Manuale Operativo

Posta Elettronica Certificata

Namirial S.p.A.

Gestore	**Namirial S.p.A.**	Modello Doc.	**NAMIRIAL-PEC-MO**
Redatto da	**Dott.sa Marina Pettinari**	Nota di riservatezza	**DOCUMENTO PUBBLICO**
Revisionato da	**Dott. Giuseppe Benedetti**	Revisione	**1.9**
Approvato da	**Dott. Paolo Giacometti**	Data emissione	**25/09/2014**

Namirial S.p.A.
Il legale rappresentante
(Dott. Paolo Giacometti)

INDICE GENERALE

INDICE DELLE FIGURE

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*	
1.3	*Cap. 4.3.1.*	*E' stata inserita la data di Certificazione Qualità UNI EN ISO 9001:2000*	*19/05/2008*
	Cap. 4.3.1.	*Inserita parte descrittiva di come Namirial gestisce i messaggi provenienti da indirizzi email non certificati.*	
	Cap. 5.1	*E' stata inserita la possibilità di acquisto di caselle base da 50 Mbytes oltre a quelle da 100 Mbytes*	
	Cap. 7.4.2.	*Aggiornata la spiegazione della gestione dei backup da parte di Namirial.*	
1.4	*Cap.2.2*	*E' stata resa più snella la descrizione dell'azienda gestore.*	*10/12/2008*
	Cap.4.3.1	*Illustrato in dettaglio il servizio di "inoltro" messaggi provenienti da caselle non certificate.*	
	Cap. 5.3	*Inserita la possibilità di trasmissione della documentazione tramite email e con firma digitale.*	
	Cap.5.4.1	*Specificato accesso tramite client di posta che rispondono ai requisiti richiesti.*	
	Cap.5.7	*Inserito periodo minimo di conservazione da parte del Gestore delle richieste di cancellazione account/dominio.*	
	Cap.6.9.2	*E' stata modificata l'indicazione della Classe di riferimento delle porte blindate e indicazioni relative al sistema di videosorveglianza.*	
	Cap.8.1	*Sono stati inseriti ulteriori punti per una maggiore completezza relativi agli obblighi del gestore.*	
	Cap.8.2	*Sono stati inseriti ulteriori punti per una maggiore completezza relativi agli obblighi del titolare.*	
1.5	*Cap.2.1*	*Dati identificativi: è variato il capitale sociale dell'azienda da €1.000.000,00 i.v. a €6.500.000,00 i.v.*	*29/10/2009*
	Cap.5.1.7	*Uffici di Registrazione: è stata inserita la possibilità per il Gestore di avvalersi di Uffici di Registrazione per l'identificazione e validazione della documentazione per l'erogazione del servizio pec*	
1.6	*Rivisitazione*	*Sono state sostituite le diciture CNIPA con DigitPA, nei punti in cui si è reso necessario.*	*01/07/2011*
	Cap5.1.7	*Visto le modificazioni al CAD come da decreto legge 30 dicembre 2010 m. 235, sono state aggiornate le mansioni dell'Ufficio di registrazione ed ha combiato denominazione, sono stati aggiornati tutti i riferimenti nel manuale.*	
	Cap.5.1	*Lo standard delle caselle è stato portato ad 1 Gigabytes*	

Versione	*Descrizione della revisione*		*Data*
	Cap.5.1.1 *Cap.5.1.2* *Cap.5.1.3*	*Viene specificato che sono previste delle limitazioni al traffico solo per l'utilizzo della casella per invii massivi*	
	Cap. 5.1.4	*È stato specificato che l'utilizzo del pannello di richiesta delle caselle PEC è previsto solo per le persone autorizzate (LRA/IR Rivenditori/Distributori)*	
	Cap. 5.3	*È stata inserita la procedura di attivazione dei servizi pec tramite compilazione diretta della modulistica scaricata dal sito*	
	Cap. 5.6	*È stata indicata la reperibilità della email per la richiesta dei file di LOG sul sito*	
	Cap.5.7	*È stata rivista la comunicazione per la chiusura di caselle pec ai Titolari*	
	Cap. 5.8.1	*È stata sostituita l'immagine del programma di Trouble Ticketing con la nuova versione*	
	Cap. 6.9.2	*È stato sostituito il badge magnetico con la chiave trasponder su lettore di prossimità per l'accesso alla sala macchine*	
	Cap.6.4	*E' stata aggiornata la versione OpenPec*	
	Cap.9.2	*E' variato il Responsabile del trattamento dei dati personali*	
1.7	*Cap.5.1.1* *Cap.5.1.2* *Cap.5.1.3*	*Sono state previste limitazioni al traffico per l'utilizzo della casella PEC: limiti alla facoltà di invio di più di 1000 comunicazioni al giorno e limiti alla facoltà di effettuare invii massivi di comunicazioni via PEC.*	*05/08/2013*
	Cap.8.2	*Integrazione degli obblighi e responsabilità ricadenti sui titolari e indicazione delle conseguenze, ricadenti sui medesimi, in caso di violazione.*	
1.8	*Cap 5.1.1* *Cap 5.1.2* *Cap 5.1.3*	*Integrata la definizione di "invio massivo" e rivisti i limiti di invio giornalieri.*	*14/10/2013*
	Cap 5.4.1	*Sono stati inseriti i parametri di configurazione del servizio.*	
	Cap 5.4.2	*Inserito il link alla webmail.*	
	Cap 8.2	*Modificato il testo da IGPEC a Elenco pubblico dei Gestori, con aggiunta del link dove consultarlo.*	
1.9		*Ristrutturazione generale del documento*	*12/09/2014*
	Cap 2.2	*Aggiornata la descrizione sintetica del Gestore*	
	Cap 2.3	*Variazione del Responsabile del Servizio e del Manuale Operativo*	
	Cap 4.2	*Eliminazione del paragrafo accorpando i contenuti con il Glossario dei termini*	
	Cap 5.1 *Cap 5.2 ss*	*Ristrutturazione della descrizione sintetica del servizio offerto.*	

Versione	*Descrizione della revisione*		*Data*
	Cap 5.6.2.1	*Adeguamento della lunghezza e complessità della password*	
	Cap 7.4.2	*Aggiornata la Gestione dei backup*	
	Cap 8	*Accorpamento degli Obblighi e Responsabilità del Gestore e del Titolare in un unico capitolo.*	

1 INFORMAZIONI DI CARATTERE GENERALE

1.1 OBIETTIVO

Il documento in oggetto rappresenta il Manuale Operativo del servizio di Posta Elettronica Certificata (PEC) del Gestore 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 scaricare dal sito del gestore al link seguente: http://www.sicurezzapostale.it/docs/manualeoperativo.pdf.

1.2 GLOSSARIO E DEFINIZIONE DEI TERMINI

Termine	Definizione
PEC	Posta Elettronica Certificata
CNIPA	Centro Nazionale per l'Informatica nella Pubblica Amministrazione
DigitPA	Ente nazionale per la digitalizzazione della Pubblica Amministrazione (ex CNIPA - Centro Nazionale per l'Informatica nella Pubblica Amministrazione)
AgID	Agenzia per l'Italia Digitale (ex DigitPA)
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 è assegnata una casella di PEC
Dominio di Posta Elettronica Certificata	dominio di posta elettronica certificata che contiene unicamente caselle di posta elettronica certificata, anche detto "dominio certificato" o dominio di PEC
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. Abbreviato in IGPEC.
Casella di Posta Elettronica Certificata	la casella di posta elettronica posta all'interno di un dominio di PEC ed alla quale è associata una funzione che rilascia ricevute di avvenuta consegna al ricevimento di messaggi di PEC
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.
Riferimento temporale	informazione contenente la data e l'ora che viene associata ad un messaggio di posta elettronica certificata
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

Termine	Definizione
Tamper evidence	sistema per segnalare qualsiasi tentativo di manomissione fisica del 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	acronimo di Mail Transfer Agent. Si tratta del modulo che ha il compito di evadere le richieste di invio/ricezione dei messaggi di posta elettronica ordinaria e certificata
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.
LDIF	acronimo di LDAP Data Interchange Format. E' uno standard di interscambio dati in formato testo usato per la rappresentazione dei contenuti di una directory LDAP e per le richieste di aggiornamento degli stessi.
SNMP	Simple Network Management Protocol. E' un protocollo utilizzato per la gestione ed il monitoraggio degli apparati nonché della struttura di una rete.
HSM	Hardware Security Module. E' un dispositivo hardware per la generazione, la memorizzazione e la protezione sicura di una coppia di chiavi di firma.
NTP	Network Time Protocol. E' un protocollo utilizzato per sincronizzare gli orologi dei computer all'interno di una rete a commutazione di pacchetto, quindi con tempi di latenza variabili ed inaffidabili
LMTP	Local Mail Transport Protocol. E' un protocollo utilizzato per la scrittura dei messaggi di PEC nelle caselle dei titolari
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).
IR	Soggetto incaricato dal Gestore all'Identificazione, Registrazione e Supporto dei Richiedenti/Titolari di caselle PEC

Termine	Definizione
LRA	Local Registration Authority. La persona fisica o giuridica, delegata dal Gestore allo svolgimento delle operazioni di Identificazione, Registrazione e Supporto dei Titolari di caselle di PEC
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 del trattamento dati	Persona fisica, persona giuridica, pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare, al trattamento dei dati personali
Incaricato al trattamento dati	Persona fisica autorizzata a compiere operazioni di trattamento dal titolare del trattamento dati o dal responsabile
Interessato al trattamento dati	Persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali
Punto di Accesso (PdA)	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 (PdR)	il sistema che riceve il messaggio all'interno di un dominio di posta elettronica 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 (PdC)	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 (RdA)	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

Termine	Definizione
Avvisio di Non Accettazione (AdNA)	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 (RPdC)	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 (RdAC)	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 (RdAC completa)	la ricevuta nella quale sono contenuti i dati di certificazione ed il messaggio originale
Ricevuta Breve di Avvenuta Consegna (RdAC breve)	la ricevuta nella quale sono contenuti i dati di certificazione ed un estratto del messaggio originale;
Ricevuta Sintetica di Avvenuta Consegna (RdAC sintetica)	la ricevuta che contiene i dati di certificazione
Avviso di Mancata Consegna (AdMC)	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 (BdT)	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 (BdA)	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

1.3 VERSIONE DEL MANUALE OPERATIVO E SUCCESSIVE REVISIONI

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 processi interni ed esterni di erogazione del servizio di posta elettronica 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 del Gestore Namirial S.p.A. e sottoposta ad approvazione degli organi competenti (AgID).
Il Cliente o il Titolare è tenuto a consultare la versione più aggiornata del Manuale Operativo, pubblicato sul sito internet del Gestore come riportato al successivo §1.4.

1.4 INDIRIZZO WEB DEL GESTORE DAL QUALE SCARICARE IL MANUALE

Il presente manuale è pubblicato sul sito web del Gestore ed è scaricabile dal link seguente: http://sicurezzapostale.it/docs/manualeoperativo.pdf. Il Gestore Namirial S.p.A. si impegna a pubblicare sul sito la versione aggiornata ed approvata del manuale operativo.

1.5 TABELLA DI CORRISPONDENZA

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

Circolare CNIPA/CR/49 del 24/11/2005 2 – Requisiti tecnico-organizzativi, § 2.1	**Manuale Operativo**
a) Dati identificativi del Gestore	**2.1**
b) Indicazione del Responsabile del Manuale Operativo	**2.3**
c) Riferimenti normativi necessari per la verifica dei contenuti	**3**
d) Indirizzo del sito web del gestore ove il Manuale Operativo è pubblicato e scaricabile	**1.4**
e) Indicazione delle procedure nonché degli standard tecnologici e di sicurezza utilizzati dal Gestore nell'erogazione del servizio	**7**
f) Definizioni, abbreviazioni e termini tecnici	**1.2**
g) Descrizione sintetica del servizio offerto	**5.1**
h) Descrizione delle modalità di reperimento e di presentazione delle informazioni presenti nei log dei messaggi	**5.9**
i) Indicazione del contenuto e delle modalità dell'offerta da parte del Gestore	**5.2**
j) Indicazione delle modalità di accesso al servizio	**5.7**
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	**5.13**
l) Indicazione delle condizioni di fornitura del servizio	Errore. L'origine riferimento non è stata trovata.
m) Indicazione delle modalità di protezione dei dati dei titolari	**9**
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, di seguito, le informazioni identificative ed una descrizione sintetica delle attività svolte e dei principali settori nei quali opera.

2.1 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 (utilizzate 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:	6.500.000 € 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 dell'Information Technology orientando la propria produzione di software verso le nuove e sempre più manifeste esigenze di adeguamento del sistema produttivo italiano ai nuovi scenari economici fortemente competitivi e globalizzati.
All'interno di una struttura economica nazionale caratterizzata per la gran parte dall'attività di piccole e medie realtà imprenditoriali si è ritenuto essenziale sviluppare soluzioni e servizi software accessibili anche sulla rete internet ed in grado di rispondere alle problematiche tecnologico-innovative emergenti in maniera professionale mantenendo una grande economicità di esercizio.
La società ha sede in una moderna struttura di oltre duemila metri quadrati, dove 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 in genere di server farm.

Namirial S.p.A. è:

Autorità di Certificazione accreditata presso AgID (ex DigitPA) ed è autorizzata all'emissione di certificati qualificati conformi alla Direttiva Europea 1999/93/CE, Certificati CNS e Marche Temporali.

Gestore di PEC, dal 26/02/2007, accreditato presso AgID (ex DigitPA) ed autorizzato alla gestione di **caselle** e **domini** di Posta Elettronica Certificata.

Certificata UNI EN ISO 9001:2008. Namirial ha conseguito il certificato n. 223776 rilasciato da **Bureau Veritas Italia S.p.A.**

Certificata ISO/IEC 27001:2005. Namirial ha conseguito il certificato n. IND12.2513U rilasciato da **Bureau Veritas Italia S.p.A.**

Certificata da Adobe. Da Giugno 2013 Namirial è **membro dell'AATL** (Adobe Approved Trust List).

2.2.1 CERTIFICAZIONE ISO 9001

Namirial S.p.A. ha ottenuto la certificazione UNI EN ISO 9001:2000 in data 28.11.2007 ed ha conseguito il certificato n. 223776 presso la Bureau Veritas Italia S.p.A. che l'ha giudicata conforme ai requisiti della norma ISO 9001:2000 con il seguente scopo: *"progettazione, elaborazione ed assistenza post vendita di software, piattaforme gestionali e siti internet. L'erogazione di servizi hosting e collocation per centri assistenza amministrativa e fiscale. L'erogazione del servizio di posta elettronica certificata. Settore/i EA di attività: 33".*

2.2.2 CERTIFICAZIONE ISO/IEC 27001:2005

Namirial S.p.A. ha ottenuto la certificazione UNI EN ISO 27001:2005 in data 19.03.2012 ed ha conseguito il certificato n. IND12.2513U presso la Bureau Veritas Italia S.p.A. che l'ha giudicata conforme ai requisiti della norma ISO/IEC 27001:2005 con il seguente scopo: *"realizzazione di soluzioni di firma elettronica avanzata rivolte alle Pubbliche Amministrazioni ed enti privati mediante utilizzo di software di acquisizione biometrica e sistemi di cifratura a norma di legge".*

2.2.3 CERTIFICAZIONE AATL

La Certification Authority Namirial, da Giugno 2013, è inserita nell'elenco AATL (Adobe Approved Trust List).

2.3 RESPONSABILE DEL SERVIZIO E DEL MANUALE OPERATIVO

Il responsabile del presente manuale operativo è:

Dott. Giuseppe Benedetti

Il responsabile può essere contattato ai seguenti recapiti:

telefono: 071-63494
email: serviziopec@sicurezzapostale.it
indirizzo: Via Caduti sul lavoro, 4 - 60019 Senigallia (AN)

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

2.4 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, via email o via web ai seguenti recapiti:

telefono: 071-63494
email: assistenzatecnica@sicurezzapostale.it
web: www.sicurezzapostale.it

2.5 INFORMAZIONI COMMERCIALI

Per ricevere informazioni commerciali riguardanti le offerte di di Namirial S.p.A. è possibile mettersi in contatto con il Gestore via telefono, via email o via web ai seguenti recapiti:

telefono: 071-63494
email: commerciale@sicurezzapostale.it
web: www.sicurezzapostale.it

3 RIFERIMENTI NORMATIVI

- Decreto del Presidente della Repubblica 28 dicembre 2000 n. 445
- Decreto Legislativo 30 giugno 2003 n. 196, "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.
- CAD 30/12/2010 n.235 - Modifiche ed integrazioni al decreto legislativo 7 marzo 2005, n. 82, recante Codice dell'amministrazione digitale, a norma dell'articolo 33 della legge 18 giugno

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 A/R. 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 (detti buste), ricevute ed avvisi che vengono inviati:

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

Ogni busta, ricevuta o avviso 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 DigitPA 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 DigitPA, 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 i quali riportano al loro interno la traccia delle comunicazioni avvenute. Tali LOG hanno la stessa validità legale delle ricevute della raccomandata e possono essere richiesti dagli utenti finali in qualsiasi momento.

4.2 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.

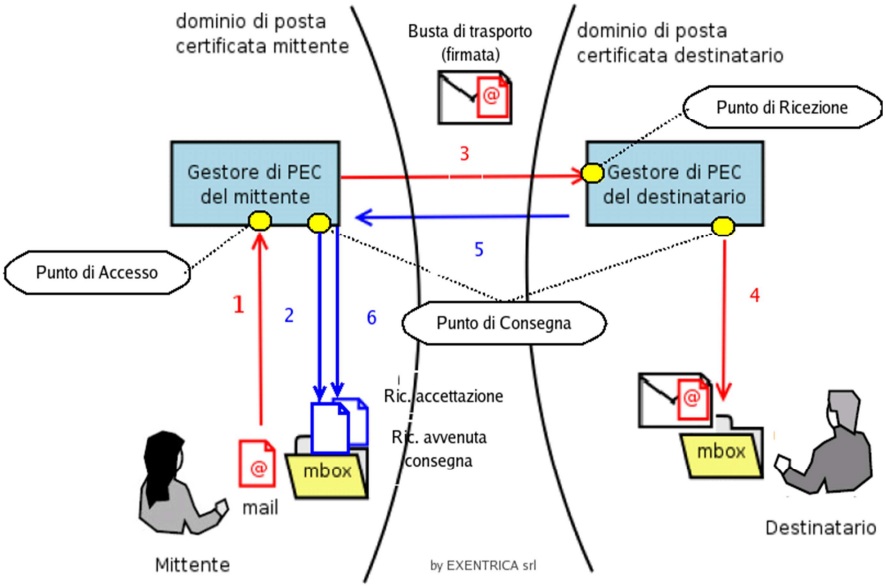

Figura 1 - Funzionamento del sistema di PEC

Nello schema sono visualizzati 2 utenti (Mittente e Destinatario) ognuno dei quali appartiene ad un proprio dominio di Posta Elettronica Certificata: il Mittente deve spedire un messaggio di PEC al Destinatario.

1) Il messaggio originale arriva al Punto di Accesso del Gestore PEC del Mittente.
2) Il Gestore PEC del Mittente, dopo aver effettuato i controlli formali e verificato che il messaggio non contenga virus, emette ed invia al Mittente la Ricevuta di Accettazione.
3) Il messaggio originale viene racchiuso in una Busta di Trasporto, la quale viene firmata dal Gestore del Mittente attraverso un apposito dispositivo e successivamente viene spedita al Punto di Ricezione del Gestore PEC del Destinatario.
4) Il Gestore PEC del Destinatario riceve, al Punto di Ricezione, la Busta di Trasporto, ne verifica l'attendibilità della firma controllando che la stessa non sia stata alterata durante il tragitto e la 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**: è la ricevuta di default. Oltre ai dati di certificazione contiene, come allegato, il messaggio originale completo di eventuali allegati in esso originariamente contenuti;
- **breve**: oltre ai dati di certificazione contiene, come allegato, il messaggio originale nel quale gli allegati originariamente presenti, vengono sostituiti dallo loro codifica hash;
- **sintetica**: contiene solamente i dati di certificazione senza il messaggio originale in allegato.

4.2.1 DETTAGLI E CASI PARTICOLARI

La comunicazione riportata in Figura 1 descrive un tipico scambio tra Mittente e Destinatario. Tuttavia, la comunicazione tra gli utenti è corredata da una serie di ricevute, buste ed avvisi tra utente e Gestore e tra Gestore e Gestore, che servono a garantire la correttezza della trasmissione, a rilevare la presenza di anomalie e/o a gestire casi particolari di seguito descritti.

4.2.1.1 RICEVUTA DI PRESA IN CARICO

Per mantenere la tracciabilità delle Buste di Trasporto, il Gestore di PEC del Destinatario invia una Ricevuta di Presa in Carico al Gestore del Mittente, ogni qualvolta riceve di una Busta di Trasporto proveniente da un dominio certificato esterno.

4.2.1.2 MESSAGGI INVIATI A INDIRIZZI EMAIL NON CERTIFICATI

Ogni messaggio originale inviato a indirizzi email non certificati arriverà a destinazione imbustato all'interno di una Busta di Trasporto.

4.2.1.3 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 una Busta di Anomalia.
Il Gestore Namirial S.p.A. non consente l'ingresso verso caselle PEC di messaggi provenienti da caselle di posta elettronica convenzionale (non certificate).
Il titolare della casella, attraverso il servizio di "Inoltro dei messaggi non certificati", ha però la possibilità di reindirizzare tali messaggi verso una casella di posta elettronica convenzionale di sua scelta. Tale servizio viene attivato attraverso l'interfaccia di gestione della casella.
Una volta completata l'operazione, tutti i messaggi convenzionali diretti alla casella PEC verranno indirizzati in maniera automatica verso la casella convenzionale indicata.

4.2.1.4 MESSAGGIO FORMALMENTE NON CORRETTO

Il Gestore invia al proprio utente (il Mittente) un **Avviso di Non Accettazione** quando il sistema rileva delle malformazioni e/o non conformità alla normativa all'interno del messaggio originale inviato dal proprio utente (il Mittente) come ad esempio la presenza del campo Ccn:.

4.2.1.5 PRESENZA DI VIRUS

Un virus contenuto nel testo o negli allegati di una mail certificata può essere rilevato dal Gestore PEC del mittente o dal Gestore PEC del destinatario.
Nel caso in cui sia il Gestore PEC del Mittente a rilevare il virus, viene inviato al mittente un **Avviso di Non Accettazione per Virus**.
Nel caso in cui sia il Gestore del Destinatario a rilevare il virus (al Punto di Ricezione), viene inviato al Gestore del mittente un avviso di rilevazione virus. Quest'ultimo, da parte sua, quando riceve un avviso di rilevazione virus provvede ad emettere e consegnare al proprio utente (cioè il mittente del messaggio originale) un A**vviso di Mancata Consegna per Virus**.
I messaggi contenenti i virus vengono conservati dal Gestore per un periodo non inferiore a 30 mesi.

4.2.1.6 SUPERAMENTO DEI TEMPI MASSIMI PREVISTI

Successivamente all'invio di una Busta di Trasporto da parte del Gestore del Mittente, il Gestore del Destinatario potrebbe, per motivi non meglio specificati, non essere in grado di scambiarsi informazioni con il Gestore Mittente (Ricevuta di Presa in Carico, Ricevuta di Avvenuta Consegna, Avviso di Mancata Consegna, etc etc). Se ciò si dovesse verificare nelle 12 ma entro le 24 ore successive all'invio, il Gestore del Mittente è tenuto a informarlo tramite l'invio di informazioni utili a conoscere l'esito delle proprie spedizioni.
Il Gestore di PEC si comporta nel seguente modo:

- Trascorse 12 ore dalla spedizione, durante le quali non si è avuta notizia della Busta di Trasporto (cioè non è arrivata alcuna comunicazione da parte del Gestore del Destinatario in termini di ricevute), il Gestore del Mittente emette ed invia al proprio utente un **Avviso di mancata consegna per superamento tempo massimo**. Nell'avviso viene fatto presente che il messaggio firmato *"non è stato consegnato nelle prime dodici ore dal suo invio"* ma non si esclude che questo possa avvenire nelle successive 12 ore.
- Trascorse altre 12 ore, successive al primo avviso, senza che si abbia ricevuto informazioni dal Gestore del Destinatario, il Gestore del Mittente emette ed invia al proprio utente un secondo **Avviso di mancata consegna per superamento tempo massimo**. Nell'avviso viene specificato al Mittente che il messaggio firmato *"non è stato consegnato nelle ventiquattro ore successive al suo invio. Si ritiene che la spedizione debba considerarsi non andata a buon fine"*.

5 IL SERVIZIO PEC DI NAMIRIAL S.P.A.

Di seguito viene delineato il servizio PEC del Gestore Namirial S.p.A. e se ne descrivono le caratteristiche principali.

5.1 CARATTERISTICHE DELL'OFFERTA STANDARD

L'offerta standard di Namirial S.p.A. è rivolta ai privati, ai professionisti, agli enti pubblici ed alla aziende di tutto il territorio nazionale. Il Gestore si riserva il diritto di modificare nel futuro le caratteristiche dell'offerta di seguito riportata.

La **casella standard** ha una capacità di **1 Gigabytes** ed è soggetta a canone in base alle offerte descritte di seguito. Ciascuno può avere a disposizione un numero illimitato di caselle di posta elettronica certificata.
Si ricorda che in base alla normativa vigente i messaggi sono da considerarsi ricevuti quando sono recapitati nella casella dell'utente e non quando l'utente li scarica e/o li consulta.
E' evidente che raggiunto il limite di capienza della casella PEC, gli ulteriori messaggi vengono rifiutati e non recapitati. Ciò premesso, il Gestore consiglia e raccomanda di **scaricare regolarmente** la casella di Posta Elettronica Certificata.

5.2 DETTAGLI OFFERTA, CONDIZIONI FORNITURA E TARIFFE APPLICATE

Per i dettagli e i costi dei vari servizi di seguito descritti nonché sulle modalità di sottoscrizione agli stessi, si rimanda al sito http://www.sicurezzapostale.it/richiesta-adesione.asp.

5.2.1 SICUREZZAPOSTALE SMART

E' l'offerta "entry-level" del Gestore e prevede la fornitura, dietro pagamento di un canone, di caselle standard di posta elettronica certificata su dominio **sicurezzapostale.it**. La casella è accessibile tramite WebMail (HTTPS) ma anche attraverso i più comuni client di posta (SMTP-S, POP3-S, IMAP-S) quali Outlook Express, Outlook, Eudora, Thunderbird, etc etc.

5.2.2 SICUREZZAPOSTALE BUSINESS

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

- registrazione e mantenimento di un sottodominio, al dominio sicurezzapostale.it, personalizzato.
- caselle standard di PEC sul sottodominio certificato.
- accessibilità delle casella tramite WebMail (HTTPS) ma anche attraverso i più comuni client di posta (SMTP-S, POP3-S, IMAP-S) quali Outlook Express, Outlook, Eudora, Thunderbird, etc etc.

Per questo tipo di offerta sono previsti i seguenti pagamenti aggiuntivi:

- canone annuale per la registrazione e mantenimento sottodominio personalizzato;

5.2.3 SICUREZZAPOSTALE BUSINESS ADV

E' la soluzione ideale per le organizzazioni strutturate e le aziende di una certa dimensione e comprende i seguenti servizi:

- possibilità di registrazione e mantenimento di un dominio personale, aziendale o istituzionale
- attivazione di un dominio certificato di terzo livello sul dominio personale, aziendale o istituzionale

- caselle standard di PEC sul dominio certificato
- accessibilità tramite WebMail (HTTPS) ma anche attraverso i più comuni client di posta (SMTP-S, POP3-S, IMAP-S) quali Outlook Express, Outlook, Eudora, Thunderbird, etc etc.

Per questo tipo di offerta sono previsti i seguenti pagamenti aggiuntivi:

- 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

5.2.4 SERVIZI AGGIUNTIVI

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

- Spazio aggiuntivo sulla casella SicurezzaPostale Smart, SicurezzaPostale Business, SicurezzaPostale Business ADV.
- Possibilità di concordare con il Gestore la gestione e l'invio di volumi messaggi giornalieri di particolare entità.
- Possibilità di acquisto di licenze per la gestione automatica delle ricevute dei messaggi di PEC.
- Personalizzazione grafica della WebMail.
- Pannello di controllo per autogestione proprie caselle (solo per Rivenditore/Distributore LRA/IR).

5.3 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 raccoglie le informazioni necessarie per identificare il cliente che ha richiesto di aderire al servizio con le relative informazioni riguardo a: offerta, numero di caselle, eventuali servizi opzionali.
Una volta acquisite tali informazioni e verificatene 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, dal Gestore Namirial S.p.A. che rimane comunque il responsabile della qualità del servizio nei confronti del proprio cliente.

5.3.1 LOCAL REGISTRATION AUTHORITY (LRA)

Il Gestore si avvale, sul territorio, di Uffici di Registrazione, che, anche tramite loro incaricati (IR), svolgono le seguenti attività di interfaccia tra il Gestore stesso e il Richiedente:

- Identificazione e pre-registrazione del Richiedente;
- Validazione della documentazione necessaria per la richiesta dell'account di posta elettronica certificata;
- Supporto al Titolare e al Gestore nel rinnovo, revoca e sospensione degli account.

Le LRA sono attivate dal Gestore a seguito di un adeguato addestramento del personale, che potrà svolgere le funzioni di identificazione, ed eventualmente registrazione, anche presso il Richiedente.
Il Gestore verifica la rispondenza tra le procedure utilizzate dalla LRA e dagli operatori (IR) addetti alla Registrazione con quanto stabilito nel presente manuale.

5.3.2 OBBLIGHI DEL LOCAL REGISTRATION AUTHORITY (LRA)

La LRA, nella persona dell'Incaricato della Registrazione Titolare (IR), è tenuto a garantire:

- la verifica dell'identità del Richiedente e la registrazione dei dati dello stesso;
- che la LRA terrà direttamente i rapporti con il Richiedente, Titolare dell'account pec, ed è tenuto ad informarlo circa le disposizioni contenute nel presente Manuale Operativo.

- che lo stesso Richiedente sia espressamente informato riguardo alla necessità di protezione della segretezza della password;
- la comunicazione al Gestore di tutti i dati e documenti acquisiti in fase di identificazione allo scopo di attivare la procedura di emissione dell'account pec;
- la verifica e l'inoltro al Gestore delle richieste di revoca o di sospensione attivate dal Titolare presso la LRA;
- che le operazioni relative al servizio di rilascio, affidate alla LRA dal Gestore, siano effettuate secondo le regole e procedure descritte nel presente Manuale Operativo;
- la rispondenza del proprio sistema di sicurezza dei dati alle misure minime di sicurezza per il trattamento dei dati personali, Dlg 30 giugno 2003, n.196.

5.4 IDENTIFICAZIONE

Il Gestore verifica l'identità del Richiedente prima di procedere al rilascio dell'account PEC. La procedura di identificazione comporta che il Richiedente sia riconosciuto personalmente dai soggetti di cui al § 5.4.1, che ne verificheranno l'identità attraverso il controllo della Carta d'Identità o di un documento ad essa equipollente (cfr. art. 35 comma 2 del DPR 28 dicembre 2000 n. 445) in corso di validità.

5.4.1 SOGGETTI ABILITATI AD EFFETTUARE L'IDENTIFICAZIONE

L'identità del Richiedente può essere accertata da uno dei soggetti di seguito indicati:

- il Gestore, anche tramite suoi Incaricati (IR)
- una LRA, anche tramite suoi Incaricati (IR)
- un Pubblico Ufficiale.

5.4.2 PROCEDURE PER L'IDENTIFICAZIONE

L'identificazione è effettuata da uno dei soggetti indicati al § 5.4.1.
Il soggetto che effettua l'identificazione verifica l'identità del Richiedente tramite il riscontro con uno dei seguenti documenti, valido e non scaduto, secondo quanto previsto dall'art. 35 comma 2 del DPR 28 Dicembre 2000 n. 445):

- Carta d'Identità
- Passaporto
- Patente di guida
- Patente nautica
- Libretto di pensione
- Patentino di abilitazione alla conduzione di impianti termici
- Porto d'armi

Sono ammesse ulteriori tessere di riconoscimento oltre a quelle indicate, purché munite di fotografia e di timbro, rilasciate da una Amministrazione dello Stato.
L'identificazione da parte dei Pubblici Ufficiali può essere altresì effettuata in base a quanto disposto dalle normative che disciplinano la loro attività, ivi comprese le disposizioni di cui al D.L. 3 maggio 1991, n. 143 e successive modifiche ed integrazioni.

5.5 NOMI DEI DOMINI E DENOMINAZIONE DELLE CASELLE

I nomi dei domini e le denominazioni delle caselle possono essere scelti ed indicati dal cliente. Tuttavia il Gestore si riserva il diritto di rifiutarli nel caso in cui li ritenga offensivi, irrispettosi o lesivi nei confronti di terzi.

5.6 RILASCIO DELLE CASELLE PEC

Nella figura seguente riportiamo uno schema del flusso che descrive il rilascio di una casella di posta elettronica certificata.

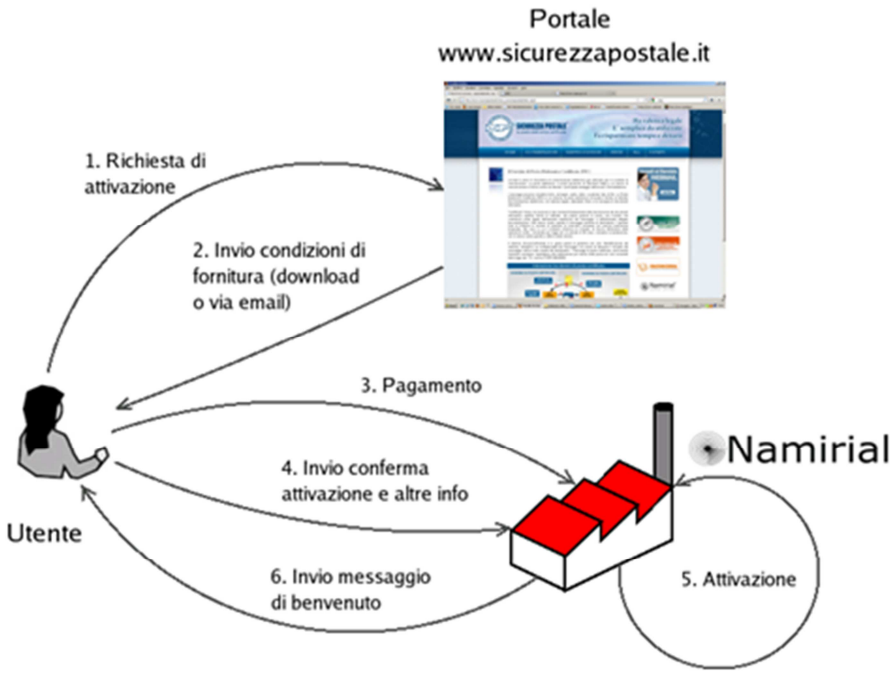

Figura 2 - Flusso dell'attivazione di una casella di PEC

5.6.1 RICHIESTA DI ATTIVAZIONE DELLA CASELLA

Per poter una casella do PEC, il richiedente deve scaricare i seguenti moduli (passi 1 e 2 di Figura 2):

- "Richiesta di Adesione"
- "Condizioni generali di contratto"
- "Informativa sui dati personali"

disponibili al seguente link: http://www.sicurezzapostale.it/richiesta-adesione.asp.
Una volta presa visione delle "Condizioni generali di contratto" e della "Informativa sui dati personali", il richiedente compila il modulo "Richiesta di Attivazione" con i propri dati anagrafici (in base al fatto che il richiedente sia una persona fisica, un'azienda, un ente, etc etc), firma la richiesta in forma autografa o digitale e la invia al Gestore unitamente alla copia di un documento di identità in corso di validità (se la richiesta è firmata in forma autografa) e alla copia del pagamento effettuato secondo le modalità riportate nella richiesta stessa (passo 3 di Figura 2).
L'invio del modulo "Richiesta di Adesione" al Gestore può avvenire tramite (passo 4 di Figura 2):

- **Fax o Raccomandata a/r:** alla modulistica, compilata e firmata, dovrà essere allegata fotocopia del documento di identità del titolare in corso di validità.
- **Email**: la scansione della modulistica firmata in forma autografa, con allegata fotocopia del documento di identità, oppure file della modulistica in formato PDF firmato digitalmente.

5.6.2 ATTIVAZIONE DELLA CASELLA

Il Gestore, dopo aver verificato la correttezza e veridicità delle informazioni inviate dal cliente, attiva la casella ed, eventualmente, i domini richiesti (passo 5 di Figura 2). Il Gestore invia al richiedente una email di benvenuto a conferma dell'avvenuta attivazione (passo 6 di Figura 2) nella quale vengono forniti tutti i dettagli del servizio erogato. In particolare vengono inviati i parametri di accesso al sistema:

- login
- password
- server smtp
- server pop/imap
- indirizzo della webmail
- Informazioni circa recupero dei log, richiesta di assistenza, modifica della password, etc etc.

5.6.2.1 RACCOMANDAZIONI PER GLI UTENTI

In aggiunta a quanto riportato nel § 8.2, elenchiamo qui di seguito un vademecum con alcuni suggerimenti per un utilizzo corretto e sicuro della posta elettronica certificata del Gestore 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 di posta elettronica.
- Poiché le email certificate si intendono ricevute non appena consegnate nella mailbox del destinatario, si suggerisce di controllare la propria casella con una certa frequenza. In caso di necessità, si consiglia di salvare e successivamente eliminare i messaggi più vecchi al fine di avere sempre dello spazio a disposizione evitando così che i messaggi di PEC vengano respinti per casella piena.
- Si consiglia di modificare frequentemente la password. In particolare si suggerisce di modificarla al primo accesso al servizio e successivamente almeno ogni 90 giorni. Per la scelta della password si consiglia di usare una sequenza di almeno 12 caratteri tra caratteri maiuscoli/minuscoli, numeri e caratteri speciali 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.
- Configurare la postazione di lavoro in modo da soddisfare i requisiti minimi di sicurezza.

5.7 ACCESSO AL SERVIZIO

La casella PEC può essere utilizzata sia attraverso i più diffusi client di posta, sia attraverso il web utilizzando la WebMail. Le guide per la configurazione e l'uso della casella PEC sono disponibili nella sezione Documentazione del sito del Gestore raggiungibile dal link seguente: http://www.sicurezzapostale.it/servizio-sicurezza-postale.asp

5.7.1 ACCESSO ATTRAVERSO I CLIENT DI POSTA

Il titolare può accedere al sistema attraverso i più comuni client di posta (quali ad esempio Thunderbird, Eudora, Outlook Express, Outlook) che rispondono ai requisiti di verifica delle firme del gestore descritte al punto 9.2 dell'Allegato al DM del 02/11/2005.
All'interno del messaggio di benvenuto vengono inviati al titolare della casella tutti i parametri di configurazione necessari per l'accesso al sistema attraverso i client di posta.
In particolare:

- login di accesso (casella PEC)
- password
- server SMTP: smtps.sicurezzapostale.it:465 con autenticazione del server necessaria
- server POP: pops.sicurezzapostale.it:995 autenticandosi fornendo la login e la password impostata per l'account
- server IMAP: imaps.sicurezzapostale.it:993 autenticandosi fornendo la login e la password impostata per l'account.

Una volta configurato il proprio client di posta, il titolare utilizza la casella di PEC come una casella di posta ordinaria. Le uniche differenze riguardano i formati dei messaggi e delle ricevute che vengono recapitate. Infatti, per ogni messaggio inviato e consegnato senza problemi, il mittente riceve:

- una **Ricevuta di Accettazione inviata dal proprio Gestore 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, che è stato accettato dal sistema e che è destinato ai destinatari presenti nel messaggio originale (distinguendo quelli certificati da quelli non certificati).
- una **Ricevuta di Avvenuta Consegna per ogni destinatario certificato presente nel messaggio originale**. Le ricevute di avvenuta consegna sono inviate dal Gestore cui il destinatario appartiene ed è un messaggio di posta con subject "CONSEGNA:" seguito dal subject del messaggio originale e con un testo che indica che il messaggio è stato recapitato nella casella del destinatario. La ricevuta contiene, in allegato, un file xml con i dati di certificazione e, in caso di ricevuta completa, il messaggio originale, completo di allegati.

Il destinatario, da parte sua, riceve:

- la **Busta 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. etc.

5.7.2 ACCESSO TRAMITE WEBMAIL

Il titolare della casella di PEC ha la possibilità di accedere a quest'ultima attraverso un comune browser Internet.
L'indirizzo (HTTPS, navigazione tramite canale sicuro) del sistema di webmail è https://webmail.sicurezzapostale.it e viene anche comunicato al titolare nel messaggio di benvenuto che viene inviato una volta completata la procedura di fornitura della casella.
Utilizzando un browser internet:

- l'utente si collega all'indirizzo specifico sopra citato;
- a tale indirizzo web, risponde l'applicativo webmail, che richiede l'inserimento delle credenziali di accesso;
- 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.

Attraverso la webmail è possibile scegliere, per ogni singolo messaggio originale da inviare, il tipo di ricevuta di avvenuta consegna. La ricevuta, come specificato al § 4.2, può essere completa (contiene il messaggio originale e gli eventuali allegati), breve (contiene il messaggio originale con una codifica hash degli allegati) o sintetica (contiene i soli dati di certificazione).

5.8 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 / Ragione Sociale
- Indirizzo (Via, Città, CAP, Nazione)
- Codice Fiscale / Partita IVA
- email valida (per eventuali comunicazioni)
- Fotocopia di un documento di identità in corso di validità

Il personale del servizio di help desk del Gestore Namirial S.p.A., una volta recuperate le informazioni richieste, le comunica al cliente via posta elettronica o con mezzi alternativi.
Il modulo per la richiesta di nuove credenziali di accesso è reperibile al link seguente: http://www.sicurezzapostale.it/docs/Richiesta_credenziali_accesso.pdf

5.9 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, il modulo disponibile al link seguente http://www.sicurezzapostale.it/docs/Modulo_Richiesta_LOG.pdf e compilato con le seguenti informazioni:

- Nome e Cognome del titolare
- Casella PEC del mittente
- Casella PEC del destinatario
- Data di riferimento del messaggio da ricercare
- Oggetto del messaggio da ricercare (opzionale)
- Identificativo del messaggio da ricercare (opzionale)

La casella di posta certificata utilizzata dal gestore per la raccolta delle richieste dei log da parte degli utenti, viene comunicata agli utenti stessi sia all'interno del messaggio di benvenuto inviato a seguito dell'attivazione sia all'interno dello stesso modulo utilizzato per la richiesta. 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 in corso di validità. Il personale del servizio di help desk del Gestore Namirial S.p.A., una volta recuperate le informazioni richieste, le comunica al cliente via posta elettronica certificata o con mezzi alternativi.

5.10 RICHIESTA DELLA CANCELLAZIONE DI UNA CASELLA PEC

Il titolare può richiedere al proprio Gestore la cancellazione della propria casella di PEC inviando, via fax o raccomandata A/R, il modulo messo a disposizione al seguente link: http://www.sicurezzapostale.it/docs/Richiesta_Cancellazione_casella_PEC.pdf.
Nel modulo vanno 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 allegare, alla richiesta, la fotocopia di un documento di identità in corso di validità.
La richiesta di cancellazione può essere effettuata solamente dal titolare della casella.
Il Gestore effettua una serie di controlli ed invia al titolare una comunicazione di chiusura via pec, nella quale lo avvisa che la casella verrà chiusa 48 ore lavorative dopo l'invio della comunicazione stessa. Trascorso tale termine, provvede alla cancellazione.
Le richieste di cancellazione vengono conservate per un periodo minimo di 12 mesi.

5.11 SERVIZIO DI HELP DESK

Il Gestore 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 § 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 il sito istituzionale del Gestore usando il seguente link: http://www.sicurezzapostale.it/pec/default.asp.
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 può anche segnalare eventuali problemi riscontrati durante l'invio e/o la ricezione dei messaggi che abbia riscontrato utilizzando i client di posta oppure la webmail. Le segnalazioni pervenute tramite portale, sono gestite attraverso un sistema di trouble ticketing che segnala, via email, ogni aggiornamento fino alla risoluzione definitiva.

5.11.1 TROUBLE TICKETING

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

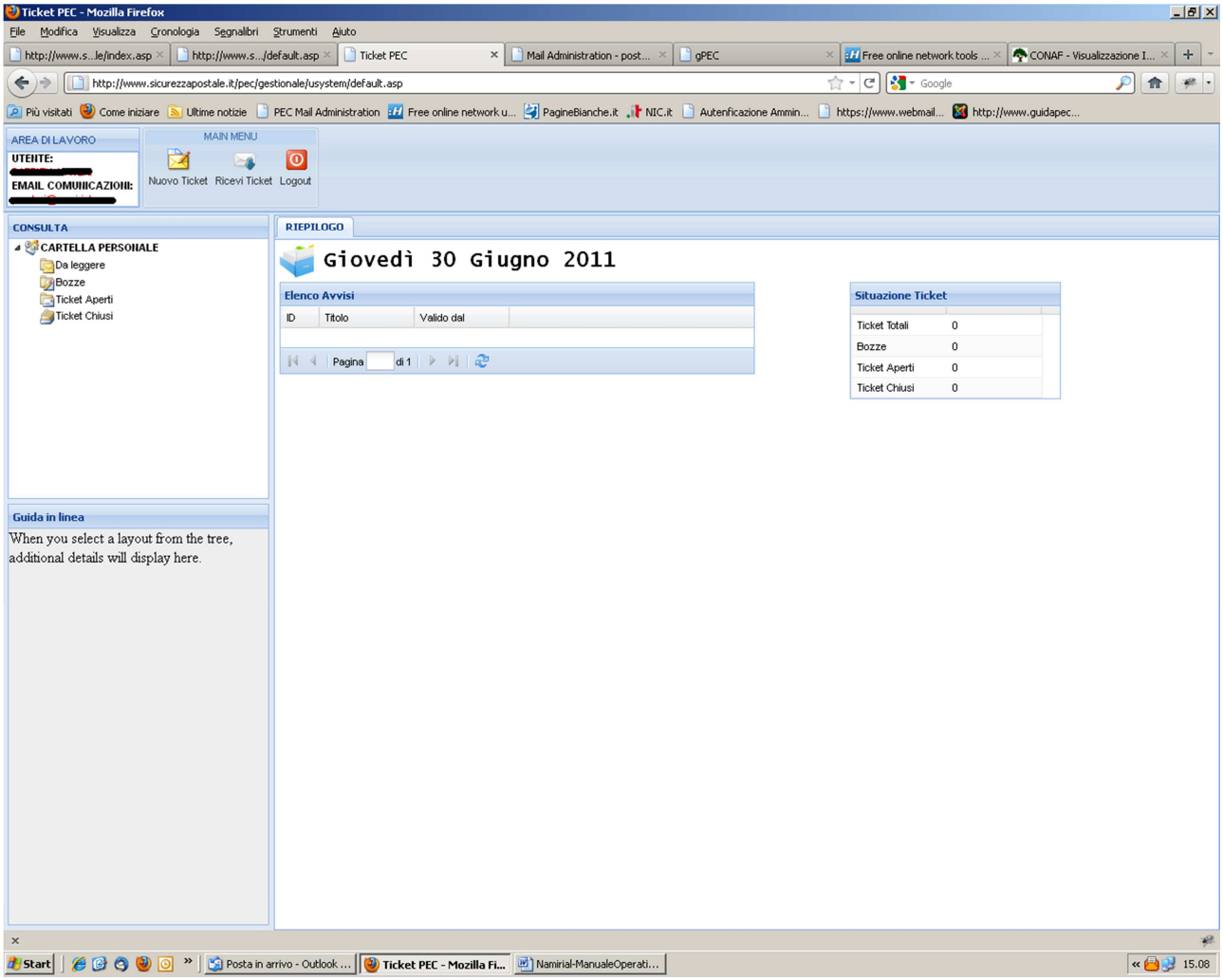

Figura 3 - Interfaccia del pannello di trouble ticketing

5.12 INTEROPERABILITÀ CON GLI ALTRI GESTORI DI PEC

Il Gestore 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. mette a disposizione una casella di PEC da utilizzare per i test con gli altri Gestori.

5.13 LIVELLI DI SERVIZIO ED INDICATORI DI QUALITÀ

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

Livelli di Servizio	
Numero massimo di destinatari contemporanei accettati in un singolo messaggio originale	**Almeno 50**
Dimensione massima di ogni singolo messaggio (intesa come prodotto tra il numero dei destinatari e la dimensione del messaggio)	**30 MB**
Disponibilità del servizio nel periodo di riferimento previsto (quadrimestre)	**Uguale o maggiore 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.	**5gg 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	**5gg 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	**5gg la settimana: dal lunedì al venerdì 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 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. 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;
- integrazione con le tipologie di rete più diffuse sul mercato;
- utilizzo di dispositivi hardware di firma ad alta sicurezza (tamper-proofness/tamper-evident) per la gestione e il mantenimento sia delle chiavi sia dei certificati di firma;
- utilizzo di dispositivi hardware per la firma e verifica dei messaggi.

6.2 SCALABILITÀ E AFFIDABILITÀ

L'architettura del Gestore Namirial S.p.A. è altamente scalabile e può essere estesa in qualsiasi momento per rispondere alle 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 dispositivi di rete, i dispositivi di firma sono installati in configurazione ridondata e bilanciata. In questo modo non esiste un "single point of failure" e l'eventuale malfunzionamento di un apparato non causa un fermo di 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 HSM utilizzati nella soluzione del Gestore 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 con modifiche richieste da DigitPA**. OpenPEC (http://www.openpec.org/index.shtml) 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 (DigitPA).
OpenPEC si propone come estensione dei mail server Open Source più diffusi sul mercato (come ad esempio Postfix) ed ha le seguenti caratteristiche:

- piena compatibilità con la normativa vigente;
- prestazioni elevate;
- affidabilità, scalabilità e 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 certificati locali al Gestore;
- marcatura temporale e storicizzazione dei log;
- gestione delle Certificate Revocation List (CRL);

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

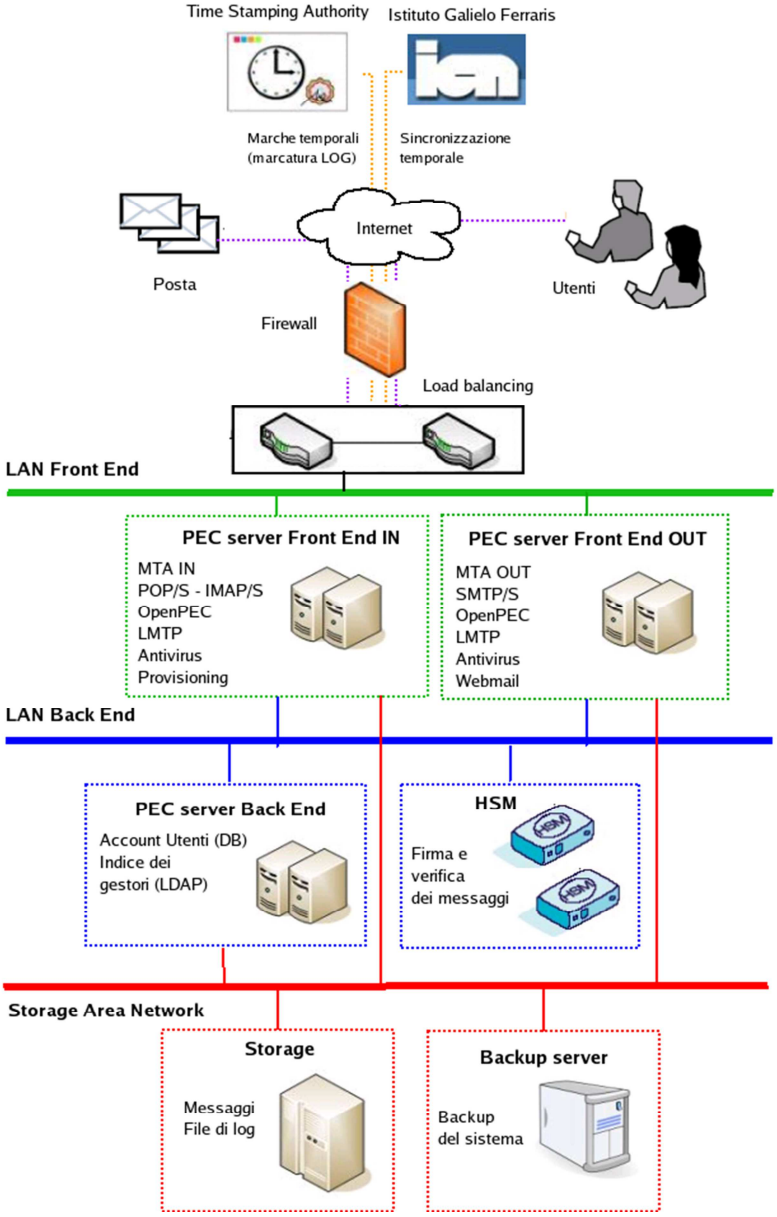

Figura 4 - Architettura logica del Sistema

L'architettura può essere suddivisa in 4 livelli.

- **Primo livello**: è costituito dagli apparati di rete (router, switch), dal modulo firewall per la protezione del sistema da accessi indesiderati, e dai bilanciatori virtuali che si occupano di suddividere il carico tra le varie macchine del livello sottostante.
- **Secondo livello**: rappresenta il front end applicativo 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: server per la ricezione e l'invio dei messaggi originali (PEC smtpout) e server per la ricezione dei messaggi firmati (PEC smtpin). Su entrambi i gruppi sono presenti il modulo MTA (incaricato del mail routing), il modulo antivirus ed il modulo OpenPEC. Sempre sullo stesso livello sono altresì presenti:

  - i servizi per la consultazione, in maniera sicura, delle caselle di posta elettronica certificata (POP/S e IMAP/S e Webmail su http/S);
  - il sistema di provisioning, per il rilascio e la gestione degli account e per l'attivazione dei domini di PEC.

  I server collocati a questo livello sono regolarmente sincronizzati con l'Istituto Galileo Ferraris di Torino mediante protocollo NTP e dispongono di un'interfaccia con una Time Stamping Authority allo scopo di effettuare la marcatura giornaliera dei log.
- **Terzo livello**: rappresenta il back end applicativo PEC e contiene i dispositivi di firma (HSM) più un gruppo di server per la realizzazione del sistema informativo degli utenti e dei domini certificati. Gli HSM si occupano della firma e della verifica dei messaggi inviati e ricevuti, mentre i server contengono il database degli account ed il mirror dei domini certificati prelevato dall'Indice dei Gestori PEC e memorizzato su server LDAP.
- **Quarto livello**: rappresenta la storage area network del sistema PEC e contiene le mailbox degli utenti, i backup di sistema ed i file di log come previsto dalla normativa vigente.

6.5 I PRINCIPALI COMPONENTI DELLA SOLUZIONE

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

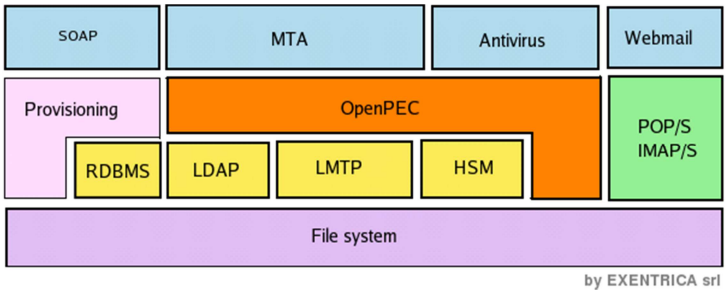

Figura 5 - Componenti del sistema PEC

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 ed altri fattori.
Il formato della data è ***gg/mm/aaaa*** dove:

- **gg** sono le 2 cifre del giorno
- **mm** sono le 2 cifre del mese
- **aaaa** sono le 4 cifre dell'anno.

Il formato dell'ora è **hh:mm:ss** dove:

- **hh** sono le 2 cifre delle ore (00-23)
- **mm** sono le 2 cifre dei minuti
- **ss** sono le 2 cifre dei secondi.

Al dato temporale viene fatto seguire, tra parentesi tonde, la **zona**, ossia la differenza, espressa 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 il riferimento temporale ***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 prodotti dal sistema deve essere apposta una marcatura temporale in modo che venga stabilito 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 temporalmente verranno trasferiti in apposite areee di storage e conservati per un periodo di almeno 30 mesi, come 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.:

- nel caso spedizione verifica la presenza dei virus nei messaggi originali di posta elettronica al Punto di Accesso, ossia nella fase immediatamente successiva all'invio del messaggio. Il sistema comunica al mittente che il suo messaggio contiene un virus attraverso l'emissione di un "AVVISO DI NON ACCETTAZIONE PER VIRUS".
- nel caso di ricezione verifica la presenza di virus al Punto di Ricezione. Il sistema emette ed invia al gestore del mittente un avviso di rilevazione virus recante oggetto "PROBLEMA DI SICUREZZA". Il gestore del mittente provvederà ad emettere un messaggio recante la dicitura "AVVISO DI MANCATA CONSEGNA PER VIRUS" e lo scrive nella casella del mittente.

I messaggi contenenti virus vengono conservati in apposite aree di storage dedicate per un periodo di almeno 30 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 infrastrutture hardware e viene fatto uso di 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 sono 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 latero-cemento 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 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 al Data Center avviene da un atrio comune del piano primo a cui si accede:

- dal piano terra, attraverso una scala 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 2 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 lettore di prossimità e chiave transponder. Per questa porta è previsto (per ragioni di sicurezza) un pulsante di sblocco dall'interno (maniglione antipanico).
Risulta presente inoltre un sistema di allarme antintrusione collegato con le forze dell'ordine ed un sistema operativo di videosorveglianza a circuito chiuso.

7 PROCEDURE, STANDARD TECNOLOGICI E DI SICUREZZA UTILIZZATI

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, il Gestore Namirial S.p.A. adotta le linee guida ed i principi previsti dallo standard di 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 dispositivi 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 dispositivi di firma utilizzati nel sistema di PEC del Gestore 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 del Gestore 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 DigitPA 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, anti 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

Oltre al Responsabile del servizio, sono previsti altri 5 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
- Responsabile 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 aziendale.

7.3.3 SICUREZZA DELL'INFRASTRUTTURA

Dal punto di vista prettamente informatico, la sicurezza del sistema del Gestore 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 apposito ambiente di testing)
- 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 datastore (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 almeno 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 sia sicuro e conforme 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, possono essere richiesti interventi di natura organizzativa come il cambiamento di una procedura interna o la sostituzione di personale giudicato non idoneo al servizio.

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 e dai seguenti responsabili di settore:

- 1 responsabile della registrazione dei titolari
- 1 responsabile del servizio
- 1 responsabile dei servizi tecnici
- 1 responsabile delle verifiche e delle ispezioni (auditing)
- 1 responsabile della sicurezza
- 1responsabile 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

Con cadenza almeno giornaliera vengono effettuati dei backup dei dati e dei sistemi e trasferiti su due ambienti di storage distinti. 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 MONITORING

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 24x7x365, vengono inviati via sms al personale preposto e in grado di intervenire prontamente per risolvere la criticità. Attraverso il sistema di monitoring del Gestore Namirial S.p.A. è possibile controllare tutte le macchine del sistema in termini di spazio disco, carico della CPU, occupazione di memoria, attività dei processi, situazione delle code, etc. 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

   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** (**TdS**).
2) Il TdS prende in carico la segnalazione, la analizza, verifica che il problema sussista realmente e ne stabilisce la risoluzione.
3) Il TdS 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.
4) Il TdS valuta la necessità di utilizzare il supporto di terzi, intesi sia come personale specializzato interno, che come consulenza esterna.
5) Il TdS 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 TdS lo assiste durante tutte le attività svolte ed effettua un presidio costante tracciando, al tempo stesso, tutte le operazioni effettuate.
6) Una volta completato l'intervento, il TdS ne informa l'Help Desk.
7) Il servizio di Help Desk verifica che il problema è stato risolto e comunica la risoluzione a chi ne 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 ad informare tempestivamente DigitPA circa i malfunzionamenti riscontrati nel proprio sistema entro 30 minuti dal loro 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	**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 è circoscritto il potenziale impatto
	1B: rilevato da terzi	
Malfunzionamento bloccante	**1A:** 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
	1B: 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 DigitPA 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 (per i messaggi che deve spedire) e non emette Ricevuta di Presa in Carico per i messaggi provenienti dagli altri Gestori.
Nel caso di sospensione il Gestore Namirial S.p.A., una volta eliminato il disservizio, può riprendere l'attività. In tal caso deve inviare a DigitPA una relazione dettagliata su quanto accaduto e sui provvedimenti adottati.

8 OBBLIGHI E RESPONSABILITÀ

8.1 OBBLIGHI E RESPONSABILITÀ DEL GESTORE

Il Gestore Namirial S.p.A., considerata la normativa vigente e visto quanto riportato nel DM 2 nov 2005 "Regole tecniche per la formazione, la trasmissione e la validazione, anche temporale, della posta elettronica certificata" e nel DPR 1 feb 2005 n. 68 "Regolamento recante disposizioni per l'utilizzo della posta elettronica certificata, a norma dell'articolo 27 della legge 16 gennaio 2003, n. 3", si impegna a:

- rispettare e garantire i livelli di servizio previsti;
- essere interoperabile con gli altri Gestori accreditati;
- conservare i log relativi alle trasmissioni avvenute e renderli disponibili, con le modalità previste nel presente manuale, per gli usi previsti dalla legge;
- inviare ai propri clienti le informazioni riguardanti le modalità di richiesta, reperimento e presentazione dei log dei messaggi;
- informare il Titolare riguardo le modalità di accesso al servizio e sui necessari requisiti tecnici;
- registrare, su apposito file di log, le singole fasi di ogni trasmissione di messaggio;
- conservare i file di log per almeno 30 mesi;
- apporre la marca temporale sui log delle trasmissioni dei messaggi;
- rilasciare tutte le ricevute, buste ed avvisi previsti dalla normativa (busta di trasporto, ricevuta di presa in carico, ricevuta di accettazione, ricevuta di avvenuta consegna, avviso di non accettazione, avviso di mancata consegna, avviso di mancata consegna per superamento tempi massimi, avviso di rilevazione virus, etc etc);
- apporre su ogni messaggio un riferimento temporale;
- conservare l'integrità del messaggio originale nella relativa busta di trasporto durante ogni trasmissione;
- rispettare le norme previste dal Dlg 30 giugno 2003, n. 196 in materia di protezione dei dati personali;
- non rendersi depositario di password private relative ai corrispondenti account di posta elettronica certificata;
- rilevare i messaggi contenenti virus informatici ed a rilasciare i relativi avvisi;
- conservare i messaggi contenenti virus informatici per il periodo previsto dalla normativa;
- adottare misure atte ad evitare l'inserimento di codici eseguibili dannosi;
- adottare procedure e servizi di emergenza al fine di assicurare il completamento della trasmissione anche in caso di incidenti (ad esclusione di eventi disastrosi improvvisi quali terremoti, attentati, etc etc);
- garantire la riservatezza, l'integrità e l'inalterabilità, anche nel tempo, dei file di log;
- garantire la segretezza della corrispondenza trasmessa attraverso il proprio sistema di posta elettronica certificata;
- utilizzare protocolli sicuri allo scopo di garantire la segretezza, l'autenticità, l'integrità delle informazioni trasmesse attraverso il sistema PEC;
- conservare le informazioni relative agli accordi stipulati con i clienti nel rispetto della normativa vigente;
- attivare/disattivare una casella PEC dopo aver verificato l'autenticità della richiesta e i dati in essa contenuti;
- associare univocamente il Titolare e la casella di posta elettronica certificata;
- rilasciare e/o rinnovare un account PEC richiesto, secondo le procedure descritte nel presente Manuale Operativo;
- revocare e/o sospendere un account PEC dandone tempestiva comunicazione e motivazione al Titolare secondo le modalità previste nel presente Manuale Operativo;
- adottare una procedura di sostituzione dei certificati elettronici relativi alle proprie chiavi di firma con una tempistica tale da non causare interruzioni di servizio;
- richiedere tempestivamente la revoca dei certificati, relativamente alle chiavi utilizzate per la firma dei messaggi e per la connessione sicura al sito del DigitPA, in caso di loro

comprovata compromissione;
- adottare misure di sicurezza tali da impedire la duplicazione abusiva e incontrollata delle chiavi private di firma o dei dispositivi che le contengono;
- comunicare tempestivamente ai propri utenti l'eventuale cessazione e/o interruzione del servizio di Posta Elettronica Certificata;
- adottare misure di sicurezza tali da consentire l'accesso logico e fisico al sistema solamente alle persone autorizzate;
- utilizzare un sistema di riferimento temporale che garantisca stabilmente una sincronizzazione, delle macchine coinvolte, con uno scarto non superiore al minuto secondo rispetto alla scala di Tempo Universale Coordinato (UTC);
- utilizzare dispositivi di firma conformi alla normativa vigente.

8.2 OBBLIGHI E RESPONSABILITÀ DEI TITOLARI

Il Titolare è l'unico ed il solo responsabile dei contenuti dei propri messaggi.
Aderendo al servizio offerto dal Gestore Namirial S.p.A., il Titolare si impegna a:

- utilizzare il servizio per i soli usi consentiti dalla legge;
- dare il consenso all'utilizzo dei propri dati personali ai sensi del Dlgs 196/03;
- fornire al Gestore tutte le informazioni necessarie ad identificare la persona ed attivare così il servizio, garantendo, sotto la propria responsabilità, la veridicità e l'esattezza dei dati comunicati;
- comunicare con tempestività le modifiche e/o aggiornamenti da apportare ai dati comunicati al Gestore qualora questi ultimi abbiano subìto variazioni;
- utilizzare in modo sicuro la casella di PEC proteggendo e conservando le proprie password con la massima accuratezza al fine di garantirne l'integrità e la riservatezza;
- conservare copia dei messaggi inviati e/o ricevuti unitamente con le relative ricevute;
- adottare misure atte ad evitare l'inserimento di codici eseguibili dannosi nei messaggi (virus/malware/etc etc);
- dotarsi di un sistema operativo aggiornato, valido e in costante aggiornamento rispetto ai requisiti indicati dalla normativa nazionale in materia di privacy, ovvero di idoneo sistema anti intrusione, antispam e antivirus.
- rendere edotte le eventuali persone abilitate ad utilizzare la propria casella riguardo le tematiche di sicurezza atte ad evitare un uso non autorizzato;

In difetto dei sopra indicati obblighi posti a carico del Titolare, il Gestore Namirial S.p.A. si riserva la facoltà di sospendere il servizio PEC, ovvero di disabilitare la casella PEC con effetto immediato e senza onere di preavviso a proprio carico, sino alla risoluzione del relativo rapporto contrattuale intercorrente con i medesimi, nei casi più gravi riscontrati.
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 l'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

Il Gestore in nessun caso risponderà di eventi ad esso non imputabili ed in particolare di danni subiti dalle LRA, dai Titolari, dai Richiedenti, dagli Utenti o da qualsiasi terzo causati direttamente o indirettamente dal mancato rispetto, da parte degli stessi, delle regole indicate nel presente Manuale Operativo, ovvero dalla mancata assunzione da parte di detti soggetti delle misure di speciale diligenza idonee ad evitare la causazione di danni a terzi che si richiedono al fruitore di servizi di certificazione, ovvero dallo svolgimento di attività illecite.
Il Gestore non sarà responsabile di qualsiasi inadempimento o comunque di qualsiasi evento dannoso determinato da caso fortuito o da eventi di forza maggiore.
Il Gestore 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;

Il Gestore Namirial S.p.A. non risponderà in alcun caso dei danni causati da malfunzionamenti, ritardi o interruzioni purché rientranti nei livelli di servizio descritti nel presente manuale.
Il Gestore Namirial S.p.A. 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;
Il Gestore 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;
Il Gestore Namirial S.p.A. non ha alcuna responsabilità sui contenuti dei messaggi inviati e ricevuti attraverso le proprie caselle di PEC;
La responsabilità del Gestore 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 dal Titolare per la singola casella 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;
Il Gestore Namirial S.p.A. si riserva la facoltà di modificare il presente manuale operativo nel caso in cui vengano apportate modifiche tecniche al sistema, variazioni all'offerta commerciale, o adeguamenti normativi.
Le limitazioni agli indennizzi stabilite dal Gestore Namirial S.p.A., per quanto non previsto dal presente capitolo, sono riportate nelle condizioni contrattuali di fornitura del servizio rese pubbliche e disponibile presso il sito http://www.sicurezzapostale.it/richiesta-adesione.asp.

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. 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 € 1.500.000,00 (un milione e cinquecentomila 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

Di 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 delle caselle e, più in generale dei clienti del servizio erogato, 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 STRUTTURA ORGANIZZATIVA DI NAMIRIAL S.P.A. IN MATERIA DI TRATTAMENTO DEI DATI PERSONALI

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 Romagnoli.
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 (DPS), 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.

9.2 TUTELA E DIRITTI DEGLI INTERESSATI

Il Gestore 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 del Gestore Namirial S.p.A..

9.3 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 del Gestore Namirial S.p.A., cui avranno accesso solo gli incaricati espressamente autorizzati.

9.4 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.

9.5 ALTRE FORME DI UTILIZZO DEI DATI

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.

9.6 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 (cfr § 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.