Manuale Operativo
Posta Elettronica Certificata
www.sicurezzapostale.it

Nome file	Namirial-ManualeOperativo
Versione	1.2
Emesso il	16/10/2007
Redatto da	Simone Francescangeli
Approvato da	Claudio Gabellini

STORIA DELLE MODIFICHE APPORTATE

Versione	***Descrizione della revisione***	***Data***
1.1	*Prima emissione*	*28/12/2006*
1.2	*Cap. 5.1.3 Sono stati modificati gli scaglioni relativamente alla quantità minima e massima di caselle acquistabili.*	*16/10/2007*
	Cap. 5.1.4 Lo spazio aggiuntivo per casella passa da 50 Mbytes a 100 Mbytes	

INDICE

INDICE DELLE FIGURE

1 – Informazioni di carattere generale

1.1 Obiettivo

Il documento in oggetto rappresenta il **Manuale Operativo della Posta Elettronica Certificata (PEC)** per Namirial S.p.A. e descrive i processi ed i metodi utilizzati dal gestore per la fornitura del servizio di Posta Elettronica Certificata (PEC).

Il manuale operativo è un documento pubblico che tutti possono scaricarsi dal sito del gestore.

1.2 Glossario

Definizione	Descrizione
PEC	Posta Elettronica Certificata
CNIPA	Centro Nazionale per l'Informatica nella Pubblica Amministrazione
Gestore di posta elettronica certificata	E' il soggetto che gestisce uno o più domini di posta elettronica certificata con i relativi punti di accesso, di ricezione e di consegna, titolare della chiave usata per la firma delle ricevute e delle buste e che si interfaccia con altri gestori di posta elettronica certificata per l'interoperabilità con altri titolari;
Titolare	E' il soggetto a cui é assegnata una casella di posta elettronica certificata;
Dominio di posta elettronica certificata	E' un dominio, fully qualified domain name (FQDN), di posta elettronica certificata dedicato alle caselle di posta elettronica certificata.
Indice dei gestori di posta elettronica certificata	E' il sistema, che contiene l'elenco dei domini e dei gestori di posta elettronica certificata, con i relativi certificati corrispondenti alle chiavi usate per la firma delle ricevute, degli avvisi e delle buste, realizzato per mezzo di un server Lightweight Directory Access Protocol, di seguito denominato LDAP, posizionato in un'area raggiungibile dai vari gestori di posta elettronica certificata e che costituisce, inoltre, la struttura tecnica relativa all'elenco pubblico dei gestori di posta elettronica certificata.
Casella di posta elettronica certificata	E' la casella di posta elettronica definita all'interno di un dominio di posta elettronica certificata ed alla quale é associata una funzione che rilascia ricevute di avvenuta consegna al ricevimento di messaggi di posta elettronica certificata;
Marca temporale	evidenza informatica con cui si attribuisce, ad uno o più documenti informatici, un riferimento temporale opponibile ai terzi secondo quanto previsto dal decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 e dal decreto del Presidente del Consiglio dei Ministri 13 gennaio 2004, pubblicato nella Gazzetta Ufficiale n. 98 del 27 aprile 2004.
Riferimento temporale	Informazione contenente la data e l'ora che viene associata ad un messaggio di posta elettronica certificata
Tamper evidence	Sistema per segnalare qualsiasi tentativo di manomissione fisica del

Definizione	Descrizione
	server che possa aver compromesso l'integrità del sistema e/o dei dati in esso contenuti; tipicamente realizzato tramite l'apposizione sulle macchine di sigilli, lucchetti, etichette autoadesive e/o qualsiasi altro mezzo di protezione il cui stato, in caso di accesso non autorizzato, risulti evidentemente compromesso ad un osservatore esterno.
Tamper proof hardware	Sistema di protezione fisica del server allo scopo di prevenire/impedire l'accesso e la manomissione del sistema dati da parte di soggetti non autorizzati.
HTML	HTML (acronimo per HyperText Mark-Up Language) è un linguaggio usato per descrivere i documenti ipertestuali disponibili su Internet. Non è un linguaggio di programmazione, ma un linguaggio di markup, ossia descrive il contenuto, testuale e non, di una pagina web.
MTA	*Mail Transfer Agent*. E' un modulo che ha il compito di effettuare il dispatching dei messaggi di posta elettronica (invio e ricezione)
LDAP	*Lightweight Directory Access Protocol.* E' un protocollo di rete utilizzato per la ricerca e memorizzazione di informazioni su un Directory Server. Una directory server LDAP è un albero di entità costituite da attributi e valori. Un classico utilizzo di un directory server è la memorizzazioni degli account email o degli utenti registrati ad un sito.
SNMP	*Simple Network Management Protocol.* E' un protocollo utilizzato per la gestione ed il monitoring degli apparati di rete
HSM	*Hardware Security Module.* E' un dispositivo hardware per la generazione, la memorizzazione e la protezione sicure.
NTP	Network Time Protocol
LMTP	Local Mail Transport Protocol
OPT-IN	Consenso preventivo esplicito. Riferimenti normativi: direttiva europea sulle comunicazioni elettroniche (direttiva 2002/58/CE), decreto legislativo 30 giugno 2003, n. 196 - Codice in materia di protezione dei dati personali
Secure Socket Layer (SSL)	Protocollo per realizzare comunicazioni cifrate su Internet. Questo protocollo utilizza la crittografia per fornire sicurezza nelle comunicazioni su Internet e consentire alle applicazioni client/server di comunicare in modo tale da prevenire il 'tampering' (manomissione) dei dati, la falsificazione e l'intercettazione. Scopo primario di SSL è fornire sistemi di crittografia per comunicazioni affidabili e riservate sul Web sfruttabili in applicazioni quali, ad esempio, posta elettronica e sistemi di autenticazione.
HTTPS	Con il termine HTTPS ci si riferisce al protocollo HTTP (Hyper Text Transfer Protocol) utilizzato in combinazione con lo strato SSL (Secure Socket Layer).

1.3 Versione del Manuale Operativo e revisioni successive

La versione corrente del documento è riportata sulla prima pagina.

Il presente Manuale può subire variazioni a seguito di modifiche apportate al sistema.

Le modifiche al sistema possono essere dettate da ottimizzazioni, adeguamenti normativi oppure cambiamenti ai processo interni ed esterni di erogazione del servizio di posta certificata.

Il gestore si impegna a mantenere il documento aggiornato e coerente con il sistema installato. Ogni futura modifica al documento verrà verificata ed approvata dai responsabili del servizio di Namirial S.p.A. e dagli organi competenti (CNIPA).

1.4 Indirizzo web del gestore dal quale scaricare il manuale

Il presente manuale è pubblicato sul sito web http://www.sicurezzapostale.it all'indirizzo http://www.sicurezzapostale.it/manualeoperativo.pdf.

Namirial S.p.A. si impegna a pubblicare sul sito la versione aggiornata del manuale operativo.

1.5 Tabella di corrispondenza

Riportiamo qui di seguito la tabella di corrispondenza tra la Circolare CNIPA n. 49 del 24 novembre 2005 ed il presente manuale.

Circolare CNIPA/CR/49 del 24/11/2005	Manuale Operativo
2.1 - a: dati identificativi del gestore	2.1
2.1 - b: indicazione del responsabile del manuale	2.3
2.1 - c: riferimenti normativi necessari per la verifica dei contenuti	3
2.1 - d: indirizzo del sito web del gestore ove il manuale è pubblicato e scaricabile – punto d circolare	1.4
2.1 - e: indicazione delle procedure nonchè degli standard tecnologici e di sicurezza utilizzati dal gestore nell'erogazione del servizio	7
2.1 - f: definizioni, abbreviazioni e termini tecnici	4.2
2.1 - g: descrizione sintetica del servizio offerto	5
2.1 - h: descrizione delle modalità di reperimento e di presentazione delle informazioni presenti nei log dei messaggi	5.6
2.1 - i: indicazione del contenuto e delle modalità dell'offerta da parte del gestore	5.1
2.1 - j: indicazione delle modalità di accesso al servizio	5.4

Circolare CNIPA/CR/49 del 24/11/2005	Manuale Operativo
2.1 - k: indicazione del livelli di servizio e dei relativi indicatori di qualità di cui all'art. 12 del decreto del Ministero per l'Innovazione e le Tecnologie 2 novembre 2005	5.11
2.1 - l: indicazione delle condizioni di fornitura del servizio	5.1.5
2.1 - m: indicazione delle modalità di protezione dei dati dei titolari	9
2.1 - n: indicazione degli obblighi e delle responsabilità che ne discendono, delle esclusioni e delle limitazioni, in sede di indennizzo, relative ai soggetti previsti all'art. 2 del DPR n.68/2005	8

2 – Il gestore

Il servizio di Posta Elettronica Certificata viene erogato da Namirial S.p.A. della quale riportiamo nel seguito le informazioni identificative ed una descrizione sintetica delle attività svolte e dei principali settori nei quali opera.

2.1 Dati identificativi

Di seguito vengono riportati i dati identificativi del gestore.

Dati identificativi del gestore	
Ragione Sociale:	Namirial S.p.A.
Sede Legale:	VIA CADUTI SUL LAVORO, 4 60019 - SENIGALLIA (AN) TEL: 071.63494 FAX: 071.60910
Sede di erogazione del servizio:	VIA CADUTI SUL LAVORO, 4 60019 - SENIGALLIA (AN) TEL: 071.63494 FAX: 071.60910
Sedi secondarie (utilizzata per la conservazione delle copie di sicurezza dei dati)	VIA VARESE, 15 21013 GALLARATE (VA)
Partita IVA:	IT02046570426
Iscrizione registro delle imprese:	Ancona
REA:	02046570426
Capitale sociale:	1.000.000 € I.V.
Sito web del servizio:	http://www.sicurezzapostale.it
Sito web del gestore:	http://www.namirial.com
Email del servizio:	info@sicurezzapostale.it
Email del gestore:	info@namirial.com

2.2 Descrizione sintetica di Namirial S.p.A.

Namirial S.p.A. è una società di informatica e web engineering che ha trovato una propria specifica collocazione all'interno del settore dell' I.T. orientando la propria produzione di software gestionale verso le nuove e sempre più manifeste esigenze di adeguamento, della Piccola e Media Impresa italiana, ai nuovi scenari economici ormai "globalizzati", fortemente competitivi e tecnologicizzati. Inoltre, in uno scenario produttivo come quello italiano, caratterizzato per circa il 98% da piccole realtà imprenditoriali che di norma non sono in grado che parzialmente di dotarsi di proprie strutture organizzative, contabili e fiscali, si e' ritenuto essenziale sviluppare e fornire il Professionista, figura centrale nelle scelte decisionali di queste imprese, di quelle dotazioni tecnico informatiche e di tutti i servizi necessari per colmare tali lacune in maniera decisamente innovativa.

La "mission" aziendale e' dunque di mettere a disposizione di questa parte consistente di operatori economici una struttura di produzione software e di competence in grado di offrire, con rapidità ed efficacia, analisi accurate dei problemi gestionali, avanzate soluzioni utilizzabili in ambienti Internet/Intranet , possibilità di integrare efficacemente preesistenti sistemi informatici con le nuove tecnologie web.

La società ha sede in una moderna struttura di oltre duemila metri quadrati, dove sono impiegati un centinaio di specialisti con una grande prevalenza di laureati in discipline scientifiche e tecnologiche (informatica, fisica, matematica, ecc.). All'interno della azienda è operativo un' **Internet Data Center** dotato di tutti i sistemi di sicurezza necessari all'inviolabilità della struttura ed in grado di supportare gli utenti anche per quanto concerne eventuali necessità di hosting, housing e colocation server.

Diverse sono le aree di sviluppo di Namiral S.p.A., tra queste:

- **Servizi e software gestionali**. Oltre 15.000 utenti, fra Professionisti e Centri Elaborazioni Dati, sono utenti diretti o indiretti di servizi gestionali appositamente progettati e realizzati da Namirial.
- **Piattaforme web per la erogazione di servizi di consultazione on line di Banche Dati:** circa 6.500 Professionisti possono consultare comodamente dal loro Studio le banche dati essenziali all'esercizio del loro lavoro quotidiano: camerali; catastali; fiscali; del lavoro; ecc..
- **Centri di Assistenza Fiscale.** Attualmente quindici C.A.F. (Centri di Assistenza Fiscale) sincronizzano le loro procedure fiscali e gestionali (elaborazione dei modelli 730,ICI,ISEE, ecc.) delle numerosissime sedi territoriali utilizzando internet e connettendosi in maniera semplice ed assolutamente controllata con server centrali posti in rete internet/intranet su architettura Namirial per una piena governance della/e strutture di controllo (circa 20.000 applicazioni fiscali operano nei tanti uffici CAF).
- **Istituzioni finanziarie**. Diverse banche di interesse nazionale adottano soluzioni web di Namirial per il servizio di pagamento delle deleghe bancarie F24 on line dei propri utenti.
- **Servizi Fiscali on line**. Circa 50.000 cittadini italiani ogni hanno effettuano la propria dichiarazione dei redditi con i programmi messi a disposizione da Namirial e distribuiti dal web site **www.taxonline.it**.

Con queste specificità Namirial S.p.A. è oggi una realtà imprenditoriale di rilievo nel panorama produttivo nazionale ed è tra le più accreditate e competitive aziende fornitrici di piattaforme

gestionali per strutture aziendali e Professionisti che hanno necessità di operare sul territorio nazionale ed internazionale (anche in modalità molto distribuita) con propri punti operativi (sedi, filiali, basi, ecc.) governati e governabili da strutture gerarchicamente definite e pianificate.

Nell'ambito di queste attività, ed in particolare di quelle rivolte specificamente ai Professionisti ed alle imprese Namirial propone una propria soluzione di Posta Elettronica Certificata, caratterizzata da una attenta proposizione tecnico/informativa, continua e sicura, affinché la PEC possa diventare nel breve periodo uno strumento di grande rilevanza nelle attività dell'impresa e più in generale nella società civile italiana.

2.3 Responsabile del Manuale Operativo

Il responsabile della stesura e del mantenimento del presente manuale operativo è:

Simone Francescangeli

Il responsabile può essere contattato ai recapiti

Tel: 071.63494

email: info@namirial.com

indirizzo: VIA CADUTI SUL LAVORO, 4 - 60019 SENIGALLIA (AN)

I responsabili della verifica ed approvazione del documento sono riportati sulla prima pagina.

2.4 Come contattare il gestore

Oltre al riferimento al precedente paragrafo, il cliente può contattare Namirial S.p.A. ai riferimenti sotto riportati.

Help desk ed assistenza al cliente

Per ottenere informazioni sul servizio e per ricevere assistenza in caso di malfunzionamenti è possibile mettersi in contatto con il gestore via telefono, email o via web.

Telefono: 071.63494

email: assistenzatecnica@sicurezzapostale.it

web: www.sicurezzapostale.it

Informazioni commerciali

Per ricevere informazioni commerciali sull'offerta di Namirial S.p.A. è possibile mettersi in contatto con il gestore via telefono, email o via web.

Telefono: 071.63494

email: commerciale@sicurezzapostale.it

web: www.sicurezzapostale.it

2.5 Certificazione ISO 9001

Namirial S.p.A. si impegna ad ottenere la certificazione UNI EN ISO 9001:2000 del proprio sistema di qualità per quanto concerne i processi e le procedure di erogazione del servizio di posta elettronica certificata.

Namirial S.p.A. Si impegna a consegnare al CNIPA copia della certificazione rispettando le tempistiche previste dalla normativa.

3 – Riferimenti normativi

- Decreto del Presidente della Repubblica 28 dicembre 2000 n. 445.
- Decreto Legislativo 30 giugno 2003 n. 193, "Codice in materia di protezione dei dati personali".
- Decreto del Presidente della Repubblica del 11 febbraio 2005 n. 68.
- Decreto Legislativo del 7 marzo 2005 n. 82 "Codice dell'Amministrazione Digitale" (CAD).
- Decreto Ministeriale del 2 novembre 2005 e successive note integrative, "Regole Tecniche del servizio di trasmissione dei documenti informatici tramite Posta Elettronica Certificata".
- Circolare CNIPA/CR/49 del 24/11/2005 , "Modalità di presentazione della domanda di accreditamento nell'elenco pubblico dei Gestori di PEC".
- circolare CNIPA n.51 del 7 dicembre 2006: "Espletamento della vigilanza e del controllo sulle attività esercitate dagli iscritti nell'elenco dei gestori di posta elettronica certificata (PEC) di cui all'art. 14 del DPR 11 febbraio 2005, n.68.

4 – Posta Elettronica Certificata: informazioni generali

4.1 Introduzione

La Posta Elettronica Certificata (PEC) è un sistema di posta elettronica nel quale al mittente viene fornita, in formato elettronico, la prova legale dell'invio e della consegna di documenti informatici.

La PEC è nata per sostituire, attraverso i moderni mezzi di comunicazione, la **Raccomandata postale con ricevuta di ritorno**, o raccomandata AR. Così come avviene per la raccomandata AR, al mittente viene inviata una ricevuta che attesta la consegna al destinatario del proprio messaggio.

I messaggi di PEC possono contenere qualsiasi tipologia di informazione ed allegato.

La comunicazione viene realizzata attraverso una serie di messaggi, ricevute ed avvisi che vengono inviati:

- all'utente da parte dei server di posta certificata
- tra i diversi server di posta certificata.

Ogni messaggio, avviso o ricevuta viene marcato con un riferimento temporale in modo da certificare in modo esatto gli istanti in cui le comunicazioni sono avvenute.

Per garantire la legalità e la correttezza del sistema, il CNIPA ha istituito un **Indice Pubblico dei Gestori di Posta Certificata (IGPEC)**. Si tratta di un elenco di enti pubblici o aziende private che, una volta ottenuto l'accreditamento da parte di una commissione esaminatrice del CNIPA, possono svolgere il proprio ruolo di Gestore, fornire all'esterno le caselle di PEC ed erogare, più in generale, il servizio.

Tra i compiti di un Gestore di PEC vi è anche quello di conservare, per un periodo di 30 mesi, i LOG del sistema che tracciano le comunicazioni avvenute all'interno del proprio sistema. Tali LOG, infatti, hanno la stessa validità legale delle ricevute e possono essere richiesti dagli utenti finali in qualsiasi momento.

4.2 Definizioni

Di seguito vengono definiti i concetti principali di un sistema PEC, così come riportato nelle Regole Tecniche del servizio (DM 2/11/2005).

PUNTO DI ACCESSO: il sistema che fornisce i servizi di accesso per l'invio e la lettura di messaggi di posta elettronica certificata, nonché i servizi di identificazione ed accesso dell'utente, di verifica della presenza di virus informatici all'interno del messaggio, di emissione della ricevuta di accettazione e di imbustamento del messaggio originale nella busta di trasporto;

PUNTO DI RICEZIONE: il sistema che riceve il messaggio all'interno di un dominio di posta ettronica certificata, effettua i controlli sulla provenienza e sulla correttezza del messaggio ed emette la ricevuta di presa in carico, imbusta i messaggi errati in una busta di anomalia e verifica la presenza di virus informatici all'interno dei messaggi di posta ordinaria e delle buste di trasporto;

PUNTO DI CONSEGNA: il sistema che compie la consegna del messaggio nella casella di posta elettronica certificata del titolare destinatario, verifica la provenienza e la correttezza del messaggio ed emette, a seconda dei casi, la ricevuta di avvenuta consegna o l'avviso di mancata consegna;

FIRMA DEL GESTORE DI POSTA ELETTRONICA CERTIFICATA: la firma elettronica avanzata, basata su un sistema di chiavi asimmetriche, che consente di rendere manifesta la provenienza e di assicurare l'integrità e l'autenticità dei messaggi del sistema di posta elettronica certificata, generata attraverso una procedura informatica che garantisce la connessione univoca al gestore e la sua univoca identificazione, creata automaticamente con mezzi che garantiscano il controllo esclusivo da parte del gestore.

RICEVUTA DI ACCETTAZIONE: la ricevuta, sottoscritta con la firma del gestore di posta elettronica certificata del mittente, contenente i dati di certificazione, rilasciata al mittente dal punto di accesso a fronte dell'invio di un messaggio di posta elettronica certificata;

AVVISO DI NON ACCETTAZIONE: l'avviso, sottoscritto con la firma del gestore di posta elettronica certificata del mittente, che viene emesso quando il gestore mittente é impossibilitato ad accettare il messaggio in ingresso, recante la motivazione per cui non é possibile accettare il messaggio e l'esplicitazione che il messaggio non potrà essere consegnato al destinatario;

RICEVUTA DI PRESA IN CARICO: la ricevuta, sottoscritta con la firma del gestore di posta elettronica certificata del destinatario, emessa dal punto di ricezione nei confronti del gestore di posta elettronica certificata mittente per attestare l'avvenuta presa in carico del messaggio da parte del sistema di posta elettronica certificata di destinazione, recante i dati di certificazione per consentirne l'associazione con il messaggio a cui si riferisce;

RICEVUTA DI AVVENUTA CONSEGNA: la ricevuta, sottoscritta con la firma del gestore di posta elettronica certificata del destinatario, emessa dal punto di consegna al mittente nel momento in cui il messaggio é inserito nella casella di posta elettronica certificata del destinatario;

RICEVUTA COMPLETA DI AVVENUTA CONSEGNA: la ricevuta nella quale sono contenuti i dati di certificazione ed il messaggio originale;

RICEVUTA BREVE DI AVVENUTA CONSEGNA: la ricevuta nella quale sono contenuti i dati di certificazione ed un estratto del messaggio originale;

RICEVUTA SINTETICA DI AVVENUTA CONSEGNA: la ricevuta che contiene i dati di certificazione;

AVVISO DI MANCATA CONSEGNA: l'avviso, emesso dal sistema, per indicare l'anomalia al mittente del messaggio originale nel caso in cui il gestore di posta elettronica certificata sia impossibilitato a consegnare il messaggio nella casella di posta elettronica certificata del destinatario;

MESSAGGIO ORIGINALE: il messaggio inviato da un utente di posta elettronica certificata prima del suo arrivo al punto di accesso e consegnato al titolare destinatario per mezzo di una busta di trasporto che lo contiene;

BUSTA DI TRASPORTO: la busta creata dal punto di accesso e sottoscritta con la firma del gestore di posta elettronica certificata mittente, all'interno della quale sono inseriti il messaggio originale inviato dall'utente di posta elettronica certificata ed i relativi dati di certificazione;

BUSTA DI ANOMALIA: la busta, sottoscritta con la firma del gestore di posta elettronica certificata del destinatario, nella quale é inserito un messaggio errato ovvero non di posta elettronica certificata e consegnata ad un titolare, per evidenziare al destinatario detta anomalia;

DATI DI CERTIFICAZIONE: i dati, quali ad esempio data ed ora di invio, mittente, destinatario, oggetto, identificativo del messaggio, che descrivono l'invio del messaggio originale e sono certificati dal gestore di posta elettronica certificata del mittente; tali dati sono inseriti nelle ricevute e sono trasferiti al titolare destinatario insieme al messaggio originale per mezzo di una busta di trasporto;

GESTORE DI POSTA ELETTRONICA CERTIFICATA: il soggetto che gestisce uno o più domini di posta elettronica certificata con i relativi punti di accesso, di ricezione e di consegna, titolare della chiave usata per la firma delle ricevute e delle buste e che si interfaccia con altri gestori di posta elettronica certificata per l'interoperabilità con altri titolari;

TITOLARE: il soggetto a cui é assegnata una casella di posta elettronica certificata;

DOMINIO DI POSTA ELETTRONICA CERTIFICATA: dominio di posta elettronica certificata che contiene unicamente caselle di posta elettronica certificata;

INDICE DEI GESTORI DI POSTA ELETTRONICA CERTIFICATA: il sistema, che contiene l'elenco dei domini e dei gestori di posta elettronica certificata, con i relativi certificati corrispondenti alle chiavi usate per la firma delle ricevute, degli avvisi e delle buste, realizzato per mezzo di un server Lightweight Directory Access Protocol, di seguito denominato LDAP, posizionato in un'area raggiungibile dai vari gestori di posta elettronica certificata e che costituisce, inoltre, la struttura tecnica relativa all'elenco pubblico dei gestori di posta elettronica certificata.

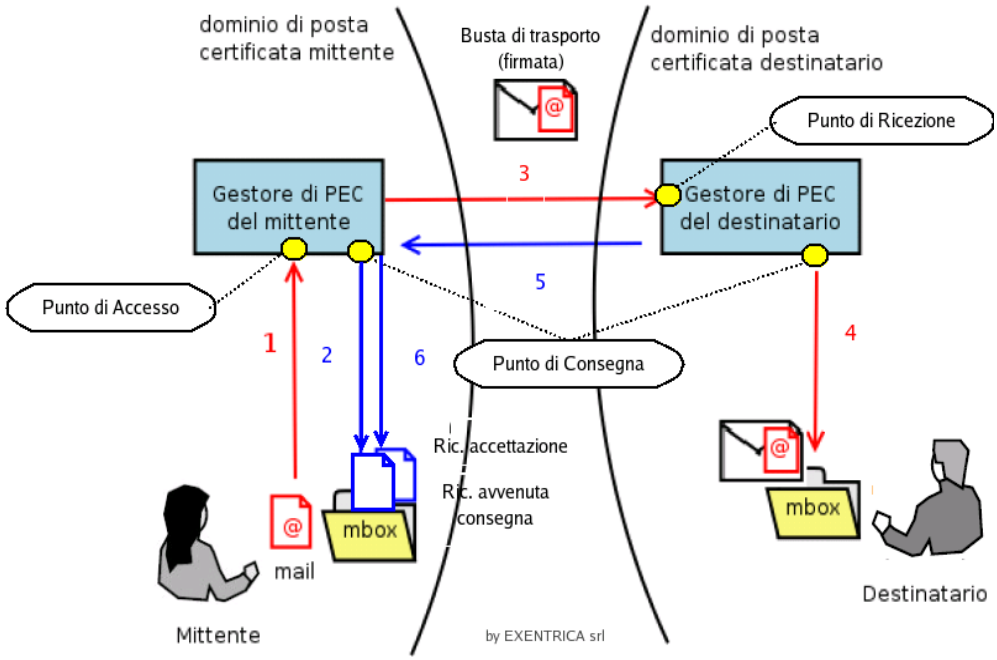
CASELLA DI POSTA ELETTRONICA CERTIFICATA: la casella di posta elettronica posta all'interno di un dominio di posta elettronica certificata ed alla quale é associata una funzione che rilascia ricevute di avvenuta consegna al ricevimento di messaggi di posta elettronica certificata;

MARCA TEMPORALE: un'evidenza informatica con cui si attribuisce, ad uno o più documenti informatici, un riferimento temporale opponibile ai terzi secondo quanto previsto dal decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 e dal decreto del Presidente del Consiglio dei Ministri 13 gennaio 2004, pubblicato nella Gazzetta Ufficiale n. 98 del 27 aprile 2004.

4.3 Posta Elettronica Certificata: il funzionamento

Per descrivere a grandi linee il funzionamento di un sistema di Posta Elettronica Certificata usiamo il disegno riportato nella figura seguente.

Figura 1 - Funzionamento di un sistema di PEC



Nello schema sono visualizzati 2 utenti ognuno dei quali appartiene ad un proprio dominio di posta elettronica certificata: il primo deve spedire un messaggio di PEC al secondo.

1. Il messaggio arriva al **punto di accesso** nel sistema PEC del gestore mittente
2. Il gestore del mittente, dopo aver verificato che il messaggio sia correttamente formato, invia una **ricevuta di accettazione** al mittente.
3. il messaggio viene racchiuso in un documento di trasporto e viene firmato attraverso un apposito device
4. Il gestore PEC del destinatario raccoglie il messaggio **nel punto di ricezione**, ne verifica l'attendibilità della firma e quindi controlla che non sia stato alterato durante il tragitto e lo consegna nella casella del destinatario (**punto di consegna**).
5. Il gestore PEC del destinatario, non appena consegnato il messaggio, crea una **ricevuta di avvenuta consegna**, la firma e la invia al mittente.
6. Il gestore PEC del mittente raccoglie la ricevuta di avvenuta consegna, ne verifica correttezza ed integrità e la consegna al proprio utente (mittente) attraverso il **punto di consegna**.

La ricevuta di avvenuta consegna può essere

- **completa**: oltre ai dati di certificazione contiene, come attachment, il messaggio originale completo di eventuali allegati;
- **breve**: oltre ai dati di certificazione contiene, come attachment, il messaggio originale nel quale gli allegati vengono sostituiti dallo loro codifica hash;
- **sintetica**: contiene solamente i dati di certificazione senza il messaggio originale.

La ricevuta completa è la ricevuta di default, quella breve ha lo scopo di minimizzare l'occupazione di memoria e la dimensione delle email in transito mentre quella sintetica è stata introdotta per poter introdurre procedure automatiche di invio e ricezione di messaggi di PEC.

4.3.1 Altri dettagli e casi particolari

In realtà la comunicazione sopra descritta è leggermente più complicata dallo scambio di una serie di ricevute ed avvisi tra l'utente e server e tra server e server, che servono a garantire la correttezza della trasmissione, a rilevare la presenza di anomalie o a gestire casi particolari .

Presa in carico

Per mantenere la tracciabilità dei messaggi i gestori di PEC, alla ricezione di un messaggio di PEC proveniente da un dominio certificato esterno, inviano una **ricevuta di presa in carico** al gestore del dominio mittente.

Messaggi inviati a indirizzi email non certificati

Ogni messaggio di PEC a indirizzi di email non certificati arrivano a destinazione imbustati all'interno di un messaggio di trasporto.

Messaggi provenienti da indirizzi email non certificati

Ogni Gestore di PEC ha la possibilità di scegliere come gestire i messaggi provenienti da indirizzi email non certificati. Tali messaggi possono infatti essere scartati oppure possono essere consegnati a destinazione racchiusi all'interno di un messaggio di anomalia.

Messaggio formalmente non corretto

Il gestore invia al proprio utente (mittente) un **avviso di mancata accettazione per vincoli formali** quando rileva delle malformazioni e non aderenze alla normativa all'interno del messaggio inviato dal proprio utente (mittente)

Presenza virus

Un virus contenuto nel testo o negli allegati di una mail certificata può essere rilevato dal sistema di PEC del mittente o da quello del destinatario.

Nel caso in cui sia il gestore del mittente a rilevare il virus, viene inviato al mittente un **avviso di mancata consegna per virus**.

Nel caso in cui sia il gestore del destinatario a rilevare il virus (al punto di ricezione), viene inviato un **avviso di rilevazione virus**. Quest'ultimo, da parte sua, quando riceve un avviso di rilevazione virus provvede a consegnare al proprio utente (mittente del messaggio originale) un **avviso di mancata consegna per virus**.

I messaggi contenenti i virus vengono conservati dal gestore per un periodo non inferiore a 30 mesi.

Ritardi di consegna

Un caso particolare si ha quando per motivi non meglio specificati il messaggio non viene consegnato a destinazione entro le 12 e 24 ore successive al suo invio. Per fornire agli utenti del servizio tutte le informazioni utili a conoscere l'esito delle proprie spedizioni i gestori di PEC si comportano nel seguente modo:

Trascorse 12 ore dalla spedizione durante le quali non si è avuta notizia del messaggio (cioè non è arrivata la ricevuta di presa in carico o di avvenuta consegna), il gestore del mittente consegna al proprio utente un **primo avviso di mancata consegna per superamento limiti di tempo**. Nell'avviso viene fatto presente che "*il messaggio potrebbe non arrivare a destinazione"*.

Trascorse altre 12 ore senza che vengano consegnate la ricevuta di presa in carico e di avvenuta consegna, il gestore del mittente consegna al proprio utente un **secondo avviso di mancata consegna per superamento limiti di tempo**. Nell'avviso viene avvertito il mittente che *"la spedizione non è andata a buon fine"*.

5 – Il servizio di Posta Elettronica certificata di Namirial S.p.A.

Il presente capitolo delinea il servizio di posta elettronica certificata di Namirial S.p.A. e ne descrive le caratteristiche principali.

5.1 Caratteristiche dell'offerta

L'offerta di Namirial S.p.A. è rivolta a privati, professionisti, enti pubblici ed aziende su tutto il territorio nazionale.

Il gestore si riserva il diritto di modificare nel futuro (ed in ottica migliorativa) le caratteristiche dell'offerta di seguito riportata; per prendere visione delle condizioni aggiornate si rimanda al sito www.sicurezzapostale.it.

Il servizio viene fornito su dominio **SicurezzaPostale.it** oppure su dominio registrato e mantenuto appositamente per il cliente. Ogni cliente può avere a disposizione un numero illimitato di caselle di posta elettronica certificata.

Le caselle hanno una capacità di **100 Mbytes**. Tale regolamentazione è stata istituita al fine di utilizzare al meglio lo spazio disponibile sulle apparecchiature. Si ricorda che, in base alla normativa, i messaggi si considerano ricevuti quando sono recapitati nella casella di ricezione e non quando il cliente li scarica. E' evidente che raggiunto il limite di capienza, gli ulteriori messaggi vengono rifiutati. Per questo è consigliato scaricare regolarmente la casella di ricezione.

I messaggi **ricevuti** non generano alcun addebito.

I messaggi **inviati** sono soggetti a canone in base alle offerte descritte di seguito.

5.1.1 SicurezzaPostale Smart

E' l'offerta "entry-level" e prevede la fornitura di una casella di posta elettronica certificata su dominio **sicurezzapostale.it.** La casella è accessibile via web (HTTPS) tramite WebMail oppure attraverso i più comuni client di posta (SMTP-S, POP3-S, IMAP-S) quali Outlook Express, Outlook, Eudora, Thunderbird, etc.

Per questo tipo di offerta è previsto il pagamento di un canone annuale senza limitazioni sul traffico effettuato.

5.1.2 SicurezzaPostale Business

E' una soluzione ideata per privati, professionisti e piccole e medie imprese e comprende i seguenti servizi:

- Registrazione e mantenimento di un dominio personale, aziendale o istituzionale (opzionale)
- Attivazione di un dominio certificato di terzo livello sul dominio personale, aziendale o istituzionale
- Caselle SicurezzaPostale (PEC) sul dominio certificato creato senza limitazioni di traffico.

Per questo tipo di offerta sono previsti i seguenti pagamenti:

- canone annuale per la registrazione e mantenimento del dominio personale, aziendale o istituzionale
- quota una tantum per l'attivazione del dominio certificato di terzo livello
- canone annuale per le caselle PEC sul dominio certificato

5.1.3 SicurezzaPostale Business ADV

Si tratta di una soluzione ideale per organizzazioni strutturate ed aziende di una certa dimensione e comprende i seguenti servizi:

- Registrazione e mantenimento di un dominio personale, aziendale o istituzionale (opzionale)
- Attivazione di un dominio certificato di terzo livello sul dominio personale, aziendale o istituzionale
- Da un minimo di 20 ad un massimo di 50 caselle SicurezzaPostale (PEC) sul dominio certificato creato senza limitazioni di traffico
- Oltre 50 caselle SicurezzaPostale (PEC) sul dominio certificato creato senza limitazioni di traffico

Per questo tipo di offerta sono previsti i seguenti pagamenti:

- canone annuale per la registrazione e mantenimento del dominio personale, aziendale o istituzionale
- quota una tantum per l'attivazione del dominio certificato di terzo livello
- canone annuale per le caselle PEC sul dominio certificato (traffico compreso); il canone dipende dal numero di caselle acquistate (tra 20 e 50, oltre 50).

5.1.4 Servizi aggiuntivi

Namirial S.p.A. mette a disposizione dei propri clienti una serie di servizi aggiuntivi e personalizzazioni:

- Spazio aggiuntivo di 100 Mbytes sulla casella SicurezzaPostale
- Personalizzazione grafica della web mail
- Pannello di controllo per autogestione proprie caselle (solo per offerta SicurezzaPostale Business ADV).

5.1.5 Dettagli offerta, condizioni fornitura e tariffe applicate

Per i dettagli sui costi dei vari servizio sopra descritti e sulle modalità di sottoscrizione si rimanda al sito www.sicurezzapostale.it.

5.1.6 Attivazione del servizio tramite partner commerciale

Namirial S.p.A. si avvale anche di partner commerciali per la diffusione del proprio servizio PEC. Il partner commerciale reperisce le informazioni necessarie per identificare il cliente che ha richiesto il servizio con i relativi requisiti in termini di numero caselle, spazio totale, eventuali servizi opzionali, etc.

Una volta acquisite tali informazioni e verificatane la correttezza e la completezza, il cliente provvede a stipulare un contratto direttamente con il gestore del servizio. Tutta la documentazione contrattuale contenente le condizioni del servizio acquistato è predisposta infatti, da Namirial S.p.A. che rimane comunque la responsabile della qualità del servizio nei confronti del cliente finale.

5.2 Nomi dei domini e delle caselle

I nomi dei domini e delle caselle potranno essere indicati dal cliente ma il gestore si riserva il diritto di rifiutarli nel caso in cui li ritenga offensivi, irrispettosi o lesivi nei confronti di terzi.

5.3 Attivazione

Nella figura seguente riportiamo uno schema del flusso di attivazione di una casella di posta certificata.

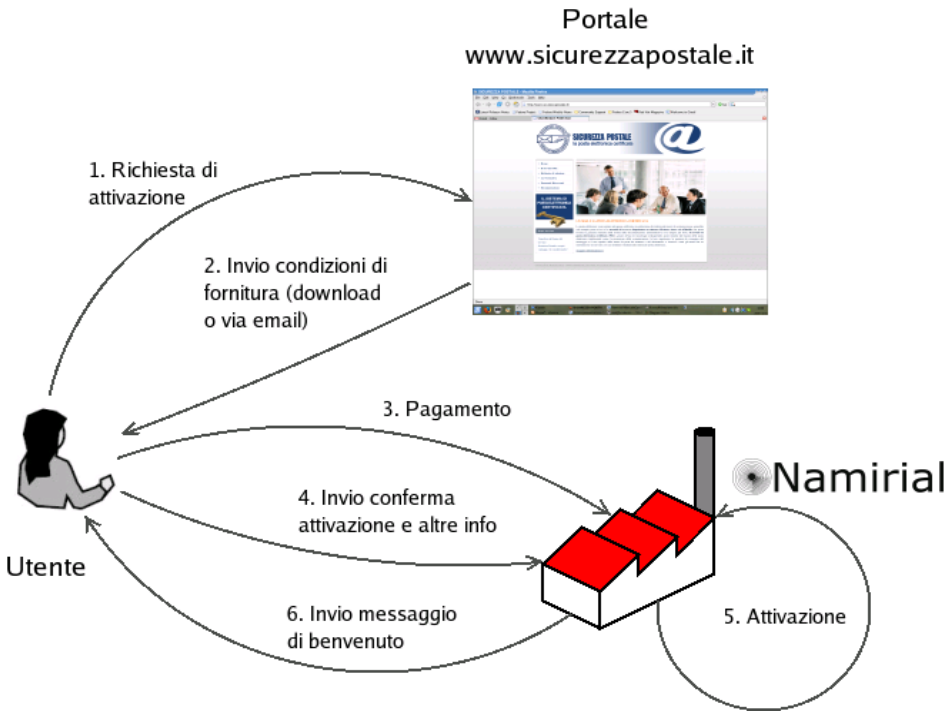


Figura 2 - Attivazione account di PEC

Passo 1: richiesta di attivazione

Per attivare il servizio il cliente deve compilare il form di registrazione presente sul sito www.sicurezzapostale.it. Nel form deve riportare i propri dati anagrafici (che dipendono dal fatto che il cliente sia un privato, un'azienda o un'ente):

- Nome
- Cognome
- Ragione Sociale
- Indirizzo
- Città
- CAP
- Nazione
- Codice fiscale o partita IVA
- email valida

Il cliente deve inoltre dare il proprio consenso affinché Namirial S.p.A. possa entrare in possesso e gestire i suoi dati personali.

Passo 2: download condizioni fornitura

Il gestore invia per email (casella tradizionale) le condizioni del servizio che possono anche essere scaricate dal sito del gestore.

Passo 3: pagamento

Il cliente effettua il pagamento di quanto ordinato secondo le modalità riportate sul sito del gestore. Il gestore invia una email al cliente nella quale indica che il pagamento è avvenuto correttamente.

Passo 4: invio conferma di attivazione ed informazioni aggiuntive

Il cliente, dopo aver firmato e compilato le condizioni di fornitura, le invia al gestore insieme alla fotocopia di un documento di identità valido. L'invio deve avvenire via fax o via raccomandata con ricevuta di ritorno.

Passo 5: attivazione

Il gestore, dopo aver verificato la correttezza delle informazioni inviate dal cliente, attiva la casella ed i domini richiesti.

Passo 6: messaggio di benvenuto

Il gestore invia al cliente una email di benvenuto nella quale vengono forniti tutti i dettagli del servizio erogato. In particolare vengono inviati i parametri di accesso al sistema: login, password server stmp, server pop, indirizzo web mail, etc.

5.4 Accesso al servizio

La casella di PEC non è altro che una casella di posta che può essere utilizzata sia attraverso i i più diffusi client di posta, che attraverso un sistema di webmail.

5.4.1 Accesso attraverso i client di posta

Il titolare può accedere al sistema attraverso i più comuni client di posta quali Thunderbird, Eudora, Outlook Express, Outlook, etc.

All'interno del messaggio di benvenuto vengono inviati al titolare della casella, tutti i parametri di accesso al sistema attraverso i client di posta. In particolare:

- login di accesso
- password
- SMTP server con indicazione della porta di accesso attraverso canale sicuro (SMTP/S)
- POP server con indicazione della porta di accesso attraverso canale sicuro (POP/S).

Inoltre sul sito www.sicurezzapostale.it sono pubblicate le informazioni necessarie a configurare i più comuni prodotti del mercato.

Una volta configurato il proprio client di posta, il titolare utilizza la casella di PEC come una casella di posta non certificata. Le uniche differenze riguardano i formati dei messaggi e delle ricevute che vengono recapitate.

Per ogni messaggio inviato e consegnato senza problemi, il mittente riceve:

- una **ricevuta di accettazione** proveniente dal proprio sistema di PEC; la ricevuta di accettazione è un messaggio di posta con subject “Accettazione:” seguito dal subject del messaggio originale inviato e con un testo che indica che il messaggio in partenza è corretto ed è stato accettato dal sistema.
- una **ricevuta di avvenuta consegna** dal sistema PEC del destinatario; la ricevuta di avvenuta consegna è un messaggio di posta con subject “Avvenuta consegna:” seguito dal subject originale e con un testo che indica che il messaggio è giunto a destinazione. La ricevuta contiene, in allegato, un file xml con i dati di certificazione ed il messaggio originale, completo di allegati.

Il destinatario riceve, da parte sua:

- il **documento di trasporto** cioè un messaggio di posta che ha come subject “Posta certificata:” seguito dal subject del messaggio originale e con testo l'indicazione che si tratta di un messaggio di PEC. Il messaggio contiene, in allegato, la mail originale completa degli eventuali allegati.

Casi particolari vengono gestiti attraverso altri avvisi o ricevute che hanno in comune il fatto di avere un subject con un prefisso particolare seguito dal subject originale ed un testo che spiega la

tipologia di avviso. Alcuni di queste ricevute/avvisi sono: avviso di mancata consegna, avviso di non accettazione per virus, avviso di mancata consegna per superamento tempi massimi, etc.

5.4.2 Accesso tramite webmail

Il titolare della casella di PEC ha la possibilità di accedervi attraverso un comune browser Internet:

1. Utilizzando un browser internet, l'utente si collega all'indirizzo specifico che gli è stato fornito dal gestore (HTTPS).
2. A tale indirizzo web, risponde l'applicativo webmail, che richiede l'inserimento delle credenziali di accesso.
3. Superata la validazione dell'accesso al Sistema, l'utente si trova all'interno dell'applicativo webmail, dove può inviare, ricevere, cercare i messaggi, gestire la rubrica personale, modificare le impostazioni dell'applicazione. Per ogni messaggio da inviare è possibile scegliere il tipo di ricevuta di avvenuta consegna. La ricevuta, come specificato al par. 4.3, può essere completa (contiene il messaggio originale completo), breve (contiene il messaggio originale con una codifica hash degli allegati) o sintetica (contiene i soli dati di certificazione).

L'indirizzo (HTTPS) del sistema di webmail viene comunicato al titolare nel messaggio di benvenuto che viene inviato una volta completata la procedura di attivazione.

5.5 Smarrimento delle credenziali di accesso al sistema

In caso di smarrimento delle credenziali di accesso al sistema il titolare di una casella di PEC potrà richiederle nuovamente al gestore. Per far questo deve inviare una richiesta via fax o raccomandata A/R nella quale devono essere riportate le seguenti informazioni:

- Nome e cognome o Ragione Sociale
- Indirizzo (Via, Città, CAP, Nazione)
- Codice fiscale o partita IVA
- email valida (per eventuali comunicazioni)

Inoltre deve essere inviata una fotocopia di un documento di identità valido.

Il personale del servizio di help desk di Namirial S.p.A., una volta recuperate le informazioni richieste, le comunica al cliente via posta elettronica o con mezzi alternativi.

5.6 Richiesta e reperimento dei log dei messaggi

Come previsto dalla normativa, i titolari delle caselle di posta elettronica certificata, hanno la possibilità di richiedere al proprio gestore gli estratti dei contenuti dei file di log relativi alla loro casella di PEC.

La richiesta può essere effettuata inviando via posta certificata le seguenti informazioni:

- nome e cognome del titolare
- indirizzo PEC del mittente

- indirizzo PEC del destinatario
- data di riferimento del messaggio da ricercare
- oggetto del messaggio da ricercare (opzionale)
- identificativo del messaggio (opzionale)

La casella di posta certificata utilizzata dal gestore per la raccolta delle richieste dei log da parte degli utenti, verrà comunicata agli utenti stessi all'interno del messaggio di benvenuto inviato a seguito dell'attivazione.

Nel caso in cui il titolare sia impossibilitato ad effettuare la richiesta via PEC, può farlo via fax o raccomandata A/R inviando, oltre alle suddette informazioni, anche una fotocopia di un documento di identità valido.

Il personale del servizio di help desk di Namirial S.p.A., una volta recuperate le informazioni richieste, le comunica al cliente via posta elettronica certificata o con mezzi alternativi.

5.7 Richiesta della cancellazione di una casella PEC

Il titolare può richiedere al proprio gestore la cancellazione della propria casella di PEC.

Per far questo deve inviare una richiesta via fax o raccomandata A/R nella quale devono essere riportate le seguenti informazioni:

- Nome e cognome o Ragione Sociale
- Indirizzo (Via, Città, CAP, Nazione)
- Codice fiscale o partita IVA
- email valida (per eventuali comunicazioni)

Inoltre deve inviare una fotocopia di un documento di identità valido.

La richiesta di cancellazione può essere fatta solamente dal titolare della casella.

Il gestore effettua una serie di controlli dopodiché provvede alla cancellazione. Al termine dell'operazione conferma via email l'avvenuta eliminazione.

5.8 Servizio di Help desk

Namirial S.p.A. ha predisposto uno specifico canale di comunicazione (help desk) con l'utenza finale, per quanto concerne la gestione di problematiche relative al servizio di posta elettronica certificata.

L' help desk è costituito da uno staff di persone individuate e preposte all'assistenza clienti per il servizio di posta elettronica certificata e risponde al numero di selezione automatica indicato al paragrafo 2.4, durante l'orario di ufficio dalle 9.00 alle 13.00 e dalle 15.00 alle 19.00, dal lunedì al venerdì.

Le richieste di assistenza possono essere inviate 24 ore su 24, tramite posta elettronica all'indirizzo pec@namirial.com o attraverso apposite pagine web presenti sul sito www.sicurezzapostale.it. In quest'ultimo caso l'utente ha la possibilità di inviare una segnalazione generica oppure di effettuare una domanda diretta ad uno specifico operatore.

Le richieste effettuate tramite posta elettronica o attraverso il portale, se pervenute fuori dall'orario lavorativo o nei giorni festivi, sono prese in carico a partire dal primo giorno lavorativo successivo.

Il cliente del servizio ha la possibilità di ottenere informazioni generali sulla posta elettronica certificata (come funziona, possibili usi del canale, validità legale dei messaggi di PEC, etc) e dettagli specifici sul servizio erogato quali, ad esempio:

- come configurare il client di posta
- come accedere e come utilizzare la webmail
- come ottenere nuovamente le credenziali di accesso in seguito al loro smarrimento
- come ottenere un estratto dei file di log
- quali sono le garanzie di sicurezza del servizio
- come vengono trattati i dati personali

Il cliente potrà segnalare eventuali problemi riscontrati durante l'invio e la ricezione dei messaggi sia attraverso i client di posta che attraverso la webmail.

Tutte le segnalazioni vengono gestite attraverso un sistema di trouble ticketing che segnala via email ogni aggiornamento fino alla risoluzione definitiva.

5.8.1 Trouble ticketing

Attraverso il sistema di trouble ticketing, Namirial S.p.A. tiene traccia di tutte le segnalazioni effettuate dai propri clienti.

Il sistema si basa su un'applicazione web-based attraverso la quale il personale Help Desk è in grado di:

- creare un nuovo ticket a seguito di una segnalazione da parte del cliente
- seguire la "vita" del ticket nel corso degli aggiornamenti e cambi di stato fino alla risoluzione finale
- aggiornare il ticket annotando gli interventi fatti e le comunicazioni con il cliente
- attingere ad una knowledge base contenente le guide ai servizi, le domande più frequenti (F.A.Q.), i casi più significativi
- ricercare i ticket in base ad una serie di informazioni quali la data di creazione, la categoria, l'identificativo dell'operatore che segue la segnalazione, etc.

Tutte le modifiche di stato vengono notificate all'utente che ha effettuato la segnalazione attraverso un messaggio di posta elettronica.

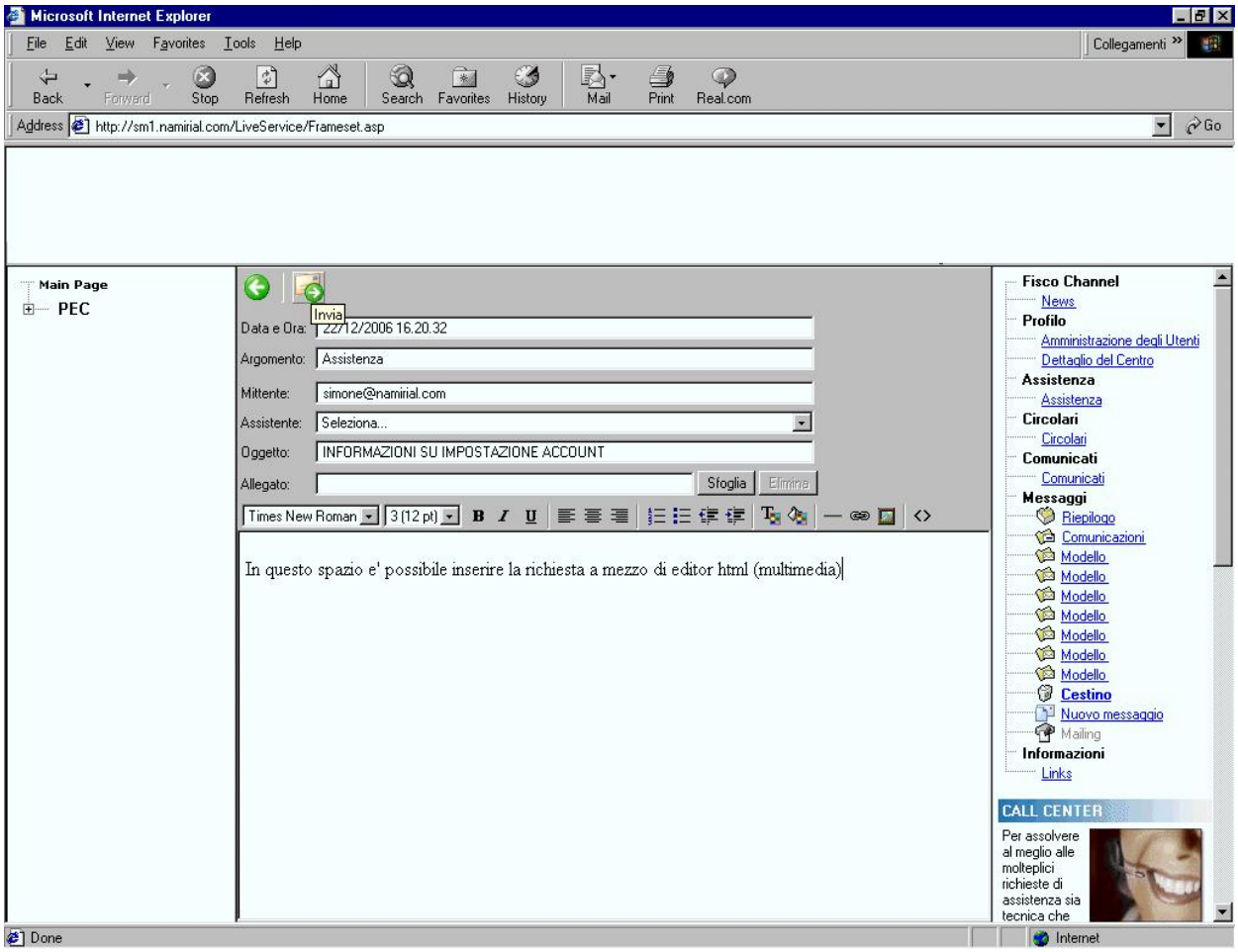


Figura 3 - Il sistema di trouble ticketing

5.9 Raccomandazioni per gli utenti

Riportiamo qui di seguito un vademecum con i suggerimenti per un utilizzo corretto e sicuro della posta elettronica certificata di Namirial S.p.A.:

- La casella di PEC dovrebbe essere utilizzata per comunicazione ufficiali e non per la corrispondenza usuale per la quale si consiglia di usare una comune casella non certificata.
- Poiché le email certificate si intendono ricevute non appena consegnate nella mailbox del destinatario, si suggerisce di controllare la propria mailbox con una certa frequenza.
- Si consiglia di controllare l'occupazione della propria mailbox ed eventualmente di eliminare i messaggi più vecchi, evitando così che le mail vengano respinte per casella piena.
- Si suggerisce di utilizzare firewall e software antivirus per proteggere il proprio computer da codice malevolo o da accessi esterni.

- Si consiglia di modificare frequentemente la password. In particolare si suggerisce di modificarla al primo accesso al servizio.
- Si suggerisce inoltre di non rivelare a nessuno le proprie credenziali di accesso e di utilizzare tutti gli accorgimenti necessari a mantenerne la segretezza.
- Come password si consiglia di usare una sequenza di almeno 8 caratteri alfanumerici che non sia facilmente ricostruibile da una conoscenza anche sommaria della persona. Ad esempio si sconsiglia di usare il nome o la data di nascita propri o dei familiari stretti.

5.10 Interoperabilità con gli altri sistemi di PEC

Namirial S.p.A. si impegna a garantire che il proprio sistema di PEC sia interoperabile con i sistemi degli altri gestori presenti nell'Indice Pubblico (IGPEC), in accordo a quanto stabilito dal Decreto Ministeriale 2 novembre 2005.

Per semplificare il controllo dell'interoperabilità Namirial S.p.A. metterà a disposizione una casella di PEC da utilizzare per i test con gli altri gestori.

5.11 Livelli di servizio ed indicatori di qualità

Per l'erogazione del servizio Namirial S.p.A. garantisce il rispetto dei livelli di servizio previsti dalla normativa.

Livelli di Servizio	
Numero massimo di destinatari contemporanei accettati in una singola mail	Almeno 50
Dimensione massima di ogni singolo messaggio (intesa come prodotto tra il numero dei destinatari e la dimensione del messaggio)	Almeno 30 MB
Disponibilità del servizio nel periodo di riferimento previsto (quadrimestre)	Maggiore o uguale al 99,8%
Indisponibilità del servizio per il singolo fermo nel periodo di riferimento previsto (quadrimestre)	Minore o uguale al 50%
Tempo massimo per il rilascio della ricevuta di accettazione nel periodo di disponibilità del servizio (calcolato escludendo i tempi di trasmissione)	30 min

Nella tabella seguente vengono riportati gli indicatori di qualità del servizio di posta certificata di Namirial S.p.A..

Indicatori di qualità	
Disponibilità del servizio (invio e ricezione email)	24 x 7 x 365
Disponibilità del servizio di richiesta di attivazione	24 x 7 x 365
Tempo per l'attivazione di un nuovo account di PEC (dalla ricezione di tutta la documentazione necessaria)	6 giorni lavorativi
Tempo massimo per l'esecuzione di interventi di manutenzione che causino il fermo servizio	2 ore
Disponibilità del servizio di richiesta da parte del titolare della traccia delle comunicazioni effettuate (log)	24 x 7 x 365
Accesso ai file di log da parte del personale di Namirial S.p.A.	5 giorni la settimana (dal lunedì al venerdì) dalle 9.00 alle 13.00 e dalle 15.00 alle 19.00
Tempo massimo per l'invio delle informazioni relative ai file di log dietro richiesta del titolare	5 giorni lavorativi
Sistema di monitoring con invio di messaggi di alert via email ed sms al presentarsi di malfunzionamenti e situazioni critiche	24 x 7 x 365
Assistenza standard tramite call center (trouble ticketing)	5 giorni la settimana (dal lunedi al venerdi) dalle 9.00 alle 13.00 e dalle 15.00 alle 19.00

6 – Descrizione della soluzione

6.1 Principali caratteristiche

La soluzione di Namirial S.p.A. presenta le seguenti caratteristiche:

- Piena conformità alla normativa vigente in materia di posta elettronica certificata sia in termini di funzionalità, che di interoperabilità e sicurezza.
- Sicurezza dell'infrastruttura hardware, software e di rete.
- Sicurezza nell'adozione di procedure e processi di erogazione del servizio
- Sicurezza nell'utilizzo di personale qualificato, preparato e responsabile.
- Sicurezza e cura nella nella gestione dei dati sensibili
- Scalabilità, modularità ed estensibilità di ogni componente del sistema.
- Compatibilità con tutti i client di posta (Outlook, Outlook Express, Thunderbird, etc) che soddisfano i requisiti minimi stabiliti dalle regole tecniche.
- Conformità allo standard internazionale RFC3161 per la marcatura temporale dei file di log e per l'interfacciamento con una Time Stamping Authority accreditata.
- Interoperabilità con ogni Certification Authority che soddisfi gli standard previsti dalla normativa.
- Integrabilità con le tipologie di rete più diffuse sul mercato.
- Utilizzo di dispositivi hardware ad alta sicurezza (*tamper-proof*/*tamper-evident*) per la gestione, mantenimento delle chiavi e dei certificati di firma.
- Utilizzo di dispositivi hardware per la firma e verifica dei messaggi.

6.2 Scalabilità e Affidabilità

L'architettura è altamente scalabile e può essere in qualsiasi momento estesa per venire incontro alle future esigenze di crescita, in modo da mantenere i tempi di risposta ed i livelli di qualità erogati dal gestore.

Riguardo l'affidabilità è importante notare che tutti i server, i device di rete, i dispositivi firma sono installati in configurazione ridondata e bilanciata. In questo modo non esiste un "single point of failure" ed il malfunzionamento su un apparato non causa un fermo servizio.

Inoltre viene utilizzato uno storage condiviso per la memorizzazione delle informazioni comuni in modo da rispondere alle esigenze di disponibilità, affidabilità e continuità del servizio.

6.3 Sicurezza dei dati

Le chiavi private ed i certificati che vengono utilizzati nelle operazioni di firma dei messaggi vengono interamente gestiti e mantenuti all'interno di dispositivi ad alta sicurezza, i cosiddetti **hardware**

security module o **HSM**. Gli stessi apparati vengono inoltre utilizzati per la firma delle mail e per la loro verifica.
Gli hardware security module utilizzati nella soluzione di Namirial S.p.A. hanno una certificazione **FIPS 140-2 level 3** e presentano caratteristiche di:

- **tamper evidence**: il device rileva se ci sono stati tentativi di manomissione o accesso non autorizzato
- **tamper proofness**: in caso di accesso o manomissione il dispositivo cancella la memoria contenente le chiavi.

6.4 Architettura del sistema

La soluzione di posta elettronica certificata di Namirial S.p.A. si basa sul prodotto **OpenPEC versione 2 (OpenPEC 2)**. OpenPEC (www.openpec.org) è un progetto Open Source nato con lo scopo di realizzare un sistema di Posta Elettronica Certificata conforme alle linee guida indicate dal Centro Nazionale per l'Informatica nella Pubblica Amministrazione (CNIPA).

OpenPEC si propone come estensione dei mail server Open Source più diffusi sul mercato come Postfix ed ha le seguenti caratteristiche:

- Piena compatibilità con la normativa vigente
- Prestazioni elevate
- Affidabilità
- Scalabilità
- Modularità
- Compatibilità con i principali fornitori di Hardware Security Module (HSM)
- Capacità di gestire sistemi con un elevato numero di domini e/o mailbox
- Aggiornamento automatico e trasparente dei domini locali (senza riavvio)
- Marcatura temporale e storicizzazione dei log
- Gestione delle Certificate Revocation List (CRL).

L'architettura di seguito riportata descrive a grandi linee la soluzione di posta certificata di Namirial S.p.A. senza scendere in dettagli implementativi. Lo schema e la descrizione che seguono non ha lo scopo di essere esaustiva circa il numero o la tipologia dei server coinvolti.

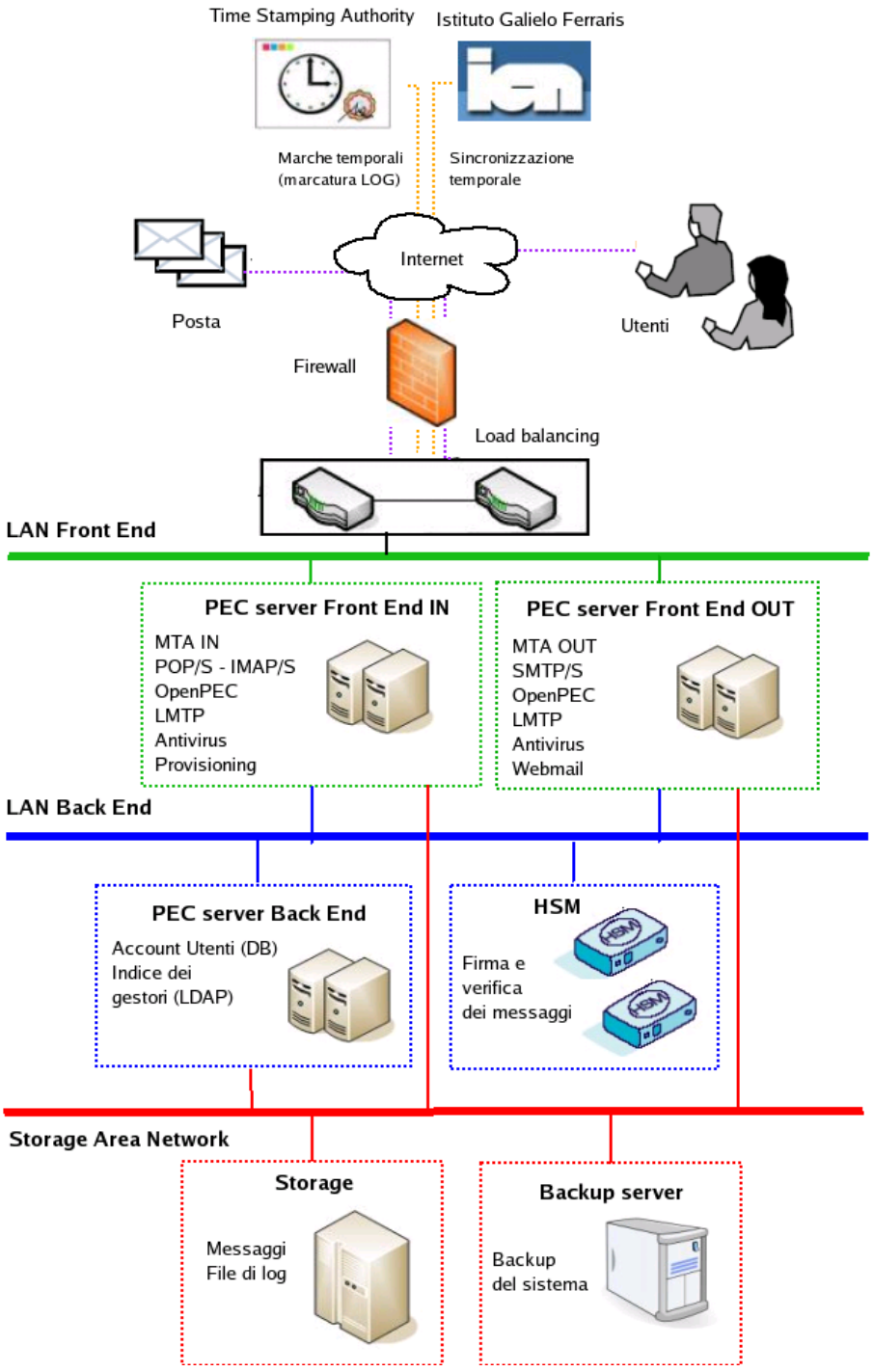


Figura 4 - Architettura di massima del sistema

L'architettura può essere suddivisa in 4 livelli.

- **Primo livello.** Il primo livello è costituito dagli apparati di rete (router, switch), dal modulo firewall per la protezione del sistema da accessi indesiderati, ed i load balancer che si occupano di suddividere il carico tra le varie macchine.
- **Secondo livello.** Il secondo livello rappresenta il **front end PEC,** cioè l'interfaccia verso il mondo esterno, il centro di elaborazione principale e l'interfaccia verso i dispositivi di memorizzazione.

  Contiene 2 gruppi di macchine: **PEC server Front End IN** e **PEC server Front End Out**.

  Il primo gruppo si occupa delle mail in ingresso, mentre il secondo delle mail in uscita. Su entrambi i gruppi è presente il modulo **MTA** che si incarica del mail routing, il modulo **antivirus** ed il nucleo centrale del sistema, **OpenPEC**.

  Il gruppo Fronte End IN contiene inoltre il server **POP** e **IMAP** (per l'accesso alla casella di posta tramite client) ed il sistema di provisioning (per la creazione e gestione degli account e dei domini di PEC), mentre il gruppo Front End OUT contiene il server **SMTP** (per la spedizione delle mail) ed il modulo di web mail (per l'accesso alla casella di posta attraverso un comune browser web).

  All'interno del secondo livello è inoltre implementata la sincronizzazione con l'Istituto Galileo Ferraris di Torino mediante protocollo NTP e l'interfaccia con una Time Stamping Authority allo scopo di effettuare la marcatura giornaliera dei log.
- **Terzo livello.** Il terzo livello contiene i dispositivi di firma, **HSM** (Hardware security module) ed il gruppo di macchine **PEC server back end**. Gli HSM si occupano della firma e della verifica dei messaggi inviati e ricevuti, mentre le macchine PEC server back end contengono il database degli account ed il mirror dell'indice pubblico dei gestori del CNIPA memorizzato su server LDAP.
- **Quarto livello:** Il quarto livello rappresenta il **data store** del sistema e contiene le mailbox degli utenti ed i file di log memorizzati all'interno di uno storage condiviso.

6.5 I principali componenti della soluzione

Di seguito riportiamo uno schema che descrive i principali componenti della soluzione:

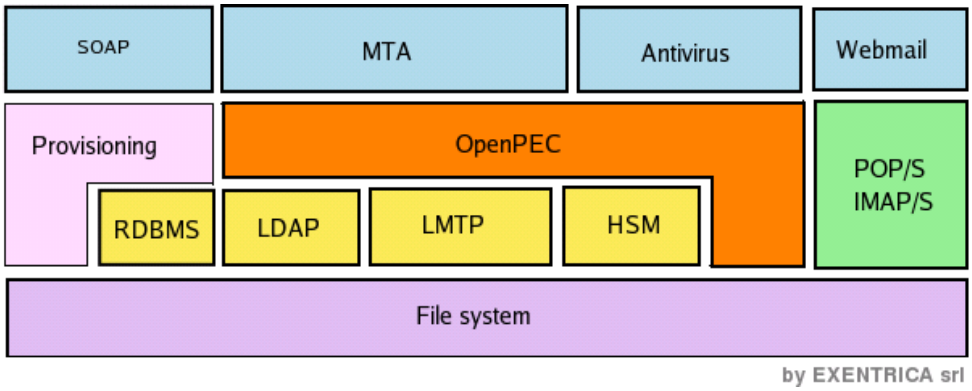


Figura 5 - Componenti del sistema

Come descritto nello schema, esiste un nucleo centrale del sistema (OpenPEC) che si interfaccia con tutti gli altri moduli:

- il Mail Transfer Agent (MTA) che si incarica del “dispatching” delle mail,
- il modulo Antivirus,
- il server LDAP (che contiene gli account ed il mirror dell'indice dei gestori),
- il server LMTP,
- i moduli HSM utilizzati per la firma dei messaggi,
- lo storage (file system),
- il server POP-IMAP,
- il modulo di provisioning (per la creazione/modifica degli account) richiamabile attraverso interfaccia SOAP,
- il modulo di web mail.

6.6 Riferimenti temporali

Il Decreto ministeriale del 2 novembre 2005 stabilisce che su ogni messaggio, ricevuta o avviso venga apposto un riferimento temporale.

Il riferimento temporale può avere uno scarto non superiore ad 1 minuto secondo rispetto alla scala di riferimento UTC (Coordinated Universal Time).

Tutti gli eventi che costituiscono la transazione nel punto di accesso, nel punto di ricezione e nel punto di consegna utilizzano un valore temporale unico. In altre parole l'indicazione dell'istante di elaborazione del messaggio risulta univoca all'interno dei log, delle ricevute, degli avvisi e dei messaggi generati dal sistema.

Il sistema si interfaccia con l'Istituto Elettrotecnico Nazionale Galileo Ferraris (IEN) di Torino mediante protocollo NTP. L'orologio di sistema viene mantenuto sincronizzato con quello di riferimento compensando anche la deriva e le fluttuazioni che possono derivare da carico del sistema, variazioni ambientali, etc.

Il formato della data è ***gg/mm/aaaa***

dove *gg* sono le 2 cifre del giorno,

mm le 2 cifre del mese e

aaaa le 4 cifre dell'anno.

Il formato dell'ora è ***hh:mm:ss***

dove *hh* sono le 2 cifre delle ore (su 24 ore),

mm le 2 cifre dei minuti,

ss le 2 cifre dei secondi.

Al dato temporale viene fatto seguire, tra parentesi tonde, la **zona**, ossia la differenza, in ore e minuti, tra l'ora legale ed il riferimento UTC. Il valore di tale differenza è preceduto da un segno + o – che indica la differenza positiva o negativa rispetto ad UTC.

Ad Esempio:

07/12/2006 17:35:16 (+0100)

indica il 7 dicembre 2006, ore 17, 35 minuti, 16 secondi,

1 ora avanti rispetto al riferimento UTC.

6.7 Storicizzazione dei Log e apposizione della marca temporale.

Il Decreto Ministeriale del 2 novembre 2005 stabilisce che ogni sistema di posta elettronica certificata deve prevedere un intervallo temporale unitario, non superiore alle ventiquattro ore, entro il quale eseguire, senza soluzioni di continuità, il salvataggio dei log dei messaggi.

Ai file di log creati dal sistema deve essere apposta una marcatura temporale che stabilisca in maniera certa e legalmente riconosciuta l'esatto istante di archiviazione del file stesso. La marca temporale è un riferimento di tempo che viene validato da una terza parte fidata, la cosiddetta **Time Stamping Authority** (**TSA**).

La validazione temporale di un documento informatico consiste nella generazione, da parte di una TSA, di una firma digitale così detta di *marcatura temporale* (time stamping).

Le marche temporali possono risolvere dispute in merito al tempo (data/ora) in cui un dato documento è stato prodotto.

L'interazione con il servizio di TSA avviene attraverso il protocollo standard RFC 3161 (http://www.ietf.org/rfc/rfc3161.txt) ed i file "marcati" verranno trasferiti su supporto ottico e conservati per il periodo di 30 mesi stabilito dalla normativa.

Nel caso in cui venisse revocato il certificato di un firmatario di un documento di cui si ha la marca temporale, è possibile determinare se la marcatura è avvenuta in un momento antecedente o successivo alla revoca.

6.8 Conservazione dei messaggi contenenti virus e relativa informativa al mittente

La soluzione di Namirial S.p.A. è compatibile con la normativa riguardo la rilevazione, la segnalazione e la conservazione dei messaggi di posta elettronica certificata contenenti virus.

In particolare il sistema di Namirial S.p.A.:

1. nel caso spedizione verifica la presenza dei virus nei messaggi di posta elettronica al Punto di Accesso, ossia nella fase immediatamente successiva all'invio del messaggio;
2. nel caso di ricezione verifica la presenza di virus al Punto di Ricezione del sistema di destinazione.

Nel primo caso il sistema comunica al mittente che il suo messaggio contiene un virus attraverso un "avviso di non accettazione per presenza di virus".

Nel secondo caso il sistema del destinatario invia un avviso di "rilevazione virus" al sistema del mittente che provvede ad avvisare il mittente attraverso un messaggio di "mancata consegna per virus".

I messaggi contenenti virus vengono conservati su supporto ottico per un periodo non inferiore a trenta mesi secondo quanto stabilito dalla normativa.

6.9 Descrizione del data center Namirial S.p.A.

Il Data Center utilizzato per l'erogazione del servizio di PEC è situato in ambienti idonei ad ospitare "complesse infrastrutture hardware" utilizzando tecnologie innovative in termini di affidabilità, sicurezza, scalabilità e ridondanza.

Di seguito si riportano le principali caratteristiche infrastrutturali del Data Center con una descrizione tecnico-funzionale dei sistemi, degli impianti e dei relativi servizi correlati.

6.9.1 Descrizione degli ambienti

I locali risultano ubicati al piano primo di un complesso edilizio di recente costruzione che si sviluppa su due livelli fuori terra. Il fabbricato è realizzato con struttura portante in cemento armato del tipo gettato in opera con solai in laterocemento e tamponamenti perimetrali in laterizio, conformemente alle vigenti norme antisismiche. Il solaio di copertura è del tipo in piano (lastrico solare) non direttamente accessibile.

Il Data Center risulta articolato in vari ambienti, nei quali i sistemi sono suddivisi per tipologia e grado di sicurezza:

- Atrio/ingresso;
- Servizi;
- Sala-1 programmatori;
- Sala-2 programmatori;
- Sala macchine;

La "sala macchine" risulta ubicata nella parte più interna, risulta priva di elementi finestrati e completamente racchiusa entro pareti di laterizio (riqualificate REI 120 a tenuta di gas), che ne garantiscono l'isolamento fisico dal resto delle attività .

6.9.2 Accesso agli ambienti e standard di sicurezza adottati

L'ingresso ai locali del Data Center avviene da un atrio comune del piano primo a cui si accede :

- dal piano terra, attraverso una scala aperta con struttura portante in cemento armato con inserito servizio ascensore;
- dal piano primo attraverso un disimpegno comune con le altre attività preesistenti.

L'accesso fisico ai locali avviene attraverso due successive porte blindate (resistenza all'effrazione non inferiore alla Classe 4 secondo la norma ENV 1627), di cui la seconda è dotata di controllo accessi a mezzo di lettore di prossimità e chiave transponder.

Ai serramenti finestrati perimetrali (del piano primo) ed ai lucernari (della copertura) risulta applicata una blindatura con “grata di acciaio” a maglie strette ad elevata resistenza all’effrazione.

L’accesso alla sala macchine è limitato al solo personale autorizzato ed avviene attraverso un’ulteriore porta blindata con caratteristiche di resistenza al fuoco REI 120, dotata anch’essa di controllo di sicurezza a badge magnetico. Per questa porta è previsto (per ragioni di sicurezza) un pulsante di sblocco dall’interno.

Risulta presente inoltre un sistema di “allarme antintrusione” collegato con le forze dell’ordine ed un sistema operativo di “videosorveglianza” a distanza.

7 – Standard tecnologici, procedurali e di sicurezza adottati

7.1 Standard tecnologici di riferimento

Di seguito l'elenco degli standard tecnologici di riferimento.

- 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).
- RFC 3161 (TSP Time-Stamp Protocol)

7.2 Standard di sicurezza

Per l'erogazione del servizio di posta elettronica certificata, Namirial S.p.A. adotta le linee guida ed i principi previsti dallo standard i sicurezza **ISO 27001:2005**.

Lo standard, che sostituisce la norma di riferimento BS 7799 (Information Security Management System ISMS), prevede l'attuazione di una serie di processi, misure e procedure al fine di fornire tutte le garanzie di sicurezza e di protezione dei dati che sono necessarie in sistemi critici e delicati come quello della posta elettronica certificata.

In un contesto dove i rischi informatici causati dalle violazioni dei sistemi di sicurezza sono in continuo aumento, lo standard ISO 27001:2005 si pone l'obiettivo di proteggere i dati e le informazioni da minacce di ogni tipo, al fine di assicurarne:

- l'**integrità** (accuratezza e completezza),
- la **riservatezza** (accessibilità ai soli individui autorizzati),

- la **disponibilità** (certezza che le informazioni siano sempre a disposizione del personale incaricato).

A tale scopo, le linee guida forniscono i requisiti necessari ad ottenere un adeguato sistema di gestione della sicurezza delle informazioni e dei dati sensibili, sia dell'azienda, che dei propri clienti.

Lo standard prevede inoltre le procedure per:

- l'**analisi dei rischi** (individuazione punti deboli, studio delle possibili minacce e probabilità che si presentino, analisi degli eventuali impatti sul sistema)
- la **gestione dei rischi** (monitoring del sistema, rilevazione dei problemi e loro risoluzione, eliminazione punti deboli, riduzione dei rischi per l'intero sistema).

7.2.1 Dispositivi di firma (HSM)

I device HSM utilizzati per la firma e la verifica dei messaggi di PEC sono certificati in base allo standard **FIPS 2** pubblicato dal **National Institute of Standards and Technology** (**NIST**). Lo standard indica i requisiti di sicurezza che devono essere rispettati dai moduli crittografici utilizzati all'interno di sistemi nei quali vengano trattati dati sensibili. Fanno parte di questa gamma le specifiche dei moduli crittografici e relative interfacce, le regole, i servizi e il processo di autenticazione. Tra i requisiti, vengono trattati anche i vincoli di sicurezza a livello fisico ed il processo del Key Management.

Lo Standard FIPS 2 si compone di quattro livelli qualitativi di sicurezza di cui i primi 3 sono soddisfatti :

Livello	Tipo di Sicurezza	Descrizione
Level 1	Moduli crittografici	Sicurezza applicata ai moduli crittografici; in particolare riguarda gli algoritmi di crittografia.
Level 2	Sicurezza fisica	*Tamper evidence* – Apposizione di rivestimenti ed etichette in grado di rilevare tentativi di manomissione o accessi non autorizzati**.**
Level 3	Sicurezza fisica	*Tamper proofness* - Meccanismi in grado di cancellare la memoria in caso di accessi non autorizzati o tentativi di manomissione. Sistemi di autenticazione sicura con controllo dei ruoli e delle autorizzazioni specifiche per ogni operatore
Level 4	Sicurezza fisica	Protegge la sicurezza dagli eventi ambientali esterni quali gli sbalzi di temperatura o di tensione. Generalmente viene utilizzato nei casi di device posizionati in ambienti non protetti o non controllati.

I device di firma utilizzati nel sistema di PEC di Namirial S.p.A. sono certificati **FIPS-2 Level 3** (http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf).

7.3 Misure di sicurezza

Il sistema di posta elettronica certificata di Namirial S.p.A. presenta tutte le garanzie di sicurezza compatibili con la tipologia di servizio erogato. Le misure di sicurezza, di seguito riportate, sono descritte in maniera più approfondita e dettagliata nel **Piano di Sicurezza**, un documento riservato, custodito presso il CNIPA e redatto in base alle disposizioni della circolare CNIPA n. 49 del 24 novembre 2005.

7.3.1 Locali di erogazione del servizio

I locali di erogazione del servizio sono dotati dei più moderni dispositivi antincendio, antifumo, antri intrusione, condizionamento e ricambio d'aria.

L'accesso, che avviene attraverso una serie di porte blindate, è consentito solo a personale autorizzato e viene controllato mediante un sistema basato su lettori di prossimità e chiavi transponder.

I clienti, i fornitori e gli eventuali visitatori occasionali possono visitare il data center, previa prenotazione, solo se accompagnati da personale interno per tutta la durata della permanenza.

Il data center è provvisto di un sistema di videosorveglianza e di allarmi anti intrusione collegati con le forze dell'ordine.

I lavori e la manutenzione su tutti gli impianti vengono sempre affidati a ditte esterne in possesso dei requisiti professionali previsti dalla legge 46/90.

Sono previsti controlli periodici per la verifica delle funzionalità dell'impianto.

7.3.2 Risorse umane adibite alla gestione del sistema

Sono previsti 4 responsabili del servizio di PEC, secondo quanto stabilito dalla normativa:

- Responsabile della registrazione dei titolari
- Responsabile dei servizi tecnici
- Responsabile delle verifiche e delle ispezioni (auditing)
- Responsabile della sicurezza, dei log dei messaggi e del sistema di riferimento temporale

I suddetti responsabili coordinano, ciascuno, un gruppo di lavoro composto da addetti in possesso della necessaria esperienza ed appositamente istruiti attraverso corsi di formazione interni. Ogni incaricato viene responsabilizzato ed istruito sulla delicatezza del servizio erogato e sulla necessità di dedicare maggior cura ed attenzione possibile allo svolgimento dei compiti assegnati.

Nelle fasi iniziali ogni nuovo incaricato viene seguito personalmente da un “tutor”.

7.3.3 Sicurezza dell'infrastruttura

Dal punto di vista prettamente informatico, la sicurezza del sistema di Namirial S.p.A. viene realizzata attraverso l'adozione di una serie di misure quali:

- Presenza di firewall con policy di accesso molto restrittive (vengono abilitate le porte strettamente necessarie).
- Sistema di antivirus aggiornato almeno 4 volte al giorno.
- Prodotti software costantemente aggiornati sia in seguito di rilascio di nuove versioni che di patch (prima di mettere in produzione l'aggiornamento vengono effettuati i test su un ambiente di staging).
- Utilizzo di protocolli sicuri per il colloquio tra l'utente ed il proprio gestore (SMTP/S, POP3/S, IMAP/S) e tra un gestore e l'altro (STARTTSL).
- Firma dei messaggi con i dispositivi HSM certificati FIPS-2 Level 3.
- Separazione fisica dei livelli di front end, back end e data store (in modo da aumentare il grado di protezione dei dati).
- Utilizzo di storage di rete esterni al sistema per aumentare la protezione delle informazioni degli utenti.
- Sistema ridondato in ogni sua parte in modo da evitare “single point of failure”.
- Sistema di backup per ridurre il rischio di perdita dei dati.

7.3.4 Analisi e gestione dei rischi

Il sistema di posta elettronica certificata di Namirial S.p.A. viene sottoposto a verifiche periodiche allo scopo di analizzarne le criticità, individuarne la vulnerabilità ed identificare i possibili rischi ai quali è sottoposto. Con un'attenta analisi è possibile prevenire una buona parte di malfunzionamenti e prepararsi a gestire e risolvere i problemi non prevedibili a priori.

Durante l'analisi i possibili guasti vengono suddivisi in

- guasti “di piccola entità”
- guasti “di grave entità”

I primi sono i tipici guasti causati da problemi dei sistemi hardware e software e generalmente possono essere risolti attraverso un'attività di manutenzione ordinaria o straordinaria come, ad esempio, la sostituzione degli apparati o l'upgrade dei componenti software.

I secondi sono guasti causati da eventi catastrofici, atti dolosi o errori umani dovuti a incompetenza o negligenza e possono provocare danni gravi ed interruzione del servizio.

7.3.5 Controllo dei livelli di sicurezza

I livelli di sicurezza vengono controllati attraverso attività di monitoring continue su tutti i principali componenti del sistema di posta certificata.

Sono inoltre previste delle visite ispettive interne con cadenza semestrale, che hanno lo scopo di esaminare il sistema nel suo complesso al fine di verificarne il livello di sicurezza ed individuarne le criticità. Per essere certi che il sistema è sicuro vengono controllati:

- gli apparati di rete (firewall, router, etc)
- le apparecchiature (server, HSM, etc)
- i componenti software
- i flussi organizzativi e procedurali messi in atto
- l'operato del personale coinvolto

Il risultato di ciascuna visita è un rapporto dettagliato che fotografa lo stato del sistema, elenca i controlli eseguiti ed evidenzia tutti gli interventi che devono essere effettuati al fine di migliorare l'intero sistema. Oltre agli interventi di natura tecnica come la sostituzione, l'aggiornamento o il potenziamento dei componenti hardware e software, potranno essere richiesti interventi di natura organizzativa come il cambiamento di una procedura interna o la sostituzione di personale giudicato non idoneo al servizio.

7.3.6 Protezione dei dati personali

I dati personali degli utenti sono trattati, conservati e protetti da Namirial S.p.A. in conformità a quanto previsto dal Decreto Legislativo n. 196 del 30 giugno 2003 “Codice in materia di protezione dei dati personali” (per i dettagli si rimanda al Cap. 9).

Adottando le misure, le procedure, i processi ed i controlli di sicurezza descritti nei precedenti paragrafi, Namirial S.p.A. è in grado di assicurare, ai propri clienti, un continuo e costante livello di protezione dei propri dati.

7.4 Procedure operative utilizzate nell'erogazione del servizio

Namirial S.p.A., attraverso un'organizzazione attenta del personale, una gestione programmata dei backup, un accurato e costante monitoraggio del sistema e con l'applicazione di procedure e metodologie di risoluzione dei problemi precise e consolidate, è certa di poter garantire, ai propri clienti, dei livelli di servizio elevati e costanti nel tempo.

7.4.1 Organizzazione del personale

Come previsto dal DM del 2 novembre 2005, Namirial S.p.A. ha creato una struttura interna composta un gruppo di incaricati e da 4 responsabili di settore:

- 1 responsabile della registrazione dei titolari
- 1 responsabile dei servizi tecnici
- 1 responsabile delle verifiche e delle ispezioni (auditing)
- 1 responsabile della sicurezza, dei log dei messaggi e del sistema di riferimento temporale

Tutto il personale coinvolto nell'erogazione del servizio è in possesso delle conoscenze e dell'esperienza necessaria a svolgere i compiti assegnati.

7.4.2 Gestione backup

I backup dei dati di tutte le macchine che implementano il sistema PEC vengono effettuati su supporto ottico (DVD) attraverso un server apposito.

Vengono effettuati dei backup incrementali con cadenza giornaliera e dei backup completi con cadenza settimanale. I backup completi vengono salvati in doppia copia e conservati in luoghi distinti in modo da garantire un più alto livello di sicurezza nel caso di eventi catastrofici quali incendi, terremoti, etc. Per la precisione le copie di sicurezza vengono conservate presso la sede di erogazione del servizio a Senigallia e presso la sede secondaria di Gallarate (VA).

7.4.3 Sistema di Monitor

Tutti i servizi di posta elettronica certificata di Namirial S.p.A. vengono costantemente controllati attraverso un apposito sistema di monitor. Il sistema genera dei segnali di alert quando vengono superate le soglie impostate in fase di amministrazione. I segnali di alert, raccolti per 365 giorni all'anno h24, vengono inviati via sms al team di reperibili che è in grado intervenire prontamente per risolvere la criticità.

Attraverso il sistema di Namirial S.p.A. è possibile controllare tutte le macchine del sistema in termini di spazio disco, carico CPU, occupazione di memoria, attività dei processi, situazione delle code, etc.

7.4.4 Gestione e risoluzione dei problemi

La gestione dei problemi avviene secondo il seguente algoritmo:

1. Il servizio di **Help Desk** (**HD**) prende in carico la segnalazione che può arrivare:
   - dall'esterno ad opera di un cliente
   - dall'interno ad opera di un addetto al servizio PEC
   - dal sistema di monitoraggio a seguito del presentarsi di un evento anomalo
2. In tutti e tre i casi un operatore di help desk prende in carico la segnalazione e la gira al team di **Team di Supporto** (**TS**);
3. Il TS prende in carico la segnalazione, la analizza, verifica che il problema sussista realmente e ne stabilisce la solvibilità.
4. Il TS individua tutti i metodi possibili per la risoluzione del problema e li mette a confronto allo scopo di selezionare il metodo migliore in termini di minore impatto sul servizio e velocità di risoluzione.
5. Il TS valuta la necessità di utilizzare il supporto di terzi, intesi sia come personale specializzato interno, che come consulenza esterna.
6. Il TS mette in atto il metodo scelto e risolve il problema. Nel caso in cui sia stato previsto il supporto di personale esterno all'azienda, il TS lo assiste durante tutte le attività svolte ed effettua un presidio costante tracciando, al tempo stesso, tutte le operazioni effettuate.
7. Una volta completato l'intervento, il TS ne informa l'HD.
8. HD verifica che il problema è stato risolto e comunica la soluzione a chi ha effettuato la segnalazione.

7.5 Azioni promosse dal gestore in caso di malfunzionamento

In base alla circolare CNIPA n.51 del 7 dicembre 2006, il gestore è tenuto a informare il CNIPA dei malfunzionamenti riscontrati nel proprio sistema entro 30 minuti dal suo presentarsi. Nella segnalazione il gestore deve fornire anche "una prima valutazione dell'incidente e descrivere le eventuali misure adottate a riguardo".

I disservizi vengono catalogati in base alla seguente tabella:

Tipologia	Codice	Descrizione
Comportamento Anomalo non circoscritto	**1A** rilevato dal gestore	Comportamento difforme dalle regole tecniche di cui all'art. 17 del DPR 11 febbraio 2005, n.68, relativo alle funzioni base (trattamento del messaggio originario, ricevute ed avvisi) per il quale non è circoscritto il potenziale impatto
	1B rilevato da terzi	
Comportamento Anomalo circoscritto	**2A** rilevato dal gestore	Comportamento difforme dalle regole tecniche di cui all'art. 17 del DPR 11 febbraio 2005, n.68, relativo alle funzioni base (trattamento del messaggio originario, ricevute ed avvisi) per il quale è circoscritto il potenziale impatto
	2B rilevato da terzi	
Malfunzionamento bloccante	**3A** rilevato dal gestore	Tipologia di malfunzionamento a causa del quale le funzionalità del sistema PEC, come definite nelle regole tecniche di cui all'art. 17 del DPR 11 febbraio 2005, n.68, non possono essere utilizzate in tutto o in parte dagli utenti
	3B rilevato da terzi	
Malfunzionamento grave	**4A** rilevato dal gestore	Tipologia di malfunzionamento a causa del quale in alcune circostanze le funzionalità del sistema PEC, come definite nelle regole tecniche di cui all'art. 17 del DPR 11 febbraio 2005, n.68, non possono essere utilizzate in tutto o in parte dagli utenti
	4B rilevato da terzi	
Malfunzionamento	**5B** rilevato dal gestore	Situazione a causa della quale le funzionalità del sistema PEC, come definite nelle regole tecniche di cui all'art. 17 del DPR 11 febbraio 2005, n.68, in tutto o in parte, risultano degradate ovvero il sistema ha un comportamento anomalo in situazioni circoscritte e per funzionalità secondarie (esclusi: la procedura di identificazione, i messaggi originari, le ricevute, gli avvisi e le buste)
	5B rilevato da terzi	

Le segnalazioni degli utenti vengono catalogati in base ai seguenti codici identificativi:

Codice	Descrizione
RC	Segnalazione di un reclamo relativo al rapporto contrattuale
AL	Segnalazione di un reclamo relativo alla procedura di accesso ai log
SA	Segnalazione di anomalia/disservizio non imputabili al gestore (client, collegamento a internet, gestione utenze decentrate)

Nei casi 1A e 1B il gestore auto-sospenderà il servizio informando i propri utenti e gli altri gestori.

Nei casi 2A e 2B i CNIPA può decidere di sospendere il servizio del gestore fino a quando il problema è stato risolto. In entrambi i casi il gestore attua la sospensione producendo un “avviso di non accettazione per eccezioni formali” e non producendo la “ricevuta di presa in carico”.

Nel caso di sospensione il gestore, una volta eliminato il disservizio può riprendere l'attività. In tal caso deve inviare al CNIPA una relazione dettagliata su quanto accaduto e sui provvedimenti adottati.

8 – Obblighi e responsabilità

8.1 Obblighi e responsabilità del gestore

Namirial S.p.A. si impegna a rispettare la normativa vigente e le Regole Tecniche contenute nel Decreto Ministeriale 2 novembre 2005, in particolare in relazione:

- ai livelli di servizio previsti;
- all'interoperabilità con gli altri gestori accreditati;
- alla conservazione e disponibilità dei log relativi alle trasmissioni avvenute per gli usi e nelle modalità previste dalla legge;
- all'informazione sulle modalità di accesso al servizio e sui necessari requisiti tecnici;
- alla registrazione delle singole fasi di ogni trasmissione all'interno di file di log;
- alla conservazione dei file di log per almeno 30 mesi;
- all'apposizione della marca temporale sui log dei messaggi;
- al rilascio di tutte le ricevute e messaggi previsti dalla normativa (messaggio di trasporto, ricevuta di presa in carico, ricevuta di accettazione, ricevuta di avvenuta consegna, avviso di mancata accettazione, avviso di mancata consegna, avviso di mancata consegna per superamento tempi massimi, avviso di rilevazione virus, etc);
- all'apposizione su ogni messaggio di un riferimento temporale
- alla conservazione dell'integrità del messaggio originale nella relativa busta di trasporto durante ogni trasmissione;
- al rispetto delle norme previste dal Decreto legislativo 30 giugno 2003, n. 196 in materia di protezione dei dati personali.

8.2 Obblighi e responsabilità dei titolari

Il titolare è il solo responsabile dei contenuti dei propri messaggi.

Il titolare si impegna:

- ad utilizzare il servizio per i soli usi consentiti dalla legge;
- ad utilizzare soltanto il servizio di posta elettronica certificata erogato da gestori presenti nell'indice pubblico dei gestori (IGPEC);
- a dare il consenso all'utilizzo dei propri dati personali ai sensi del Dlgs 196/03;
- a fornire a Namirial S.p.A. tutte le informazioni necessarie ad identificare la persona ed attivare il servizio, garantendo, sotto la propria responsabilità, la veridicità e l'esattezza dei dati comunicati;
- ad utilizzare in modo sicuro il sistema evitando di rivelare a terzi le credenziali di accesso;

- a conservare copia dei messaggi inviati o ricevuti con le relative ricevute.

I privati che intendono utilizzare il servizio di posta elettronica certificata nei rapporti con la Pubblica Amministrazione, devono espressamente dichiarare il proprio indirizzo mentre le imprese, nei rapporti tra loro intercorrenti, possono dichiarare la esplicita volontà di accettare l'invio di posta elettronica certificata mediante indicazione nell'atto di iscrizione al registro delle imprese. Entrambe le dichiarazioni obbligano solo il dichiarante e possono essere revocate.

8.3 Limitazioni ed indennizzi

Namirial S.p.A. non risponderà in alcun caso dei danni causati direttamente o indirettamente dagli utilizzatori del servizio imputabili ad un utilizzo improprio del sistema ed al mancato rispetto delle regole e degli obblighi contenuto nel presente manuale;

Namirial S.p.A. non risponderà in alcun caso ai danni causati da malfunzionamenti, ritardi o interruzioni purché rientranti nei livelli di servizio descritti nel presente manuale.

il gestore non potrà in alcun modo essere ritenuto responsabile, a titolo esemplificativo ma non esaustivo, per danni derivanti da cause di forza maggiore, caso fortuito, eventi catastrofici (incendi, terremoti, esplosioni) o comunque non imputabili a Namirial S.p.A. che provochino ritardi, malfunzionamenti o interruzioni del servizio;

Namirial S.p.A. non assume alcun obbligo riguardo la conservazione dei messaggi inviati e trasmessi attraverso le proprie caselle di PEC. Tale responsabilità viene assunta unicamente dal cliente cliente/titolare;

Namirial S.p.A. non ha alcuna responsabilità sui contenuti dei messaggi inviati e ricevuti attraverso le proprie caselle di PEC;

La responsabilità di Namirial S.p.A. per ogni tipo di danno derivato dall'utilizzo del servizio, fatti salvi i casi di dolo o colpa grave, sarà limitata al doppio del corrispettivo pagato e/o dovuto per la singola casella dal titolare secondo gli accordi contrattuali.

Qualsiasi contestazione del titolare e/o cliente relativa all'erogazione del servizio dovrà essere comunicata a Namirial S.p.A., pena decadenza, entro 30 giorni dalla data dell'evento mediante raccomandata con ricevuta di ritorno;

Namirial S.p.A. si riserva la facoltà di modificare il presente manuale nel caso in cui vengano apportate modifiche tecniche al sistema, variazioni all'offerta commerciale, o adeguamenti normativi.

Le limitazioni agli indennizzi stabilite da Namirial S.p.A., per quanto non previsto dal presente capitolo, sono riportate nelle condizioni contrattuali di fornitura del servizio rese pubbliche nel sito www.sicurezzapostale.it

8.4 Polizza assicurativa

Namirial S.p.A. ha stipulato una polizza assicurativa per la copertura dei rischi e dei danni causati a terzi nell'esercizio dell'attività di gestore di posta elettronica certificata secondo quanto previsto nel DPR n. 68 del 2005.

La polizza copre i rischi derivanti dall'attività ed eventuali danni causati a terzi ai sensi del DPR 11 Febbraio 2005, n° 68 con il massimale di € 1.000.000,00 (un milione di euro) per ogni singolo atto illecito per anno assicurativo per tutte le perdite patrimoniali derivanti da tutte le richieste di risarcimento presentate contro tutti gli assicurati per tutte le coperture assicurative combinate.

9 – Protezione dei dati personali

Nel seguito vengono descritti i processi e le modalità operative adottate da Namirial S.p.A., in qualità di titolare del trattamento dei dati personali, nello svolgimento della propria attività.

Le informazioni personali dei titolari del servizio e, più in generale dei clienti, vengono trattate, conservate e protette in conformità a quanto previsto nel Decreto Legislativo n. 196 del 30 giugno 2003 - "Codice in materia di protezione dei dati personali".

9.1 Definizioni

Definizioni in materia di trattamento dei dati personali	
Dato personale	Ai sensi dell'art. 1 comma 2 lett. B) del D.lgs per dato personale si intende "qualunque informazione relativa a persona fisica, persona giuridica, ente o associazione, identificati o identificabili, anche mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale. Dati personali sono anche quelli relativi all'utente ovvero ad eventuali terzi e contenuti nei campi informativi presenti sui moduli e negli archivi – elettronici e/o cartacei – di registrazione, di richiesta di sospensione, di riabilitazione, di revoca, di cambio anagrafica e nei certificati di cui al presente manuale operativo.
Titolare del trattamento dati	Persona fisica giuridica, pubblica amministrazione o qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza
Responsabile	Persona fisica, persona giuridica, pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare, al trattamento dei dati personali
Incaricato	Persona fisica autorizzata a compiere operazioni di trattamento dal titolare del trattamento dati o dal responsabile
Interessato	Persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali

9.2 Struttura organizzativa di Namirial S.p.A. in materia di trattamento dei dati personali

Il **Dr. Claudio Gabellini**, in qualità di amministratore unico di Namirial S.p.A., è il **Titolare del trattamento dei dati personali**, secondo quanto previsto dal D.LGS. 196/2003 – Testo Unico in materia di protezione dei dati personali.

Il **Responsabile del Trattamento dei dati personali** è il Sig. Luca Fattori.

Namirial S.p.A. individua e nomina gli incaricati del trattamento che operano sotto la diretta autorità del titolare o del responsabile attenendosi alle istruzioni impartite.

Namirial S.p.A.ha redatto un apposito documento programmatico sulla sicurezza (DPSS), a norma con quanto previsto dai requisiti minimi di sicurezza nel trattamento di dati personali, di cui all'allegato tecnico b del D.LGS. 196/2003.

9.3 Tutela e diritti degli interessati

Namirial S.p.A. garantisce la tutela degli interessati in ottemperanza al Decreto legislativo 196/03 in materia di trattamento dei dati personali. In particolare il gestore fornisce tutte le informazioni necessarie agli interessati in relazione ai diritti di accesso ai dati personali ed agli usi consentiti dalla legge.

Gli interessati dovranno fornire consenso scritto al trattamento dei propri dati da parte di Namirial S.p.A..

9.4 Modalità del trattamento

Tutte le informazioni personali raccolte durante l'erogazione del servizio di PEC vengono trattate dal gestore con tutte le misure di sicurezza descritte all'interno del presente manuale allo scopo di prevenirne la perdita, evitarne usi illeciti o accessi da parte di personale non espressamente autorizzato.

I dati in formato elettronico vengono mantenuti in appositi data server adibiti allo scopo e su supporti ottici conservati in armadi protetti.

I dati in formato cartaceo saranno conservati negli archivi cartacei presso la sede centrale di Namirial S.p.A., cui avranno accesso solo gli incaricati espressamente autorizzati.

9.5 Finalità del trattamento

I dati personali vengono raccolti per le seguenti finalità:

- erogazione del servizio di posta certificata;
- gestione del rapporto contrattuale
- eventuali controlli sulla qualità del servizio e sulla sicurezza del sistema;

- scopi di natura commerciale per l'invio di informative legate al lancio di prodotti e/o servizi analoghi o direttamente legati al servizio di PEC. Per questa tipologia di comunicazioni l'interessato ha la possibilità di opporsi al trattamento.

I dati raccolti non verranno in alcun modo utilizzati per attività di profiling da parte di Namirial S.p.A. e non verranno venduti o forniti a terze parti per usi commerciali o di marketing o per statistiche ed indagini di mercato.

9.6 Altre forme di utilizzo dei dati

Namirial S.p.A., per motivi d'ordine pubblico, nel rispetto delle disposizioni di legge per la sicurezza e difesa dello Stato, per la prevenzione, accertamento e/o repressione dei reati,

I dati personali potranno essere usati con finalità diverse rispetto alla fornitura dei servizi di PEC ed essere comunicati a soggetti pubblici, quali forze dell'ordine, autorità pubbliche e autorità giudiziarie, per motivi d'ordine pubblico, nel rispetto delle disposizioni di legge per la sicurezza e difesa dello Stato, per la prevenzione, accertamento e/o repressione dei reati.

9.7 Sicurezza dei dati

Come previsto dalla normativa vigente, Namirial S.p.A. adotta tutte le misure di sicurezza necessarie al fine di ridurre al minimo:

- i rischi di distruzione o perdita, anche accidentale, dei dati;
- i rischi di danneggiamento risorse hardware su cui sono memorizzati i dati;
- i rischi di danneggiamento ai locali nei quali sono custoditi i dati;
- l'accesso non autorizzato ai dati;
- le modalità di trattamento non consentite dalla legge o dai regolamenti aziendali

Attraverso le misure di sicurezza adottate dal gestore (descritte al par. 7.3) vengono garantite:

- l'integrità e la salvaguardia dei dati contro manomissioni o modifiche da parte di soggetti non autorizzati
- la disponibilità dei dati e quindi la loro fruibilità;
- la riservatezza dei dati cioè la garanzia che le informazioni vengano accedute dalle sole persone autorizzate.

Senigallia 16/10/2007

Namirial S.p.A.
Il legale rappresentante
(Dr. Claudio Gabellini)