CEDACRI

Manuale Operativo Servizio di Posta Elettronica Certificata (PEC)

20-02-2025

Unrestricted

Legal Notices

Contenuti

Scopo e ambito di applicazione

Scopo

L'attuale posta certificata ha un nome preciso: raccomandata con avviso di ricevimento. Un metodo sicuro per far pervenire le informazioni al destinatario, ma anche lento e costoso.

Secondo una recente stima, i costi finali di una raccomandata con ricevuta di ritorno per una pubblica amministrazione o per un'impresa oggi si attestano intorno ad una cifra piuttosto significativa.

L'e-mail certificata è, sul piano legale, l'esatto equivalente di una raccomandata con ricevuta di ritorno con la fondamentale differenza che i costi ed i tempi di consegna di ogni raccomandata si riducono drasticamente, mantenendo intatte la sicurezza, la riservatezza e l'affidabilità della spedizione.

Il servizio offerto da Cedacri S.p.A. consiste in una serie di caselle e-mail certificate la cui architettura e gestione è resa flessibile in funzione delle particolari esigenze dei clienti che ne fanno richiesta.

Lo scopo del presente documento è quello di descrivere le modalità di utilizzo del servizio per la Posta Elettronica Certificata (PEC) erogato dalla Cedacri S.p.A., nel pieno rispetto della normativa esterna e interna di riferimento.

La conformità dei contenuti del presente Manuale Operativo ai servizi di Posta Elettronica Certificata offerti dalla Cedacri S.p.A., sarà verificata con frequenza annuale, fatti salvi tutti gli aggiornamenti richiesti dalla normativa che saranno effettuati tempestivamente sia dal punto di vista tecnologico sia redazionale.

Ambito di applicazione

Il presente documento ha validità per Cedacri S.p.A.

1 Definizioni e abbreviazioni

- Nessuna definizione

2 Riferimenti normativi

Di seguito sono riportati alcuni riferimenti (norme / direttive / documenti) sulla Posta Elettronica Certificata, utili a ricostruirne il fondamento normativo e gli sviluppi attuali:

1) Decreto del Presidente della Repubblica 28 dicembre 2000 n. 445
2) “Direttiva sulla trasparenza dell'azione amministrativa e gestione elettronica dei flussi documentali” (Ministro per l'innovazione e le tecnologie, 9 dicembre 2002)
3) Legge 16 gennaio 2003, n. 3 "Disposizioni ordinamentali in materia di pubblica amministrazione" (G.U. n. 15 del 20 gennaio 2003, Suppl. Ordinario n. 5)
4) D.P.R. 28 dicembre 2000 n. 445, “Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa”
5) Decreto legislativo 30 giugno 2003 n. 196 “Codice in materia di protezione dei dati personali”
6) Decreto "Approvazione delle linee guida per l'adozione del protocollo informatico e per il trattamento informatico dei procedimenti amministrativi" (Ministro per l'innovazione e le tecnologie, 14 Ottobre 2003)
7) “Direttiva per l'impiego della posta elettronica nelle pubbliche amministrazioni” (Ministro per l'innovazione e le tecnologie, 27 novembre 2003)
8) “Linee guida in materia di digitalizzazione dell'amministrazione per l'anno 2004” (Ministro per l'innovazione e le tecnologie, 18 dicembre 2003)
9) D.P.C.M. 30 marzo 2009 (GU del 06-06-2009), “Regole tecniche in materia di generazione, apposizione e verifica delle firme digitali e validazione temporale dei documenti informatici”
10) Decreto Legislativo 7 marzo 2005, n. 82, e s.m.i., “Codice dell’amministrazione digitale”
11) D.P.R.11 febbraio 2005, n. 68 (G.U. 28 aprile 2005, n. 97), ”Regolamento recante disposizioni per l’utilizzo della Posta Elettronica Certificata, a norma dell’art. 27 della legge 16 gennaio 2003 n. 3”
12) Circolare della Agenzie delle Entrate n. 45/E 19 ottobre 2005
13) Decreto del Consiglio dei Ministri, dipartimento per l’innovazione tecnologica e le tecnologie del 2 novembre 2005, “Regole tecniche per la formazione, la trasmissione e la validazione, anche temporale, della Posta Elettronica Certificata" (G.U. 15 novembre 2005, n. 266)
14) Circolare CNIPA n. 56 del 21 maggio 2009, “Modalità per la presentazione della domanda di iscrizione nell’elenco pubblico dei gestori di posta elettronica certificata (PEC) di cui all’articolo 14 del decreto del Presidente della Repubblica 11 febbraio 2005, n. 68”
15) Circolare CNIPA 7 dicembre 2006, n. 51, “Espletamento della vigilanza e del controllo sulle attività esercitate dagli iscritti nell’elenco dei gestori di posta elettronica certificata (PEC) di cui all’articolo 14 del decreto del Presidente della Repubblica 11 febbraio 2005, n. 68” (G.U. 21 dicembre 2006, n. 296)
16) DELIBERAZIONE del 19 febbraio 2004, n. 11, “Regole tecniche per la riproduzione e conservazione di documenti su supporto ottico idoneo a garantire la conformità dei

documenti agli originali - Art. 6, commi 1 e 2, del testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa, di cui al decreto del Presidente della Repubblica 28 dicembre 2000, n. 445" (GU n. 57 del 9 marzo 2004)

3 Informazioni di carattere generale

Il presente documento viene consegnato, unitamente all'informativa tecnica alla persona fisica e/o giuridica che materialmente fa richiesta di attivazione del servizio.

È conforme ai requisiti contenuti nella circolare CNIPA n. 56 del 21 maggio 2009, nel DPR n. 68 dell'11 febbraio 2005 e nel DPCM del 2 novembre 2005 , "Regole Tecniche per la formazione, la trasmissione e la validazione, anche temporale, della Posta Elettronica Certificata".

È inoltre disponibile per la consultazione ed il Download, nel formato PDF, presso il sito del gestore Cedacri S.p.A. all'indirizzo:

https://www.cedacricert.it/

3.1 Dati identificativi del Gestore

Ragione Sociale	Cedacri S.p.A.
Sede legale	Corso Monforte, 30 20122 Milano (Milano)
Legale Rappresentante nato a Funzione	Luca Peyrano Milano (Milano), 09 gennaio 1971 Executive Chairman
N. Iscrizione al Registro delle Imprese di MILANO MONZA BRIANZA LODI	00432960342
Partita IVA	00432960342
Gruppo IVA	02952290340
Codice ABI	89002
N° telefonico	0521 8071 (centralino)
N° di Fax	0521 807373

Tabella 1 -Dati identificativi del Gestore

3.2 Responsabile del Manuale Operativo

Il responsabile del presente manuale è	
Nome	Giuliano
Cognome	Merlo
Telefono	+39 0521-80771
Fax	+39 0521- 807372
E-mail	giuliano.merlo@iongroup.com servizifiduciari-cedacri@iongroup.com
Il responsabile del presente manuale è	Giuliano
Nome	Giuliano
Cognome	Merlo

Tabella 2 -Responsabile del Manuale Operativo

3.3 Tabella disponibilità del servizio

Il Servizio viene erogato come dalla seguente tabella:

Tipo del Servizio	Giorni di disponibilità	Orario di disponibilità
Disponibilità delle caselle di PEC (dall'attivazione)	7 giorni su 7	24 ore su 24
Attivazione delle caselle di PEC	Giorni feriali	09:00 - 13:00 e 15:00 - 17:00
Tempistiche di attivazione delle caselle di PEC	3 gg feriali dalla richiesta	09:00 – 13:00 e 15:00 – 17:00

Tabella 3 -Tabella disponibilità del servizio

3.4 Indicazione dei livelli di servizio

Nel rispetto di quanto prescritto dall'articolo 12 del Decreto 2 novembre 2005 rif. [13], sono garantiti i seguenti livelli minimi di SLA:

- invio del messaggio ad almeno 50 destinatari (contestuali)
- invio fino a 100 Mb (numero destinatari x dimensione messaggio)
- in un quadrimestre (periodo temporale di riferimento) la disponibilità del servizio di Posta Elettronica Certificata è garantita almeno al 99,8%
- il massimo fermo continuativo del servizio non sarà più lungo del 50% del totale previsto per l'intervallo di tempo di riferimento, ovvero 2h 55m
- a norma del comma 6 del suddetto art.12 del DM rif.[13], la Cedacri S.p.A., dichiara che visto che la ricevuta di accettazione viene generata subito dopo aver fatto il controllo antivirus, che parte al termine della ricezione del messaggio sul server, questa sarà fornita entro 5 minuti nel 99% dei casi, e comunque sempre entro un massimo di 15 minuti nel restante 1% dei casi, rappresentati da mail di grande dimensioni che possono giungere in momenti di punta di carico.
- tutte le altre ricevute rilasciate dalla Cedacri S.p.A. in qualità di gestore saranno fornite entro 5 minuti nel 99% dei casi; entro un massimo di 15 minuti nel restante 1% dei casi.

3.5 Tariffe

I prezzi delle caselle di PEC del servizio di Posta Elettronica Certificata erogato da Cedacri S.p.A. possono variare in funzione della quantità richiesta, delle personalizzazioni, delle dimensioni e dei servizi aggiuntivi concordati di volta in volta con i clienti.

3.6 Polizza assicurativa

È stata stipulata specifica polizza assicurativa per la copertura dei rischi derivanti dall'attività e dagli eventuali danni causati a terzi, rilasciata da una società di assicurazione abilitata ad esercitare nel campo dei rischi industriali a norma delle vigenti disposizioni così come richiesto dall'articolo 14 del D.P.R. n. 68/2005.

Il massimale di indennizzo per eventuali danni causati dall'inadempienza o negligenza del Gestore di Posta Elettronica Certificata è fissato in:

- € 1.500.000,00 per anno e per sinistro; per l'attività di gestione della Posta Elettronica Certificata.
- € 500.000,00 per anno e per sinistro; per quanto il Gestore sia tenuto a pagare quale civilmente responsabile a titolo di risarcimento di perdite patrimoniali cagionate a terzi in conseguenza di un fatto accidentale verificatosi in relazione allo svolgimento dell'attività di Gestore del servizio di Posta Elettronica Certificata.

3.7 Indirizzo web del Gestore Accreditato

Il Gestore Accreditato è contattabile ai seguenti indirizzi:

Cedacri S.p.A.
Servizi di Posta Elettronica Certificata
Corso Monforte, 30
20122 Milano (MI)

E-mail: servizifiduciari-cedacri@iongroup.com

Sito Web: https://www.postacert.cedacri.it

4 Postacert

Cedacri S.p.A. ha attivato il servizio di Posta Elettronica Certificata, denominato POSTACERT rivolto alla propria clientela tradizionale, le banche, ai privati ed alle Pubbliche Amministrazioni.

Il Servizio di Posta Elettronica Certificata è svolto da Cedacri S.p.A. che si avvale di strutture organizzative per la gestione dei vari elementi necessari per la corretta erogazione del servizio suddetto, sia nei confronti dei propri utenti, sia nei confronti degli altri gestori di Posta Elettronica Certificata.

Premesso che il servizio di Posta Elettronica Certificata è svolto da Cedacri S.p.A. per mezzo di infrastrutture tecniche concentrate fisicamente presso la sede di Collecchio (PR) e di personale espressamente organizzato per la gestione del servizio, esso è così suddiviso:

- Gestione rete e collegamenti con il mondo Internet
- Gestione infrastruttura interna di sala macchine e sicurezza fisica
- Gestione sicurezza logica attraverso i Firewall perimetrali
- Gestione dei server PEC, comprendente la gestione tecnica ordinaria.

Gli update di sicurezza, gli update funzionali e gli eventuali updati normativi, sono affidati a società di consulenza, specializzate nel settore, con le quali la Cedacri S.p.A. ha stipulato apposito contratto. Le suddette aziende sono certificate ISO 9001:2000; Cedacri S.p.A. è certificata secondo le più recenti norme ISO 27001 e ISO 9001 per tutti i servizi erogati.

La gestione delle caselle di Posta Elettronica Certificata, intesa come loro creazione, modifica di attributi e cancellazione, è effettuata da ACSE (Access Security) o dal cliente finale in caso di persone giuridiche.

Particolare attenzione viene posta sui due aspetti concernenti i livelli di servizio e la sicurezza logica, per cui sono attivati contratti specifici con i fornitori per:

1) la verifica della disponibilità e la misurazione dei livelli di servizio delle applicazioni, con allarmi specifici verso i gestori delle varie parti del servizio, e documentazione completa degli SLA
2) la verifica periodica da Internet della sicurezza dei server PEC in merito agli attacchi informatici
3) i servizi propri della PEC vengono monitorati costantemente dall' esterno, replicando il copione d'uso del cliente, comprensivo della autenticazione e dell'accesso alla propria casella di posta. Nel caso il test automatizzato non abbia avuto successo, vengono generati gli allarmi relativi alla funzione non eseguita, e questi vengono inviati via mail e SMS alla funzione organizzativa preposta alla gestione della funzione specifica:
    - linee internet,
    - router,
    - firewall,
    - rete interna,
    - cluster PEC.

Il gestore della area specifica si attiva quindi per il ripristino del servizio nel minore tempo possibile. Cedacri S.p.A. ha in tal senso stabilito dei sistemi di turnazione e di reperibilità del proprio personale, e dei contratti specifici con i propri fornitori.

4.1 Caratteristiche del servizio

4.1.1 Standard tecnologici e di sicurezza adottati

Cedacri S.p.A. facendo riferimento a quanto prescritto nel DM rif.[13] ha adottato, per l'erogazione dei propri servizi di PEC, i seguenti standards tecnologici:

- RFC 1847 – Security Multiparts for MIME: Multipart/Signed and Multipart/Encrypted
- RFC 1891 – SMTP Service Extension for Delivery Status Notifications
- RFC 1912 – Common DNS Operational and Configuration Errors
- RFC 2252 – Lightweight Directory Access Protocol (v3): Attribute Syntax Definitions
- RFC 2315 – PKCS#7: Cryptographic Message Syntax Version 1.5
- RFC 2633 – S/MIME Version 3 Message Specification
- RFC 2660 – The Secure HyperText Transfer Protocol
- RFC 2821 – Simple Mail Transfer Protocol
- RFC 2822 – Internet Message Format
- RFC 2849 – The LDAP Data Interchange Format (LDIF) Technical Specification
- RFC 3174 – US Secure Hash Algorithm 1 – SHA1
- RFC 3207 – SMTP Service Extension for Secure SMTP over Transport Layer Security
- RFC 3280 – Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List CRL profile

Nel rispetto della norma ISO 27001 gli standard di sicurezza seguiti per l'erogazione del servizio di PEC sono quelli previsti in codesto documento.

Inoltre, Cedacri S.p.A. si avvale per l'erogazione del servizio di Posta Elettronica Certificata di cluster di macchine Linux, che in questa fase è costituito da due sistemi in cluster ridondati.

I software installati sono di tipo open source, offrono la massima trasparenza del codice, e avendo i sorgenti ispezionabili sono tipicamente liberi da funzioni interne nascoste che danneggiano la sicurezza.

Le distribution di riferimento utilizzate sono la Debian e la SuSe, che sono considerate fra le distribuzioni Linux più stabili e sicure.

Periodicamente vengono applicate le patch necessarie a mantenere la sicurezza al massimo livello.

Le definizioni dell'antivirus CLAMAV vengono aggiornate con cadenza almeno giornaliera, ed è attiva una procedura che effettua aggiornamenti addizionali nel caso sia necessari per fronteggiare particolari diffusioni di nuovi virus.

Viene previsto un doppio livello di firewalling, gestito per la massimizzazione della sicurezza, e per evitare la ripetizione di errori umani, da due unità organizzative differenti.

Non solo nei firewall, ma anche a bordo del cluster sono definite, attraverso il software Iptables, le chiusure di tutte le porte ed i protocolli non contemplati dalla specifica tecnica per la erogazione dei servizi PEC.

Ovviamente tutte le password utente e di gestione, dove non già basate su smart card, devono essere più lunghe di 8 caratteri e cambiate almeno ogni 3 mesi.

4.1.2 Cenni sull'organizzazione e funzioni del personale

La struttura organizzativa individuata per il Servizio di PEC Cedacri S.p.A. riconosce il valore di tale funzione all'interno dell'offerta di servizi di Cedacri, attribuendo la responsabilità del suddetto Servizio al responsabile della CISO.

Nell'ottica di garantire un ridotto tempo di risposta alle richieste della Clientela è stato individuato un work-flow che separa le funzioni di front-office (ricezione richieste/feed-back della Clientela, gestione dei rapporti commerciali) da quelle di back-office, definite in ottemperanza alle normative vigenti. L'integrazione tra le due parti avviene utilizzando strumenti di work-flow che consentono una gestione completa dell'attivazione delle caselle di PEC e della registrazione dei titolari, oltre che delle attività collaterali di controllo.

Le diverse responsabilità sono state quindi attribuite a risorse e strutture dedicate ma inserite nel contesto delle Funzioni Aziendali già in essere le cui capacità ed esperienze potevano agevolare l'assolvimento dei nuovi compiti.

Nella gestione della sicurezza e secondo quanto previsto dalla normativa, sono stati separati i compiti tra la definizione delle regole, la loro esecuzione e l'auditing.

Facendo quindi riferimento a quanto disposto dall'art. 21, comma 1, del DM rif.[13] nel gruppo del personale dedicato al servizio di PEC erogato da Cedacri S.p.A. sono state individuate le seguenti figure organizzative:

- responsabile registrazione dei titolari
- responsabile dei servizi tecnici
- responsabile verifiche ed ispezioni (auditing)
- responsabile sicurezza
- responsabile sicurezza dei log dei messaggi
- responsabile sistema di riferimento temporale

Come previsto dal comma 2 del suddetto articolo, alcune responsabilità sono affidate allo stesso soggetto.

5 Modalità operative

5.1 Descrizione sintetica del servizio

Viene offerto il servizio completo di Posta Elettronica Certificata come definito nel D.M. 2 novembre 2005 (GU n. 266 del 15-11-2005) "Regole tecniche per la formazione, la trasmissione e la validazione, anche temporale, della Posta Elettronica Certificata." rif.[13].

5.2 Descrizione sintetica del flusso

Quando il mittente invia un messaggio (1) dalla propria casella di PEC sui sistemi Cedacri S.p.A., riceverà dallo stesso una ricevuta di accettazione, cioè la ricevuta, sottoscritta con firma digitale, contenente i dati di certificazione, rilasciata al mittente dal punto di accesso a fronte dell'invio del messaggio di Posta Elettronica Certificata (2). In alcuni casi il mittente potrà ricevere una ricevuta di non accettazione, ossia l'avviso sottoscritto con firma del gestore di Posta Elettronica Certificata (Cedacri S.p.A., nel nostro caso), quando il gestore è impossibilitato ad accettare il messaggio in ingresso, specificando i motivi per i quali non è possibile accettare il messaggio e l'esplicitazione che il messaggio non sarà consegnato al destinatario.

Il gestore del mittente (Cedacri S.p.A.) genera il messaggio di trasporto (3), anch'esso firmato digitalmente, che viene recapitato al gestore di PEC del destinatario, che potrebbe essere o meno Cedacri S.p.A.

Il gestore del destinatario, dopo le necessarie verifiche, invierà a Cedacri S.p.A. (gestore del mittente) la ricevuta di presa in carico (4) del messaggio, cioè la ricevuta, sottoscritta con firma digitale, emessa dal punto di ricezione nei confronti del gestore PEC del mittente per attestare l'avvenuta presa in carico del messaggio da parte del sistema di PEC di destinazione. Tale ricevuta reca i dati di certificazione atti a consentirne l'associazione con il messaggio al quale si riferisce, rendendolo disponibile nella casella di PEC del destinatario (5), inviando contestualmente la ricevuta di avvenuta consegna al mittente (6).

Quest'ultima può essere di 3 differenti tipologie:

- **ricevuta completa** di avvenuta consegna, ovvero quella nella quale sono contenuti dati di certificazione ed il messaggio originale;
- **ricevuta breve** di avvenuta consegna, ovvero quella nella quale sono contenuti i dati di certificazione ed un estratto del messaggio originale;
- **ricevuta sintetica** di avvenuta consegna, ovvero quella che contiene i dati di certificazione.

Con i client di posta elettronica (MS Outlook®, etc…) si riceve sempre una ricevuta completa di avvenuta consegna; con i prodotti webmail il mittente può scegliere quale tipo di ricevuta ricevere: di default si riceve quella completa (vedi Figura 3).

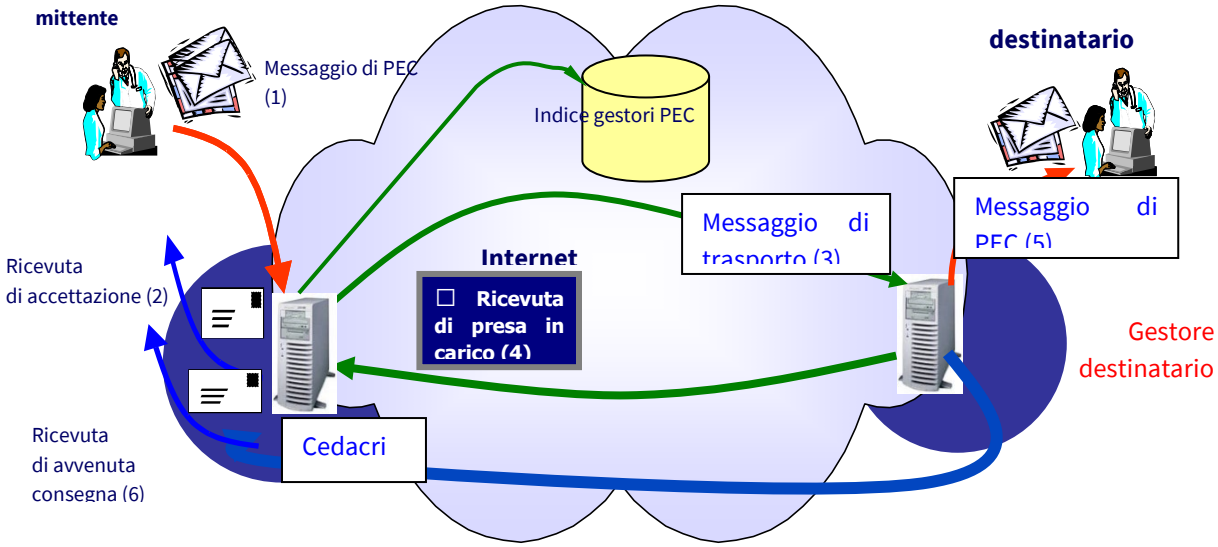

Figura 1 - Processo per la ricevuta di avvenuta consegna

5.3 Attivazione del servizio

Sono previste differenti tipologie di utenze:

- utenti singoli
- istituti bancari e loro clienti
- comunità/PA

Per i primi sarà sufficiente inviare il modulo di adesione al servizio di Posta Elettronica Certificata, scaricabile via Internet dal sito del Gestore www.cedacricert.it, debitamente compilato e sottoscritto insieme alla fotocopia del documento d'identità in corso di validità.

Si ricorda che, a norma dell'art. 35 del DPR 445/2000 rif.[4] sono considerati documenti d'identità validi equipollenti alla carta di identità, il passaporto, la patente di guida, la patente nautica, il libretto di pensione, il patentino di abilitazione alla conduzione di impianti termici, il porto d'armi, le tessere di riconoscimento, purché munite di fotografia e di timbro o di altra segnatura equivalente, rilasciate da un'amministrazione dello Stato.

L'invio della suddetta documentazione potrà avvenire sia via posta ordinaria, sia via fax.

Per quanto concerne la seconda e terza tipologia, gli utenti che intendono richiedere il servizio di Posta Elettronica Certificata erogato da Cedacri S.p.A., dovranno rivolgersi alla Direzione Commerciale, con la quale stipuleranno il contratto. La suddetta struttura si occuperà anche della raccolta della documentazione necessaria.

Il richiedente munito di poteri di rappresentanza o di altri titoli relativi all'attività professionale o a cariche rivestite, è tenuto ad indicarli all'atto della richiesta ed a munirsi della documentazione comprovante l'esistenza dei predetti poteri e/o titoli.

Sarà cura del responsabile dell'unità organizzativa CISOattivare la registrazione dei titolari in base alla documentazione pervenuta per permettere l'assegnazione delle singole caselle.

La modalità di accesso alla casella richiesta avviene tramite Userid/Password. Le credenziali di accesso alla casella di Posta Elettronica Certificata vengono spedite a mezzo mail all'indirizzo fornito in fase di richiesta di attivazione.

Il nome della casella è a discrezione di Cedacri SpA, che si riserva la facoltà di rifiutare la proposta del cliente a causa di omonimie, eccessiva lunghezza, nomi riservati, ecc..

Dalla data della firma del contratto decorrono i tre (3) giorni lavorativi necessari alla creazione ed attivazione delle caselle di Posta Elettronica Certificata, per la seconda e terza tipologia di clienti; per la tipologia di primo tipo, ossia gli utenti singoli, detto termine decorre dal ricevimento di tutta la documentazione necessaria all'attivazione del servizio.

5.4 Modalita' di revoca di una casella di pec

Per revocare una casella di PEC, occorre inviare a mezzo posta elettronica o fax, il Modulo di richiesta di revoca scaricabile dal sito del Gestore www.cedacricert.it, opportunamente compilato e sottoscritto, accompagnato dalla fotocopia di un documento di identità in corso di validità e del codice fiscale.

Effettuate le opportune verifiche, Cedacri effettuerà la revoca della casella.

Si ricorda che una volta avvenuta la revoca, non sarà più possibile accedere alla casella di Posta Elettronica Certificata del Servizio Posta Elettronica Certificata.

5.5 Personalizzazioni offerte da Cedacri

5.5.1 Casella di PEC su dominio istituzionale

In questo caso le caselle di Posta Elettronica Certificata saranno attivate sul dominio istituzionale del Gestore postacert.cedacri.it, pertanto potranno essere indirizzo@postacert.cedacri.it.

5.5.2 Casella di PEC su dominio dedicato

In questo caso le caselle di Posta Elettronica Certificata saranno attivate su un dominio personalizzato il cui nome sarà deciso dal cliente, comunque gestito dalla Cedacri S.p.A., anche se potrà essere data al cliente una certa autonomia per la gestione/creazione/cancellazione delle caselle su questo dominio. Il tutto dovrà essere concordato in fase di contrattazione. Il nome delle caselle sarà indirizzo@nomedominiocliente.it.

Sarà anche possibile personalizzare il portale di accesso via webmail, ovvero l'interfaccia grafica della pagina di accesso con logo, immagini e quant'altro.

L'erogazione del servizio e ciò che ne consegue rimangono comunque in carico alla Cedacri S.p.A. in quanto Gestore di Posta Elettronica Certificata.

5.6 Modalità di accesso

Ci sono almeno due modalità per leggere e inviare le e-mail:

- direttamente, tramite un Web browser (attraverso una procedura di login)
- usando programmi mail client (tipo MSOutlook Express®) residenti sulla propria postazione di lavoro o personal computer.

5.6.1 Modalità di accesso via web browser

La prima modalità è quella che potremmo definire "a bordo server", e consiste semplicemente nell'accedere a tutte le funzioni del mail server direttamente da interfaccia web, permettendo anche una consultazione più rapida, alla url https://www.postacert.cedacri.it (Figura 2).

Per effettuare il logon, sarà necessario digitare userid e password.

È consigliabile cambiare la password di default assegnata automaticamente dal gestore del servizio con una lunga almeno otto (8) caratteri e contenente diversi tipi di caratteri, non solamente di tipo alfabetico; è consigliabile cambiarla periodicamente, almeno con cadenza mensile (l'optimum sarebbe ogni 15 giorni).

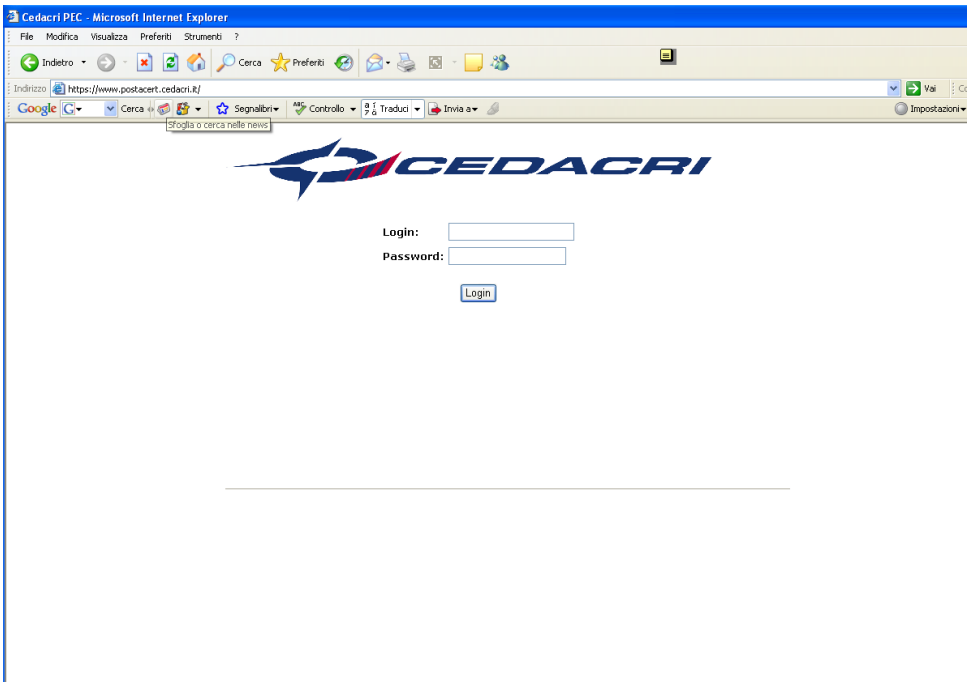

Figura 2 - https://www.postacert.cedacri.it

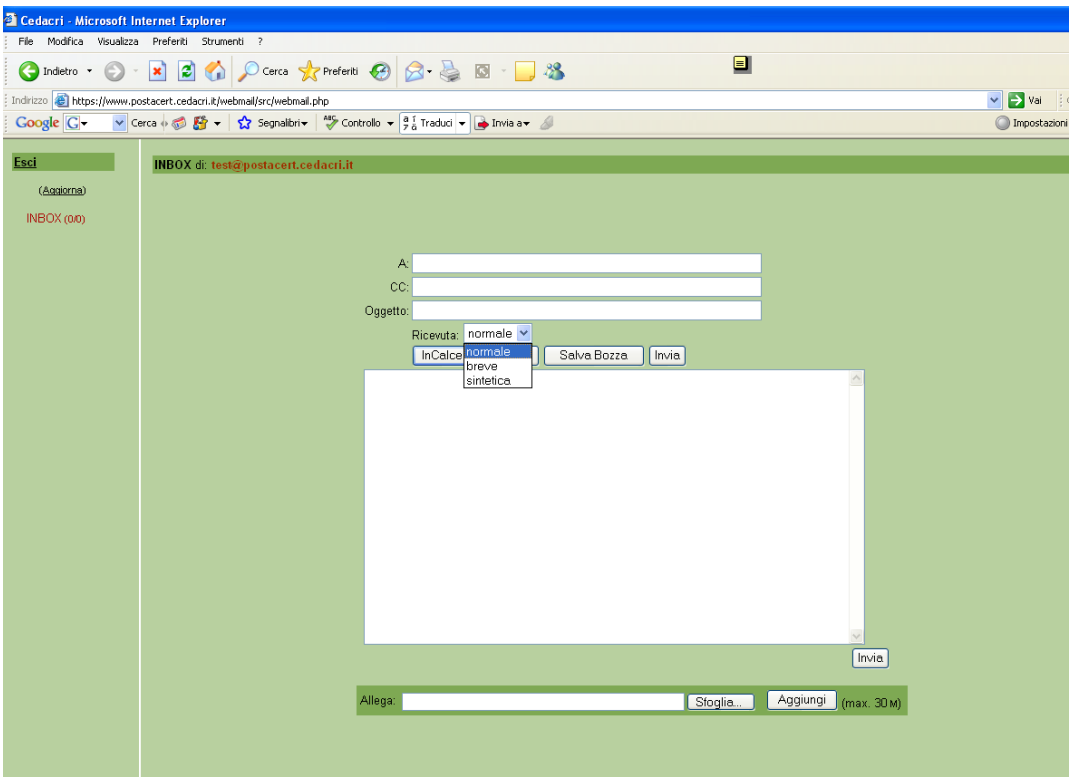

Figura 3 – Selezione per la scelta del tipo di ricevuta

5.6.2 Modalità di accesso via client

La prima operazione, da svolgere una tantum, consiste nel configurare il proprio account di Posta Elettronica Certificata presso il proprio client.

In questo caso facciamo riferimento a MS Outlook Express 6 anche se la procedura di setup è di poco dissimile per gli altri client.

Recandosi sul menu Strumenti e selezionando la voce Account (Figura 4) si accede alla gestione degli account inclusa la creazione.

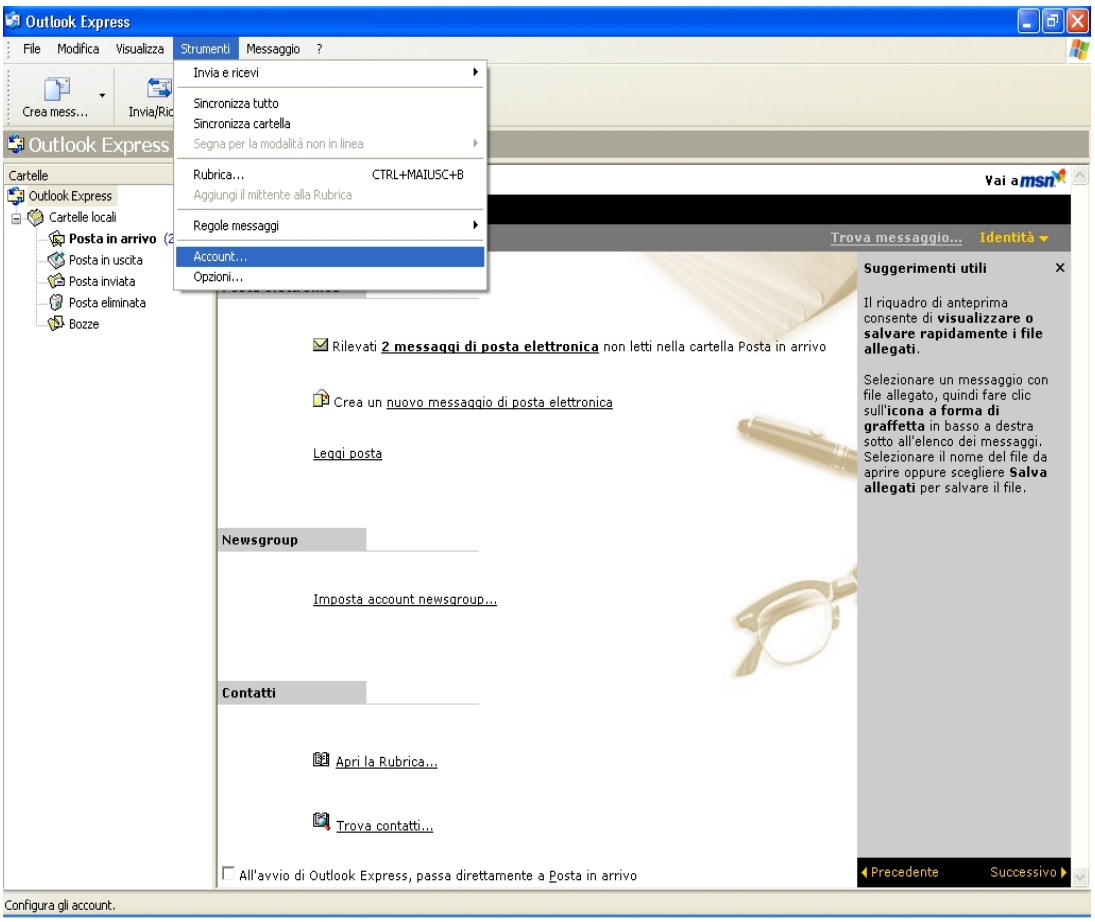

Figura 4 - Gestione degli account inclusa la creazione

La piccola finestra che si apre ha un tab inerente gli account di posta elettronica.

Selezionarlo e procedere premendo il tasto **Aggiungi** sulla destra.

Scegliere sempre la voce inerente la posta elettronica (Figura 5).

Questa scelta aprira' un wizard (Connessione Guidata Internet) per la configurazione.

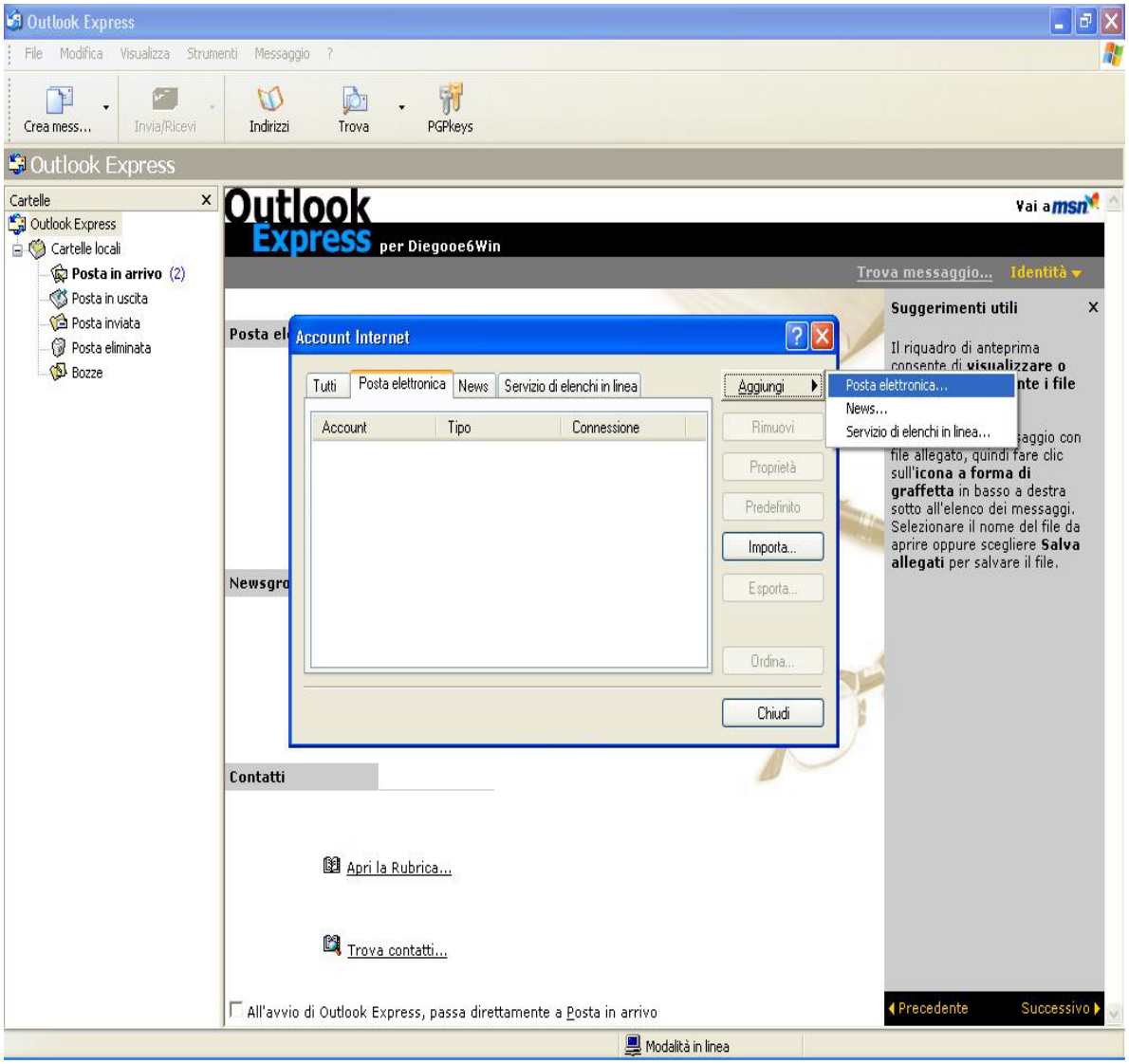

Figura 5 – Configurazione account internet

Inserire il proprio nominativo, ovvero il Display Name, cioè quello della persona associata all'indirizzo e-mail. (Figura 6)

Premere **Avanti** una volta inseriti i dati.

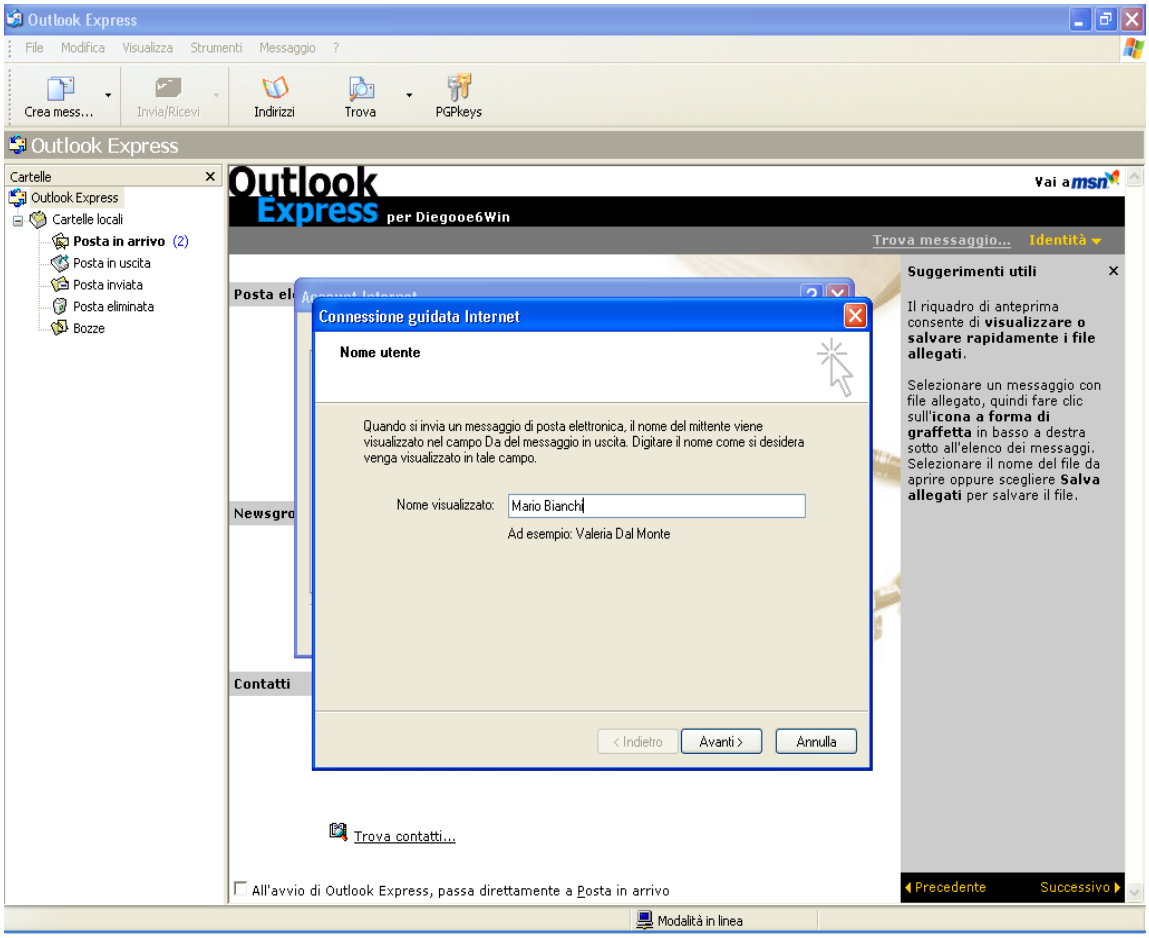

Figura 6 – Connessione guidata internet

Inserire il proprio indirizzo e-mail, quello della mailbox PEC assegnata.

Premere **Avanti** una volta inseriti i dati (Figura 7).

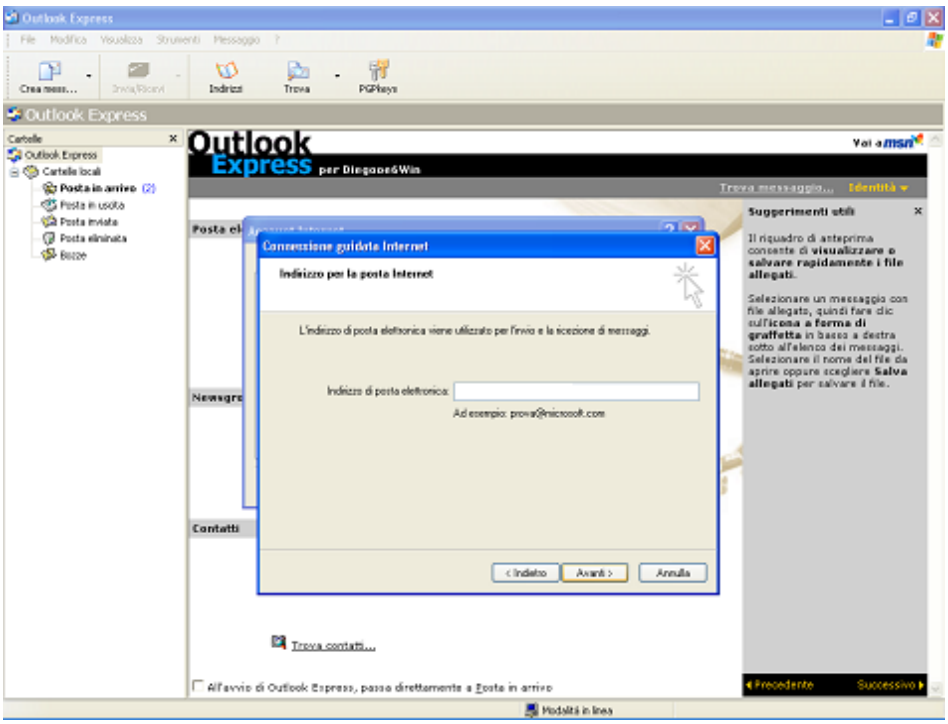

Figura 7 – Connessione guidata internet – inserimento indirizzo di posta elettronica

Alla schermata successiva bisogna inserire gli indirizzi dei server di posta POP3 (Ricezione) e SMTP (Invio).

Per entrambi inserire lo stesso indirizzo: client.postacert.cedacri.it (Figura 8)

Nota: in questa fase di configurazione, è possibile scegliere in alternativa al protocollo di ingresso POP3S, il protocollo IMAPS, selezionandolo dal menu del server della posta in arrivo (Figura 8)

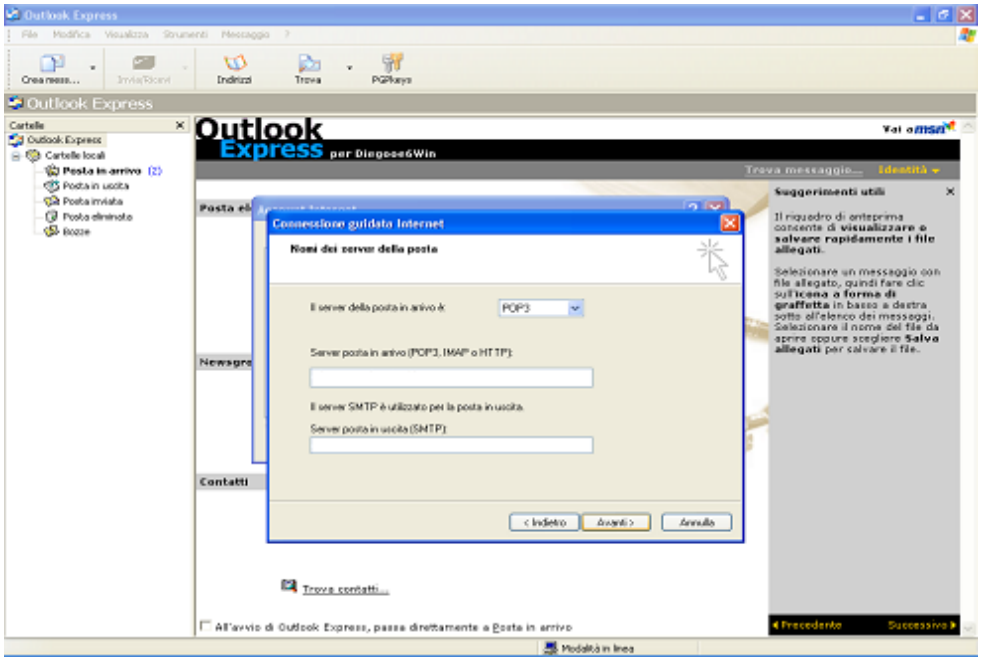

Figura 8 – Connessione guidata internet – server della posta

Il passo seguente consiste nell'inserire l'utenza (account) assegnata.

Inserire il Nome Utente (UserID).

Per quel che riguarda la password, è possibile inserirla nella casella di testo sottostante e far si che il client la memorizzi per comodita' dell'utente.

Se però si vuole ottenere un livello di sicurezza maggiore e prevenire un eventuale utilizzo dell'account di PEC con il solo accesso ad Outlook, una via consigliabile è quella di non far memorizzare la password, ma di far sì che il client la chieda per ogni sessione di invio o ricezione di messaggi di PEC.

La password può essere memorizzata o appuntata da qualche parte non ovvia a scelta dell'utente.

Per far ciò, togliere la spunta alla voce Memorizza Password e premere Avanti. (Figura 9)

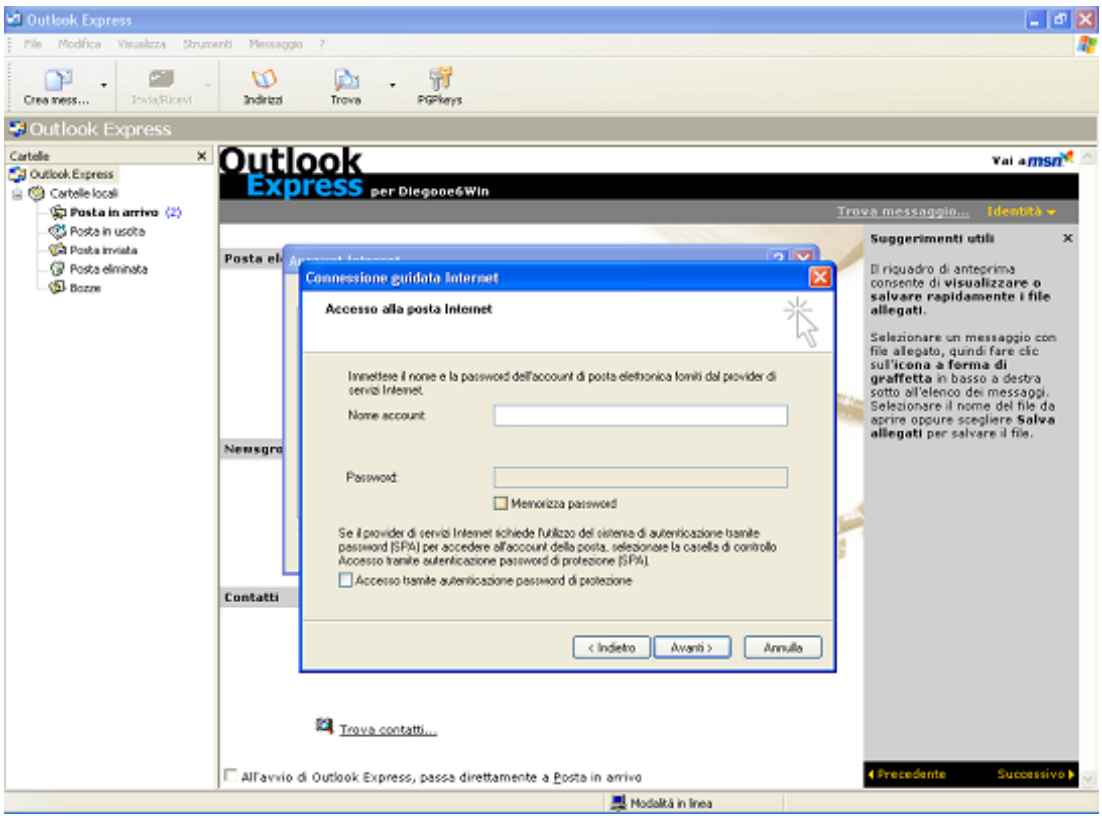

Figura 9 – Connessione guidata internet – accesso alla posta internet

Premere il tasto Fine del Wizard di configurazione.

Una volta terminata l'operatività di configurazione del client attraverso il Wizard si ritorna alla finestrella degli account e si vede quello appena creato (ha il nome del server di posta per default).

Il setup non èancora terminato poiché bisogna configurare l'accesso con canale securizzato e la spedizione autenticata.

Selezionare l'account appena creato e premere il tasto Proprietà (Figura 8)

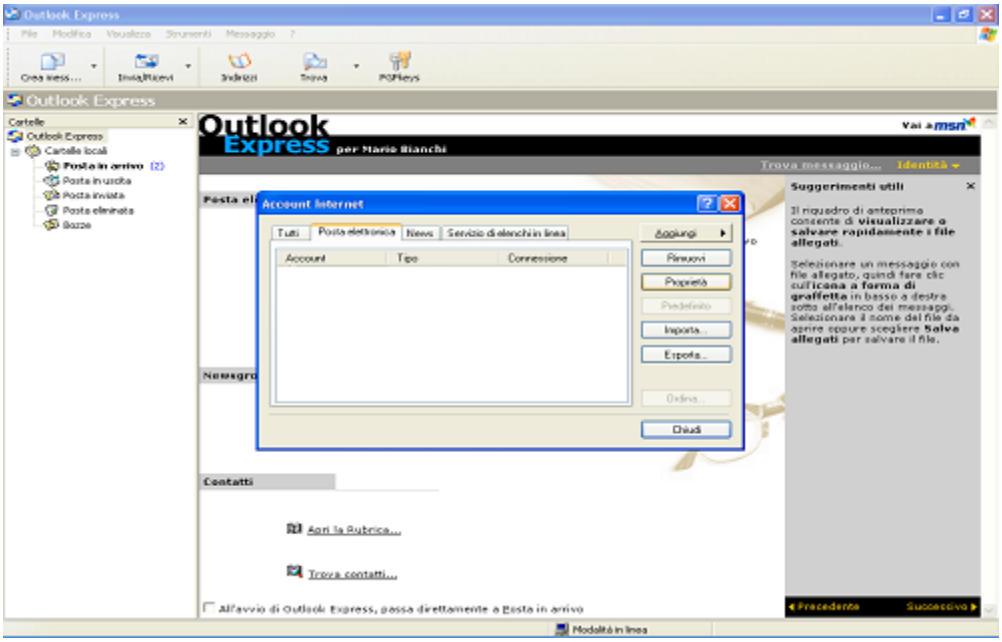

Figura 10 – Connessione guidata internet – account internet

All'apertura del tab Generale dell'account e' possibile cambiare nome di riferimento all' account e configurare un indirizzo per le risposte. Premere Applica se si sono effettuate modifiche.

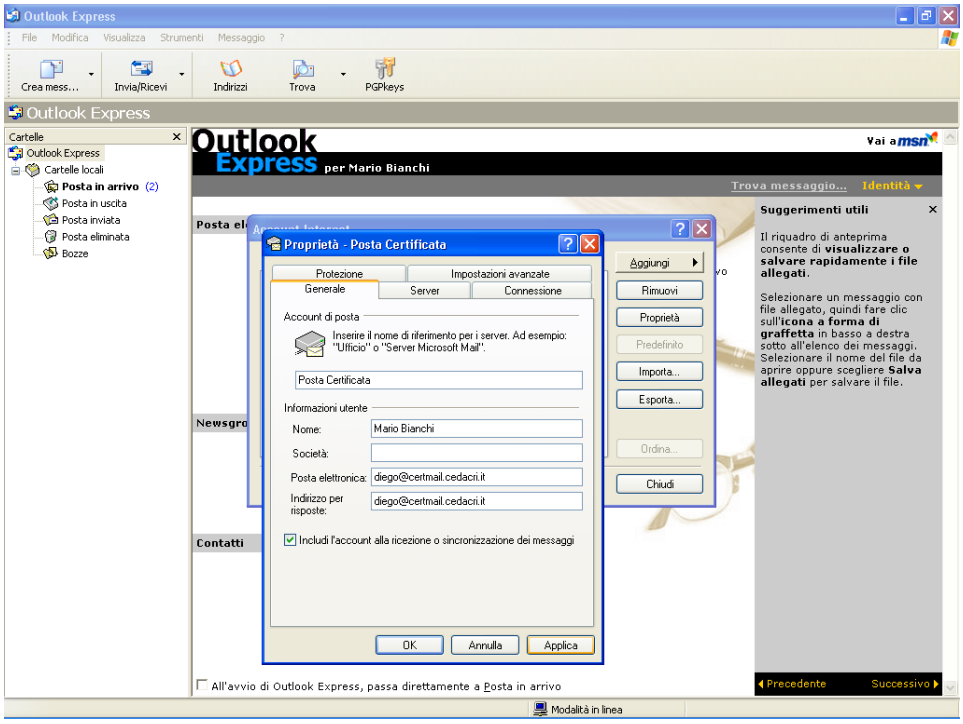

Figura 11 – Proprietà – Posta Certificata

Selezionare il tab **Server.**

Il sistema PEC richiede l'autenticazione per la spedizione (SMTP AUTH), quindi alla voce **Server della Posta in uscita** selezionare la spunta **Autenticazione del server necessaria** (Fig 10).

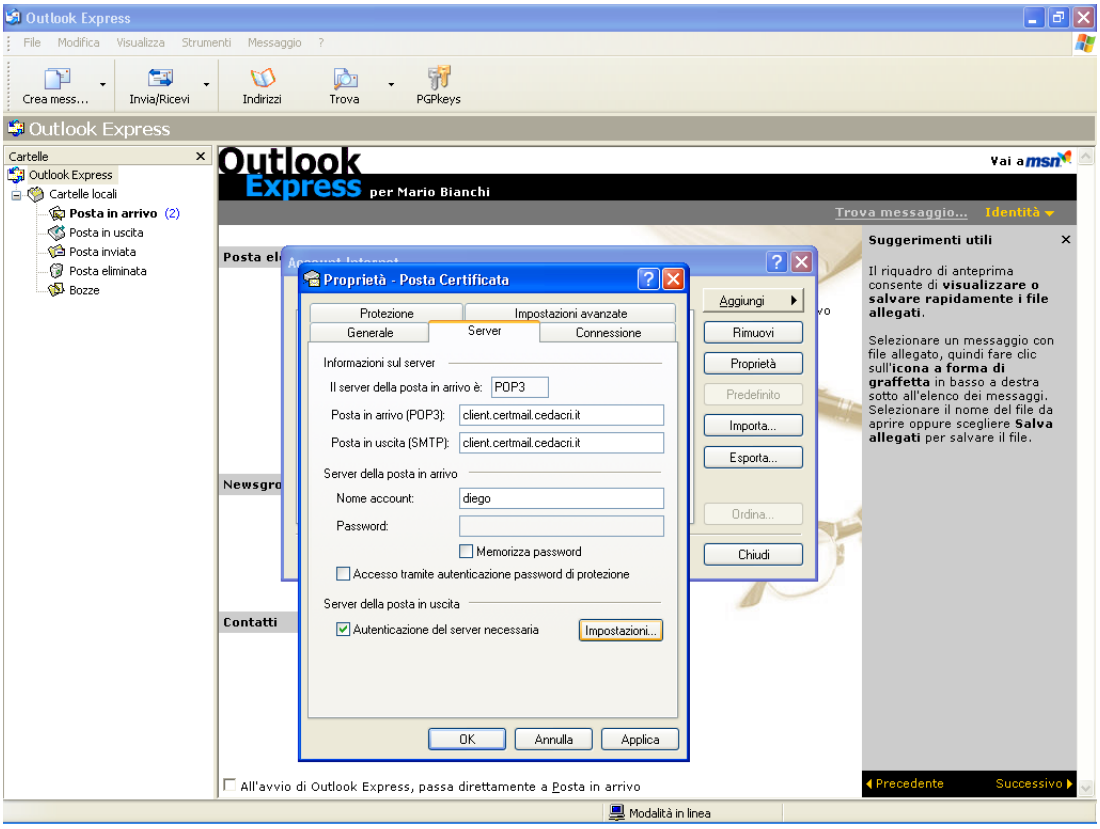

Figura 11 – Proprietà – Posta Certificata - Server

Il tasto Impostazioni a fianco permette di specificare una coppia Utente/Password per la spedizione o usare le stesse della ricezione precedentemente configurate. Controllare che le impostazioni siano uguali a quelle per la ricezione (Figura 12).

Nota: Se al momento della configurazione della parte POP3 dell'account si èscelto di non far memorizzare la password al client, questa configurazione ovviamente eredita il fatto di richiedere una password per sessione (la stessa in tutti e due i casi) anche per la spedizione di messaggi PEC.

Questo comportamento offre il livello di sicurezza di non poter spedire e-mail certificate da quel client/postazione se non inserendo la password per ogni sessione.

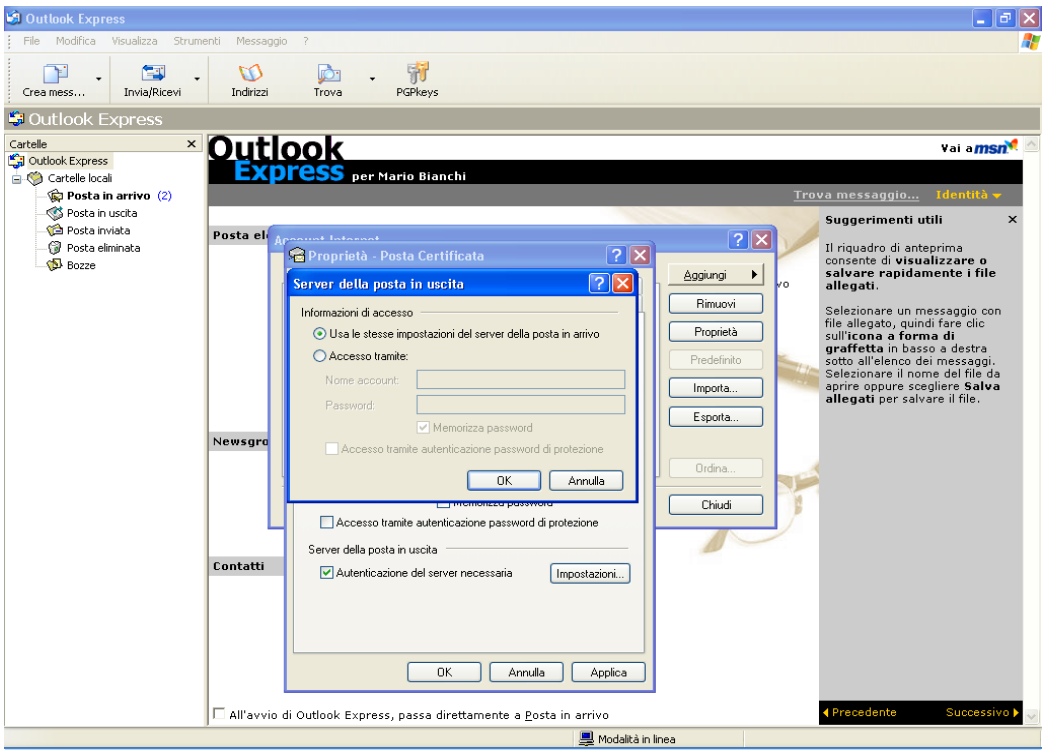

Figura 12 – Proprietà – Posta Certificata – Server della posta in uscita

Cliccare sul tab Impostazioni Avanzate per configurare l'accesso su canale criptato per ricezione e spedizione da e verso il server di posta certificata.

Alla voce Numeri di porta del server, bisogna indicare su quali porte connettersi per ricezione e spedizione, nonche' specificare se i canali useranno crittografia SSL (Secure Socket Layer) da e verso il server PEC.

Spuntare il check, per la posta in arrivo POP3, Il server necessita di una connessione protetta, automaticamente Outlook imposta il numero di porta a 995 che è il valore corretto per POP3S per il server PEC.

Spuntare il check, per la posta in uscita SMTP, Il server necessita di una connessione protetta, e impostare il valore della porta a 465 per SMTP su SSL tra client e server.

Nota: MS Outlook Express, stranamente imposta automaticamente il numero di porta corretto per POP3 securizzato ma non per la parte SMTP. Ricordarsi quindi di inserire manualmente il valore prima di selezionare Applica. (Figura 13)

Nota: se si è scelto come protocollo della posta di ingresso l'IMAPS al posto del POP3S, la porta di ingresso da configurare è la 993.

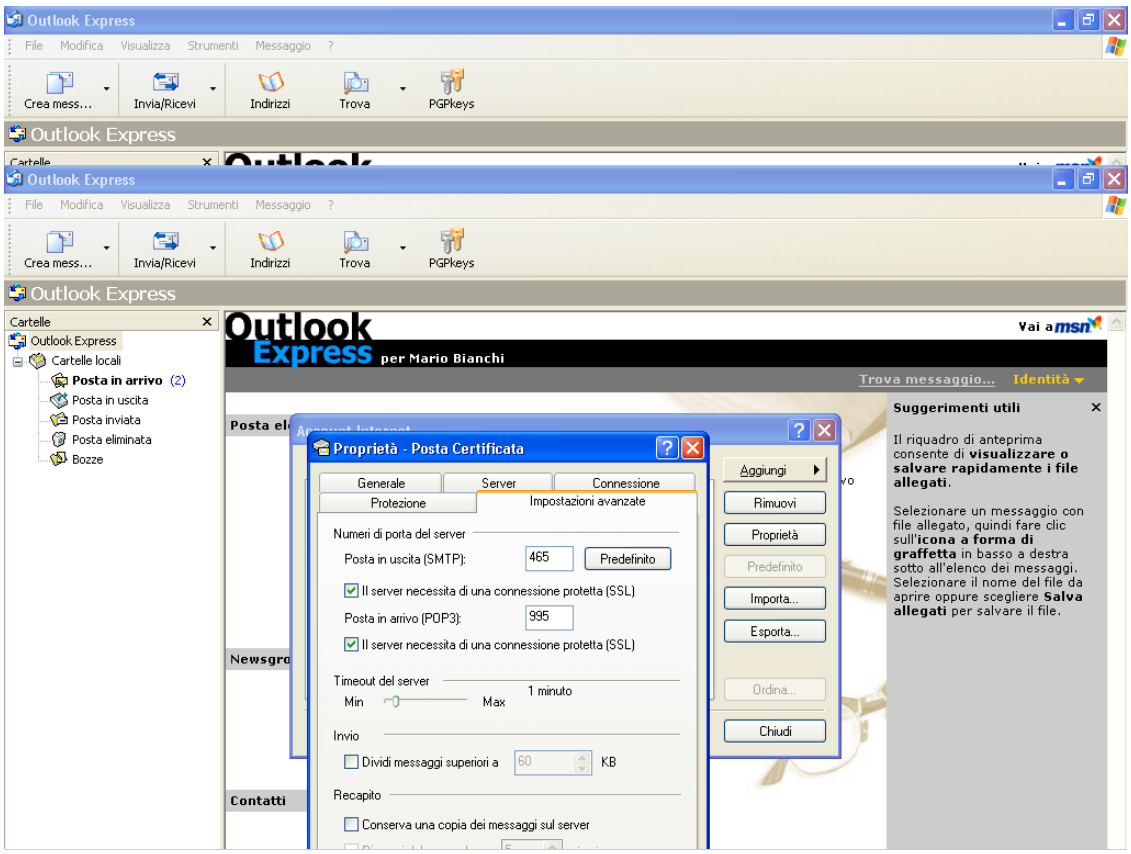

Figura 13 – Proprietà – Posta Certificata – Impostazioni avanzate

5.6.2.1 Inviare una mail

Una volta configurato correttamente l'account, la metodologia da applicare per la spedizione di e-mail è quella di un classico client di posta.

Una accortezza da seguire è quella di scegliere correttamente il server della posta in uscita (SMTP) in caso di account multipli.

Step 1:

Creare un nuovo messaggio utilizzando il tasto **Crea Messaggio/Scrivi Messaggio** (Fig 14)

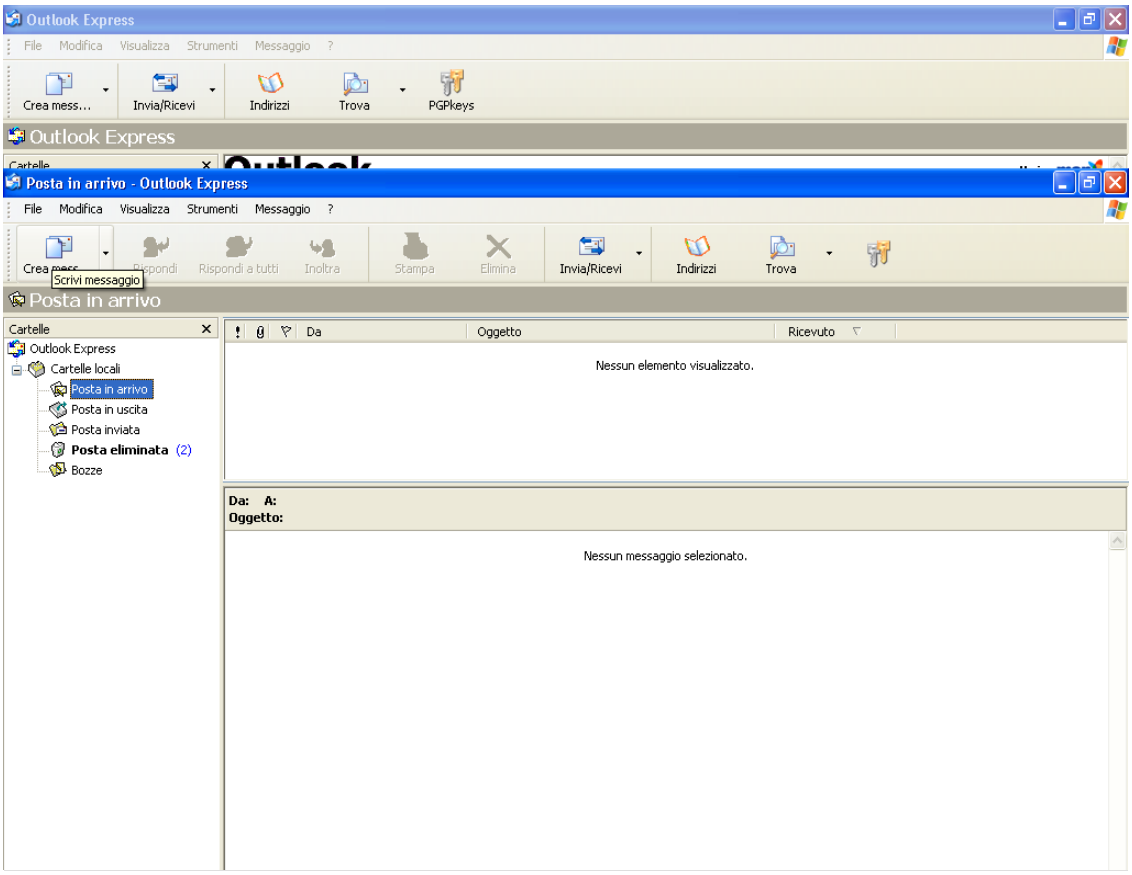

Figura 14 – Posta in arrivo - Crea Messaggio/Scrivi Messaggio

Step 2:

Inserire nel campo **A:** (**To:**) il destinatario del messaggio (eventualmente anche altri destinatari nel campo Cc).

Inserire l'oggetto, il testo del messaggio ed eventualmente degli allegati.

Cliccare su **Invia.** (Figura15)

Nota: Se il destinatario è associato ad un indirizzo PEC, a fronte di questo invio il mittente dovra' aspettarsi 2 messaggi in risposta dai sistemi PEC coinvolti: una ricevuta di accettazione di invio ed una ricevuta di consegna.

Nota: Essendo la connessione con il server criptata SSL, sono coinvolti certificati digitali e Certification Authority (CA), è possibile che non su tutti i client di posta sia installata (e "trustata") la CA che ha erogato il certificato, per cui è possibile che venga segnalato questo fatto tramite messaggio apposito al momento della spedizione (nonché della ricezione). Per ovviare a questo, installare il certificato root della Certification Authority che ha rilasciato i certificati sulla postazione dalla quale si utilizza il servizio (a tal fine consultare le istruzioni

contenute nella documentazione consegnata insieme alle informazioni relative alla casella attivata).

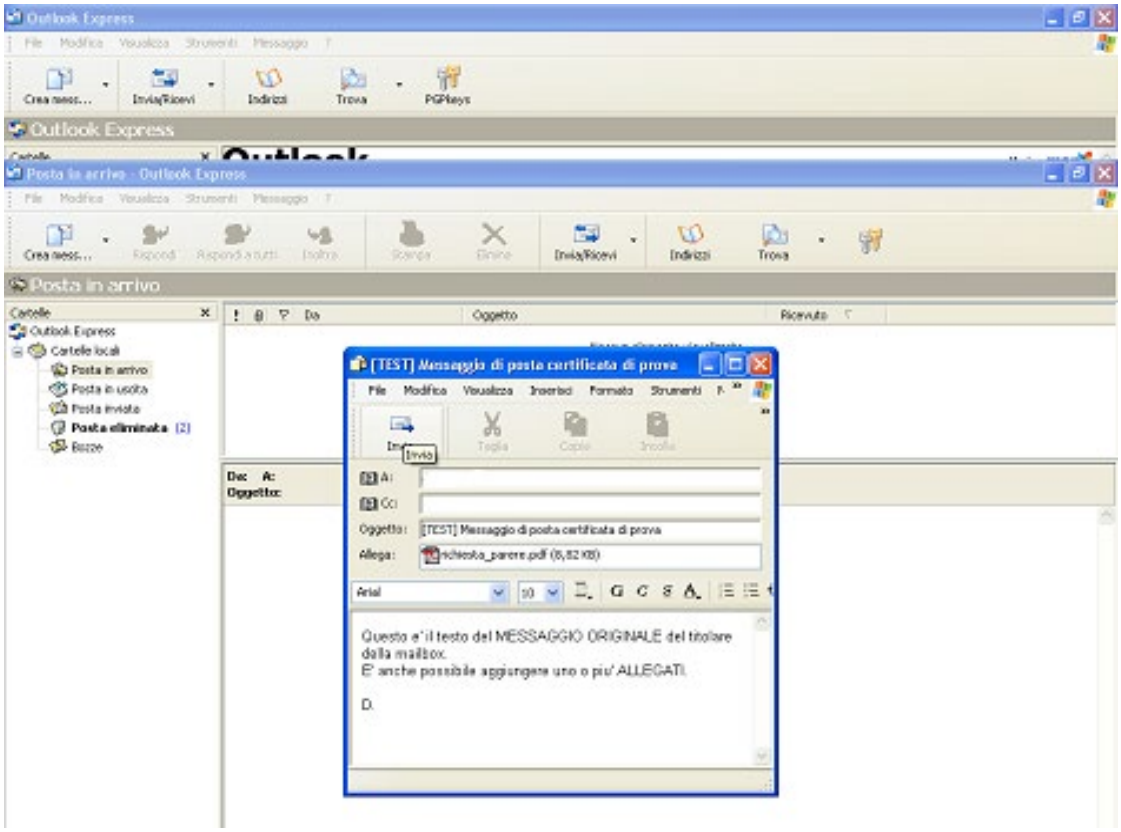

Figura 15 – Posta in arrivo – Invio

5.6.2.2 Ricevere una mail

Per ricevere una mail bisogna procedere allo scaricamento dall'account di posta certificata, selezionandolo dal Menu' **Strumenti** (Fig 16)

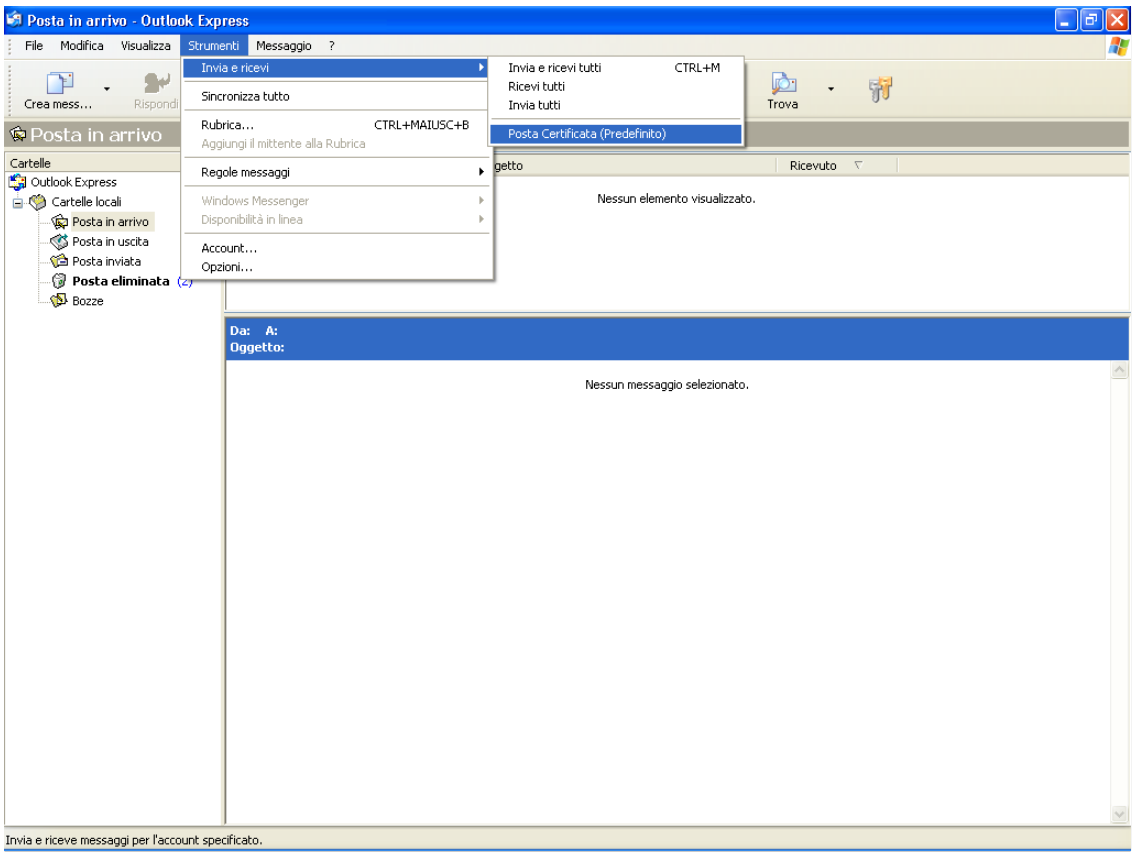

Figura 16 – Ricezione mail

Nota: Anche durante lo scaricamento da sessione criptata potrebbe essere visualizzato il messaggio di CA sconosciuta (Figura 17). Se tutti gli altri dati sono corretti, procedere comunque e importare al piu' presto il certificato di CA dal proprio gestore.

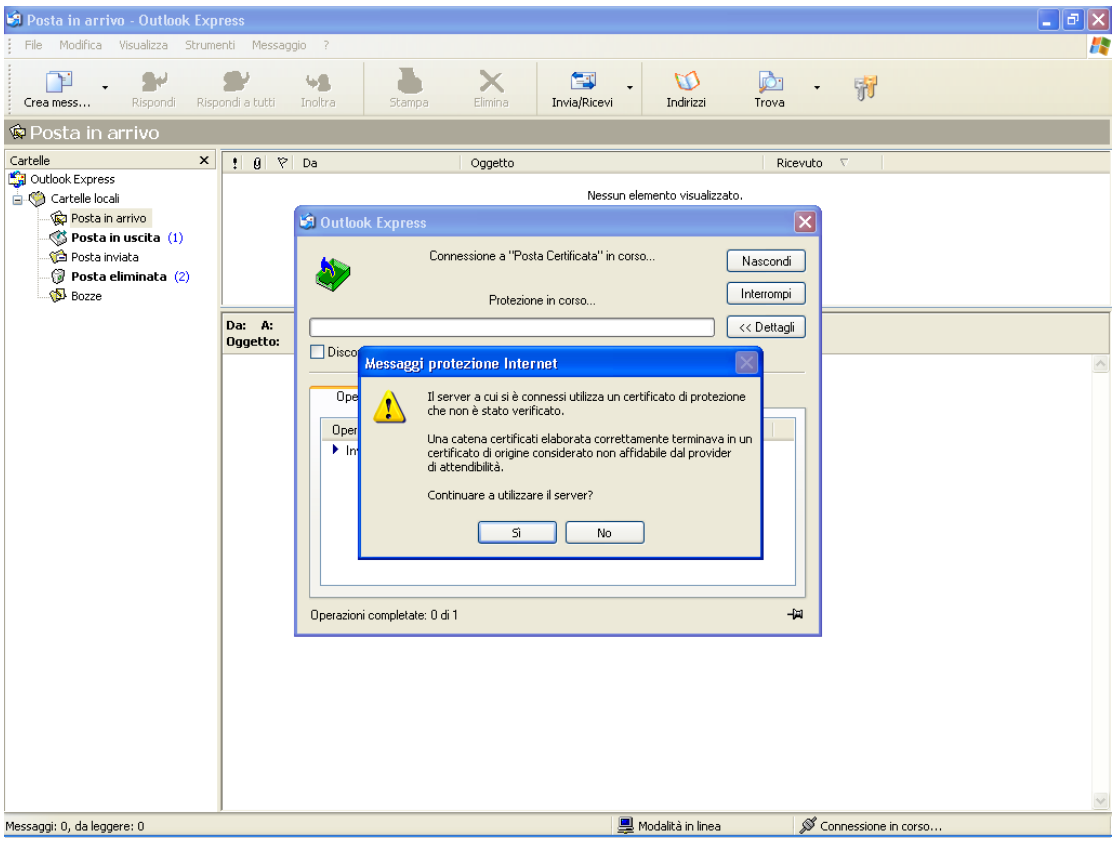

Figura 17 – messaggio di CA sconosciuta

Una volta scaricati i messaggi contenuti nella mailbox certificata si può procedere alla lettura e/o alla loro archiviazione.

L'archiviazione immediata è tipica per le **ricevute digitali** peculiari del sistema PEC, e sono quella di **accettazione** e quella di **consegna**.

Entrambe arrivano sotto forma di mail e sono riconoscibili dall'oggetto che riporta rispettivamente le parole “ACCETTAZIONE” e “CONSEGNA” nell'oggetto.

Nota: TUTTI i messaggi di PEC sono mail firmate digitalmente, quindi il client di posta deve essere di tipo S/MIME e deve permettere la verifica di integrità e provenienza del messaggio.

Un messaggio corretto riporta una coccarda rossa in alto a destra.

Un messaggio con firma invalida riporta una coccarda grigia con un punto esclamativo.

A seconda del client di posta utilizzato, in caso di verifica fallita, prima di mostrare il messaggio viene visualizzato un avviso informativo (Figura 18) che permette anche di aprire il contenuto del messaggio con un tasto Apri o Visualizza.

È possibile cliccare sulla coccarda per ottenere ulteriori informazioni sulle motivazioni del fallimento della verifica.

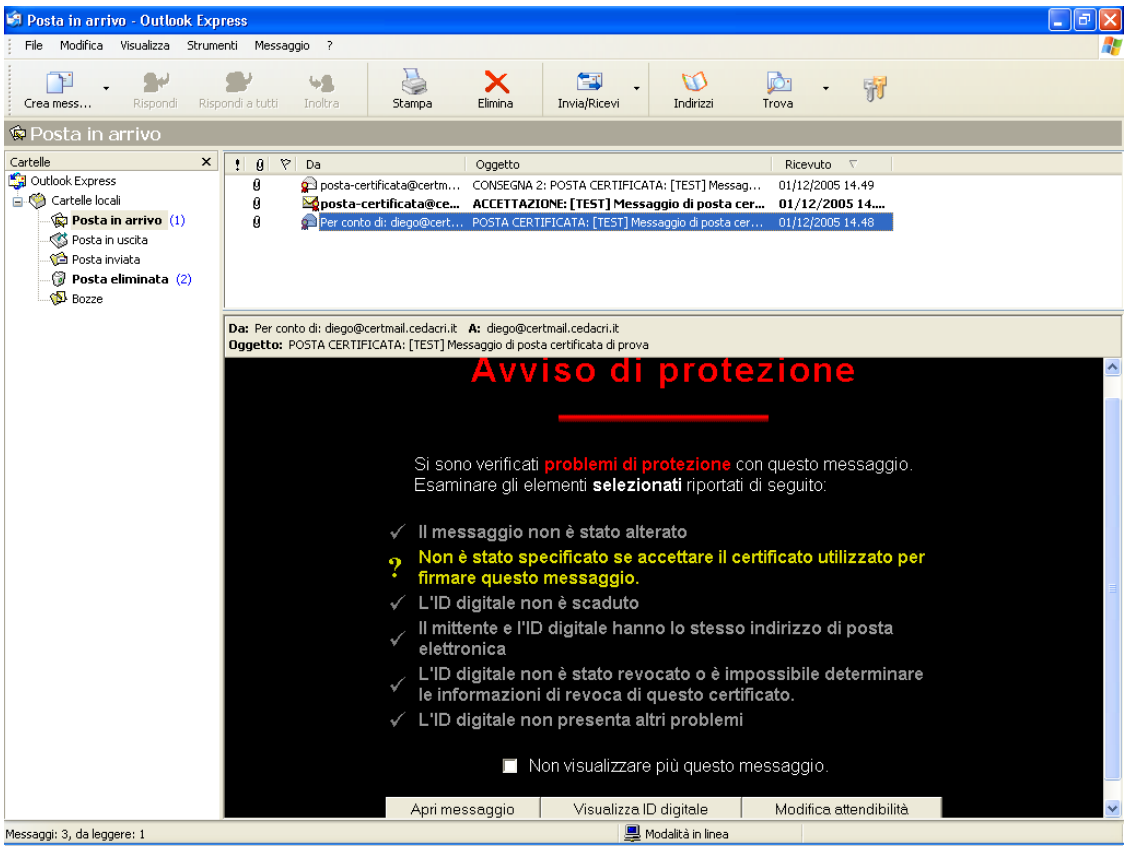

Figura 18 – avviso di protezione

5.6.2.3 Leggere un messaggio di posta certificata

La lettura del messaggio originale, su client MSOutlook®, è leggermente laboriosa in quanto bisogna aprire lo stesso con doppio click del mouse, e confermare l'apertura di un messaggio contenuto nel messaggio (dal nome **postacert.eml**)

Postacert.eml è il messaggio che contiene i dati che ci interessano ed è contenuto all'interno del messaggio di trasporto che, anch'esso firmato digitalmente dal server mittente.

Il messaggio di trasporto si identifica facilmente dalle prime parole dell'oggetto che recita: “POSTA CERTIFICATA: [.. Oggetto originale ...]” (Figura 18)

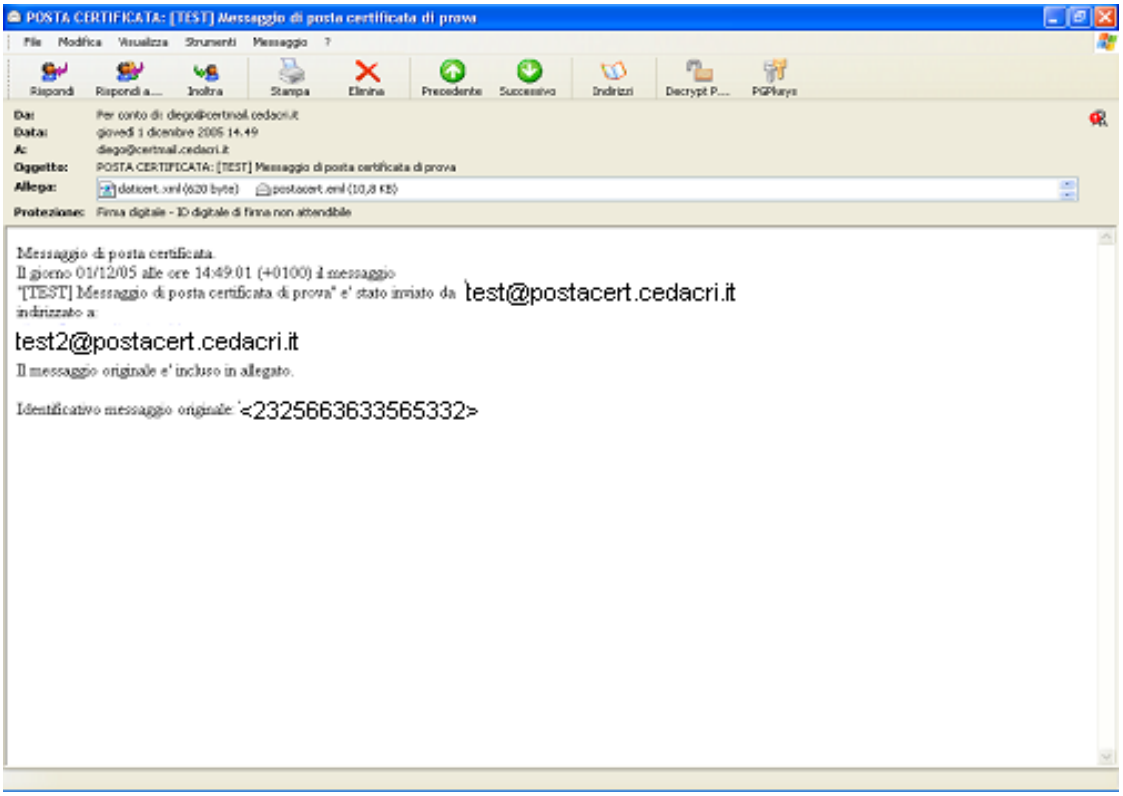

Figura 19 – lettura posta certificata

5.6.2.4 Leggere un messaggio di posta elettronica ordinaria

Nel caso venisse inviato un messaggio da una mailbox ordinaria verso una certificata, il messaggio originale, non potendo essere validato, non e' considerato di Posta Elettronica Certificata e viene inserito dal sistema in un messaggio di **ANOMALIA DI TRASPORTO** riconoscibile dall'oggetto recante la scritta: ANOMALIA: [...Oggetto Originale ...]

La lettura di questo messaggio avviene nel medesimo modo del messaggio di trasporto corretto, con la sola esclusione del fatto che l'allegato contenente il messaggio si chiama **anomalia.eml.**

5.6.3 Raccomandazioni generali per l'utenza

Per un corretto utilizzo delle caselle di posta si suggerisce al Titolare di consultare frequentemente la casella; infatti ogni messaggio ricevuto nella casella di posta elettronica certificata si intende pervenuto al Titolare della casella stessa (DPR 11 febbraio 2005, n. 68 - rif. [11]).

È bene cancellare dal server di posta i messaggi con una frequenza sufficiente per evitare che, venendo occupato tutto lo spazio assegnato contrattualmente alla casella stessa, i messaggi successivi vengano rifiutati. Il servizio Postacert tiene traccia dei soli log degli eventi principali, ma non comprende il sistema di conservazione a norma dei documenti scambiati via posta elettronica né delle relative ricevute.

Ai fini di garantire il più alto livello di sicurezza nel controllo degli accessi, come già scritto in precedenza, si invita l'utente a cambiare al più presto la password di accesso impostata all'atto della creazione della casella.

È opportuno dotare le stazioni di lavoro di un antivirus costantemente aggiornato per garantire maggiore sicurezza per quanto viene spedito e ricevuto. Infatti, se pure la casella Postacert è dotata di antivirus in grado di proteggere l'utente dai principali pericoli di infezione, non è possibile controllare automaticamente tutti i contenuti potenzialmente dannosi; in particolare si fa presente che i messaggi o file crittografati non possono essere sottoposti a controlli efficaci.

È opportuno portare a conoscenza i propri corrispondenti che si è in possesso di una casella di posta a valore legale. Questo costituisce una garanzia anche per i destinatari.

5.6.4 Cessazione del servizio

Nel caso di cessazione dell'attività di provider di Posta Elettronica Certificata, Cedacri S.p.A. comunicherà questa intenzione a AgID con un anticipo di almeno 60 giorni.

Con pari anticipo Cedacri S.p.A. informerà (a mezzo posta elettronica certificata e/o apposito annuncio sul sito https://www.postacert.cedacri.it) della cessazione dell'attività tutti i possessori di caselle PEC da esso gestiti.

Nella comunicazione sarà chiaramente specificato che tutte le caselle non saranno più accessibili dal momento della cessazione della attività del Gestore. Cedacri S.p.A. comunque prevede che le caselle oggetto di cessazione del servizio restino attive in sola lettura (senza possibilità di invio/ricezione messaggi) per un periodo non inferiore a 30 giorni a decorrere dal giorno definito per la cessazione del servizio.

5.7 Descrizione delle modalità di reperimento e di presentazione dei log dei messaggi

Vengono mantenuti sui server PEC i log degli ultimi 30 mesi; tali log sono anche archiviati giornalmente con una procedura che garantisce la loro conservazione, in conformità con quanto previsto dalla Deliberazione CNIPA 11/2004 rif.[16], per almeno 30 mesi, come richiesto dal DPR 68/2005 all'art. 11, comma 2 rif.[11], e la possibilità di recupero qualora se ne presenti la necessità.
Come previsto dall'art. 6, comma 7, del DPR rif.[11], qualora il titolare della casella di Posta Elettronica Certificata non abbia più la disponibilità delle ricevute dei messaggi di Posta Elettronica Certificata inviati, le informazioni contenute nel registro informatico del servizio, ovvero i log, sono opponibili a terzi.

Per richiedere la copia del log dei messaggi, il titolare deve inoltrare la richiesta dalla propria casella di posta certificata all' indirizzo recuperolog@postacert.cedacri.it.

La richiesta dovrà contenere i seguenti dati:

- data di riferimento del messaggio
- indirizzo di Posta Elettronica Certificata del corrispondente.

Acquisiti i dati, il responsabile dei servizi tecnici di Cedacri provvederà all'evasione della richiesta in prima persona o delegando un operatore del suo servizio.

Reperite le informazioni, dalla casella di Posta Elettronica Certificata recuperolog@postacert.cedacri.it verrà inviata una mail certificata al richiedente contenente le informazioni richieste.

Nel caso il richiedente non sia più utente della casella di posta elettronica per cui richiede i log, la richiesta dovrà pervenire, previo accertamento dell'identità del richiedente, tramite raccomandata postale ed essere accompagnata da "Dichiarazione Sostitutiva di Atto di Notorietà (art. 47, DPR 28 dicembre 2000, n. 445)", attestante la titolarità della casella alla data di riferimento, che sarà verificata nei confronti degli archivi delle funzioni amministrative di Cedacri S.p.A., e dall'indirizzo di posta ordinaria a cui inviare i log estratti.

Nel caso si debba produrre il log completo, comprensivo di firma e timestamping, questo verrà prodotto solamente di fronte all'autorità giudiziaria quando questa lo richieda, in quanto tali file contengono elementi di altre sessioni su cui deve essere applicata la legge 196/03 rif.[5] perché sia garantita la privacy.

6 Marcatura Temporale

Tutti i log dei messaggi e i messaggi con virus, che devono essere conservati per trenta mesi, sono salvati con l'apposizione della Marca temporale, emessa dal TimeStamp Server del Servizio Cedacricert di Firma Digitale erogato da Cedacri S.p.A. in qualità di Certificatore Accreditato.

Il TimeStamp Server Cedacri S.p.A. tiene allineato il proprio orologio interno con l'Istituto Elettrotecnico Nazionale "G. Ferraris", a norma del decreto ministeriale n. 591 del 30/11/1993, con un discostamento al massimo di ± 2 ms rispetto alla scala di tempo nazionale (UTC).

Così come disposto dalla normativa vigente, tutti gli eventi (generazione di ricevute, buste di trasporto, log, etc.) che costituiscono la transazione di elaborazione di un messaggio presso i punti di accesso, ricezione e consegna, impiegano un unico valore temporale rilevato all'interno della transazione stessa. In questo modo l'indicazione dell'istante di elaborazione del messaggio è univoca all'interno dei log, delle ricevute, dei messaggi, etc., generati dal server.

Le informazioni relative alle indicazioni temporali sono fornite in formato leggibile dall'utente (testo delle ricevute, buste di trasporto, etc.) e con riferimento all'ora solare/legale vigente al momento indicato per l'operazione. Per la data il formato impiegato è "gg/mm/aaaa" mentre per l'indicazione oraria si utilizza il formato "hh:mm:ss", dove hh è in formato 24 ore.

Al dato temporale è fatta seguire tra parentesi la differenza (in ore e minuti) tra l'ora solare/legale locale ed UTC. La rappresentazione di tale valore è in formato "[+|-]hhmm", dove il primo carattere indica una differenza positiva o negativa."

7 Gestione dati dei Titolari

7.1 Riservatezza

Le informazioni raccolte dal Gestore Accreditato nell'esercizio delle proprie funzioni vengono inizialmente raccolte su supporti cartacei e successivamente immesse nel sistema informatico dello stesso. Esse sono da considerarsi riservate, fatte salve quelle destinate all'uso pubblico delle caselle di posta.

I supporti cartacei sono archiviati anche elettronicamente e mantenuti per il periodo di tempo previsto dalla normativa in essere.

In ogni caso, il Gestore Accreditato si atterrà a quanto previsto dal d. lgs. 30 giugno 2003, n. 196 e successive modificazioni, nel trattamento dei dati personali di cui verrà in possesso e nell'adozione delle relative misure di sicurezza.

7.2 Sicurezza

È stato redatto un Piano per la Sicurezza secondo le disposizioni della circolareCNIPA [rif. 14], che costituisce un documento riservato, comunque consegnato a AgID. Nel Piano sono dettagliate le misure di sicurezza fisiche e logiche adottate per la protezione dell'integrità e della riservatezza dei dati.

In particolare, i locali nei quali sono situate le apparecchiature utilizzate dal Gestore Accreditato per l'esercizio delle proprie funzioni, sono protetti da un sistema di controllo accessi e da videocamere, che fanno capo ad un servizio di vigilanza costituente un presidio permanente. Solo al personale addetto è concessa l'abilitazione ad entrare nei suddetti locali, e comunque ogni accesso è rigorosamente registrato.

Oltre al controllo fisico, vengono effettuati controlli ed analisi di tipo logico sulle registrazioni effettuate dai vari sistemi (files di log), in modo da verificare che tutti gli eventi verificatesi facciano parte della normale attività del Gestore Accreditato.

Tutti i dati rilevanti (log degli accessi fisici alle aree protette riservate ai sistemi della Posta Elettronica Certificata, i log di tutti i sistemi coinvolti nell'erogazione del servizio, etc..) per il Servizio sono periodicamente salvati su copie di sicurezza, opportunamente conservate per gli eventuali ripristini in caso di guasto e per tutti gli altri casi previsti dalla normativa vigente.

7.3 Emergenze

Cedacri S.p.A. ha predisposto un piano di intervento per affrontare eventuali situazioni di emergenza, includendovi quelle catastrofiche che potrebbero causare l'indisponibilità totale e/o parziale del sito principale del Servizio di Posta Elettronica Certificata.

Cedacri S.p.A., nella sua funzione di Gestore Accreditato, allo scopo di garantire i livelli di servizio come richiesti dal D.P.C.M. 2 novembre 2005 rif.[13], ha dotato la propria infrastruttura tecnologica per l'erogazione del servizio delle seguenti caratteristiche:

- server ridondati con macchine secondarie in standby che subentrano automaticamente nel caso di mancanza di servizio da parte del sistema principale
- gruppi di continuità distinti che servono i due sistemi ridondati e generatore autonomo di elettricità nel caso di mancanza di tensione della rete elettrica
- monitoring esterno continuo dei servizi con allarmi verso la struttura tecnica di gestione per l'adozione di interventi di ripristino immediati
- i sistemi sono protetti da firewalls ridondati che permettono solamente l'accesso per i servizi in modalità sicura come definita dalla normativa tecnica in vigore, e il collegamento per la gestione avviene attraverso connessioni criptate sicure ssh dai singoli indirizzi autorizzati.

8 Condizioni di fornitura del servizio

8.1 Soggetti del servizio

- **Gestore**: soggetto che gestisce domini di Posta Elettronica Certificata con i relativi punti di accesso, ricezione e consegna, definiti dalla normativa vigente in materia.
- **Titolare/Cliente**: soggetto che acquista il servizio dal Gestore affinché sia utilizzato da sé stesso e/o da soggetti afferenti alla propria organizzazione; in quest'ultimo caso il Gestore può demandare al Titolare le attività di registrazione e amministrazione di coloro che utilizzeranno il servizio.
- **Utilizzatore/Utente**: soggetto che utilizza il servizio del Gestore al quale sono rilasciate le credenziali di accesso alla casella di PEC.
- **Mittente**: utilizzatore che si avvale del servizio di PEC del Gestore per la trasmissione di documenti.
- **Destinatario**: utilizzatore che si avvale del servizio PEC del Gestore Cedacri S.p.A. o altri riconosciuti per ricevere documenti.

8.2 Obblighi e responsabilità del Gestore

Cedacri S.p.A. si impegna a fornire i servizi richiesti dal Cliente in osservanza di quanto stabilito dalle vigenti normative, non assumendo alcuna responsabilità al di fuori di quanto in esse espressamente stabilito.

In particolare in qualità di Gestore, Cedacri S.p.A. è tenuta a :

- rispettare i dettami del DM rif.[13];
- informare gli Utenti sulle modalità di accesso al servizio e sui necessari requisiti tecnici;
- rispettare quanto contenuto nel dlgs. 30 giugno 2003, n. 195 rif.[5], in particolare i dettami dell'art.33;
- garantire il funzionamento del servizio;
- fornire al Mittente, facente parte di un dominio PEC gestito da Cedacri S.p.A., la ricevuta di accettazione con i dati di certificazione; nonché fornire la ricevuta di avvenuta consegna contenente i dati di certificazione, se anche il Destinatario fa parte di un dominio da lui gestito;
- comunicare la mancata consegna del messaggio entro le 24 ore successive all'invio;
- utilizzare per l'erogazione del servizio la firma elettronica avanzata ai sensi dell'art. 9, comma 1 D.P.R. 11 febbraio 2005, n. 68 rif.[11];
- apporre riferimenti temporali così come prescritto dalla normativa vigente;
- marcare temporalmente i logs dei messaggi quotidianamente;

- trasmettere dal Mittente al Destinatario il messaggio di posta nella sua integrità, includendolo nella busta di trasporto;
- tenere traccia delle operazioni svolte durante l'erogazione del servizio sul log dei messaggi;
- conservare il log dei messaggi per trenta mesi;
- garantire l'integrità e l'inalterabilità nel tempo suddetto delle informazioni contenute nei logs;
- gestire i messaggi contenenti virus così come disposto dall'art.12, D.P.R.11 febbraio 2005, n. 68 rif.[11];
- predisporre procedure di emergenza che garantiscano il completamento della trasmissione del messaggio ed il rilascio delle ricevute;
- assicurare i minimi SLA previsti dal DM e dalle regole tecniche rif.[13];
- non riassegnare il medesimo indirizzo di posta elettronica certificata a soggetto diverso dal titolare originario.

8.3 Limitazioni di responsabilità e di indennizzo del Gestore

Cedacri S.p.A., salvo il caso di dolo o colpa grave, non incorrerà in responsabilità per danni diretti o indiretti di qualsiasi natura ed entità che dovessero verificarsi al Cliente, e/o a terzi in conseguenza dell'uso e/o del mancato uso del Servizio di Posta Elettronica Certificata anche a fronte di ritardi o interruzioni, o per errori e/o malfunzionamenti dello stesso qualora rientranti nell'ambito dei parametri di indisponibilità indicati nel presente Manuale Operativo ovvero derivanti dall'errata utilizzazione del servizio da parte del Cliente.

Cedacri S.p.A. inoltre, salvo il caso di dolo o colpa grave non sarà gravata da oneri o responsabilità per danni diretti o indiretti di qualsiasi natura ed entità che dovessero verificarsi al Cliente causati da manomissioni o interventi sul servizio o sulle apparecchiature effettuati dal Cliente da parte di terzi non autorizzati da Cedacri S.p.A..

In nessun caso Cedacri S.p.A. sarà responsabile nei confronti del Cliente per i danni costituiti da lucro cessante, perdita di opportunità commerciali o di risparmi, perdita di interesse, perdita di efficienza amministrativa, danni all'immagine o perdita di reputazione commerciale.

Il Cliente, in caso di superamento dei parametri di indisponibilità stabiliti nei livelli di servizio indicati nel presente manuale, avrà diritto ad ottenere, a titolo di risarcimento di tutti i danni diretti/indiretti eventualmente subiti a qualsiasi titolo, il rimborso del prezzo pagato per il Servizio di Posta Elettronica Certificata correlato al periodo di mancata fruizione dello stesso.

Il rimborso non potrà essere richiesto qualora la mancata fruizione sia imputabile al gestore della rete di telecomunicazioni ovvero derivante da caso fortuito, forza maggiore o cause comunque non imputabili a Cedacri S.p.A., quali, a titolo esemplificativo, scioperi, sommosse,

terremoti, atti di terrorismo, tumulti popolari, sabotaggio organizzato, eventi chimici e/o batteriologici, guerra, alluvioni, provvedimenti delle competenti autorità in materia o inadeguatezza delle strutture, dei macchinari hardware e/o dei software utilizzati dal Cliente.

Cedacri S.p.A. si riserva, di poter modificare le modalità di erogazione del servizio di Posta Elettronica Certificata per adeguarlo e renderlo conforme alle disposizioni normative che saranno eventualmente emanate a disciplina dei servizi di Posta Elettronica Certificata.

8.4 Responsabilità del Titolare/Cliente

Il Cliente si assume ogni responsabilità sul contenuto delle comunicazioni inviate attraverso il Servizio di Posta Elettronica Certificata.

Cedacri S.p.A. è esonerata da ogni potere di controllo, di mediazione o di vigilanza sui contenuti dei messaggi inviati dal Cliente e nessuna responsabilità è imputabile a Cedacri S.p.A. riguardo al contenuto illecito o immorale degli stessi, non sussistendo alcun obbligo di cancellazione circa il contenuto dei messaggi in capo a Cedacri S.p.A..

Il Cliente pertanto è tenuto a manlevare Cedacri S.p.A. da ogni pretesa o azione avanzata da soggetti terzi per eventuali violazioni commesse dai Titolari della casella di posta attraverso il Servizio di Posta Elettronica Certificata.

È fatto divieto di utilizzare il servizio di Posta Elettronica Certificata al fine di depositare, inviare, pubblicare, trasmettere e/o condividere applicazioni o documenti informatici che:

- siano in contrasto o violino diritti di proprietà intellettuale, segreti commerciali, marchi, brevetti o altri diritti di proprietà di terzi;
- abbiano contenuti diffamatori, calunniosi o minacciosi;
- contengano materiale pornografico, osceno o comunque contrario alla pubblica morale;
- contengano virus, worm, Trojan Horse o, comunque, altre caratteristiche di contaminazione o distruttive;
- danneggino, violino o tentino di violare il segreto della corrispondenza e il diritto alla riservatezza;
- in ogni caso siano in contrasto alle disposizioni normative e/o regolamentari applicabili.

Il Cliente si obbliga ad informare gli utenti utilizzatori della casella di Posta Elettronica Certificata del divieto di cui al presente articolo, impegnandosi a non utilizzare ed a non far utilizzare il Servizio di Posta Elettronica Certificata dagli stessi con modalità che contrastino i succitati divieti, vigilando sulla loro applicazione.

Cedacri S.p.A. non ha alcun obbligo di sorveglianza sui documenti e sui dati che sono memorizzati, visualizzati o condivisi per mezzo del Servizio di Posta Elettronica Certificata, e, pertanto, non avrà alcun obbligo di monitoraggio o di esame degli stessi.

Cedacri S.p.A. si riserva la facoltà di sospendere l'erogazione del Servizio, ovvero di impedire l'accesso ai documenti e/o ai dati ivi contenuti qualora:

1) venga resa edotta ovvero prenda conoscenza in altro modo della violazione di uno o più divieti sopra indicati, indipendentemente dalla richiesta di cui al numero successivo;
2) venga avanzata espressa richiesta in tal senso da un organo giurisdizionale o amministrativo competente in materia in base alle norme vigenti.

Nelle ipotesi di cui sopra, Cedacri S.p.A. provvederà a comunicare a mezzo e-mail firmata al Cliente/Utente utilizzatore, le motivazioni dell'adozione dei provvedimenti ivi stabiliti, e avrà facoltà di risolvere le prestazioni dei Servizi stessi senza alcun preavviso e senza per questo essere tenuta ad alcun risarcimento e fatta salva ogni altra azione di rivalsa nei confronti del responsabile delle violazioni.

8.5 Obblighi-responsabilità del Titolare

Il Titolare si impegna a:

- consultare e conoscere i contenuti del presente Manuale Operativo;
- fornire al Gestore tutta la documentazione e le informazioni necessarie per una corretta attivazione del servizio;
- informare gli Utenti afferenti la propria organizzazione degli obblighi e responsabilità derivanti dall'utilizzo del servizio di PEC;
- se necessario per la corretta erogazione del servizio dare il consenso all'utilizzo dei dati a norma del d. lgs. rif.[5];
- conservare e far conservare con cura e diligenza dagli Utenti afferenti la propria organizzazione le credenziali di accesso al servizio;
- informare il Gestore di eventuali compromissioni delle credenziali di accesso al servizio.

Alla scadenza del contratto o alla sua risoluzione il Titolare non potrà più accedere al servizio, utilizzare la/le caselle di PEC e visualizzarne il contenuto. Il Titolare si impegna a comunicare tempestivamente agli utenti afferenti la propria organizzazione la scadenza e/o risoluzione del contratto, e ad impedire loro l'accesso e utilizzo del servizio; il Titolare si impegna altresì a sollevare il Gestore da ogni responsabilità derivante dall'impossibilità all'accesso.

8.6 Obblighi e responsabilità dell'utilizzatore

L'Utilizzatore si impegna a:

- consultare e conoscere i contenuti del presente Manuale Operativo;
- attenersi alle modalità di utilizzo del servizio specificate dal Gestore sia nel presente Manuale Operativo sia nelle Istruzioni Operative all'utilizzo del servizio fornite dal Gestore in un documento scaricabile via Internet dal sito web;
- conservare con cura e diligenza le credenziali di accesso al servizio;
- comunicare al Titolare e/o al Gestore l'eventuale compromissione delle credenziali di accesso al servizio.

9 Glossario

9.1 Definizioni/abbreviazioni

AGID	Sostituisce DigitPA
ANTIVIRUS	Il software antivirus è un programma che ricerca all'interno dei dischi di un computer tutti i virus conosciuti, ovvero quei programmi che cercano di prendere il controllo del proprio computer
ASCII	American Standard Code for Information Interchange – E' il formato più comunemente utilizzato per i file di testo in informatica
DigitPA	Agenzia per l'Italia Digitale (ex CNIPA)
BGP	Border Gateway Protocol – Protocollo per lo scambio di informazioni tra Autonomous Systems
CA	Certification Authority – Autorità di certificazione - Certificatore
CDP	CRL Distribution Point – Punto di distribuzione delle CRL
CERTIFICATO DIGITALE	Attestato di corrispondenza tra una chiave pubblica e il soggetto titolare cui essa appartiene, in associazione ad una chiave privata appartenente solo al titolare medesimo
CERTIFICATORE	Entità che certifica la corrispondenza del Titolare alla sua chiave pubblica. E' tenutaria delle chiavi pubbliche ed è obbligata a rendere disponibile una lista aggiornata delle chiavi in vigore e di quelle revocate o sospese
CRL	Certificate Revocation List – Lista dei certificati revocati
DISPOSITIVO DI FIRMA	Supporto elettronico programmabile solo all'origine, utilizzato dal titolare, sul quale viene generata la coppia di chiavi asimmetriche, quella pubblica e quella privata, munito di una passphrase di sblocco
DOWNLOAD	Procedura con la quale vengono scaricati e salvati files da internet
DMZ	DeMilitarized Zone – Insieme di apparecchiature di una rete comprese fra due barriere di firewall
DN	Distinguished Name - Identificatore dell'Utente Titolare – Stringa formattata estesa dei dati anagrafici del Titolare

FIREWALL	Dispositivo hardware/software per la protezione delle reti private
FIRMA ELETTRONICA	In altri termini la firma elettronica è il risultato di una procedura informatica che garantisce l'autenticità e l'integrità di messaggi e documenti scambiati e archiviati con mezzi informatici, al pari di quanto svolto dalla firma autografa per i documenti cartacei
HUB	Apparecchio di connessione tra le reti
HSM	Hardware Security Module – Modulo di sicurezza hardware
HTTP	HyperText Transfer Protocol – Protocollo di trasmissione per reti Internet
HTTPS	Secure HyperText Transfer Protocol - Protocollo sicuro (crittografato) di trasmissione per reti Internet
IPADDRESS	L'indirizzo IP address è un numero di 32 bit che identifica ciascun mittente o destinatario di informazioni che sono spedite in pacchetti attraverso la rete. Viene tipicamente assegnato ai computer
LDAP	Lightweight Directory Access Protocol – Protocollo di accesso ai dati del DS
LDIF	Lightweight Directory Interchange Format – File in formato ASCII usato per scambiare dati e mantenere sincronizzati gli LDAP servers.
LINUX	Linux è un sistema operativo simile allo Unix, scritto per fornire agli utenti di personal computer un sistema gratuito o a basso costo rispetto allo Unix tradizionale
MAIL SERVER	Il mail server è un computer dedicato a far girare le applicazioni che ricevono e-mail in entrata dagli utenti del dominio locale e le girano all'esterno per la spedizione
MULTIPART MIME	formato dei messaggi di posta elettronica, come definito nello standard RFC 2045
NAT	Network Address Translation – Traduzione indirizzi di rete
OPEN SOURCE	Generalmente ci si riferisce a quei programmi il cui codice sorgente è disponibile e gratuito
PASSWORD	La password è una sequenza di caratteri senza spazi usata per verificare che un utente richiedente l'accesso ad un sistema sia realmente quel particolare utente
PEC	Posta Elettronica Certificata

PDF	Portable Document Format, è un formato file che ingloba tutti gli elementi di un documento stampato come fosse un'immagine elettronica che si può navigare, stampare, etc..
PIN	Personal Identification Number – Numero identificativo personale
PIXEL	(picture element): il più piccolo punto che compone la rappresentazione di un'immagine nella memoria di un computer
PHP	(PHP: Hypertext Preprocessor): linguaggio di programmazione interpretato con licenza open source, utilizzato principalmente per la realizzazione di applicazioni web lato server e pagine web dinamiche
PKI	Public Key Infrastructure – Infrastruttura hardware/software per la certificazione
POP3	Post Office Protocol 3 – Protocollo per la ricezione della posta elettronica
ROUTER	Dispositivo hardware/software per l'indirizzamento dei pacchetti di dati; generalmente collega due o più reti
SLA	Service Level Agreement
SHUTDOWN	Parola usata in linguaggio "tecnico" per indicare la chiusura ordinata (non il semplice spegnimento brutale) di un servizio, di un'applicazione software o di un sistema operativo
SMART-CARD	Tessera in plastica, di formato simile al Bancomat, dotata di microchip (apparato elettronico) programmabile solo all'origine, che può contenere informazioni in modo sicuro
SMTP	Simple Mail Transfer Protocol – Protocollo per l'invio e la ricezione della posta elettronica
SQUIRREMAIL	una applicazione web, scritta in linguaggio PHP, che lavorando sulla porta sicura ssl (443) implementa le funzioni di web mail
SSH	Conosciuto come Secure Socket Shell è un'interfaccia comandi Unix ed un protocollo per l'accesso sicuro ai server Unix remoti
SSL/TLS	Secure Socket Layer – Transport Layer Security
STARTUP	Parola usata in linguaggio "tecnico" per indicare l'avvio o la partenza di un servizio, di un'applicazione software o di un sistema operativo
TITOLARE	Soggetto al quale previa identificazione da parte del Gestore, sono rilasciate caselle di Posta Elettronica Certificata

TOKEN	Chiavetta dotata di microchip con software con caratteristiche del tutto simili alla Smart-card
UNIX	Sistema operativo originario dei Laboratori Bell scritto in linguaggio C
URL	Uniform Resource Locator è l'unico indirizzo di un file accessibile via Internet
UTC	Coordinated Universal Time – tempo comune nel mondo
VULNERABILITY ASSESSMENT	Test di controllo sulle vulnerabilità
WEB BROWSER	Interfaccia per il collegamento e la navigazione sulla rete internet
WIZARD	Programma di utilità che guida l'utente nell'installazione di software
XML	Extensible Markup Language, linguaggio flessibile per la scrittura di file/programmi

10 Bibliografia

[1] RFC 1847 – Security Multiparts for MIME: Multipart/Signed and Multipart/Encrypted

[2] RFC 1891 – SMTP Service Extension for Delivery Status Notifications

[3] RFC 1912 – Common DNS Operational and Configuration Errors

[4] RFC 2252 – Lightweight Directory Access Protocol (v3): Attribute Syntax Definitions

[5] RFC 2315 – PKCS#7: Cryptographic Message Syntax Version 1.5

[6] RFC 2633 – S/MIME Version 3 Message Specification

[7] RFC 2660 – The Secure HyperText Transfer Protocol

[8] RFC 2821 – Simple Mail Transfer Protocol

[9] RFC 2822 – Internet Message Format

[10] RFC 2849 – The LDAP Data Interchange Format (LDIF) Technical Specification

[11] RFC 3174 – US Secure Hash Algorithm 1 – SHA1

[12] RFC 3207 – SMTP Service Extension for Secure SMTP over Transport Layer Security

[13] RFC 3280 – Internet X.509 Public Key Infrastructure Certificate and Certificate

[14] Revocation List CRL profile

11 Elenco allegati

- Non sono presenti allegati