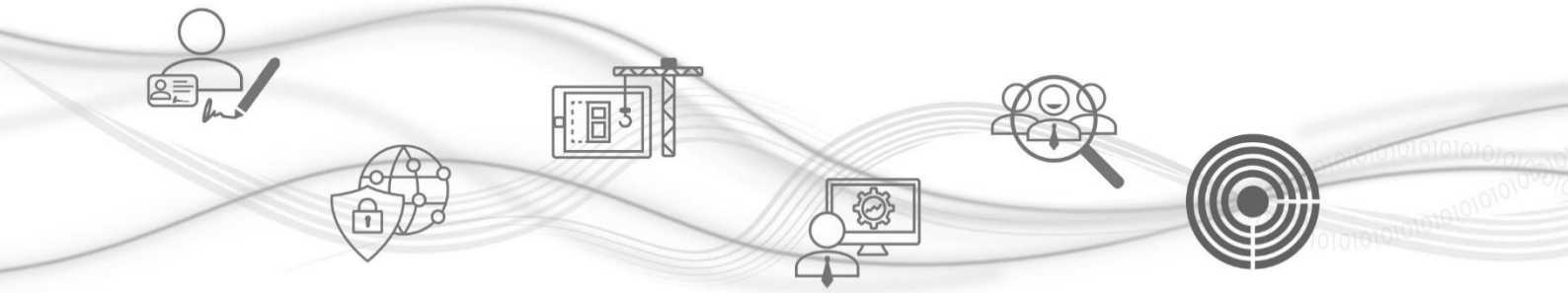
Posta Elettronica Certificata

Manuale Operativo del Gestore PEC Namirial S.p.A.



Categoria	**PEC**	Codice Documento	**NAM-PEC-MO**	**Namirial S.p.A.**
Redatto da	**Marina Pettinari**	Nota di riservatezza	**Documento Pubblico**	Il Legale Rappresentante
Verificato da	**Flavio Fanton**	Versione	**2.4**	**Massimiliano Pellegrini**
Approvato da	**Massimiliano Pellegrini**	Data di emissione	**06/09/2023**	

Signed by: PELLEGRINI MASSIMILIANO
Issued by: Namirial CA Firma Qualificata
Signing time: 08-09-2023 15:57:39
IP address: 93.38.49.65

Namirial S.p.A.
Via Caduti sul Lavoro n. 4, 60019 Senigallia (An) - Italia | Tel. +39 071 63494
www.namirial.com | amm.namirial@sicurezzapostale.it | P.IVA IT02046570426
C.F. e iscriz. al Reg. Impr. Ancona N. 02046570426 | REA N. AN - 157295
Codice destinatario T04ZHR3 | Capitale sociale € 7.762.625,20 i.v.

Sommario

Storia delle modifiche apportate

VERSIONE	2.4
Data	06/09/2023
Motivazione	Aggiornamento ai sensi dell'adeguamento alla REM
Modifiche	Revisione definizioni §5 Adeguamento della PEC ai nuovi standard europei §4.9.3 Aggiunta possibilità di accesso federato

VERSIONE	2.3
Data	06/03/2023
Motivazione	Aggiornamento
Modifiche	§4.6 Esteso il capitolo integrando l'identificazione dei titolari per le caselle SpidMail §4.6.1 Rivista la modalità di richiesta di attivazione §4.7.2 Inserito il capitolo relativo alla scadenza della password di accesso della casella §4.6 Esteso il capitolo integrando la tipologia di casella SpidMail §4.8 Aggiunta paragrafo per servizio SPIDmail §4.9.1 Accesso attraverso i client di posta – integrata la gestione dei protocolli di posta §4.9.2 Accesso tramite webmail – integrata l'accesso a SpidMail

	§4.12 Esteso il capitolo relativamente alla proroga della chiusura di una casella pec in caso di abbonamento

VERSIONE	**2.2**
Data	07/07/2021
Motivazione	Aggiornamento
Modifiche	§2.1 Aggiornato il capitale sociale §2.2 Verificare §2.4 Aggiornati i riferimenti §3.2.1.3 Aggiornato ed esteso il capitolo §4.11 Rivisto il flusso di chiusura della casella PEC §6.3 Aggiornato ed esteso l'intero capitolo

VERSIONE	**2.1**
Data	27/08/2020
Motivazione	Aggiornamento
Modifiche	§2.2 Rivista e aggiornata la sezione delle certificazioni del Gestore §4.6.2.1 Raccomandazioni per gli utenti §4.8.1 Aggiunti parametri di accesso per i client di posta §4.8.2 Aggiunto cambio password obbligatorio al primo accesso da webmail

	§6.3.5 Controllo degli allegati §7.3 Limitazioni e indennizzi

VERSIONE	**2.0**
Data	14/10/2019
Motivazione	Aggiornamento
Modifiche	Cap 7 Aggiunto paragrafo 7.3.5 Contrasto allo spam Cap 2.1 aggiornata la sede secondaria del servizio; aggiornata l'email del servizio Cap 2.4 aggiornato il riferimento telefonico dell'help desk Cap 4.1 aggiunta la possibilità di eliminazione delle PEC più vecchie di 30 giorni. Cap 4.8 modificata la procedura di recupero delle credenziali di accesso Cap 4.10 modificata la modalità di chiusura della casella PEC Cap 4.11 aggiunto il piano di cessazione del servizio PEC Cap 4.13 incrementata la dimensione massima del messaggio gestito Cap 5.7, Cap 5.8 modificata la modalità di apposizione della marcatura temporale ai LOG e la loro conservazione Cap 6.4.3, Cap 6.4.4 modificata la descrizione del sistema di monitoraggio e delle azioni intraprese a seguito di riscontro/segnalazione di errori. Cap 7.4 aggiornate le informazioni circa la polizza assicurativa.

VERSIONE	1.9
Data	12/09/2014
Motivazione	Aggiornamento
Modifiche	Ristrutturazione generale del documento. Cap 2.2 Aggiornamento della descrizione sintetica del Gestore Cap 2.3 Variazione del Responsabile del Servizio e del Manuale Operativo. Cap 4.2 Eliminazione del paragrafo, il cui contenuto è accorpato al il Glossario dei termini Cap 5.1, Cap 5.2 Ristrutturazione della descrizione sintetica del servizio offerto. Cap 5.6.2.1 Adeguamento della lunghezza e complessità della password Cap 7.4.2 Aggiornamento della Gestione dei backup Cap 8 Accorpamento degli Obblighi e Responsabilità del Gestore e del Titolare in un unico capitolo.

VERSIONE	1.8
Data	14/10/2013
Motivazione	Aggiornamento
Modifiche	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.

	Cap 5.4.1 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 per la consultazione dello stesso

VERSIONE	**1.7**
Data	05/08/2013
Motivazione	Aggiornamento
Modifiche	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. Cap.8.2 Integrazione degli obblighi e responsabilità ricadenti sui titolari e indicazione delle conseguenze, ricadenti sui medesimi, in caso di violazione.

VERSIONE	**1.6**
Data	01/07/2011
Motivazione	Aggiornamento e ristrutturazione del documento
Modifiche	È stato sostituito l'acronimo CNIPA con DigitPA, nei punti in cui si è reso necessario. Cap 5.1.7 A seguito delle modifiche al CAD, come da decreto legge 30 dicembre 2010 m. 235, sono state aggiornate le mansioni

	dell'Ufficio di registrazione, il quale ha cambiato denominazione; sono stati aggiornati tutti i riferimenti nel manuale. Cap.5.1 Lo standard delle caselle è stato portato ad 1 Gigabyte Cap.5.1.1, Cap.5.1.2, Cap.5.1.3 E' stato specificato che sono previste delle limitazioni al traffico solo nel caso di utilizzo della casella per invii massivi. Cap. 5.1.4 È stato specificato che l'utilizzo del pannello di richiesta delle caselle PEC è consentito solo alle 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 sul sito della email per la richiesta dei file di LOG Cap.5.7 È stata rivista la comunicazione, ai Titolari, della chiusura di caselle pec Cap. 5.8.1 L'immagine del programma di Trouble Ticketing è stata sostituita con la nuova versione Cap. 6.9.2 Il badge magnetico per l'accesso alla sala macchine è stato sostituito con la chiave trasponder su lettore di prossimità Cap.6.4 È stata aggiornata la versione OpenPec Cap.9.2 È variato il Responsabile del trattamento dei dati personali

VERSIONE	**1.5**
Data	29/10/2009
Motivazione	Aggiornamento

Modifiche	Cap.2.1 Dati identificativi: è stato modificato il capitale sociale dell'azienda da €1.000.000,00 i.v. a €6.500.000,00 i.v. Cap.5.1.7 Uffici di Registrazione: è stata inserita la possibilità per il Gestore di avvalersi di Uffici di Registrazione per identificazione e validazione della documentazione, richiesta per l'erogazione del servizio PEC.

VERSIONE	**1.4**
Data	10/12/2008
Motivazione	Aggiornamento
Modifiche	Cap.2.2 È stata resa più lineare la descrizione dell'azienda gestore. Cap.4.3.1 È stato illustrato in dettaglio il servizio di “inoltro” messaggi provenienti da caselle non certificate. Cap. 5.3 È stata menzionata la possibilità di trasmissione della documentazione tramite email e con firma digitale. Cap.5.4.1 È stato Specificato l’accesso tramite client di posta che rispondano ai requisiti richiesti. Cap.5.7 È stato inserito periodo minimo di conservazione, da parte del Gestore, delle richieste di cancellazione di account/dominio. Cap.6.9.2 È stata modificata l'indicazione della Classe di riferimento delle porte blindate e quella del sistema di videosorveglianza. Cap.8.1 Ai fini di maggiore completezza, sono stati inseriti ulteriori punti relativi agli obblighi del gestore. Cap.8.2 Ai fini di maggiore completezza, sono stati inseriti ulteriori punti relativi agli obblighi del titolare.

VERSIONE	1.3
Data	19/05/2008
Motivazione	Aggiornamento
Modifiche	Cap. 4.3.1. È stata inserita la data di Certificazione Qualità UNI EN ISO 9001:2000 Cap. 4.3.1. È stata inserito un passo, descrittivo dei modi in cui 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. È stata aggiornata l'indicazione della gestione dei backup da parte di Namirial.

VERSIONE	1.2
Data	16/10/2007
Motivazione	Aggiornamento
Modifiche	Cap. 5.1.3 Sono stati modificati gli scaglioni, relativamente alla quantità minima e massima di caselle acquistabili. Cap. 5.1.4 Lo spazio aggiuntivo per casella passa da 50 Mbytes a 100 Mbytes

VERSIONE	1.1

Data	28/12/2006
Motivazione	Prima emissione del documento.
Modifiche	---

1 Introduzione

1.1 Scopo del documento e campo di applicazione

Il documento in oggetto costituisce 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: pertanto, può essere liberamente scaricato dal sito del gestore al link seguente: http://www.sicurezzapostale.it/docs/manualeoperativo.pdf.

1.2 Definizioni ed Acronimi usati all'interno del documento

TERMINE	SIGNIFICATO
PEC	Posta Elettronica Certificata
CNIPA	Centro Nazionale per l'Informatica nella Pubblica Amministrazione
DigitPA	Ente nazionale per la digitalizzazione della Pubblica Amministrazione (ex CNIPA)
AgID	Agenzia per l'Italia Digitale (ex DigitPA)
Gestore di Posta Elettronica Certificata	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. Tale soggetto si rapporta con altri gestori di posta elettronica certificata per l'interoperabilità delle caselle di tutti i titolari
Titolare	Soggetto al quale è assegnata una casella di PEC. Con l'introduzione della REM, il termine identificherà la persona fisica o la persona giuridica che si "sottoscrive" al servizio presso un REM Service Provider dal quale viene identificato, può assumere la facoltà o l'obbligo di sospenderla, cessarla o revocarla.
Responsabile	Con l'avvento della REM, il termine individuerà la persona fisica identificata in quanto legale rappresentante, o in quanto persona

	munita di delega, della persona giuridica intestataria della casella 6 che svolge il compito di permettere la fase di autenticazione nell'uso della casella da parte del REM Service Provider.
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	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	Casella di posta elettronica, attivata all'interno di un dominio di PEC ed alla quale è associata una funzione che rilascia una ricevuta di accettazione a seguito dell'invio ed una di avvenuta consegna a seguito del ricevimento, da parte del destinatario, di messaggi di PEC
Servizio elettronico di recapito certificato qualificato	Servizio elettronico di recapito certificato qualificato è la definizione nel Regolamento eIDAS con le seguenti proprietà: Servizio di recapito elettronico certificato [ossia che consente la trasmissione di dati fra terzi per via elettronica e fornisce prove relative al trattamento dei dati trasmessi, fra cui prove dell'avvenuto invio e dell'avvenuta ricezione dei dati, e protegge i dati trasmessi dal rischio di perdita, furto, danni o di modifiche non autorizzate] che soddisfa i requisiti di: fornitura da parte di un prestatore qualificato, garanzia dell'identificazione di mittente e destinatario, apposizione di firma o sigillo del prestatore nell'invio/ricezione dei dati per garantirne immodificabilità, indicazione esplicita all'utente di eventuali modifiche ai dati necessarie per la trasmissione, validazione temporale qualificata per invio e ricezione. (v. art, 3, def. 37 eIDAS e art. 44)

Registered Electronic Mail (REM)	Istanza specifica di servizio elettronico di recapito certificato che utilizza i sistemi di posta elettronica ordinaria come protocolli di trasferimento dei messaggi: «specific type of electronic registered delivery, which builds on the formats, protocols and mechanisms used in ordinary e-mail messaging» (cfr. ETSI EN 319 531 V1.1.1 (2019-01)}.
Marca temporale	Evidenza informatica con cui si attribuisce, ad uno o più documenti informatici, un riferimento temporale opponibile ai terzi secondo quanto previsto dal decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 e dal decreto del Presidente del Consiglio dei Ministri 13 gennaio 2004, pubblicato nella Gazzetta Ufficiale n. 98 del 27 aprile 2004.
Riferimento temporale	Informazione contenente la data e l'ora, associate ad un messaggio di posta elettronica certificata
Dati di Certificazione	Dati, quali ad esempio giorno ed ora di invio, mittente, destinatario, oggetto, identificativo del messaggio, che descrivono l'invio del messaggio originale e che sono certificati dal gestore di posta elettronica certificata del mittente; tali dati sono contenuti nelle ricevute e sono trasferiti, per mezzo di una busta di trasporto, al titolare destinatario insieme al messaggio originale
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, finalizzato a prevenire/impedire l'accesso e la manomissione del sistema dati da parte di soggetti non autorizzati.

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. Un directory server LDAP è un albero di entità costituite da attributi e valori. Un classico utilizzo di directory server è la memorizzazione 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
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), la falsificazione e l'intercettazione dei dati. Scopo primario di SSL è fornire sistemi di crittografia per comunicazioni

	affidabili, riservate sul Web e 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 ad Identificazione, Registrazione e Supporto dei Richiedenti/Titolari di caselle PEC
LRA	Local Registration Authority: persona fisica o giuridica, delegata dal Gestore allo svolgimento delle operazioni di Identificazione, Registrazione e Supporto dei Titolari di caselle di PEC
Dato personale	Come da definizioni di cui al Regolamento Europeo 679/2016 (GDPR), 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 altresì quelli relativi all'utente ovvero ad eventuali terzi e contenuti nei campi informativi presenti sui moduli, 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 o 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 o 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 dal titolare del trattamento o dal responsabile a compiere operazioni di trattamento dei dati
Interessato al trattamento dati	Persona fisica o giuridica, ente o associazione cui si riferiscono i dati personali
Punto di Accesso (PdA)	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)	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)	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	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; è generata attraverso una procedura informatica che garantisce la connessione univoca al gestore e la sua univoca identificazione ed è creata automaticamente con mezzi che garantiscano il controllo esclusivo da parte del gestore

Ricevuta di Accettazione (RdA)	Ricevuta, sottoscritta con la firma del gestore di posta elettronica certificata del mittente, contenente i dati di certificazione e rilasciata al mittente dal punto di accesso, a fronte dell'invio di un messaggio di posta elettronica certificata
Avvisio di Non Accettazione (AdNA)	Avviso, sottoscritto con la firma del gestore di posta elettronica certificata del mittente, che viene emesso quando il gestore mittente è impossibilitato ad accettare il messaggio in ingresso e che reca la motivazione per cui non è possibile accettare il messaggio, insieme all'informazione che il messaggio non potrà essere consegnato al destinatario
Ricevuta di Presa in Carico (RPdC)	Ricevuta, sottoscritta con la firma del gestore di posta elettronica certificata del destinatario ed emessa dal punto di ricezione nei confronti del gestore di posta elettronica certificata mittente, la quale attesta l'avvenuta presa in carico del messaggio da parte del sistema di posta elettronica certificata di destinazione e reca i dati di certificazione per consentirne l'associazione con il messaggio al quale si riferisce
Ricevuta di Avvenuta Consegna (RdAC)	Ricevuta, sottoscritta con la firma del gestore di posta elettronica certificata del destinatario, emessa al mittente dal punto di consegna nel momento in cui il messaggio è depositato nella casella di posta elettronica certificata del destinatario
Ricevuta Completa di Avvenuta Consegna (RdAC completa)	Ricevuta nella quale sono contenuti i dati di certificazione ed il messaggio originale
Ricevuta Breve di Avvenuta Consegna (RdAC breve)	Ricevuta nella quale sono contenuti i dati di certificazione ed un estratto del messaggio originale;

Ricevuta Sintetica di Avvenuta Consegna (RdAC sintetica)	Ricevuta nella quale sono contenuti i dati di certificazione
Avviso di Mancata Consegna (AdMC)	Avviso, emesso dal sistema per indicare al mittente l'anomalia 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	Messaggio inviato da un utente di posta elettronica certificata, nella fase precedente all'arrivo al punto di accesso e consegnato al titolare destinatario per mezzo di una busta di trasporto che lo contiene
Busta di Trasporto (BdT)	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)	Busta, sottoscritta con la firma del gestore di posta elettronica certificata del destinatario, nella quale è inserito un messaggio errato ovvero di posta elettronica non certificata; è consegnata ad un titolare, con il fine di segnalare al destinatario detta anomalia

Tabella 1: definizioni ed Acronimi

1.3 Versione del Manuale Operativo e successive revisioni(m)

La versione corrente del documento è indicata nella prima pagina; tuttavia, il presente Manuale potrebbe subire variazioni a seguito di modifiche apportate al sistema e dettate da necessità di ottimizzazioni, adeguamenti normativi oppure variazioni dei 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 di servizio del Gestore Namirial S.p.A. e sottoposta ad approvazione degli organi competenti (AgID). Il Cliente o il Titolare

sono tenuti a consultare la versione più aggiornata del Manuale Operativo, pubblicato sul sito web del Gestore, menzionato nel successivo § 1.4

1.4 Pubblicazione del Manuale Operativo del gestore(d)

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 pubblicarne sul sito la versione aggiornata ed approvata.

1.5 Tabella di corrispondenza

Circolare CNIPA/CR/56 del 21/05/2009	§ Manuale Operativo
a. Dati identificativi del Gestore	**2.1**
b. Nominativo del Responsabile del Manuale Operativo	**2.3**
c. Riferimenti normativi necessari per la verifica dei contenuti	**RIFERIMENTI**
d. Indirizzo del sito web del gestore, nel quale è pubblicato e scaricabile il Manuale Operativo	**1.4**
e. Indicazione delle procedure nonché degli standard tecnologici e di sicurezza, utilizzati dal Gestore nell'erogazione del servizio	**7.4**
f. Definizioni relative alle abbreviazioni e termini tecnici	**1.2**
g. Descrizione e modalità del servizio offerto	**4**
h. Descrizione delle modalità di reperimento e di comunicazione delle informazioni presenti nei LOG dei messaggi	**4.10**
i. Modalità di accesso e fornitura del servizio	**4.8**

j. Livelli di servizio con i relativi indicatori di qualità, ex articolo 12 del decreto del Ministro per l'innovazione e le tecnologie 2 novembre 2005	**4.15**
k. Criteri di protezione dei dati dei titolari delle caselle, obblighi e responsabilità conseguenti, esclusioni ed eventuali limitazioni in caso di indennizzo, inerenti ai soggetti previsti all'articolo 2 del decreto del Presidente della Repubblica n. 68/2005	**8, 9**
l. Procedure operative da attuare nel caso di cessazione dell'attività di gestore di posta elettronica certificata	**4.12**
m. Versione del Manuale Operativo	**1.3**

Tabella 2: tabella di corrispondenza CNIPA/CR/56 e Manuale Operativo

2 Il Gestore

Il servizio di Posta Elettronica Certificata viene erogato da Namirial S.p.A. della quale sono riportate le informazioni identificative insieme ad una descrizione sintetica delle attività svolte e dei principali settori di competenza.

2.1 Dati identificativi del Gestore[(a)]

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) - Italia Tel: 071.63494 Fax: 071.60910
Sedi secondarie (utilizzate per la conservazione delle copie di sicurezza dei dati)	Digital Campus @ Milan Via Monzoro, 101-105 20010 Cornaredo (MI) — Italia
Partita IVA:	IT02046570426
Iscrizione registro delle imprese:	Ancona
REA:	02046570426
Capitale sociale:	7.559.253,20€ I.V.

Sito web del servizio:	http://www.sicurezzapostale.it
Sito web del gestore:	http://www.namirial.com
Email del servizio:	serviziopec@sicurezzapostale.it
Email del gestore:	info@namirial.com

Tabella 3: dati identificativi del Gestore

2.2 Descrizione sintetica di Namirial S.p.A.

Namirial S.p.A. è una società di informatica e web engineering che opera specificamente nell'ambito dell'Information Technology, orientando la propria produzione di software verso le nuove e sempre più manifeste esigenze di adeguamento del sistema produttivo italiano agli attuali scenari economici fortemente competitivi e globalizzati. Nel quadro di un panorama economico nazionale, prevalentemente caratterizzato da attività imprenditoriali di piccole e medie dimensioni, Namirial S.p.A. ritiene essenziale sviluppare soluzioni e servizi software accessibili anche sulla rete internet ed in grado di rispondere in maniera professionale alle problematiche tecnologico-innovative emergenti; il tutto, mantenendo una grande economicità di esercizio. La società ha sede in una moderna struttura di oltre duemila metri quadrati, nella quale è allestito un *Internet Data Center* dotato di tutti i sistemi di sicurezza necessari all'inviolabilità della struttura ed in grado di assistere gli utenti anche per quanto concerne eventuali necessità di hosting, housing e di server farm in genere.

Namirial S.p.A. è:

eIDAS Qualified Trust Service Provider (Certificato N. IT269191)

Per i servizi di:

- emissione, verifica e validazione di marche temporali qualificate

- autorità di certificazione per l'emissione di certificati di firma elettronica qualificata e sigilli elettronici qualificati

secondo gli standard

- **ETSI EN 401**
- **ETSI EN 411 parti 1 e 2**
- **ETSI EN 421**
- **ETSI EN 422**
- **ETSI EN 319 412 per quanto applicabile.**

Gestore di PEC, dal 27/02/2007, accreditato presso AgID (ex DigitPA) ed autorizzato alla gestione di **caselle** e **domini** di Posta Elettronica Certificata.

Identity Provider accreditato presso AgID per l'emissione di identità digitali in conformità al DPCM 24 Ottobre 2014, ai requisiti tecnici del Regolamento di attuazione UE 2015/1502 della

Commissione e all'Art. 24 del Regolamento (UE) 910/2014 eIDAS (Certificato N°IT273825)

Conservatore accreditato presso AgID per attività di conservazione dei documenti informatici di cui all'articolo 44-bis, comma 1, del decreto legislativo 7 marzo 2005, n. 82 (Certificato N. IT277150).

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

Certificata ISO/IEC 27001 (con estensioni 27017/27018). Namirial ha conseguito il certificato n. IT280490 rilasciato da **Bureau Veritas Italia S.p.A.**

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

Tabella 4: certificazioni dei Gestore

2.3 Responsabile del Servizio e del Manuale Operativo[(b)]

Il Responsabile del presente manuale operativo è:

Flavio Fanton

Il Responsabile può essere contattato ai seguenti recapiti:

telefono: +39 071.63494

email: serviziopec@sicurezzapostale.it

indirizzo: Via Caduti sul lavoro, 4 - 60019 Senigallia (AN)

I Responsabili della verifica ed approvazione del documento sono citati nella prima pagina.

2.4 Help Desk ed assistenza al cliente

Al fine di ottenere informazioni sul servizio e ricevere assistenza in caso di rilevati malfunzionamenti, è possibile fare riferimento alla pagina **https://support.namirial.com/it/supporto-tecnico** :

2.5 Informazioni commerciali

Al fine di ricevere informazioni commerciali riguardanti le offerte di Namirial S.p.A., è contattare il Gestore via telefono, via email o via web ai seguenti recapiti:

telefono: 071-63494

email: **commerciale@sicurezzapostale.it**

web: www.sicurezzapostale.it

3 Posta Elettronica Certificata: informazioni generali

3.1 Introduzione

La Posta Elettronica Certificata (PEC) è un sistema di posta elettronica nel quale al mittente viene rilasciata, 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 A/R, al mittente viene inviata una ricevuta che attesta la consegna del proprio messaggio al destinatario. I messaggi di PEC possono contenere qualsiasi tipo di informazione ed allegato. La comunicazione si attua attraverso una serie di messaggi (detti buste), ricevute ed avvisi che vengono inviati:

- agli utenti (mittente e destinatario), 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 che attesta in modo esatto gli istanti in cui avvengono le comunicazioni.

Al fine di garantire legalità, trasparenza e correttezza del sistema, AgID 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 di AgID, 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 contengono la traccia delle comunicazioni avvenute. Tali LOG hanno la stessa validità legale delle ricevute della raccomandata e possono essere richiesti dagli utenti, titolari di caselle, in qualsiasi momento.

3.2 Posta Elettronica Certificata: il funzionamento

Al fine di descrivere a grandi linee il funzionamento di un sistema di Posta Elettronica Certificata, si consideri il disegno riportato nella figura seguente.

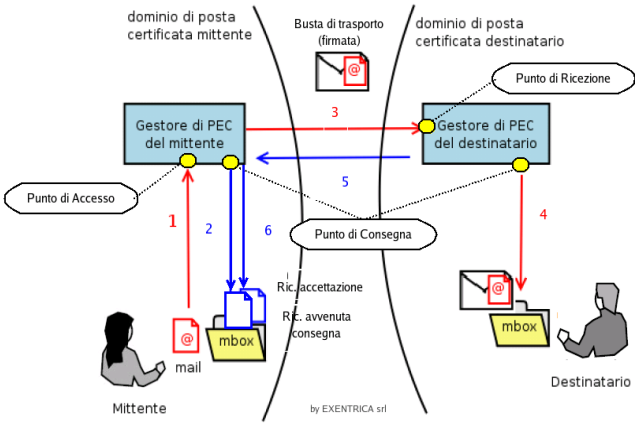


Figura 1: Funzionamento del sistema di PEC

Nello schema sono visualizzati 2 utenti (Mittente e Destinatario), ognuno dei quali appartiene ad un dominio di Posta Elettronica Certificata:

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 la Ricevuta di Accettazione e la invia al Mittente.
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) Non appena consegnato il messaggio, il gestore PEC del destinatario crea una ricevuta di avvenuta consegna, la firma e la invia al mittente.
6) Il gestore PEC del mittente accoglie 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 preimpostata nella webmail. Oltre ai dati di certificazione contiene, come allegato, il messaggio originale, completo degli eventuali file allegati, in esso originariamente contenuti;
- **breve**: oltre ai dati di certificazione contiene, come allegato, il messaggio originale nel quale gli eventuali file allegati, originariamente presenti,

vengono sostituiti dalla loro codifica hash;
- **sintetica**: contiene solamente i dati di certificazione, senza il messaggio originale in allegato.

3.2.1 Dettagli e casi particolari

La comunicazione riprodotta 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 i casi particolari descritti di seguito.

3.2.1.1 Ricevuta di Presa in Carico

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

3.2.1.2 Messaggi inviati a indirizzi email non certificati

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

3.2.1.3 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 – messaggi di posta elettronica ordinaria.

Il Gestore Namirial S.p.A. permette all'utente di scegliere se rifiutare tali messaggi, inoltrarli in modo automatico ad un secondo indirizzo oppure di consegnarli a destinazione racchiusi all'interno di una Busta di Anomalia. L'opzione è disponibile nella sezione *Impostazioni* della webmail.

In quest'ultimo caso i messaggi suddetti vengono analizzati dal sistema antispam che si limita a segnalare all'utente attraverso opportuni avvisi e spostare in un folder dedicato i messaggi ritenuti indesiderati o pericolosi.

Il servizio antispam di Namirial S.p.A. agisce nel pieno rispetto della normativa vigente e agisce sul traffico di posta elettronica ordinaria in ingresso alla casella PEC.

3.2.1.4 Messaggio formalmente non corretto

Il Gestore invia al proprio utente (il Mittente) un **Avviso di Non Accettazione** ogni qualvolta rilevi, all'interno del messaggio originale inviato dallo stesso Mittente, malformazioni e/o non conformità alla normativa, come ad esempio la presenza del campo Ccn.

3.2.1.5 Presenza di virus

Un virus, contenuto nel testo o negli allegati di una mail certificata, può essere rilevato dal Gestore PEC del Mittente o da quello del Destinatario.

Nel caso in cui sia il Gestore PEC del Mittente a rilevare il virus, allo stesso Mittente viene inviato un **Avviso di Non Accettazione per Virus**.

Nel caso in cui sia il Gestore del Destinatario, al proprio Punto di Ricezione, a rilevare il virus, lo stesso invia al Gestore del Mittente un avviso di rilevazione virus. Quest'ultimo Gestore, da parte sua, non appena ricevuto un avviso di rilevazione virus provvede ad emettere e consegnare al proprio utente (cioè il mittente del messaggio originale) un **Avviso di Mancata Consegna per Virus**.

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

3.2.1.6 Superamento dei tempi massimi previsti

In seguito all'invio di una Busta di Trasporto da parte del Gestore del Mittente, il Gestore del Destinatario potrebbe non essere in grado di scambiare informazioni con il Gestore Mittente (Ricevuta di Presa in Carico, Ricevuta di Avvenuta Consegna, Avviso di Mancata Consegna, etc). Se tale situazione perduri oltre le 12 e le 24 ore successive all'invio, il Gestore del Mittente è tenuto a informarlo tramite l'invio di informazioni concernenti l'esito del proprio invio.

In tali casi, il protocollo previsto è il seguente:

- trascorse 12 ore dalla spedizione, durante le quali non si sia avuta notizia della Busta di Trasporto (cioè non sia 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 12 ore successive al primo avviso (per un totale di 24 dalla spedizione), senza che siano state ricevute 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"*.

4 Il servizio PEC di Namirial S.p.A.[g]

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

4.1 Caratteristiche dell'offerta

L'offerta di posta certificata da parte di Namirial S.p.A. si rivolge ai privati, ai professionisti, agli enti pubblici ed alle aziende di tutto il territorio nazionale

Si ricorda che, in base alla normativa vigente, i messaggi sono da considerarsi ricevuti quando siano recapitati nella casella dell'utente e non quando l'utente li scarichi e/o li consulti.

È' evidente che, una volta 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.

Il Gestore si riserva la facoltà di eliminare definitivamente i messaggi di PEC che risultino permanere nel Cestino della casella PEC del Titolare per un periodo superiore a 30 giorni.

Il Gestore si riserva la facoltà di modificare nel tempo le caratteristiche dell'offerta, di seguito riportata.

4.2 Dettagli offerta, condizioni fornitura e tariffe applicate

Al fine di conoscere i dettagli e i costi dei vari servizi di seguito descritti nonché le modalità di sottoscrizione degli stessi, si rimanda al sito http://www.sicurezzapostale.it

4.3 Attivazione del servizio tramite partner commerciale

Namirial S.p.A. si avvale anche di partner commerciali per la distribuzione del proprio servizio PEC. Il partner commerciale raccoglie le informazioni necessarie ad identificare il cliente (c.d. Richiedente) che ha richiesto di aderire al servizio nonché quelle relative a: offerta, numero di caselle, eventuali servizi opzionali richiesti.

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 infatti predisposta dal Gestore Namirial S.p.A.

4.3.1 Local Registration Authority (LRA)

Il Gestore si avvale di Uffici di Registrazione distribuiti sul territorio (LRA) i quali, direttamente o tramite loro incaricati (IR), svolgono le seguenti attività intermedie tra il Gestore stesso e il Richiedente:

- Identificazione e preregistrazione del Richiedente;
- Controllo sulla regolarità 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, al termine di un adeguato addestramento del proprio personale preposto alle funzioni di identificazione e, eventualmente, di registrazione. Il Gestore verifica la rispondenza delle procedure utilizzate dalla LRA e dagli operatori (IR) addetti alla Registrazione con quanto stabilito nel presente manuale.

4.3.2 Obblighi della Local Registration Authority (LRA)

La LRA, nella persona dell'Incaricato alla Registrazione (IR), è tenuta a garantire:

- la verifica dell’identità del Richiedente e la registrazione dei dati dello stesso;
- che lo stesso Richiedente sia espressamente informato della necessità di proteggere la segretezza della password;
- la comunicazione al Gestore di tutti i dati e documenti acquisiti in fase di identificazione, allo scopo di avviare la procedura di attivazione dell'account

PEC;
- la verifica e l'inoltro al Gestore della richiesta di chiusura della casella PEC;
- che le attività, affidate dal Gestore alla LRA, siano effettuate secondo le regole e le procedure descritte nel presente Manuale Operativo;
- la rispondenza del proprio sistema di sicurezza dei dati alle misure di sicurezza per il trattamento dei dati personali, come descritto al §8.6 in ottemperanza alle disposizioni del GDPR.

4.4 Identificazione

Prima di procedere al rilascio dell'account PEC, il Gestore verifica l'identità del Richiedente. La procedura di identificazione comporta che il Richiedente sia riconosciuto personalmente dai soggetti di cui al § 4.4.1, i quali ne verificano 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.

Namirial si avvale inoltre della modalità di identificazione del Richiedente tramite SPID per il rilascio degli account di tipo SpidMail. SPID è il Sistema Pubblico di Identità Digitale che garantisce a tutti i cittadini e le imprese un accesso unico, sicuro e protetto ai servizi digitali della Pubblica Amministrazione e dei soggetti privati aderenti.

4.4.1 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.

4.4.2 Procedure per l'identificazione

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.

Oltre a quelle indicate, sono ammesse ulteriori tessere di riconoscimento, purché munite di fotografia e di timbro e 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.

4.5 Nomi dei domini e denominazione delle caselle

I nomi dei domini e le denominazioni delle caselle sono 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.

4.6 Rilascio delle caselle PEC

Nella figura seguente viene delineato uno schema, esemplificativo e non esaustivo, del flusso che descrive il rilascio di una casella di posta elettronica certificata.

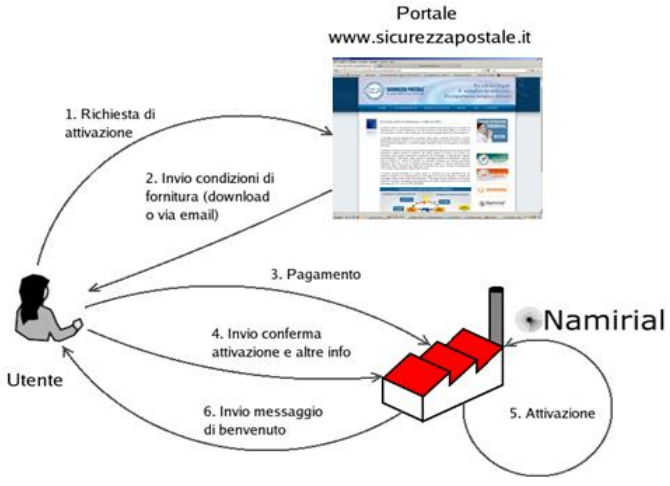


Figura 2: Flusso di attivazione di una casella di PEC

4.6.1 Richiesta di attivazione della casella

Al fine di attivare una casella di PEC, il Richiedente deve seguire una procedura guidata completamente online. Il processo si compone dei seguenti passaggi:

- scegliere l'indirizzo da assegnare alla casella;
- prendere visione delle "Condizioni generali di contratto" e della "Informativa sul trattamento dei dati personali";
- indicare i dati di fatturazione e dell'intestatario casella;
- firmare il modulo "Richiesta di Attivazione" attraverso la procedura online, che prevede l'apposizione di una firma elettronica tramite codice SMS di autorizzazione trasmesso al numero di cellulare preliminarmente verificato;
- completare con il pagamento del canone annuale.

4.6.2 Attivazione della casella

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

- login;
- prima password temporanea;
- server smtp;
- server pop/imap;
- indirizzo della webmail;
- informazioni circa il recupero dei LOG, la richiesta di assistenza, la modifica della password, etc.

4.6.2.1 Raccomandazioni per gli utenti

In aggiunta a quanto previsto nel § 7.2, si fornisce di seguito un vademecum contenente alcuni suggerimenti per un utilizzo corretto e sicuro della posta elettronica certificata nonché per la gestione della casella di PEC 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 invita il titolare a controllare

frequentemente la propria casella. In caso di necessità, si consiglia di salvare e successivamente eliminare i messaggi più vecchi, al fine di avere sempre spazio a disposizione e di evitare così che i messaggi di PEC vengano respinti per casella piena. Il Gestore si riserva la facoltà di eliminare definitivamente i messaggi di PEC che risultino permanere nel cestino per più di 30 giorni;
- l'utente è obbligato dal sistema ad aggiornare la password al primo accesso. La nuova password deve rispettare il formato e le policy di sicurezza indicate ed è inibito il riutilizzo per un periodo fissato dal Gestore. Si consiglia di aggiornare la password con frequenza almeno ogni 90gg.
- si consiglia di configurare la postazione di lavoro in modo da soddisfare i requisiti minimi di sicurezza.

4.7 Servizi aggiuntivi

Namirial S.p.A. mette a disposizione dei propri clienti una serie di servizi aggiuntivi con l'intento di arricchire l'offerta base:

- Apertura alla posta convenzionale in ingresso o suo inoltro a email convenzionale, scelta dal titolare della casella
- Abilitazione della scadenza della password di accesso alla casella
- Notifica di ricezione PEC
- Report giornaliero via email e sms
- Archiviazione dei messaggi di PEC
- Conservazione a norma dei messaggi di PEC
- Caselle per invio massivo
- Domini certificati personalizzati
- Dominio chiuso

4.7.1 Apertura alla posta convenzionale in ingresso o suo inoltro

Per impostazione di base, non è consentito l'ingresso di posta convenzionale nella casella di PEC. È, questa, una scelta consapevole del Gestore Namirial S.p.A. e dettata dall'opportunità di preservare il contenuto della casella dall'ingresso di messaggi non aventi valore di legge.

È comunque possibile, tramite il pannello "Impostazioni" della webmail, modificare questa regola nei seguenti modi:

- Accettare l'ingresso nella casella anche di messaggi non certificati. Il sistema li tratterà conformemente alle regole tecniche, recapitandoli pertanto all'interno di una busta di anomalia.

- Inoltrare i messaggi provenienti da email convenzionali, verso un indirizzo di posta convenzionale scelto dal titolare; i messaggi non certificati non entreranno in webmail ma saranno reindirizzati verso tale indirizzo.

4.7.2 Abilitare la scadenza della password di accesso alla casella

Per impostazione di base, la scadenza della password di accesso alla casella è disabilitata. È comunque possibile, modificare la configurazione tramite il pannello “Impostazioni” della webmail. Il Gestore Namirial S.p.A. suggerisce di attivarla per migliorare la sicurezza della casella.

Il sistema invia delle notifiche all’utente quando la password sta per scadere.

In caso di password scaduta il titolare potrà sempre re-impostarla tramite la funzione di Reset Password cliccando su "Hai dimenticato la password" nella pagina di login.

4.7.3 Notifica di ricezione PEC

La notifica di ricezione PEC è una funzione che consente al titolare di ricevere uno specifico messaggio di posta convenzionale, ad un indirizzo da lui scelto, ogni qualvolta riceva una PEC (busta di trasporto).

La notifica contiene gli elementi caratterizzanti della email PEC appena ricevuta e può essere configurata nella sezione “Impostazioni” della webmail.

ATTENZIONE: il gestore non si ritiene responsabile per la mancata ricezione della notifica che, essendo recapitata ad una email non certificata, non gode della piena certezza tecnico-legale del recapito stesso. Il titolare ha pertanto l’onere di controllare la propria casella di PEC, indipendentemente dalla ricezione delle notifiche.

4.7.4 Report giornaliero via email e sms

Il report consiste in una notifica giornaliera, via email oppure via SMS, riportante la situazione riassuntiva di quanto ricevuto nella casella PEC nelle ultime 24h.

Il report viene inviato, agli estremi ed all’orario indicati dal titolare, nel caso siano stati ricevuti nuovi avvisi, ricevute o messaggi certificati nelle ultime 24h.

ATTENZIONE: il gestore non si ritiene responsabile per la mancata ricezione del report che, essendo recapitato a canali non certificati, non gode della piena certezza tecnico-legale del recapito stesso. Il titolare ha pertanto l’onere di

controllare la propria casella di PEC, indipendentemente dalla ricezione del report.

4.7.5 Archiviazione dei messaggi di PEC

L'archivio PEC consente di salvare automaticamente, in un'area separata e sicura, una copia dei messaggi in ingresso e delle ricevute. Al fine di semplificarne la consultazione, l'archivio è accessibile sia dalla webmail che tramite client di posta.

È possibile liberare spazio per l'archiviazione, cancellando messaggi o cartelle attraverso la webmail; tuttavia, è necessario prestare la massima attenzione durante l'operazione di cancellazione, in quanto la stessa è irreversibile.

Non è invece possibile effettuare, sull'archivio, operazioni di cancellazione o, in generale, di modifica attraverso il client di posta.

Nella sezione "Impostazioni" della webmail, il titolare può decidere la tipologia dei messaggi da archiviare, scegliendo tra le opzioni proposte ed avendo, di fatto, la possibilità di limitare lo spazio occupato nell'archivio.

4.7.6 Conservazione a norma dei messaggi di PEC

StrongPEC è il servizio di Conservazione digitale a Norma dei messaggi PEC del gestore Namirial S.p.A.

È attivabile su ogni casella PEC e consente di porre automaticamente in conservazione a norma una copia dei messaggi in ingresso.

Una volta conservati, i messaggi sono accessibili attraverso la webmail; per garantire l'integrità del sistema, non è possibile liberare spazio o apportare modifiche al servizio.

Lo spazio disponibile per la Conservazione e quello occupato sono aggiornati all'interno della webmail.

Nella sezione "Impostazioni" della webmail, il titolare può decidere la tipologia dei messaggi da conservare, scegliendo tra le voci proposte ed avendo, di fatto, la possibilità di limitare lo spazio occupato nel servizio.

4.7.7 Caselle per invio massivo

Il servizio di invio massivo di Namirial S.p.A. consiste nella predisposizione di caselle PEC a performance garantita, sia in termini di invio/ricezione che di consultazione.

È un servizio mirato a soddisfare le esigenze delle grandi aziende che necessitano di sistemi PEC con tempi di risposta garantiti e volumi di traffico elevati.

4.7.8 Domini certificati personalizzati

Namirial eroga servizi personalizzati sui domini PEC e gestione DNS, in particolare fornisce:

- **Certificazione Dominio PEC** Certificazione PEC del dominio scelto dal cliente
- **Gestione e certificazione Dominio PEC** Registrazione, gestione DNS e certificazione dominio
- **Gestione, certificazione Dominio PEC e personalizzazione interfacce** Registrazione, gestione DNS e certificazione dominio, personalizzazione grafica della webmail e dei punti di accesso ad essa.

4.7.9 Dominio chiuso

Un Dominio PEC Chiuso è un dominio, certificato dal gestore Namirial, le cui caselle sono finalizzate alla corrispondenza certificata esclusivamente con altre caselle PEC del gestore stesso preventivamente censite.

In altri termini, Namirial offre l'opportunità di richiedere l'attivazione di caselle PEC su un dominio dedicato, le quali possano ricevere o inviare e ricevere esclusivamente nei confronti di altre caselle di PEC preventivamente identificate.

In particolare, quando un utente tenta di inviare una mail ad una casella non censita, appare una finestra bloccante e contenente l'avviso che la mail non può essere inviata. Nel caso in cui si tenti di inviare, ad una casella con dominio chiuso, un messaggio da una PEC non censita o da una email convenzionale, lo stesso viene bloccato ed il mittente riceve un avviso, indicante che la casella di destinazione è finalizzata alla comunicazione esclusiva con caselle specifiche e non può quindi ricevere dall'indirizzo di invio. Il servizio Dominio PEC Chiuso di Namirial S.p.A. è pienamente conforme alla normativa in materia.

4.8 SPIDmail

Namirial S.p.A offre, inoltre, il servizio SPIDmail, un recapito elettronico certificato che consente ai cittadini di gestire tutte le comunicazioni ufficiali direttamente online, la cui attivazione è facile e immediata: grazie a SPID, infatti, non sono necessari alcuna password o codice aggiuntivi. Il cittadino utilizza le credenziali SPID sia per registrarsi la prima volta, che per accedere ed utilizzare il servizio.

Nell'ottica dell'identificazione certa del mittente del messaggio di posta certificata, SPIDmail è inoltre già avviato verso il recapito qualificato internazionale rispetto al Regolamento eIDAS e allo standard REM, in quanto identifica in modo forte il titolare.

La casella può essere usata esclusivamente attraverso il web, utilizzando la webmail: il titolare della casella di PEC ha la possibilità di accedervi attraverso un comune browser Internet. L'indirizzo (HTTPS, navigazione tramite canale sicuro) del sistema webmail di Namirial è https://webmail.spidmail.it/ e viene comunicato al titolare nel messaggio di benvenuto, che viene inviato a seguito dell'attivazione della casella.

Utilizzando un browser Internet:

- l'utente si collega all'indirizzo specifico sopra citato;
- a tale indirizzo web risponde l'applicativo webmail, l'accesso al quale è subordinato all'inserimento delle credenziali Spid del titolare della casella;
- una volta superata la validazione dell'accesso al sistema, l'utente si trova all'interno dell'applicativo webmail dove può inviare, ricevere, cercare i messaggi, gestire e utilizzare gli eventuali servizi aggiuntivi richiesti e modificare le impostazioni dell'applicazione.

Il servizio è distribuito secondo il modello "pay per use", pertanto l'utente conferisce un corrispettivo per ciascun messaggio spedito; è possibile, comunque, convertire il sistema da "pay per use" a "flat", attivando un abbonamento annuale che prevede l'invio illimitato di messaggi secondo quanto previsto dalle condizioni generali di contratto.

4.9 Accesso al servizio(i)

La casella PEC può essere utilizzata sia attraverso il web, utilizzando la webmail, sia attraverso i più diffusi client di posta. Le guide per la configurazione e l'uso della casella PEC su client sono disponibili sul sito web del Servizio del Gestore.

4.9.1 Accesso attraverso i client di posta

Il titolare può accedere alla casella attraverso i più comuni client di posta (quali ad esempio Thunderbird, Outlook Express, Outlook) che rispondano ai requisiti di verifica delle firme del Gestore, descritte nel documento al riferimento [V] (paragrafo 9.2 Appendice A).

Prima di utilizzare la casella su un client di posta è necessario abilitare i protocolli IMAP/SMPT o il protocollo POP tramite le impostazioni della webmail. In caso contrario l'utente può scegliere di mantenere queste opzioni disabilitate.

All'interno del messaggio di benvenuto, inviato al titolare della casella a seguito dell'attivazione della stessa, e nella sezione dedicata nelle impostazioni della webmail, sono elencati tutti i parametri di configurazione, necessari per l'accesso al sistema attraverso i client di posta ed in particolare:

Parametri accesso Base:

IMAPS	
Indirizzo del server IMAP	**imaps.sicurezzapostale.it**
Nome account	indirizzo di posta certificata
Password	la password assegnata alla casella
Usa SSL	attiva
Porta	993

POPS	
Indirizzo del server POP	**pops.sicurezzapostale.it**
Nome account	indirizzo di posta certificata
Password	la password assegnata alla casella
Usa SSL	attiva

Porta	995

SMTPS	
Indirizzo del server SMTP	**smtps.sicurezzapostale.it**
Nome account	indirizzo di posta certificata
Password	la password assegnata alla casella
Usa SSL	attiva
Porta	465

Parametri accesso Pro:

IMAPS	
Indirizzo del server IMAP	**pro-imaps.sicurezzapostale.it**
Nome account	indirizzo di posta certificata
Password	la password assegnata alla casella
Usa SSL	attiva
Porta	993

POPS	
Indirizzo del server POP	**pro-pops.sicurezzapostale.it**
Nome account	indirizzo di posta certificata
Password	la password assegnata alla casella
Usa SSL	attiva
Porta	995

SMTPS	
Indirizzo del server SMTP	**pro-smtps.sicurezzapostale.it**
Nome account	indirizzo di posta certificata
Password	la password assegnata alla casella
Usa SSL	attiva
Porta	465

Una volta configurato il proprio client di posta, il titolare può utilizzare 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 anomalie, 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 recante un testo che indica che il messaggio in partenza è corretto, è stato accettato dal sistema ed è stato indirizzato 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**. La ricevuta di avvenuta consegna è inviata dal Gestore della casella PEC del destinatario ed è un messaggio di posta con subject "CONSEGNA:", seguito dal subject del messaggio originale e recante un testo che indica che il messaggio è stato recapitato nella casella del destinatario. La ricevuta include, in allegato, un file xml contenente 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** la quale è un messaggio di posta che ha come subject "POSTA CERTIFICATA:", seguito dal subject del messaggio originale e recante nel 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 differenti avvisi, che hanno in comune il fatto di avere un subject con un prefisso particolare, seguito dal subject originale; tali avvisi includono un testo che ne spiega la tipologia. Alcuni di questi sono: avviso di mancata consegna, avviso di non accettazione per virus, avviso di mancata consegna per superamento tempi massimi, etc.

4.9.2 Accesso tramite webmail

URL di accesso

https://webmail.sicurezzapostale.it

https://webmailpro.sicurezzapostale.it

Spidmail: https://spidmail.namirial.it/

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

L'indirizzo (HTTPS, navigazione tramite canale sicuro) del sistema webmail di Namirial viene comunicato al titolare nel messaggio di benvenuto che viene inviato a seguito dell'attivazione della casella.

Utilizzando un browser internet:

- l'utente si collega all'indirizzo specifico sopra citato;
- a tale indirizzo web risponde l'applicativo webmail, l'accesso al quale è subordinato all'inserimento delle credenziali di accesso;
- al primo accesso l'utente dovrà obbligatoriamente procedere al cambio della password;
- una volta superata la validazione dell'accesso al sistema, l'utente si trova all'interno dell'applicativo webmail dove può inviare, ricevere, cercare i messaggi, gestire e utilizzare gli eventuali servizi aggiuntivi richiesti e modificare le impostazioni dell'applicazione.
-

Esclusivamente per le caselle di tipo SpidMail, il cittadino dovrà collegarsi all'indirizzo dedicato ed utilizzare le proprie credenziali SPID per accedere. Le caselle SpidMail non supportano l'accesso con il client di posta.

Attraverso la webmail l'utente può scegliere, per ogni singolo messaggio originale da inviare, il tipo di ricevuta di avvenuta consegna. La ricevuta, come specificato al § 3.2, può essere completa (contenente cioè il messaggio originale e gli eventuali allegati), breve (contenente il messaggio originale con una codifica hash degli allegati) o sintetica (contenente i soli dati di certificazione).

4.9.3 Delega dell'autenticazione – accesso federato

Namirial consente ai propri utenti di accedere al Servizio PEC anche per il tramite di meccanismi di autenticazione delegati. Nello specifico, questi sono federati con il servizio di autenticazione PEC Namirial, consentendo l'accesso in modalità Single Sign-On (SSO) alla webmail a fronte dell'autenticazione effettuata utilizzando SPID, CIE o CNS da parte del titolare della casella.

4.10 Smarrimento delle credenziali di accesso al sistema

In caso di smarrimento delle credenziali di accesso al sistema, il titolare di una casella di PEC può resettare la password seguendo le indicazioni contenute nel seguente link: https://adesione.sicurezzapostale.it/RESETPSW/.

In alternativa, il titolare può richiedere al Gestore una nuova password attraverso l'invio di un modulo, scaricabile al link http://www.sicurezzapostale.it/docs/Richiesta_credenziali_accesso.pdf, nel quale devono essere indicate le seguenti informazioni:

- Casella PEC
- Nome, Cognome ed eventuale Ragione Sociale
- Indirizzo (Via, Città, CAP, Nazione)
- Codice Fiscale ed eventuale Partita IVA
- email valida (per eventuali comunicazioni)

La richiesta può essere inviata via posta certificata, fax o raccomandata A/R, come indicato all'interno del modulo di richiesta.

Con il modulo, il titolare deve inviare fotocopia di un documento di identità in corso di validità.

Il personale di servizio dell'help desk del Gestore Namirial S.p.A. si occupa della elaborazione delle richieste pervenute.

4.11 Richiesta e reperimento dei log dei messaggi(h)

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 propria casella di PEC. La richiesta può essere effettuata attraverso il modulo disponibile al link: 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 richiesta può essere inviata via posta certificata, fax o raccomandata A/R, come indicato all'interno del modulo di richiesta.

In alternativa, la richiesta dei file di LOG può essere esercitata inviando una richiesta direttamente dalla propria casella di PEC alla PEC del Gestore indicando i dati minimi necessari al recupero degli stessi (vedi punto elenco precedente).

Con il modulo, il titolare deve inviare fotocopia di un documento di identità in corso di validità.

L'indirizzo di posta certificata, utilizzato dal gestore per la ricezione delle richieste dei LOG da parte degli utenti, viene comunicato agli stessi anche nel messaggio di benvenuto inviato a seguito dell'attivazione della casella.

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

4.12 Richiesta di chiusura di una casella PEC

Il titolare può richiedere al Gestore la chiusura della propria casella certificata attraverso il modulo disponibile al seguente link:

http://www.sicurezzapostale.it/docs/Richiesta_Cancellazione_casella_PEC.pdf.

Nel modulo vanno indicate le seguenti informazioni:

- PEC da chiudere
- Nome, Cognome ed eventuale Ragione Sociale
- Indirizzo (Via, Città, CAP, Nazione)
- Codice fiscale ed eventuale partita IVA
- email PEO valida (per eventuali comunicazioni)

La richiesta può essere inviata via posta certificata, fax o raccomandata A/R, come indicato all'interno del modulo di richiesta.

In alternativa, la chiusura della casella PEC può essere esercitata inviando una richiesta direttamente dalla propria casella di PEC alla PEC del Gestore indicando i dati minimi necessari (vedi punto elenco precedente).

Con il modulo, il titolare deve inviare fotocopia di un documento di identità in corso di validità.

La richiesta di chiusura può essere effettuata solamente dal titolare della casella. A seguito di essa, il Gestore effettua una serie di controlli ed invia al titolare una comunicazione, via PEC, recante la data di chiusura della casella.

Il Gestore ha altresì facoltà di chiudere una casella PEC a fronte di inadempienze contrattuali del Titolare, descritte nelle Condizioni Generali del Servizio.

All'approssimarsi della scadenza del contratto, il Gestore invia al Titolare avvisi di scadenza ed invito al rinnovo della stessa. Qualora il titolare non rinnovi nei tempi previsti, il Gestore si riserva la facoltà di sospendere l'account per 30 giorni, trascorsi i quali ed in mancanza di rinnovo, la casella viene chiusa.

In caso di abbonamento attivo, l'utente ha disposizione ulteriori 30 giorni a partire dalla data di scadenza per regolarizzare il pagamento, al termine dei quali in mancanza di rinnovo, il Gestore provvederà alla sospensione dell'account per i successivi 30 giorni. Qualora il titolare non rinnovi entro il termine dei complessivi 60 giorni dalla scadenza della casella, la casella viene chiusa.

Quando una casella è chiusa:

- il Titolare non può più utilizzarla per spedire o ricevere nuovi messaggi;
- il Gestore ne mantiene il contenuto per i 180 giorni successivi alla chiusura; inoltre, ne riserva la denominazione, che non potrà quindi essere assegnata a un diverso richiedente; pertanto, durante questo periodo di 180 giorni il titolare ha la possibilità di richiedere il ripristino della casella, delle sue funzionalità e del suo contenuto;
- trascorso il termine dei 180 giorni ed in assenza di iniziativa da parte del titolare, tutto il contenuto della casella chiusa viene eliminato. Il nome della casella rimane altresì riservato e non più utilizzabile per nuove attivazioni. Il titolare può sempre chiedere l'attivazione di una nuova casella, con la stessa denominazione ma priva del contenuto della precedente.

4.13 Cessazione del servizio di Posta Elettronica certificata[(l)]

Nel caso di cessazione dell'attività di Gestore di Posta Elettronica Certificata, Namirial S.p.A. ne dà comunicazione all'Agenzia per l'Italia Digitale almeno sessanta (60) giorni prima della data di cessazione indicando, qualora conosciuto, il Gestore Sostitutivo che prenderà in carico le caselle di PEC attive.

Contestualmente, con medesimo preavviso il Gestore annuncia ai titolari la cessazione dell'attività di Gestore, tramite una comunicazione diretta via PEC e tramite una comunicazione ufficiale pubblicata sul sito internet.

Qualora non sia previsto un Gestore Sostitutivo che prenderà in carico le caselle PEC, nella comunicazione di cessazione viene specificato che tutte le caselle diverranno inaccessibili dal momento della cessazione dell'attività.

4.14 Servizio di Help Desk

Per quanto concerne la gestione di problematiche relative al servizio di posta elettronica certificata, il Gestore Namirial S.p.A. ha predisposto uno specifico canale di comunicazione (Help Desk) con l'utenza finale.

L' Help Desk è costituito da uno staff di persone formate e preposte all'assistenza clienti per il servizio di posta elettronica certificata ed è raggiungibile al numero di selezione automatica, indicato al § 2.4, durante l'orario di ufficio: dalle 9.00 alle 19.00, dal lunedì al venerdì.

Le richieste di assistenza possono altresì essere inviate 24 ore su 24, tramite posta elettronica all'indirizzo pec@namirial.com oppure attraverso il sito istituzionale del Gestore, al seguente link: https://support.namirial.com/it/supporto-tecnico/ indicando il servizio per il quale si richiede l'assistenza e compilando quanto richiesto.

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

Il cliente del servizio ha la facoltà 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 ed 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 segnalare eventuali problemi riscontrati durante l'invio e/o la ricezione dei messaggi attraverso il client di posta oppure la webmail.

4.14.1 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 dell'assistenza;
- aggiornare il ticket, annotando gli interventi fatti e le comunicazioni con il cliente;
- 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.

4.15 Livelli di servizio ed indicatori di qualità[(j)]

Il Gestore Namirial S.p.A. garantisce il rispetto dei livelli di erogazione del 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)	**Almeno 100MB da client di posta**

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 minuti**

Tabella 5: livelli di servizio

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

Indicatori di qualità	
Disponibilità del servizio (invio, ricezione e consultazione dei messaggi PEC)	**24x7x365**
Disponibilità del servizio di richiesta di attivazione	**24x7x365**
Tempo per l'attivazione di un nuovo account di PEC (dalla ricezione di tutta la documentazione necessaria)	**6 giorni lavorativi**
Disponibilità del servizio di richiesta, da parte del titolare, dei LOG dei messaggi, relativi alle comunicazioni effettuate	**24x7x365**
Accesso ai file di LOG da parte del personale di Namirial S.p.A.	**da lunedì a venerdì dalle 9.00 alle 19.00**
Tempo massimo per l'invio delle informazioni relative ai file di LOG, a seguito di richiesta del titolare	**5 giorni lavorativi**

Disponibilità del sistema di monitoring, con invio di messaggi di alert via email e/o sms al verificarsi di malfunzionamenti e situazioni critiche	**24x7x365**
Assistenza tramite call center	**da lunedì a venerdì dalle 9.00 alle 19.00**
Ricezione segnalazioni da parte della clientela	**24x7x365**

Tabella 6: indicatori di qualità del servizio

5 Adeguamento della PEC ai nuovi standard europei

Il Regolamento EU n. 910/2014 del 23.07.2014 cosiddetto eIDAS introduce i "servizi elettronici di recapito certificato" o "Electronic Registered Delivery services" come parte dei servizi fiduciari ed inoltre introduce il concetto di "servizio fiduciario qualificato".

La PEC che già soddisfa i requisiti per il servizio elettronico di recapito certificato, si prepara a soddisfare anche quelli per il servizio qualificato.

Un servizio elettronico di recapito certificato (ERDS) fornisce la consegna sicura e affidabile di messaggi tra le parti, fornendo la prova del processo di consegna per la responsabilità legale.

Un servizio elettronico di recapito certificato qualificato (QERDS), soddisfa alcuni requisiti aggiuntivi, in particolare, l'identificazione certa del titolare e l'autenticazione forte.

Pertanto, la PEC *tradizionale* evolve normativamente e diventerà uno strumento di scambio sicuro di comunicazioni elettroniche, con valore legale riconosciuto in tutti gli stati europei.

Il primo dei requisiti per adeguare la PEC ai nuovi standard Europei è l'identificazione del titolare della casella.

Solo dopo la corretta identificazione, la casella sarà pronta a rispettare i nuovi standard normativi e le regole tecniche ed otterrà da subito la "Spunta blu".

Il secondo requisito è l'autenticazione forte, che prevede l'utilizzo di almeno due fattori appartenenti a categorie differenti.

5.1 Reidentificazione

Namirial, in prospettiva della REM (Registered Electronic Mail, la cosiddetta "PEC Europea"), ha avviato le procedure per la re-identificazione degli utenti, che dovrà avvenire prima dell'entrata in esercizio di questa.

Il titolare di una casella può essere una persona fisica, un'impresa o un ente/pubblica amministrazione. L'identificazione certa si riferisce sempre all'identificazione di una persona fisica e avviene mediante meccanismi anche elettronici.

Nel caso di impresa o ente/pubblica amministrazione il soggetto legittimato ad essere identificato,è colui che ne ha la rappresentanza legale, vale a dire colui che ha il potere di compiere atti e negozi giuridici in nome e per conto dell'ente, manifestando all'esterno la volontà di questo ed essendo quindi dotato di potere di firma.

È possibile, pertanto, distinguere tra la re-identificazione per le caselle intestate alla persona fisica e quelle intestate alla persona giuridica.

In caso di casella intestata a persona fisica, è condizione necessaria che l'utente da reidentificare coincida con il titolare PEC registrato nei sistemi Namirial.

Qualora l'utente che abbia intrapreso la procedura di re-identificazione dovesse risultare non corrispondente al soggetto avente titolo, il sistema consentirà di inoltrare via mail alla persona fisica corretta il link per il riconoscimento.

Il processo prevede che l'utente possa scegliere un metodo di identificazione tra quelli disponibili, la re-identificazione avrà esito positivo soltanto se i dati della persona correttamente identificata dovessero corrispondere a quelli del titolare registrato nei sistemi di Namirial; al contrario, la richiesta di identificazione fallirebbe, e pertanto occorrerà eseguirne una nuova.

Nel caso di casella intestata ad una persona giuridica, è invece condizione necessaria che i dati societari restino invariati (rispettivamente ragione sociale, P.IVA, codice fiscale aziendale e/o codice IPA), mentre è possibile variare i dati del responsabile e il responsabile da identificare può non corrispondere a quello già registrato.

A tal fine è possibile sia aggiornare i dati del responsabile con quelli di un altro soggetto legittimato, sia invitare l'effettivo responsabile a identificarsi come dettagliato sopra.

Al superamento degli opportuni controlli sul codice fiscale aziendale e sulla carica del soggetto responsabile la procedura di re-identificazione potrà considerarsi positivamente conclusa.

Qualora l'utente non perfezioni la procedura di identificazione entro la data di attivazione del Servizio REM, la Casella PEC rimarrà attiva in sola consultazione sino alla scadenza del contratto.

5.2 Spunta blu

Alcuni gestori hanno aderito all'iniziativa "Spunta blu", per sensibilizzare gli utenti ad adeguare la PEC agli standard europei.

Per ottenere la spunta blu è necessario che il titolare si sia re-identificato in modo certo, secondo le modalità descritte nel paragrafo dedicato: subito dopo la re-identificazione, accedendo alla webmail l'utente vedrà l'elemento grafico .

Inoltre, l'elemento grafico sarà presente anche nei messaggi ricevuti a condizione che questi provengano da un mittente identificato dal proprio Gestore e che sia il Gestore della casella mittente che abbia aderito all'iniziativa: l'obiettivo è evidenziare che il mittente sia stato identificato secondo i requisiti degli standard europei.

5.3 Autenticazione a due fattori

Il secondo requisito per il passaggio alla PEC Europea è garantire una maggiore sicurezza nell'utilizzo del servizio e nell'accesso alla casella. Infatti, per accedere al servizio sarà richiesta l'autenticazione a due fattori; quindi, oltre alla password sarà necessario inserire un codice temporaneo.

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, formato 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.) che soddisfino i requisiti minimi stabiliti dalle regole tecniche di cui al [V];
- conformità allo standard internazionale RFC3161 per la marcatura temporale dei file di LOG e per l'interfacciamento con una Time Stamping Authority accreditata;

- 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 la verifica dei messaggi.

6.2 Scalabilità e Affidabilità

L'architettura del Gestore Namirial S.p.A. è altamente scalabile; pertanto, può essere estesa in qualsiasi momento per rispondere alle esigenze di crescita della domanda, in modo tale da mantenere i tempi di risposta ed i livelli di qualità erogati dal Gestore.

In tema di affidabilità dell'architettura, 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 del servizio. Inoltre, viene utilizzato uno storage condiviso per la memorizzazione delle informazioni comuni, in modo da garantire 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 sono interamente gestiti e mantenuti all'interno di dispositivi ad alta sicurezza (**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**: rilevazione di tentativi di manomissione o accesso non autorizzato;
- **tamper proofness**: cancellazione della memoria e delle chiavi in caso di accesso o manomissione.

6.4 Caratteristiche del sistema

La soluzione di posta elettronica certificata adottata da Namirial S.p.A. si fonda sul prodotto **OpenPEC**, 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 del Gestore;
- marcatura temporale e storicizzazione dei log.

6.5 Riferimenti temporali

Il Decreto Ministeriale di cui al [V] stabilisce che ad 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 altri termini, l'indicazione dell'istante di elaborazione del messaggio risulta univoca all'interno dei LOG, delle ricevute, degli avvisi e dei messaggi generati dal sistema.

La fonte primaria di riferimento temporale della piattaforma PEC è costituita dagli stessi dispositivi utilizzati da Namirial per erogare il servizio di Time Stamp Autority accreditato. Namirial è Qualified Trust Service Provider eIDAS anche per l'emissione di validazioni temporali e certificati qualificati. In particolare ha conseguito il certificato n. IT269191 rilasciato da Bureu Veritas Italia SpA per l'emissione di validazioni temporali qualificate (marche temporali).

Il sistema PEC quindi si interfaccia con i server del servizio di Certificazione e Validazione Temporale erogato da Namirial S.p.A. Al fine di garantire un corretto e puntuale valore temporale, vengono contattati anche i server NTP dell'Istituto Nazionale di Ricerca Metrologica (INRIM). L'orologio di sistema viene mantenuto sincronizzato con quello di riferimento e ciò compensa anche la deriva e le fluttuazioni che possano 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 segue, 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, minuti 35, secondi 16, 1 ora avanti rispetto al riferimento UTC.

6.6 Storicizzazione dei Log, dei messaggi contenenti virus e loro conservazione a norma

Il Decreto Ministeriale di cui al [V] stabilisce che ogni sistema di posta elettronica certificata deve prevedere un intervallo temporale unitario non superiore alle ventiquattro ore, entro il quale eseguire, senza soluzione di continuità, il salvataggio dei LOG legali dei messaggi; i LOG vengono conservati per un periodo di almeno 30 mesi.

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

Il Decreto Ministeriale stabilisce inoltre le modalità per la rilevazione, la segnalazione e la conservazione dei messaggi di posta elettronica certificata contenenti virus; in particolare:

- nel caso di spedizione, è al Punto di Accesso, ossia nella fase immediatamente successiva all'invio del messaggio, che il gestore mittente deve verificare la presenza di virus nei messaggi originali di posta

elettronica. Il sistema deve quindi comunicare al mittente che il suo messaggio contiene un virus e tale comunicazione avviene attraverso l'emissione di un "AVVISO DI NON ACCETTAZIONE PER VIRUS".
- nel caso di ricezione, il gestore destinatario deve verificare la presenza di virus al Punto di Ricezione. Il sistema deve emettere ed inviare al gestore del mittente un avviso di rilevazione virus, avente ad oggetto "PROBLEMA DI SICUREZZA"; di conseguenza, il gestore del mittente emette un messaggio, recante la denominazione "AVVISO DI MANCATA CONSEGNA PER VIRUS" e lo deposita nella casella del mittente.

I messaggi contenenti virus devono essere conservati per un periodo di almeno 30 trenta mesi, secondo quanto stabilito dalle normative di cui al [V] e al [X].

In data 5 luglio 2016, AgID ha inoltre emanato le "ISTRUZIONI PER LA CONSERVAZIONE DEI LOG DEI MESSAGGI E DEI MESSAGGI DI POSTA ELETTRONICA CERTIFICATA CON VIRUS", le quali obbligano il gestore a sottoporre a Conservazione a Norma i file di LOG legali ed i messaggi contenenti virus, in conformità alle disposizioni del Dlgs. 82/2005 ed ai requisiti tecnici previsti dal DPCM 3 dicembre 2013.

Il processo di conservazione è finalizzato a garantire:

- l'identificazione certa del soggetto che ha formato il documento (tipicamente il soggetto che ha la responsabilità del documento) e dell'amministrazione che ha prodotto il documento;
- l'integrità del documento;
- l'intellegibilità e l'agevole reperibilità dei documenti e delle informazioni identificative, inclusi i dati originari di registrazione e di classificazione;
- il rispetto delle misure di sicurezza, descritte al §8.6, in ottemperanza alle disposizioni del GDPR

La soluzione adottata da Namirial S.p.A. è conforme alla regolamentazione in oggetto e realizza quanto necessario per garantire la massima continuità di servizio.

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

Ai fini dell'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 27001:2013**.

Lo standard, che sostituisce la norma di riferimento BS 7799 (Information Security Management System ISMS), prevede l'esecuzione di una serie di processi, misure e procedure volti a fornire tutte le garanzie di sicurezza e di protezione dei dati, 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 27001:2013 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, sia dell'azienda che dei propri clienti, i requisiti necessari ad ottenere un adeguato sistema per gestire la sicurezza delle informazioni e dei dati sensibili.

Lo standard prevede inoltre le procedure per:

- l'analisi dei rischi (individuazione dei punti deboli, studio delle possibili minacce e della probabilità che si presentino, analisi degli eventuali impatti sul sistema)
- la gestione dei rischi (monitoring del sistema, rilevazione dei problemi e loro risoluzione, eliminazione dei 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 quali requisiti di sicurezza debbano essere rispettati dai moduli crittografici, utilizzati all**'**interno di sistemi nei quali vengono trattati dati sensibili. Fanno parte di questa serie le specifiche dei moduli crittografici e le 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, i primi 3 dei quali 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.

Tabella 7: livelli sicurezza HSM

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. offre tutte le garanzie di sicurezza, compatibili con la tipologia del servizio erogato. Le misure di sicurezza, di seguito elencate, sono descritte in maniera più approfondita e dettagliata nel **Piano di Sicurezza**, un documento riservato, redatto in base alle

disposizioni della circolare di cui al [VI] custodito presso la sede del Gestore e consegnato ad AgID.

7.3.1 Risorse umane adibite alla gestione del sistema

In ottemperanza a quanto stabilito dalla normativa, oltre al Responsabile del Servizio sono previsti altri 5 responsabili del servizio di PEC:

- 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 informato sulla delicatezza del servizio erogato e sulla necessità di dedicare la maggior cura ed attenzione possibili allo svolgimento dei compiti assegnati. Nelle fasi iniziali, ogni nuovo incaricato viene seguito personalmente da un tutor aziendale.

7.3.2 Sicurezza dell'infrastruttura

Dal punto di vista prettamente informatico, la sicurezza del sistema viene realizzata dal Gestore Namirial S.p.A 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 al 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 storage (in modo da aumentare il grado di protezione dei dati)
- utilizzo di storage di rete esterni al sistema, per aumentare il livello di protezione delle informazioni degli utenti
- sistema ridondato in ogni sua parte, al fine di evitare “single point of failure”

- sistema di backup, per ridurre il rischio di perdita dei dati

7.3.3 Analisi e gestione dei rischi

Il sistema di posta elettronica certificata di Namirial S.p.A. viene sottoposto a verifiche periodiche, finalizzate ad analizzarne le criticità, individuarne la vulnerabilità ed identificare i possibili rischi ai quali è sottoposto. Grazie ad un'attenta analisi, il Gestore Namirial S.p.A. è in grado di prevenire la maggior parte dei malfunzionamenti e di 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 difetti causati da problemi dei sistemi hardware e software e generalmente possono essere risolti attraverso attività di manutenzione ordinaria o straordinaria come, ad esempio, la sostituzione degli apparati o l'upgrade dei componenti software. I secondi sono avarie causate da eventi catastrofici, atti dolosi o errori umani, dovuti a incompetenza o negligenza e possono provocare danni gravi ed interruzione del servizio.

7.3.4 Azioni di contrasto alla diffusione di contenuto malevolo

Namirial S.p.A. lavora costantemente per migliorare la qualità e la sicurezza del servizio introducendo tecnologie aggiornate e personale qualificato. Per garantire la massima velocità ed efficacia di intervento quanto descritto nel seguito deve essere inteso come indicativo e non esaustivo.

Ricordiamo inoltre che tutte le azioni e gli sforzi messi in campo da Namirial S.p.A. per contrastare il fenomeno in oggetto restano un supporto all'utente che deve sempre porre la massima attenzione per utilizzare in maniera sicura il servizio di PEC.

7.3.4.1 Tecnologie antimalware

Namirial S.p.A. adotta più tecnologie antimalware in parallelo costantemente aggiornate.

Le soluzioni in uso non si limitano alla ricerca delle firme dei virus su repository differenti ma utilizzano sistemi innovativi come sandbox e algoritmi brevettati per l'individuazione degli 0-day.

L'analisi dei servizi antimalware non comprende solo gli allegati ma è estesa al corpo di messaggi con particolare attenzione alle URL.

Vengono inoltre monitorati i falsi positivi per adattare il comportamento dei sistemi alle specificità del traffico ed ai suoi cambiamenti nel tempo.

I messaggi rilevati come malevoli vengono gestiti secondo normativa e segnalati al mittente o al suo gestore.

7.3.4.2 Analisi degli allegati

Gli allegati sono il componente dei messaggi maggiormente attenzionato dai sistemi di sicurezza.

Sono previsti controlli specifici sugli allegati in aggiunta all'azione degli antimalware, per inibirne l'invio o semplicemente per avvisare l'utente di casi sospetti a cui porre la massima attenzione.

In particolare:

- la webmail applica alcune limitazioni sulle tipologie di file che è possibile allegare ad un nuovo messaggio PEC: l'utente che tenterà di allegare uno o più file considerati potenzialmente pericolosi riceverà un avviso con l'indicazione del nome file che è stato bloccato.
  Sono stati inoltre presenti controlli sugli allegati che vengono visualizzati o scaricati dalla webmail e qualora il sistema rileverà condizioni potenzialmente pericolose verrà mostrato un apposito messaggio all'utente;
- punto di accesso: sono presenti le stesse limitazioni che causano l'inibizione dell'invio di nuovi messaggi certificati da client di posta e l'emissione di ricevute di mancata accettazione contenenti un messaggio di avviso idoneo;
- punto di ricezione: nel caso di situazioni sospette come la presenza di macro o allegati criptati viene aggiunto un apposito header speciale alla busta di trasporto in ingresso sfruttabile dagli integratori per eventuali segnalazioni.

7.3.4.3 Password policy

Namirial S.p.A. applica una serie di regole per aiutare l’utilizzatore a scegliere una password sicura e affidabile.

La password è scelta dal titolare della casella e deve soddisfare requisiti di complessità prestabiliti che Namirial S.p.A. si riserva di aggiornare in qualsiasi momento:

- deve avere una lunghezza minima di 8 caratteri;
- deve contenere caratteri alfanumerici, caratteri speciali _.-?#+;:!@, maiuscole e minuscole;
- è inibito il riutilizzo di password recenti;
- si verifica che non siano presenti parole di utilizzo frequente o sequenze ripetute di caratteri;
- si verifica che la password non sia inclusa in elenchi di password oggetto di data breach;
- viene fornito uno strumento informativo che consente all'utente di stabilire con facilità la bontà della password immessa.

La password può essere modificata dal titolare della casella dalla sezione *Impostazioni* della webmail.

In caso di smarrimento è possibile impostarne una nuova accedendo tramite il link apposito disponibile sulla pagina di login sempre della webmail.

7.3.4.4 Sistemi di monitoraggio delle attività sospette

Sono adottati sistemi di analisi del traffico non solo automatici che evidenziano schemi di attacco mettendo in relazione, tra gli altri, numero di invii nel periodo temporale di riferimento, indirizzi di provenienza, tipologia di casella e analisi antispam in modalità trasparente sulle buste di trasporto in uscita.

Nel caso in cui Namirial S.p.A. rilevi un comportamento anomalo sul traffico in uscita, le credenziali della casella PEC verranno immediatamente resettate ed il titolare sarà avvisato attraverso le informazioni di contatto in possesso suggerendo una scansione antivirus approfondita della propria postazione prima di aggiornare le credenziali di accesso.

7.3.4.5 Procedure di mutua assistenza tra gestori

Namirial S.p.A. si riserva di predisporre procedure di mutua assistenza tra gestori al fine di rafforzare il contrasto alla diffusione di contenuto malevolo veicolato attraverso il canale PEC.

Ciò può comportare la condivisione di URL, tipologie di messaggi, schemi e analisi comportamentali, IOC (Indication Of Compromise) e altre informazioni in modo anonimo garantendo sempre la massiva riservatezza nel rispetto di quanto previsto dal regolamento privacy.

7.3.5 Contrasto allo spam

Nel rispetto della normativa vigente, Namirial S.p.A. fornisce il servizio antispam sul traffico di posta elettronica ordinaria in ingresso alla casella PEC. La ricezione di tale traffico è opzionale e deve essere abilitata attraverso la sezione *Impostazioni* della webmail.

Tale servizio si limita a segnalare all'utenza attraverso opportuni avvisi e spostare in un folder dedicato i messaggi ritenuti indesiderati e/o pericolosi.

È importante ricordare che il servizio antispam non garantisce un intervento esatto ma rappresenta uno strumento di ausilio per l'utilizzatore che deve sempre valutare accuratamente la bontà dei messaggi ricevuti.

7.3.6 Controllo dei livelli di sicurezza

I livelli di sicurezza vengono controllati attraverso continue attività di monitoring su tutti i principali componenti del sistema di posta certificata. Sono inoltre previste, con cadenza almeno semestrale, visite ispettive interne che hanno lo scopo di esaminare il sistema nel suo complesso, al fine di verificarne il livello di sicurezza ed individuarne eventuali criticità. Per raggiungere la certezza che il sistema sia sicuro e conforme vengono monitorati:

- 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

Ciascuna visita termina con 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 effettuate modifiche 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(e)

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

7.4.1 Organizzazione del personale

Come già accennato nel **§** 6.3.2 ed in ottemperanza al Decreto di cui al [V], Namirial S.p.A. ha predisposto una struttura interna, composta dai seguenti responsabili di settore:

- 1 responsabile del Servizio;
- 1 responsabile della Registrazione dei titolari;
- 1 responsabile dei Servizi tecnici;
- 1 responsabile delle Verifiche e delle ispezioni (auditing);
- 1 responsabile della Sicurezza;
- 1 responsabile 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 necessarie a svolgere i compiti assegnati.

7.4.2 Sistema di Monitoring

Tutti i servizi di posta elettronica certificata di Namirial S.p.A. vengono costantemente controllati attraverso un apposito sistema di monitoring. Il sistema genera segnali di alert ogni qualvolta vengano superate le soglie critiche, impostate in fase di amministrazione. I segnali di alert, raccolti 24x7x365, vengono inviati, attraverso messaggi di posta, al personale preposto e in grado di intervenire prontamente per risolvere la criticità. Attraverso il sistema di monitoring, il Gestore Namirial S.p.A. controlla, per tutte le macchine del sistema, i seguenti parametri: spazio disco, carico della CPU, occupazione di memoria, attività dei processi, situazione delle code, etc.

Oltre ai controlli interni, per i controlli di sicurezza e per il monitoraggio dei sistemi Namirial si avvale di un partner esterno, in servizio 24/7/365 il quale, in seguito alla rilevazione di malfunzionamenti e/o anomalie, effettua segnalazioni nelle modalità e nei tempi indicati dal manuale.

L’infrastruttura di monitoraggio è dotata di un sistema SIEM che elabora tutte le informazioni provenienti dai dispositivi e dai Server, eseguendo in real time un’analisi che permette di intercettare eventuali attacchi ed inviare la relativa segnalazione al suddetto al SOC esterno, con il quale sono concordate le procedure di escalation H24, in base alla gravità degli eventi riscontrati.

7.4.3 Gestione e risoluzione dei problemi

La gestione dei problemi avviene secondo la seguente procedura:

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 della constatazione di un evento anomalo

   In tutti e tre i casi, un operatore di help desk prende in carico la segnalazione e la inoltra al **Team di Supporto** (**TdS**).

2) Il TdS prende in carico la segnalazione, la analizza, verifica l’effettiva consistenza del problema e ne cerca la risoluzione.
3) Il TdS individua le possibili risoluzioni del problema e le mette a confronto, allo scopo di selezionare quella migliore in termini di minore impatto sul servizio e velocità di risoluzione.
4) Il TdS può valutare l’opportunità di utilizzare il supporto di terzi, intesi sia come personale specializzato interno che come consulenti esterni.
5) Il TdS mette in atto la risoluzione e risolve il problema. Nel caso in cui sia stato previsto il supporto di personale esterno all'azienda, il TdS fornisce ad esso assistenza durante tutte le attività svolte ed effettua un presidio costante tracciando, in tempo reale, tutte le operazioni effettuate.
6) Una volta completato l'intervento, il TdS ne informa l'Help Desk.
7) Il servizio di Help Desk effettua un’ulteriore verifica circa l’avvenuta risoluzione del problema e comunica la stessa all’autore della segnalazione.

7.5 Azioni promosse dal gestore in caso di malfunzionamento

In base alla circolare CNIPA di cui al [VII], il Gestore è tenuto comunicare tempestivamente AgID i malfunzionamenti riscontrati nel proprio sistema. Nella segnalazione, il Gestore deve comunicare 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 decreto del Presidente della Repubblica 11 febbraio 2005, n. 68, relativo alle funzioni base (trattamento del messaggio originario, ricevute e avvisi) per il quale non è circoscritto il potenziale impatto.
	1B: rilevato da terzi	
Comportamento anomalo circoscritto	2A: rilevato dal gestore	Comportamento difforme dalle regole tecniche di cui all'art. 17 del decreto del Presidente della Repubblica 11 febbraio 2005, n. 68, relativo alle funzioni base (trattamento del messaggio originario, ricevute e avvisi) per il quale è circoscritto il potenziale impatto.
	2B: rilevato da terzi	
Malfunzionamento bloccante	3A: rilevato dal gestore	Tipologia di malfunzionamento a causa del quale le funzionalità del sistema di PEC, come definite nelle regole tecniche di cui all'art. 17 del decreto del Presidente della Repubblica 11 febbraio 2005, n. 68,
	3B: rilevato da terzi	

		non possono essere utilizzate in tutto o in parte dagli utenti.

Tabella 8: azioni promosse in caso di malfunzionamenti

Le segnalazioni degli utenti vengono catalogate 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)

Tabella 9: catalogazione degli eventi di malfunzionamento

Nei casi 1A e 1B il gestore auto-sospende il servizio, dandone informazione ai propri utenti e agli altri gestori. Nei casi 2A e 2B l'Organo di Vigilanza può decidere di sospendere il servizio del gestore, fino a quando il problema non sia stato risolto. In entrambi i casi il gestore attua la sospensione; ciò comporta un "AVVISO DI NON ACCETTAZIONE" per eccezioni formali (per i messaggi in uscita) e la mancata emissione della Ricevuta di Presa in Carico per i messaggi provenienti dagli altri Gestori.

Nel caso di sospensione e una volta eliminato il disservizio, il Gestore Namirial S.p.A. può riprendere l'attività. In tal caso deve inviare all'Organo di Vigilanza una relazione dettagliata su quanto accaduto e sui provvedimenti adottati.

8 Obblighi e responsabilità

8.1 Obblighi e responsabilità del Gestore

In ottemperanza alla normativa vigente e visto quanto riportato nel Decreto di cui al [V], il Gestore Namirial S.p.A. si impegna a:

- rispettare e garantire i livelli di servizio previsti;
- garantire l'interoperabilità 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, ricerca e presentazione dei LOG dei messaggi;
- informare il titolare riguardo alle modalità di accesso al servizio e ai necessari requisiti tecnici;
- registrare, su apposito file di LOG, le singole fasi di trasmissione di ogni 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.);
- 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 Regolamento Europeo 679/2016 (GDPR) in materia di protezione dei dati personali;
- non conservare le 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'introduzione di codici eseguibili dannosi;
- adottare procedure e servizi di emergenza, al fine di assicurare il completamento della trasmissione anche in caso di incidenti (ad eccezione di eventi disastrosi ed improvvisi quali terremoti, attentati, 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 e 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 la verosimiglianza dei 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 per la sostituzione dei certificati elettronici relativi alle proprie chiavi di firma, in termini tali 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 di AgID, 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 l'interruzione del servizio di Posta Elettronica Certificata;
- adottare misure di sicurezza, tali da consentire soltanto alle persone autorizzate l'accesso logico e fisico al sistema;
- utilizzare un sistema di riferimento temporale, che garantisca stabilmente la sincronizzazione delle macchine coinvolte, con uno scarto non superiore al minuto, in 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 e solo responsabile del contenuto 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 Regolamento Europeo 679/2016 (GDPR);
- fornire al Gestore tutte le informazioni necessarie ad identificare la propria persona ed ad attivare il servizio garantendo, sotto la propria

responsabilità, l'autenticità e l'esattezza dei dati comunicati;
- trasmettere con tempestività le modifiche e/o gli 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 alle relative ricevute;
- adottare misure atte ad evitare l'introduzione, nei messaggi, di codici eseguibili dannosi (virus/malware/etc.);
- dotarsi di un sistema operativo aggiornato, valido e in costante aggiornamento rispetto ai requisiti indicati dalla normativa nazionale in materia di privacy, oltre che di idonei sistemi antintrusione, antispam e antivirus;
- rendere edotte le eventuali persone abilitate ad utilizzare la propria casella, circa le regole di sicurezza atte ad evitare un uso non autorizzato della stessa.

Nel caso in cui il Titolare non ottemperi ai predetti oneri, 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 il Titolare, nei casi più gravi.

I privati che intendano utilizzare il servizio di posta elettronica certificata nei rapporti con la Pubblica Amministrazione, devono espressamente dichiarare il proprio indirizzo; le imprese, nei rapporti tra loro intercorrenti, possono dichiarare l'esplicita volontà di accettare l'invio di posta elettronica certificata, mediante indicazione della propria casella PEC nell'atto di iscrizione al Registro delle Imprese. Entrambe le dichiarazioni obbligano solo il dichiarante e sono revocabili.

8.3 Limitazioni ed indennizzi

In nessun caso il Gestore Namirial S.p.A. risponde di eventi ad esso non imputabili ed in particolare di danni procurati dalle LRA, dai Titolari, dai Richiedenti, dagli Utenti o da qualsiasi terzo direttamente o indirettamente e causati dal mancato rispetto, da parte degli stessi, delle regole e degli obblighi indicati nel presente Manuale Operativo; inoltre, in nessun caso il Gestore risponde per la mancata

assunzione, da parte di detti soggetti, delle misure di speciale diligenza, idonee ad evitare la causazione di danni a terzi e che si richiedono al fruitore di servizi di certificazione, ovvero per lo svolgimento di attività illecite.

In nessun caso il Gestore Namirial S.p.A. è responsabile per inadempimenti o per eventi dannosi, determinati da caso fortuito o da forza maggiore.

Fatti salvi i limiti inderogabili di legge, il Gestore Namirial S.p.A. non risponderà dei danni causati da malfunzionamenti, ritardi o interruzioni, purché rientranti nei livelli di servizio, descritti nel presente manuale.

Fatti salvi i limiti inderogabili di legge, in alcun modo il Gestore Namirial S.p.A. può 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. qualora gli stessi provochino ritardi, malfunzionamenti o interruzioni del servizio.

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

Il Gestore Namirial S.p.A. non ha alcuna responsabilità sul contenuto dei messaggi inviati e ricevuti attraverso le proprie caselle di PEC.

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.

Relativamente a quanto non previsto dal presente capitolo, le limitazioni agli indennizzi, stabilite dal Gestore Namirial S.p.A., sono reperibili nelle condizioni contrattuali di fornitura del servizio, rese pubbliche e disponibili 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 € 7.500.000 (sette milioni e cinquecentomila euro), per ogni singolo atto illecito, per anno assicurativo e per tutte le

perdite patrimoniali derivanti dalla totalità delle richieste di risarcimento, presentate contro tutti gli assicurati e per tutte le coperture assicurative combinate.

9 Protezione dei dati personali[(k)]

Di seguito vengono descritte le procedure e le modalità operative che Namirial S.p.A., in qualità di titolare del trattamento dei dati personali, adotta nello svolgimento della propria attività. Le informazioni personali, concernenti i titolari delle caselle e, più in generale i clienti del servizio erogato vengono trattate, conservate e protette in conformità a quanto previsto nel [II] materia di protezione dei dati personali.

9.1 Struttura organizzativa di Namirial S.p.A.

Namirial S.p.A. è il **Titolare del trattamento dei dati personali**, secondo quanto previsto dal [II] in materia di protezione dei dati personali. Il responsabile della protezione dei dati, DPO, è Vanessa Cocca.

Namirial S.p.A. individua e nomina gli incaricati al trattamento che operano sotto la diretta autorità del Titolare o del Responsabile, attenendosi alle istruzioni dagli stessi impartite.

9.2 Tutela e diritti degli interessati

Il Gestore Namirial S.p.A. garantisce la tutela degli interessati, in ottemperanza al Regolamento Europeo 679/2016 (GDPR) in materia di trattamento dei dati personali. In particolare, il gestore fornisce agli interessati tutte le informazioni necessarie, in relazione al diritto di accesso ai dati personali ed agli usi degli stessi, consentiti dalla legge.

L'accesso ai propri dati, non ché tutti i diritti esercitabili dagli artt. 15-22 del GDPR, da parte degli interessati è consentito tramite richiesta scritta, a mezzo del format scaricabile dal sito web di Namirial ww.namirial.com, da far pervenire al responsabile per la protezione dei dati anche tramite e-mail dpo@namirial.com che provvederà ad evadere la richiesta senza ingiustificato ritardo. Gli interessati devono prestare consenso scritto al trattamento dei propri dati da parte del Gestore Namirial S.p.A.

9.3 Modalità del trattamento

Tutte le informazioni personali, acquisite durante l'erogazione del servizio di PEC, vengono trattate dal gestore che adotta 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 conservati in appositi data server adibiti allo scopo e su supporti ottici all'interno di armadi protetti. I dati in formato cartaceo vengono conservati da un'azienda esterna, denominata Archivi Service. La consultazione di tali dati avviene mediante istanza, effettuata esclusivamente da parte del personale autorizzato da Namirial S.p.A. e a seguito della spedizione ad Archivi Service di un apposito modulo di richiesta. Namirial S.p.A. si riserva l'opportunità di conservare i dati cartacei presso la propria sede centrale, all'interno di archivi cartacei cui hanno accesso solo gli incaricati espressamente autorizzati.

9.4 Finalità del trattamento

I dati personali vengono acquisiti con le seguenti finalità: (queste finalità devono essere le stesse che si accettano in informativa)

- erogazione del servizio di posta certificata;
- gestione del rapporto contrattuale;
- eventuali controlli sulla qualità del servizio e sulla sicurezza del sistema;
- attività di natura commerciale, effettuata tramite invio di informative legate alla emissione di prodotti e/o servizi analoghi o direttamente connessi al servizio di PEC. L'interessato ha la possibilità di opporsi al trattamento dei dati personali, avente ad oggetto tale tipologia di comunicazioni.

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

9.5 Altre forme di utilizzo dei dati

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

9.6 Sicurezza dei dati

In ottemperanza 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 di risorse hardware sulle quali siano memorizzati i dati;
- i rischi di danneggiamento ai locali nei quali siano custoditi i dati;
- l'accesso non autorizzato ai dati;
- le attività di trattamento non consentite dalla legge o dai regolamenti aziendali

Attraverso le misure di sicurezza adottate dal gestore, comprovate anche dalle certificazioni acquisite in ambito 27001 con estensione agli standard 27017 e 27018 (ambito Cloud) (cfr § 6.3) vengono garantite tra le altre, le seguenti caratteristiche:

- l'integrità e la salvaguardia dei dati, contro manomissioni o modifiche da parte di soggetti non autorizzati
- la disponibilità dei dati e la loro conseguente fruibilità;
- la riservatezza dei dati ovvero la garanzia che alle informazioni abbiano accesso le sole persone autorizzate.

Riferimenti

NUMERO	DESCRIZIONE
[I]	Decreto del Presidente della Repubblica 28 dicembre 2000 n. 445
[II]	REGOLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)
[III]	Decreto del Presidente della Repubblica del 11 febbraio 2005 n. 68.
[IV]	Decreto Legislativo del 7 marzo 2005 n. 82 “Codice dell'Amministrazione Digitale” (CAD).
[V]	Decreto Ministeriale del 2 novembre 2005 e successive note integrative, “Regole Tecniche del servizio di trasmissione dei documenti informatici tramite Posta Elettronica Certificata”.
[VI]	Circolare CNIPA/CR/49 del 24/11/2005, “Modalità di presentazione della domanda di accreditamento nell’elenco pubblico dei Gestori di PEC”.
[VII]	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.
[VIII]	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
[IX]	Istruzioni per la conservazione dei log dei messaggi e dei messaggi di posta elettronica certificata con virus. Versione 1.0 del 05/07/2016

[X]	DECRETO DEL PRESIDENTE DEL CONSIGLIO DEI MINISTRI 3 dicembre 2013. Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, commi 3 e 5 -bis, 23 -ter , comma 4, 43, commi 1 e 3, 44 , 44 -bis e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005.
[XI]	AgID - Istruzioni per la conservazione dei log dei messaggi e dei messaggi di posta elettronica certificata con virus – ver 1.0 del 05 luglio 2016