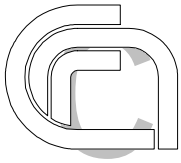

Consiglio Nazionale delle Ricerche

Una proposta per il servizio di Posta Elettronica del CNR

IAT-B41999002

Laura Abba, Marina Buzzi, Francesco Gennai

e-mail:

Laura.Abba@iat.cnr.it
Marina.Buzzi@iat.cnr.it
Francesco.Gennai@iat.cnr.it

Pisa, Maggio 1999

i a t

Istituto per le Applicazioni Telematiche

Indice

INTRODUZIONE 1

OBIETTIVI 2

Riorganizzazione topologica 2

Innovazione tecnologica 3

AZIONI 3

Analisi e descrizione delle azioni 3

Riduzione del numero totale dei server di posta elettronica presenti nel CNR 3

Descrizione 4

Soluzioni tecnologicamente avanzate 6

Compatibilità MIME 6

Supporto delle estensioni SMTP 7

Conversione del formato dei messaggi 7

Sicurezza 8

Sicurezza applicata ai server 8

Sicurezza relativa al contenuto dei dati trasportati 9

Gestione e controllo del backbone per il servizio di posta elettronica della rete del CNR 9

CONCLUSIONI 10

BIBLIOGRAFIA 10

Introduzione

Uno dei ruoli fondamentali del CNR è evidenziare, promuovere, adottare le più avanzate tecnologie ogni qualvolta queste diventino usufruibili da parte di rilevanti comunità di utenti. In accordo a questo ruolo del CNR una delle attività primarie del neo-nato Istituto per le Applicazioni Telematiche è la promozione di servizi di rete, basati su tecnologie innovative, da offrire in primo luogo alla comunità scientifica CNR, ma anche a Pubbliche Amministrazioni e Industrie.

Nella società globale dell'informazione, la rete Internet ha acquisito il ruolo di comprimario mezzo di comunicazione per una vasta massa di utenza caratterizzabile per la sua eterogeneità in termini di interessi, scopi e cultura. Ogni servizio che la rete mette a disposizione è caratterizzato da vari parametri che vanno dall'aspetto innovativo del servizio, al suo grado di affidabilità, alla sua diffusione, etc. La rete Internet è in continua evoluzione: vengono introdotti nuovi servizi, e quelli preesistenti sono soggetti ad una continua revisione. Tra questi ultimi si annovera il servizio di posta elettronica uno dei più "antichi" ed importanti.

L’ampia diffusione del servizio di posta elettronica è causa, in parte, della lentezza con cui questo servizio si adatta alle nuove tecnologie. E’ da considerare infatti, come parte della tecnologia su cui tale servizio si basa, sia totalmente nelle mani degli utenti finali che, con la loro tipica riluttanza di fronte ai cambiamenti, costituiscono una notevole "massa inerziale" che si oppone all'introduzione di possibili innovazioni tecnologiche. Ciò non toglie che proprio il CNR possa promuovere al proprio interno, con sufficiente convinzione, le innovazioni del servizio che oggi, se pur ancora opzionali, risultano già consolidate nella definizione degli standard e delle implementazioni. Presumibilmente, queste tecnologie diverranno ben presto necessarie ed auspicabili, affinché il servizio di posta elettronica possa risultare globalmente più affidabile ed efficace rispetto all’utilizzo attuale.

Fino ad oggi il servizio di posta elettronica è stato principalmente visto come mezzo per lo scambio di messaggi in semplice formato testo, ma già da alcuni anni sono presenti funzionalità avanzate per lo scambio di documenti multimediali. Purtroppo, una semplice mancanza di un coordinamento che possa tracciare delle linee guida del servizio può portare a risultati disastrosi. Attachment spediti possono risultare non leggibili (per il destinatario), a causa del prodotto utilizzato per elaborare il documento, della versione con cui è salvato il

file, etc. Per dare una soluzione a questo problema, si potrebbe pensare di obbligare tutti gli utenti ad utilizzare lo stesso client di posta elettronica e lo stesso word processor (versione compresa!), ma questa sarebbe una limitazione inaccettabile; invece, nel rispetto delle scelte di ognuno, è possibile far si che il sistema di posta elettronica si prenda l'onere di gestire e risolvere il problema, lasciando libero l'utente di spedire i propri documenti, nel formato prescelto, senza doversi preoccupare di chi li riceverà.

Tra i protocolli innovativi emergenti citiamo IMAP (*Internet Message Access Protocol*) che rispetto a POP (*Pop Office Protocol*) introduce nuovi funzionalità attraverso le quali è, per esempio, possibile organizzare efficienti servizi di helpdesk via e-mail, basandosi sulla condivisione e sincronizzazione di una stessa casella postale tra più utenti.

E che dire della sicurezza e riservatezza del servizio di posta elettronica? Un’altra problematica oggi sempre più sentita, anche in previsione della normative legali in corso di definizione.

Obiettivi

Gli obiettivi primari di questo progetto sono:

- *riorganizzazione topologica* del servizio all'interno del CNR;

- *innovazione tecnologica* del servizio.

Riorganizzazione topologica

La riorganizzazione topologica del servizio dovrà portare ad una maggiore centralizzazione della gestione tecnico/operativa, mantenendo allo stesso tempo la massima distribuzione della gestione amministrativa del servizio stesso.

Con questa scelta i problemi tecnico/operativi saranno ristretti al mantenimento del servizio presso un limitato numero di centri qualificati, dando comunque una maggiore distribuzione e indipendenza amministrativa ai vari gruppi di utenza (Organi CNR, Progetti, etc.) nella gestione del loro dominio e degli utenti ad esso appartenenti.

Innovazione tecnologica

L'innovazione tecnologica del servizio dovrà basarsi sulla introduzione delle più innovative tecnologie per il trasporto di messaggi multimediali, conversione tra vari formati, utilizzo di firma digitale, di cifratura di messaggi e/o sessioni, controllo degli accessi, gestione delle configurazioni degli utenti tramite directory service, configurazioni anti-spamming.

Una corretta gestione di questo servizio comporterà aggiornamenti ed ampliamenti funzionali dei server la cui operatività sarà garantita mediante opportune procedure di monitoraggio sistemistico/operativo.

Azioni

Le azioni per il conseguimento dei due precedenti obiettivi possono essere suddivise e descritte nei seguenti punti:

a) *riduzione del numero totale dei server di posta elettronica presenti nel CNR;*

b) *introduzione di soluzioni tecnologicamente avanzate;*

c) *creazione di un centro di gestione e controllo del backbone per il servizio di posta elettronica della rete del CNR.*

Alla base di questa proposta vi sono le esperienze maturate nella gestione e coordinamento del servizio di posta elettronica avviato presso il CNUCE ed attualmente mantenuto dal Reparto Applicazioni Telematiche dello IAT, che offre l'hosting di servizi di Posta Elettronica a vari Istituti CNR (http://www.iat.cnr.it/supporti_telematici/mail.shtml).

Analisi e descrizione delle azioni

Riduzione del numero totale dei server di posta elettronica presenti nel CNR

Come vedremo in questo paragrafo è oggi possibile la realizzazione di una infrastruttura per un sistema di posta elettronica del CNR omogeneo e ben distribuito che ne semplifichi il mantenimento operativo e aumenti la sicurezza dei dati che esso gestisce.

Omogeneità negli standard di servizio, efficienza nel mantenimento operativo, sicurezza nei dati gestiti, sono obiettivi perseguibili riducendo il numero di server di posta elettronica ed indicando le caratteristiche tecniche a cui dovranno essere conformi.

Descrizione

Un limitato numero di server di posta elettronica (server SMTP, *Simple Mail Transfer Protocol* [1], [2]) favorisce la centralizzazione delle attività di gestione e controllo del servizio.

Tecnicamente la soluzione consiste nel concentrare la gestione di più domini su un limitato numero di server di posta elettronica, a favore di una riduzione del numero di quelli attualmente presenti nella infrastruttura di rete del CNR.

Parallelamente occorre promuovere l'adozione dei sistemi client/server per la gestione di una mailbox (POP [3], IMAP [4]) e al tempo stesso consentire l'integrazione di quelle consistenti realtà presenti nell'ente che utilizzano altri tipi di sistemi di messaggistica basati su tecniche di "Groupware" (Lotus Note, Microsoft Mail, etc.).

Si deve notare che attualmente nel CNR sono presenti un eccessivo numero di server SMTP (Workstation di utente con server SMTP, server di Istituto) che oltre a complicare la migrazione verso un servizio di posta elettronica omogeneo, costituiscono un punto debole per la sicurezza dei sistemi. Spesso l'utente/gestore della propria workstation tende a svincolarsi dall'utilizzo di un semplice client per l'accesso al server centralizzato, preferendo l'installazione di un server SMTP sulla propria workstation assumendosi anche gli oneri di gestione e configurazione che sicuramente non sono paragonabili a quelli necessari per il semplice client, a tutto ciò dovremmo aggiungere il fatto che tale workstation dovrebbe essere sempre attiva (per esempio: anche quando l'utente/gestore è in ferie o in missione) e il suo server SMTP sempre perfettamente funzionante.

Utilizzare un server SMTP personale può dare la sensazione di poter controllare al meglio il proprio ambiente e servizio di posta elettronica. In realtà importanti condizioni di servizio, quali la necessità di utilizzare un naming centralizzato secondo una sintassi uniforme [5] e la stessa topologia della rete, ci permettono di dimostrare l'infondatezza di tale sensazione.

Infatti un problema di rete che isoli la propria LAN conduce più o meno agli stessi effetti: l'impossibilità di accedere al server centralizzato tramite client, contro l'impossibilità di ricevere/spedire messaggi dal server della propria workstation.

Inoltre, con l'auspicabile adozione del naming centralizzato, con configurazioni degli utenti memorizzate su server LDAP (*Lightweight Directory Access Protocol*) [6], [7], [8], un problema che metta fuori servizio il server centrale, potrà "isolare" le singole workstation anche se dotate di un proprio server, infatti il messaggio dovrà comunque attraversare il server centrale per essere inoltrato verso la workstation di destinazione.

E' quindi ragionevole la centralizzazione delle mailbox d'utente su pochi e ben distribuiti server che garantiscano una alta qualità del servizio, concentrando su essi competenze ed investimenti allo scopo di renderli estremamente affidabili ed efficienti.

Da un punto di vista strettamente topologico si potrebbe pensare ad un server per ogni Area del CNR. Per la sua collocazione all'interno di un'Area, va dato grande rilevanza all'aspetto affidabilità della rete piuttosto che alla velocità e modalità con cui l'utente potrà accedere il server. Infatti occorre notare che il servizio di email non risente particolarmente di problemi relativi alla velocità dei canali trasmissivi.

Considerando che l'infrastruttura di base della rete CNR/GARR offre soddisfacenti prestazioni nelle interconnessioni delle varie sedi, non dovrebbero esserci particolari controindicazioni a ridurre i server di posta elettronica addirittura ad un numero inferiore rispetto a quello delle aree.

La relazione topologica tra il client e il server di posta elettronica è principalmente dipendente dalla affidabilità e prestazioni delle connessioni che costituiscono il percorso di rete tra essi esistenti. Ovvero è preferibile avere la propria mailbox su un server, ben configurato e ben gestito, che si trova in una sede geograficamente distante dal punto di accesso alla rete del client, piuttosto che su server locali per i quali vi sono carenze nella loro gestione e configurazione.

A supporto di questa affermazione di debole dipendenza topologica di un client di posta elettronica dal proprio server, vi è l'attività di servizio da alcuni anni condotta presso il CNUCE e negli ultimi mesi presso lo IAT, dove il server di posta elettronica ha offerto e/o offre servizio per diversi domini appartenenti a sedi CNR e Universitarie geograficamente distribuite quali: Area di Ricerca e Istituto IRII di Cagliari, IRIDISS di Salerno, IRPEM di Ancona, IAS di Porano (TR), Regione Toscana, più di 20 domini per vari Dipartimenti dell'Università di Pisa, vari Istituti CNR con sede in Pisa.

La centralizzazione del servizio di posta elettronica su un unico server e quindi la conseguente centralizzazione della gestione tecnico/operativa non deve però corrispondere ad

una centralizzazione dell'amministrazione del servizio stesso. Occorre che al singolo organo di ricerca, gruppo di lavoro, etc., resti la completa facoltà di amministrare il proprio dominio di posta elettronica, potendo gestire un proprio database di utenti, proprie informazioni di logging sull'attività del servizio, etc. Noi chiamiamo questo approccio “Delega Amministrativa di Servizi di Rete”.

Una delle principali diffidenze verso la centralizzazione del servizio, potrebbe essere determinata dal timore di perdere quel controllo amministrativo che tipicamente si trova nelle mani dello stesso gestore tecnico del servizio. Il servizio attivo presso lo IAT rispetta i principi sopra esposti di completa centralizzazione tecnico/operativa in parallelo alla distribuzione della gestione amministrativa dei singoli domini di posta elettronica.

In pratica il server opera per utenti appartenenti a diversi domini di posta elettronica, per esempio: ict.pi.cnr.it, iggi.pi.cnr.it, irpem.an.cnr.it. Ciascun dominio è poi gestito da una semplice procedura che consente al rispettivo responsabile amministrativo la completa gestione del database degli utenti. Alla scadenza di ogni mese vengono automaticamente generati file contenenti informazioni statistiche sul traffico di posta elettronica di ciascun dominio ed inviati ai rispettivi responsabili.

La prima interfaccia a caratteri è stata sostituita da una interfaccia web che oltre ad essere intuitiva per l’utente e a non necessitare quindi di personale tecnico specializzato, permette di controllare le operazione effettuate sui file di configurazione.

Le procedure ampiamente collaudate da anni di servizio sono state sviluppate su un server OpenVMS. Il software di gestione della posta elettronica utilizzato è il PMDF prodotto dalla Innosoft (http://www.innosoft.com).

Soluzioni tecnologicamente avanzate

Vengono qui descritte alcune delle fondamentali specifiche tecniche e funzionalità dei server di posta elettronica che andranno a costituire il backbone del servizio.

Compatibilità MIME

Il server dovrà essere in grado di poter riconoscere e gestire opportunamente i vari formati MIME [9], [10], [11], [12], [13]. Questo consentirà una corretta manipolazione del contenuto dei messaggi a favore di diverse interessanti funzionalità alcune delle quali sono già indicate nel presente documento. E' da notare come in genere si tende ad associare MIME, o meglio i

formati da esso definiti, alle sole funzionalità dei client. Riconoscere tale formati anche a livello di server è da ritenersi altrettanto fondamentale e corretto.

Supporto delle estensioni SMTP

Diverse sono le estensioni all'originale protocollo SMTP. Per alcune di queste la loro adozione è ritenuta obbligatoria.

In particolare le estensioni SMTP che vanno sotto il nome di NOTARY [14], [15], [16], [17] e 8bitMIME [18] dovranno essere supportate da tutti i server SMTP che costituiscono l'infrastruttura primaria del servizio.

NOTARY introduce alcune importanti modifiche al protocollo SMTP e definisce il protocollo DSN (Delivery Service Notification) per la gestione delle segnalazioni di errore o successo del servizio di posta elettronica. In tal senso NOTARY tende ad eliminare notevoli limitazioni che il protocollo SMTP ha dimostrato negli ultimi anni.

8bitMIME è un estensione al protocollo SMTP per il trasporto di messaggi contenenti caratteri rappresentati con 8 bit. L'originale protocollo SMTP prevede solo il trasporto di caratteri rappresentabili con 7 bit (US-ACSII).

Il supporto del comando ESMTP ETURN sarà necessario per quei server che dovranno distribuire la posta verso domini connessi ad Internet attraverso linee ISDN. In questo caso il server installato presso la sede di utente avrà il compito di aprire la connessione verso il server primario (uno dei server del backbone di servizio) per lo scaricamento dei messaggi in coda. Questo consente di evitare l'apertura di un canale ISDN (generazione di una chiamata) ogni qualvolta un messaggio debba essere trasmesso. Sarà l'amministratore locale a decidere l'intervallo di tempo con cui effettuare la chiamata ISDN per aprire una connessione client/server SMTP e tramite il comando ETURN attivare lo scaricamento della coda dei messaggi.

Conversione del formato dei messaggi

Un server compatibile MIME ci consente di convertire parti del formato di un messaggio in base alle esigenze del destinatario o del mittente.

Ad esempio un utente che legga la propria posta su una workstation Unix potrebbe avere evidenti problemi nel ricevere messaggi contententi documenti Word. Su richiesta del singolo

utente sarà quindi possibile convertire ogni parte da un formato non leggibile sulla propria workstation a quello desiderato (esempio Word->Postscript, Word->HTML).

Ovviamente la conversione di formato è applicabile a vari livelli: singolo user, dominio di posta elettronica, lista di distribuzione.

Sicurezza

La sicurezza per un servizio di posta elettronica comprende vari aspetti. Il presente progetto contempla la sicurezza applicata ai server e la sicurezza relativa al contenuto dei dati trasportati.

Sicurezza applicata ai server

I server di posta elettronica dovrannno essere dotati dei più sofisticati strumenti di controllo e monitoraggio degli accessi.

Si ritiene indispensabile la presenza delle seguenti funzionalità:

- Le connessioni tra client e server e tra server del CNR possono essere criptate. Queste funzionalità sono ottenibili mediante l'utilizzo del protocollo TLS [19] per le connessioni SMTP [20], POP e IMAP [21].
- Supporto ai meccanismi per user/password criptati (CRAM/MD5) [22].
- Rifiuto degli accessi SMTP se questi non provengono da utenti registrati nel server (utenti POP/IMAP o ad accesso diretto).
- Rifiuto degli accessi SMTP se questi non provengono dal client per cui l'utente di posta elettronica è stato registrato (condizione estremamente restrittiva che associa il nome (o indirizzo IP) del client ad uno o più indirizzi di e-mail, i soli che potranno comparire nel campo from dei messaggi provenienti da quel client).
- Rifiuto degli accessi SMTP per messaggi destinati a domini per i quali il server non funge da mail relay.
- Eliminazione, dall'header dei messaggi uscenti, di tutte quelle informazioni che potranno essere ritenute riservate o comunque di dominio interno alla rete CNR.
- Registrazione dell'attività del sistema (accessi, messaggi in ingresso/uscita) in un file di log da utilizzarsi anche per la generazione di statistiche di traffico.

- Gestione di liste di distribuzione con controllo dell'accesso basato su meccanismi di sicurezza a chiave pubblica:

  validazione dell'indirizzo del mittente mediante meccanismi di sicurezza a chiave pubblica.

- Rilevazione di messaggi contenenti virus.

- Funzionalità di gateway verso altri sistemi di posta elettronica largamente diffusi quali quelli basati su LAN (Lotus Notes, Microsoft Mail, Novell MHS, WordPerfect Office (GroupWise)). In tal caso saranno fondamentali le funzionalità del gateway tra Internet (MIME/RFC822) e il sistema di e-mail proprietario; il gateway dovrà offrire la massima e più corretta integrazione tra le funzionalità presenti nei due sistemi che interconnette (esempio: formato degli attachment, formato delle notifiche di errore o di delivery, etc.).

Sicurezza relativa al contenuto dei dati trasportati

Gli utenti del servizio potranno far uso di interfacce per l'accesso al servizio di posta elettronica in grado di gestire crittografia a chiave pubblica.

Si possono identificare una o più "sottoreti di servizio" all'interno della rete degli organi del CNR, a cui apparterranno dei server di posta elettronica che saranno in grado di crittografare i dati con algoritmi a chiave pubblica prima di trasmetterli al server di destinazione.

Utilizzando anche alcune delle importanti funzionalità elencate nel precedente paragrafo relativo alla "sicurezza applicata ai server", sarà possibile realizzare un sistema sicuro per il trasferimento dati tra sedi CNR geograficamente distribuite.

Le applicazioni dei vari servizi amministrativi del CNR trarrebbero sicuri benefici dall'utilizzo di una "sottorete di servizio" di questo tipo.

Gestione e controllo del backbone per il servizio di posta elettronica della rete del CNR

Le attività gestionali e di monitoraggio di un backbone di servizio costituito da server omogenei, saranno estremamente semplici e produttive.

Varie entità proprie del server possono essere monitorate mediante una stazione di monitoraggio: allarmi sull'occupazione di spazio disco, stato delle porte SMTP, POP e IMAP suggeriscono all'operatore l'intervento più opportuno.

Anche se la fattibilità tecnica di questa ipotesi è da verificare, sarebbe interessante, salvare il limitato spazio disco occupato dai messaggi di posta elettronica presenti su un server mediante procedure di backup "geografico" condotte durante la notte, in modo da non sovraccaricare la rete durante le ore di servizio primario. Il backup potrebbe venire condotto da unico server di backup centralizzato.

Conclusioni

Il presente documento dovrebbe attivare una discussione su alcuni importanti punti che restano volutamente aperti, per la soluzione dei quali è richiesta la volontà politica e un contributo da parte dei vari responsabili del servizio. Tra questi vi sono:

- analisi della attuale situazione del servizio di posta elettronica nel CNR;
- definizione di un nuovo schema di indirizzamento che individui non solo il formato del dominio ma anche della parte locale di un indirizzo; che definisca vari indirizzi di ruolo ed una loro politica di utilizzazione; che preveda sin d'ora i meccanismi per la gestione dei cambi di indirizzo (persone che si spostano tra enti, etc.);
- studio per la definizione di meccanismi interni all'ente per la certificazione di documenti in forma elettronica, firma digitale, crittografia [23];
- progetto della nuova infrastruttura per il servizio di posta elettronica (topologia, hardware, software, etc.);
- studio per la migrazione dall'attuale servizio verso la nuova infrastruttura.

Bibliografia

[1] Jonathan B. Postel. *RFC821: Simple Mail Transfer Protocol*. ftp://ftp.isi.edu/in-notes/rfc821.txt, August 1982.

[2] David H. Crocker. *RFC 822: Standard for the format of ARPA Internet text messages* - ftp://ftp.isi.edu/in-notes/rfc822.txt, August 1982.

[3] J. Myers & M. Rose. *RFC1939: Post Office Protocol - Version 3*. ftp://ftp.isi.edu/in-notes/rfc1939.txt, May 1996.

[4] M. Crispin. *RFC 2060: Internet Message Access Protocol - Version 4rev1*. ftp://ftp.isi.edu/in-notes/rfc2060.txt, December 1996.

[5] D. Crocker. *Mailbox Names for Common Services, Roles and Functions.* ftp://ftp.isi.edu/in-notes/rfc2142.txt, May 1997.

[6] M. Wahl, T. Howes, S. Kille. *Lightweight Directory Access Protocol (v3)* - ftp://ftp.isi.edu/in-notes/rfc2251.txt, December 1997.

[7] Howes, S. Kille. *Lightweight Directory Access Protocol (v3*) - ftp://ftp.isi.edu/in-notes/rfc2252.txt, December 1997.

[8] M. Wahl, S. Kille, T. Howes. *Lightweight Directory Access Protocol (v3)* December 1997 - ftp://ftp.isi.edu/in-notes/rfc2253.txt, December 1997.

[9] N. Freed, N. Borenstein. *RFC 2045: Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies.* ftp://ftp.isi.edu/in-notes/rfc2045.txt, November 1996.

[10] N. Freed, N. Borenstein. *RFC 2046: Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types.* ftp://ftp.isi.edu/in-notes/rfc2046.txt, November 1996.

[11] K. Moore. *RFC 2047: Multipurpose Internet Mail Extensions (MIME) Part Three: Message Header Extensions for Non-ASCII Text*. ftp://ftp.isi.edu/in-notes/rfc2047.txt, November 1996.

[12] N. Freed, J. Klensin, J. Postel. *RFC 2048: Multipurpose Internet Mail Extensions (MIME) Part Four: Registration Procedures.* ftp://ftp.isi.edu/in-notes/rfc2048.txt, November 1996.

[13] N. Freed, N. Borenstein. *RFC 2049: Multipurpose Internet Mail Extensions (MIME) Part Five: Conformance Criteria and Examples*. ftp://ftp.isi.edu/in-notes/rfc2049.txt, November 1996.

[14] K. Moore. *SMTP Service Extension for Delivery Status Notifications*, ftp://ftp.isi.edu/in-notes/rfc1891.txt, January 1996.

[15] G. Vaudreuil. The Multipart/Report Content Type for the Reporting of Mail System Administrative Messages - ftp://ftp.isi.edu/in-notes/rfc1892.txt, January 1996.

[16] G. Vaudreuil. Enhanced Mail System Status Codes - ftp://ftp.isi.edu/in-notes/rfc1893.txt, January 1996.

[17] K. Moore, G. Vaudreuil. An Extensible Message Format for Delivery Status Notifications - ftp://ftp.isi.edu/in-notes/rfc1893.txt, January 1996.

[18]J. Klensin, N. Freed, M. Rose, E. Stefferud, D. Crocker. *SMTP Service Extension for 8bit-MIMEtransport*. ftp://ftp.isi.edu/in-notes/rfc1652.txt, July 1994.

[19] T. Dierks, C. Allen. *The TLS Protocol (Version 1.0).* ftp://ftp.isi.edu/in-notes/rfc2246.txt, January 1999.

[20] P. Hoffman. SMTP Service Extension for Secure SMTP over TLS. ftp://ftp.isi.edu/in-notes/rfc2487.txt, January 1999.

[21] C. Newman. *Using TLS with IMAP, POP3 and ACAP*. ftp://ftp.isi.edu/in-notes/rfc2595.txt, June 1999.

[22] J. Myers. *SMTP Service Extension for Authentication* - ftp://ftp.isi.edu/in-notes/rfc2554.txt, March 1999.

[23] F. Gennai. *Creazione di una "Certification Authority" per il Consiglio Nazionale delle Ricerche.* Dicembre 1996.

[24] F. Gennai. *Bozza di progetto per l'evoluzione tecnologica e riorganizzazione del servizio di Posta Elettronica del Consiglio Nazionale delle Ricerche*. http://mail.iat.cnr.it/www_service/www/doc/new_email.html, Ottobre 1997.