a program previously developed by a student of the institute. As far as the sever program is concerned, we started from a server made by a group of various types of programming experts.

The client program was created with the intention to make a program which uses POP3 for showing the e-mail in the server without need to download it, so that to decide which message must be deleted for avoiding the spam messages and the virus messages.

The reasons for which we have developed this project are:

- To Deepen the knowledge of the programming languages;
- To Learn the POP3 and SMTP protocol;
- To Try to make a client for receiving mails;
- To Try to make a mail server;

Introduzione

Con il termine protocollo si intende insieme di regole che governano ogni attività di scambio di dati fra due entità. Nel nostro caso le due entità sono, il server che fornisce il servizio di posta e l'utente che riceve il servizio.

Per apprendere il funzionamento dei protocolli POP3 e SMTP è stata svolta una ricerca su internet e grazie alle informazioni forniteci dal professore, abbiamo progettato un programma server e un client che ci permettessero di studiare i due protocolli. Entrambi sono stati sviluppati con l'utilizzo di Delphi (un ambiente di programmazione visuale ad oggetti per il rapido sviluppo di applicazioni in ambiente windows).

Per quanto riguarda il programma client abbiamo preso come spunto un programma precedentemente creato da degli alunni del istituto, mentre per quanto riguarda il programma server siamo partiti dalla base di un server creato da un gruppo di esperti di vari linguaggi di programmazione.

Il programma server è stato creato per approfondire la conoscenza dei protocolli che stanno alla base della trasmissione di messaggi di posta elettronica.

Il programma client è nato con l'intenzione di creare un programma che utilizzasse il protocollo POP3 per mostrare le e-mail presenti nelle varie mailbox di un server senza doverle necessariamente scaricare, in modo da poter decidere a priori quali cancellare per evitare messaggi di spam o contenenti virus.

Gli scopi che ci hanno spinto a sviluppare questo progetto sono:

- Approfondire le nostre conoscenze sui linguaggi di programmazione;
- Apprendere i protocolli POP3 e SMTP;
- Costruire un client che riceva le e-mail;
- Costruire un server di posta elettronica POP3;
- Approfondire le conoscenze sulla posta elettronica certificata;

Come avviene la trasmissione di una e-mail?

Quando si spedisce una e-mail da un computer ad un altro attraverso la rete, ciò che succede non è la semplice copia di un file di testo da un disco fisso ad un altro. La principale differenza è che, oltre ai due computer mittente e destinatario, ne sono coinvolti anche altri. Un primo computer che non si vede è quello ove risiede la casella del destinatario. Questo computer, che deve essere per quanto possibile sempre attivo e accessibile in rete, ha il compito di ricevere tutte le e-mail dirette agli utenti che hanno la casella su di esso e conservarle finché ciascun destinatario, con suo comodo, non avrà provveduto a scaricarle. Spesso ci si riferisce a tale computer come server POP3.

Il mittente, così come il destinatario, sul proprio computer dispone solamente di un client di posta elettronica, ossia un programma in grado di gestire un archivio di e-mail (in arrivo e in partenza), di scaricare la posta in arrivo da un server POP3, spedire posta tramite protocollo SMTP.

In teoria, il client del mittente potrebbe, tramite la rete, aprire una sessione direttamente con il server POP su cui risiede la casella del destinatario, ma ciò in genere non avviene per ragioni pratiche: è opportuno che il client sia configurato per parlare sempre con uno stesso server, lasciando a questo il compito di contattare, attraverso la rete, il server del destinatario. Disponendo di un server apposito per la spedizione, il mittente può quindi fare uscire in pochi istanti la e-mail dal proprio computer, disinteressandosi di quanto tempo sarà necessario al server per farla giungere a destinazione. Inoltre, se una stessa e-mail deve essere inviata in copia a tanti destinatari che hanno le caselle su vari server POP3 sparsi per la terra, il mittente passerà al proprio server di spedizione una *unica* copia del mail: sarà il server a "fare le copie" e contattare tutti i computer destinatari. Pertanto, è consuetudine di tutti i provider mettere a disposizione dei propri clienti anche un server SMTP.

CLIENT/SERVER

Il server e' il computer che per mezzo di uno o più processi, gestisce ed offre dei servizi all'utente tramite un'applicazione chiamata client (un altro processo). Possono essere anche molti gli utenti che contemporaneamente accedono tramite il loro client alle informazioni (risorse) offerte dal server. La comunicazione avviene con la richiesta di un servizio da parte del client e la conseguente realizzazione del compito da parte del server, utilizzando i protocolli necessari per la comunicazione, per esempio quelli dello stack TCP/IP. Per compito si intende il funzionamento di qualcosa come i database, l'elaborazione on-line (server-side, ossia prodotta dal server e successivamente inviata al client), videogames, le pagine web, sistemi di posta elettronica, newsgroup, ecc. Un esempio ludico: i giochi Client/Server sono quelli che hanno bisogno di almeno due computer collegati tra loro (quindi in rete) e di due programmi: per esempio se pensiamo ad un gioco di gare automobilistiche, ebbene il programma del computer centrale a cui siete collegati che gestisce coordinate, carburante e condizioni di gara e' il server, che oltre a controllare il gioco terrà conto anche delle auto di ciascun utente collegato il quel momento insieme a voi. Il client invece e' il vostro computer che ha bisogno di un programma freeware o di rado ottenibile versando una piccola quota (shareware). Questo programma client fornisce l'utente di un'interfaccia che consente di interagire sia con la vostra automobile che con quella degli altri utenti connessi al server. Il paradigma client/server divide la comunicazione tra due applicazioni, non necessariamente presenti entrambe nello stesso computer, in due distinte categorie, caratterizzate da chi aspetta una comunicazione o da chi la inizia. Chi inizia la comunicazione è denominato client (cliente), server (servente) chi la aspetta. Normalmente l'applicazione client contatta l'applicazione server e le invia una richiesta, dopo di che si mette nell'attesa della risposta, e quando questa sarà arrivata continuerà nella sua esecuzione. L'applicazione server aspetta l'arrivo di una richiesta da un'applicazione client, esegue la necessaria computazione e invia il risultato al client (vedi figura a lato).



Protocollo POP3

Il protocollo POP3 (post office protocol) sta alla base della ricezione dei messaggi di posta elettronica, infatti è il POP3 che viene utilizzato per mezzo di internet per leggere la posta, contenuta nei server, in modo rapido e semplice. Essendo adibito solo alla ricezione e visualizzazione non contiene comandi per l'invio di messaggi.

Funzionamento Generale

Il protocollo POP3 descritto nella RFC 1939, fornisce le funzioni base per scambiare e cancellare la posta da un server di posta.

Per eseguire il processo di download viene instaurata una connessione di tipo TCP tra il client ed il server POP3 è di default in attesa sulla porta 110.

Una sessione POP3 consiste in una serie di comandi di tipo case-insensitive scambiati tra client e server seguiti da uno o più argomenti conclusi da CRLF.

La sessione POP3 è formata da tre stati:

Stato di autorizzazione

Questo stato si ha una volta avvenuta la connessione TCP. Il server mostra il messaggio di benvenuto e l'utente deve autenticarsi e ricevere l'autorizzazione per gestire la posta;

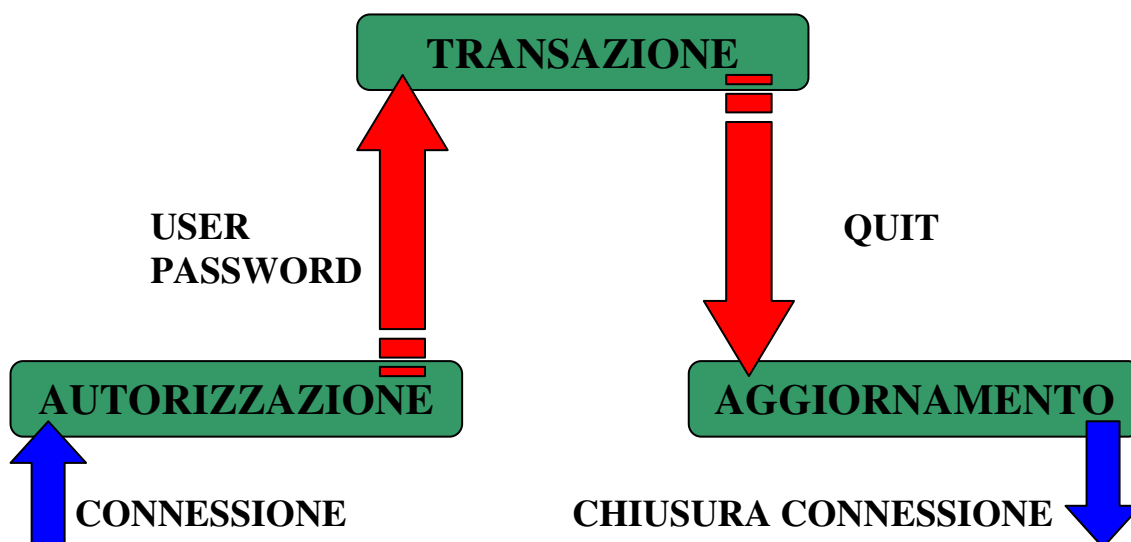
Stato di transazione

Dopo l'autenticazione si passa allo stato di transazione dove è possibile inviare i comandi al server per gestire i messaggi di posta;

Stato di aggiornamento

Dopo aver inviato il comando QUIT nello stato di transazione si passa nella fase di aggiornamento. Vengono eseguiti i comandi di cancellazione precedentemente memorizzati e successivamente la connessione TCP termina;

E' possibile che su un server POP3 sia impostato un tempo di inattività, trascorso il quale si viene automaticamente disconnessi senza passare nello stato di aggiornamento. In questo modo la connessione TCP termina e gli eventuali comandi di cancellazione inviati al server non saranno eseguiti.



COMANDI POP3

STATO DI AUTORIZZAZIONE

USER nome utente

- È il nome utente di un account di posta elettronica presente solo sul server al quale è connesso;
- Può essere inviato dopo la riga di benvenuto del server POP3 o dopo una sequenza USER/PASS che non si è conclusa con successo.

Se il server risponde con un messaggio di stato positivo (+OK), allora il client può fornire il comando PASS per completare l'autenticazione, oppure il comando QUIT per terminare la sessione POP3.

Se invece il server risponde con un messaggio di stato negativo (-ERR) al comando USER, allora il client può inviare di nuovo il comando di autenticazione, oppure può inviare il comando QUIT.

PASS password

- È la password dell'account identificato precedentemente tramite il nome utente;
- Deve essere inviato al server nello immediatamente dopo il comando USER accettato dal server.

Quando il client invia il comando PASS, il server utilizza la coppia di parametri inviati con la sequenza di comandi USER e PASS per determinare se quel client è autorizzato ad accedere a quella appropriata mailbox.

APOP name digest

- Può essere inviato al server dopo la riga di benvenuto del server o dopo una sequenza USER/PASS che non si è conclusa con successo.

Di norma una sessione POP3 inizia con la coppia di messaggi USER/PASS. Ciò comporta che sia l'utente sia la password relativa viaggino in chiaro sulla rete. Perciò il rischio di cattura della password è molto marcato. Quindi è necessario un metodo alternativo di autenticazione. Questa funzionalità è fornita dal comando APOP. Il server che implementa il comando APOP invia, nella riga di benvenuto indirizzata al client, dopo l'apertura della connessione, un "timestamp", una sorta di contrassegno temporale, che deve essere diverso ogni volta che il server invia una riga di benvenuto. Il client prende nota del "timestamp" e invia il comando APOP al server. Il parametro "name" ha lo stesso significato che nel comando USER.

Il parametro "digest" è calcolato dal client seguito da un codice segreto noto solamente al client e al server. Quando il server riceve il comando APOP, verifica il "digest" trasmesso dal client, se esso è corretto, il server risponde positivamente al client e passa di stato di TRANSAZIONE altrimenti il server rimane in stato di AUTORIZZAZIONE.

STATO DI TRANSAZIONE

STAT

Il server fornisce una risposta positiva con un messaggio (costituito da una riga) contenente informazioni riguardo alla mailbox. Questa riga viene chiamata "drop listing" per quella mailbox.

La drop listing contiene il numero di messaggi presenti sul server e le dimensioni totali della casella di posta in byte. I messaggi contrassegnati come DELETED non vengono riportati nelle drop listing.

LIST [msg]

- Msg è un "message-number" (opzionale), che se presente non si può riferire ad un messaggio contrassegnato DELETED;

Se viene fornito un parametro valido dopo il comando LIST il server invia una risposta positiva contenente le informazioni sul messaggio indicato. Se non viene fornito nessun parametro la risposta fornita è di tipo multi-linea e dopo la risposta positiva, il server invia una linea per ogni messaggio contenente le informazioni riguardanti quel messaggio, che consistono nel numero progressivo del messaggio contenuto nella mailbox, seguita dalla dimensione esatta del messaggio espressa in byte.

TOP msg n (comando opzionale)

- Msg è un “message-number” (obbligatorio), che non si può riferire ad un messaggio con contrassegno DELETED e un numero “n” non negativo di linee (richieste);

Se il server fornisce una risposta positiva, allora la risposta data è di tipo multi-linea. Dopo la sequenza iniziale “+OK”, il server invia le intestazioni (headers) del messaggio, la linea vuota che separa le intestazioni dal corpo del messaggio, e successivamente il numero di linee indicate nel corpo del messaggio, prestando attenzione a introdurre il carattere terminale (come accade in tutte le risposte di tipo “multi-linea”). Se il numero di linee richieste è superiore al numero di linee del corpo del messaggio il server invia l’intero messaggio.

RETR msg

- Msg è un “message-number” (obbligatorio), che non si può riferire a un messaggio con il contrassegno “DELETED”;

Se il server fornisce una risposta positiva, allora la risposta data è di tipo multi-linea. Dopo la sequenza iniziale “+OK”, il server invia il messaggio corrispondente al “message-number” fornito, prestando attenzione a introdurre il carattere terminale (come accade in tutte le risposte di tipo “multi-linea”).

DELE msg

- Msg è un “message-number” (obbligatorio), che non si può riferire ad un messaggio con il contrassegno “DELETED”;

Il server assegna al messaggio il contrassegno DELETED. Il server non cancella il messaggio fino a che la sessione POP3 non entra nello stato di AGGIORNAMENTO.

NOOP

Il server non fa nulla, risponde semplicemente con una risposta di tipo positivo; ad esempio quando si attiva il comando NOOP il server darà sempre una risposta “+OK”.

RSET

- Viene tolto il contrassegno “DELETED” a tutti i messaggi marchiat “DELETED” dal server. Il server restituisce poi una risposta positiva.

UIDL [msg] (comando opzionale)

- Un “message-number” (obbligatorio), che non si può riferire a un messaggio con il contrassegno “DELETED”.

Se è stato inserito un parametro (il numero del messaggio) dopo il comando e il server fornisce una risposta positiva, tale risposta giunge al client con una linea contenente informazioni riguardo a quel messaggio. Questa linea viene chiamata “inque-id listing” per quel messaggio.

Protocollo SMTP

Il Simple Mail Transfer Protocol (SMTP) è il protocollo utilizzato per trasmettere messaggi di posta elettronica tra due PC.

Il protocollo SMTP utilizza il protocollo di trasporto **TCP**, ed in particolare un server SMTP rimane costantemente in ascolto sulla **porta 25**. Il server SMTP si occupa poi di trasferire i messaggi nelle caselle di posta (mailbox) dei destinatari, oppure qualora non fosse il diretto responsabile di queste, inoltrarli (operazione di relay) al server che provvederà a farlo. La sintassi dei comandi è case-insensitive, ed è composta da istruzioni seguite da uno o più parametri terminate da un CRLF (Invio in codice ASCII). Il protocollo è descritto nella **RFC 821**, che però aveva diversi limiti riguardanti per esempio la dimensioni dei messaggi oppure la trasmissione di mail non in inglese o diverse dal semplice plain text. Per ovviare a questa restrizione è stato necessario estendere il protocollo tramite la RFC 1425 riguardante le SMTP Service Extensions.

Comandi SMTP

HELO NOME

Identifica il client SMTP al server SMTP.

EHLO NOME

E' possibile usare anche questo comando per identificarsi, se il server supporta le SMTP Service Extensions risponderà in modo positivo altrimenti con un errore di tipo 500 (*Syntax Error*).

MAIL FROM: <indirizzo mittente>

Indicata la mailbox del mittente del messaggio.

RCPT TO: <indirizzo destinatario>

Indica la mailbox del destinatario. E' possibile specificare attraverso molteplici RCPT TO diversi destinatari.

DATA

Indica al server che quanto digitato successivamente saranno i dati del messaggio di posta. Dopo il comando data possono essere inseriti dei "sotto-comandi" come, "FROM:" , "TO" , "SUBJECT" , "DATE" , "CC" , tutto quello che non verrà preceduto da questi comandi verrà considerato come corpo del messaggio cioè il testo del messaggio, per concludere il messaggio si deve digitare il punto "." Dopo essere andati a capo.

RSET

Annulla i comandi precedentemente inviati nella sessione SMTP corrente.

VRFY <stringa>

Chiede al server se la stringa di testo immessa rappresenta un nome utente presente ed in tal caso visualizza l'intero indirizzo.

HELP

Visualizza i comandi disponibili sul server.

NOOP

Non esegue nessuna operazione restituisce solo un messaggio Ok se il server risponde.

QUIT

Termina la sessione SMTP corrente.

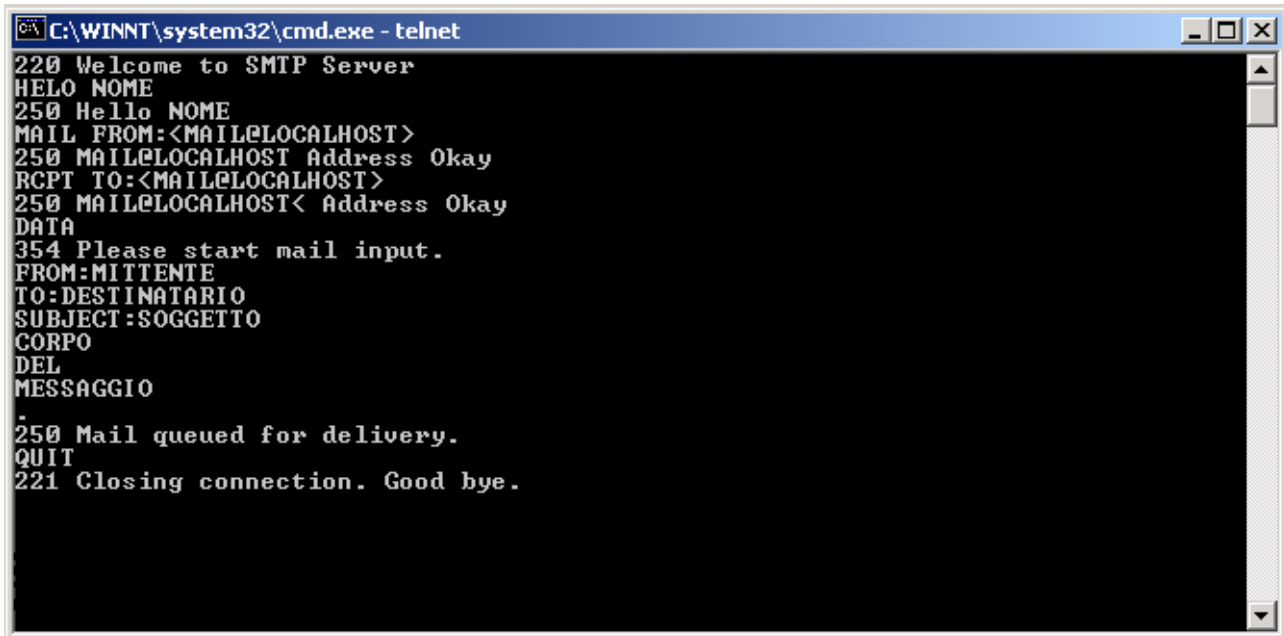
Fasi di una sessione SMTP

Una sessione SMTP attraversa almeno sei fasi:

1. Il client SMTP contatta il server sulla porta TCP 25. Se questo è in ascolto e la connessione è accettata risponde con un messaggio 220 (Ready);
2. Il client chiede di stabilire la sessione SMTP inviando il comando **HELO** seguito dal FQDN (Fully Qualified Domain Name). Se il server accetta risponde con un messaggio 250 (Ok);
3. Il client indica il proprio indirizzo tramite il comando **MAIL FROM**. Il server risponde con 250 (Ok) per ogni destinatario accettato;
4. Successivamente il client indica al server i destinatari del messaggio tramite **RCPT TO** ed il server risponde per ogni destinatario accettato un codice 250 (Ok);
5. Il client comunica al server l'intenzione di scrivere il corpo del messaggio con **DATA**. Il server risponde con un codice 354 e indica come marcare il termine del messaggio. I campi come Date, Subject, To, Cc, From vanno inseriti tra i dati della mail;

6. Completato il messaggio da scrivere tramite `.` il server memorizza la mail. A questo punto è possibile, scrivere un nuovo messaggio oppure inviare il comando **QUIT**, dopo il quale il server invia i messaggi e risponde con un codice 221 (Closing) e la connessione TCP viene terminata;

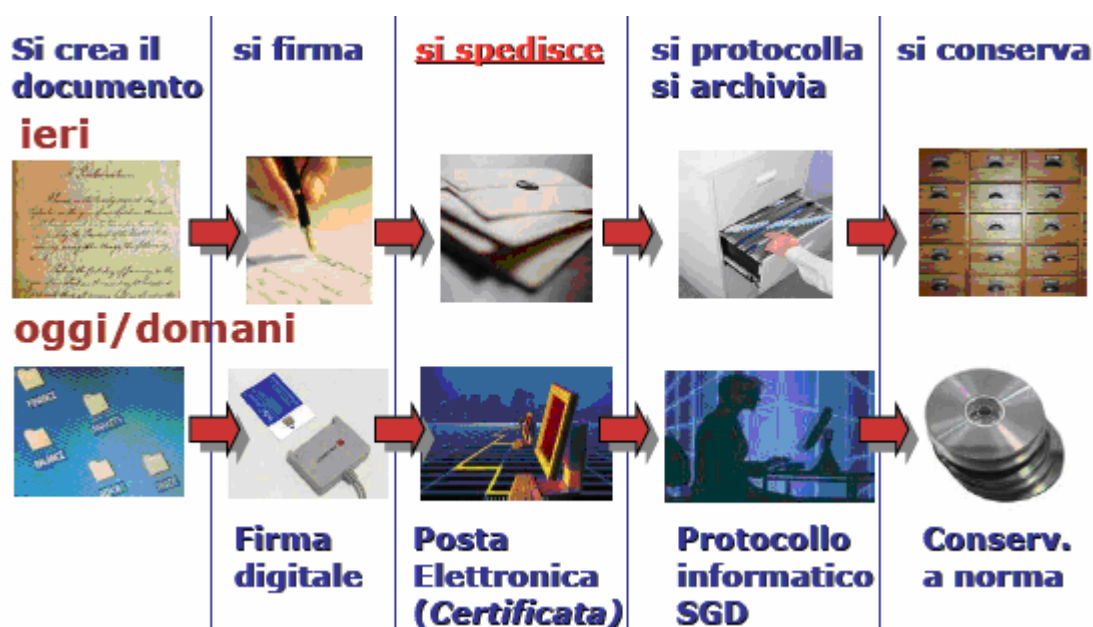
Esempio di una sessione SMTP



```
C:\WINNT\system32\cmd.exe - telnet
220 Welcome to SMTP Server
HELO NOME
250 Hello NOME
MAIL FROM:<MAIL@LOCALHOST>
250 MAIL@LOCALHOST Address Okay
RCPT TO:<MAIL@LOCALHOST>
250 MAIL@LOCALHOST< Address Okay
DATA
354 Please start mail input.
FROM:MITTENTE
TO:DESTINATARIO
SUBJECT:SOGGETTO
CORPO
DEL
MESSAGGIO
.
250 Mail queued for delivery.
QUIT
221 Closing connection. Good bye.
```

POSTA ELETTRONICA CERTIFICATA

Posta Elettronica Certificata è un sistema di comunicazione elettronica che, grazie alla sue "doti" di tracciabilità ed inviolabilità, stabilisce l'equivalenza tra il messaggio e-mail (inviato tramite questo sistema) e la tradizionale raccomandata A/R (avviso di ritorno). Ovviamente ciò che più interessa all'utente finale, oltre alla onnipresente sicurezza delle comunicazioni, è proprio il valore legale che viene riconosciuto alle e-mail certificate, che le rende opponibili come prove in caso di giudizio. Ma la PEC non offre solo questo; le sue garanzie superano quelle offerte dalla raccomandata A/R; innanzitutto gli utenti di PEC non certificano solo i messaggi che inviano ma anche la certezza dell'identità del mittente e del destinatario. Sappiamo benissimo quanto è semplice inviare un messaggio di posta elettronica falsificando la propria identità senza correre il rischio di essere scoperti. Con la PEC il destinatario di un messaggio potrà essere sicuro che l'identità mostrata dal mittente è quella reale. Un messaggio di PEC viene certificato in ogni fase del suo percorso: l'utente che invia un messaggio tramite questo sistema riceverà una ricevuta per la presa in carico del messaggio da parte del suo mail server, una ricevuta per l'arrivo del messaggio sul mail server del destinatario (solo se anch'egli è utente di PEC), ed infine una ricevuta della consegna del messaggio nella casella del destinatario (anche in questo caso solo se anch'egli è utente di PEC). Queste ricevute non si limitano a certificare data e ora, ma anche l'oggetto del messaggio e-mail e la presenza di eventuali allegati.



Come funziona

Quando inviamo una raccomandata con la ricevuta di ritorno l'ufficio delle Poste si fa carico della corrispondenza per inoltrarla. Così avviene se inviamo un messaggio o un documento mediante il servizio di posta certificata: questo viene preso in consegna da chi ci fornisce il servizio per il suo inoltro e il recapito;

Invio

Dopo aver consegnato la nostra raccomandata con avviso di ricevimento, allo sportello postale ci viene rilasciata una ricevuta dove sono registrate alcune informazioni, come la data e l'ora dell'invio, il destinatario. Similmente, subito dopo aver inviato il messaggio come posta elettronica certificata il nostro gestore di posta elettronica lo "imbusta" e ci rilascia immediatamente una ricevuta, che in questo caso è la sua e-mail firmata. In questa e-mail sono riportate la data e l'ora della spedizione e il destinatario. Questa è per noi una garanzia legale che attesta l'invio del nostro messaggio di posta elettronica.

Consegna

Nel caso della raccomandata con avviso di ricevimento, abbiamo la certezza della consegna quando ci viene restituita la ricevuta di ritorno firmata dal destinatario. Per quanto riguarda il nostro messaggio o documento informatico, esso viene inoltrato al gestore della posta elettronica certificata del destinatario (naturalmente, può anche essere lo stesso che fornisce il servizio a noi). Gestore che effettuerà la consegna e ce ne darà ricevuta con una sua e-mail firmata, che ci dirà quando è stato consegnato il messaggio e conterrà la copia completa del messaggio recapitato.

In tal modo, avremo l'attestato legalmente valido che il nostro messaggio è effettivamente pervenuto (non letto!) al nostro destinatario.

E' disposto che quando il messaggio non risulta consegnabile il gestore del ricevente fornisce ricevuta di errore di consegna al mittente.

Tra l'altro, niente paura se perdiamo o cancelliamo per errore una ricevuta: infatti i gestori di posta elettronica certificata ne conserveranno una copia nei loro archivi per trenta mesi .



Caratteristiche della PEC

Le modalità di accesso sono sostanzialmente le stesse di una e-mail tradizionale. Si può accedere alla propria casella di PEC, infatti, sia attraverso un client di posta elettronica che attraverso un browser Internet o una webmail. Nel primo caso, prima di poter utilizzare la propria casella sarà necessario configurare il proprio client con i parametri forniti dal Gestore di PEC scelto.

La casella di PEC è indicata soprattutto per effettuare comunicazioni "ufficiali" per le quali il mittente vuole avere delle evidenze con valore legale dell'invio e della consegna del messaggio. Ciò non toglie che, volendo, la casella possa essere utilizzata per qualsiasi comunicazione anche nel caso in cui non sia indispensabile la certificazione dell'invio e della consegna.

La PEC non certifica la lettura del messaggio da parte del destinatario, la certificazione è relativa ai soli eventi di invio del messaggio e di consegna dello stesso nella casella di PEC del destinatario. Ma è in grado di garantire l'identità della casella mittente in quanto è assicurata l'inalterabilità dell'indirizzo associato alla casella dalla quale si effettua l'invio del messaggio.

La PEC consente di individuare in modo certo la provenienza del messaggio dal momento che è garantita l'inalterabilità dell'indirizzo associato alla casella dalla

quale si effettua l'invio del messaggio; inoltre, proprio questa particolarità del servizio PEC, risulta essere un valido deterrente contro il fenomeno dello SPAM.

E' possibile inviare messaggi di Posta Elettronica Certificata tra utenti che utilizzano Gestori di PEC differenti, la normativa impone ai differenti gestori di PEC di garantire la piena interoperabilità dei servizi offerti.

Nel caso in cui il messaggio sia stato effettivamente consegnato, il destinatario non può negare l'avvenuta ricezione, dal momento che la ricevuta di avvenuta consegna del messaggio, firmata ed inviata al mittente dal Gestore di PEC scelto dal destinatario, riporta la data e l'ora in cui il messaggio è stato consegnato nella casella di PEC del destinatario, certificandone l'avvenuta consegna.

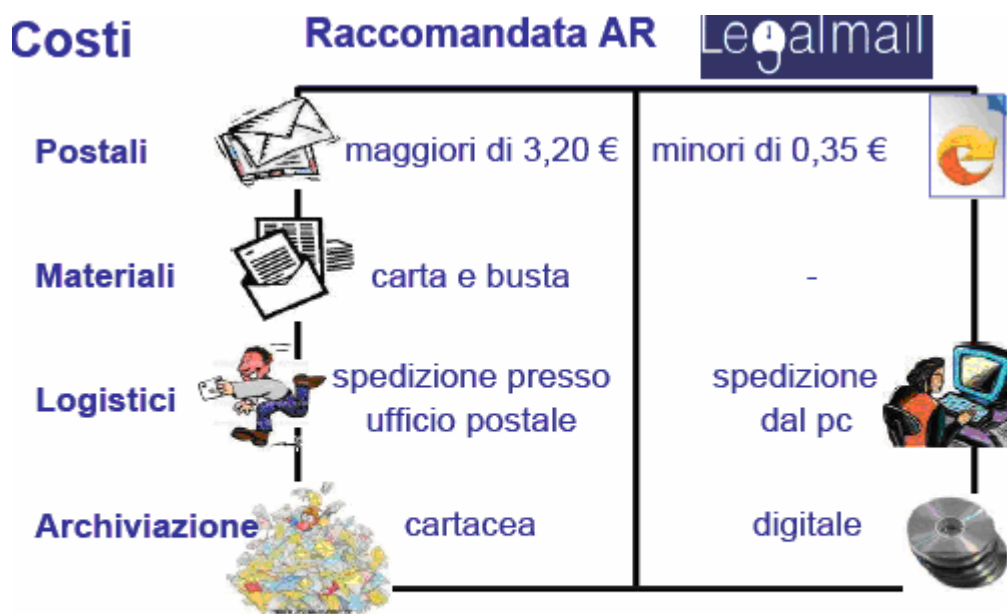
La Norma sulla sicurezza e la privacy dei dati personali dei titolari di caselle PEC, impone ai Gestori di PEC di applicare tutte le procedure atte a garantire la sicurezza e la privacy dei dati personali. Analogo livello di sicurezza è garantito anche per le informazioni archiviate nel Log delle trasmissioni. La normativa di riferimento fissa i livelli minimi di sicurezza che devono essere garantiti dal Gestore ai propri utenti. In particolare, il Gestore è tenuto ad informare il mittente, bloccandone la trasmissione, della eventuale presenza di virus nelle e-mail inviate/ricevute.

Differenze tra A/R e PEC

	Raccomandata AR	Da PEC a PEC
Certezza d'invio	SI	SI
Certezza di consegna	SI	SI
Tempi di consegna	giorni	secondi
Contemporaneità della spedizione	NO	SI
Certezza del contenuto	NO	SI
Identità mittente	NO	casella autentica <i>firma del msg</i>
Valore legale dell'allegato	<i>Firma autografa lettera</i>	<i>Firma digitale allegato</i>

La posta elettronica certificata rispetto alla raccomandata con ricevuta di ritorno racchiude molti vantaggi qui sotto elencati:

- Risparmi consistenti rispetto ai costi di invio delle raccomandate;
- Maggiore efficienza grazie all'eliminazione della gestione della carta, delle code agli sportelli e dei tempi di consegna;
- Opponibilità a terzi delle ricevute in caso di contenzioso, come previsto dalla norma;
- Certificazione completa del contenuto delle comunicazioni (messaggio e allegati);
- Invio simultaneo a più destinatari;
- Accesso sicuro alla webmail anche con certificato di autenticazione;



Firma digitale

La firma digitale è 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.

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).

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 (oggi 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.

L'articolo DLGS 23 gennaio 2002 n.10, al comma 3, prescrive che " 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 " Quindi, alla sottoscrizione con firma digitale viene data la medesima validità giuridica di una firma autografa autenticata da un pubblico ufficiale.