

---

Servizio Posta Elettronica Certificata – P.E.C.

Manuale Operativo

---

( ) register.it  
by team.blue

Codice documento: REGIT-PEC-MO

Versione: 6.2

Data: 09/03/2026

## Indice del Manuale Operativo

Manuale Operativo .....	1
1 Introduzione .....	1
1.1 Scopo del documento.....	1
1.2 Dominio di applicabilità.....	1
1.3 Definizioni abbreviazioni e termini tecnici.....	1
2 Dati identificativi del Gestore .....	5
2.1 Organizzazione del personale .....	6
3 Struttura e storia del Manuale Operativo .....	7
3.1 Reperibilità del Manuale Operativo .....	7
3.2 Versione e storia del Manuale Operativo .....	7
3.3 Convenzioni utilizzate.....	8
3.4 Riferimenti normativi per la verifica dei contenuti.....	8
3.5 Tabella di corrispondenza Normativa – Manuale Operativo .....	10
4 Procedure per l’aggiornamento del Manuale Operativo .....	11
4.1 Responsabile del Manuale Operativo .....	11
4.2 Revisione del Manuale Operativo ed approvazione delle modifiche .....	11
5 Contenuto e modalità di offerta.....	12
5.1 Introduzione al servizio di Posta Elettronica Certificata .....	12
5.2 Tipologie di servizio offerte (Funzionalità, dimensioni casella e messaggi) .....	12
5.2.1 Servizio di conservazione a norma dedicato alla casella PEC .....	14
5.2.2 Offerta PEC di Register SpA.....	15
5.3 Interoperabilità gestori .....	16
5.4 Modalità elaborazione dei messaggi.....	16
5.5 Modalità di archiviazione dei messaggi .....	18
5.6 Conservazione dei Log delle ricevute dei messaggi PEC.....	19
6 Guida all’uso dei Servizi PEC Register .....	20
6.1 Requisiti tecnici minimi per l’utilizzo del servizio .....	20
6.2 Connettività e configurazione browser e software di posta elettronica .....	20

6.3	Gestione della password .....	20
6.4	Modalità di accesso alla casella PEC.....	21
6.4.1	Accesso via WebMail .....	21
6.4.1.1	Accesso via WebMail: accesso a singolo fattore .....	22
6.4.1.2	Accesso via WebMail: Autenticazione con credenziali SPID .....	22
6.4.2	Accesso via client di posta elettronica.....	23
6.4.3	Accesso tramite Token di accesso sicuro.....	24
7	Modalità di erogazione del servizio e procedure di gestione .....	25
7.1	Attivazione del servizio.....	25
7.1.1	Attivazione PEC con credenziali SPID.....	27
7.2	Area Selfcare PEC .....	28
7.3	Modifica del Titolare assegnatario di casella PEC attiva e riassegnazione di casella PEC disattivata.....	28
7.3.1	Modifica del Titolare assegnatario di casella PEC attiva: .....	28
7.3.2	Riassegnazione di casella PEC disattivata .....	29
7.4	Rinnovo e disattivazione di una casella PEC .....	29
7.5	Richiesta dei Log contenenti le ricevute PEC .....	32
7.6	Richiesta di assistenza (canali e tempistiche) .....	33
8	Procedure e standard tecnologici e di sicurezza .....	34
8.1	Standard e procedure di riferimento .....	34
8.2	Procedure di gestione dei sistemi .....	35
8.2.1	Monitoraggio dei sistemi .....	35
8.2.2	Antivirus e contrasto allo SPAM .....	35
8.2.3	Backup dei dati.....	36
8.3	Gestione della continuità operativa.....	37
8.3.1	Sistemi di continuità/backup .....	37
8.3.2	Procedure di ripristino .....	38
8.3.3	Gestione guasti / disservizi e disastri.....	39
8.4	Standard tecnologici e di sicurezza .....	42

8.4.1	Analisi dei rischi.....	42
8.4.2	Soluzioni tecniche adottate .....	42
8.4.3	Misure di sicurezza per la protezione di dati e architetture.....	43
8.5	Indicazione delle modalità di protezione dei dati dei titolari .....	46
8.5.1	Gestione delle credenziali applicative (Token) .....	46
9	Indicazione delle condizioni di fornitura .....	47
9.1	Obblighi e responsabilità del Gestore per l'erogazione del servizio PEC.....	47
9.2	Obblighi del Titolare della casella, contraente del servizio .....	48
9.3	Indicazione dei livelli di servizio .....	49
9.4	Limitazioni ed indennizzi .....	51
9.5	Polizza assicurativa .....	52
9.6	Procedura prevista in caso di cessazione di erogazione del servizio PEC da parte di Register	52

## Indice delle Figure

Figura 1	– Flusso End to End in caso di invio positivo del messaggio di PEC.....	17
Figura 2	– Login Webmail PEC.....	21
Figura 3	– Processo di attivazione della casella PEC .....	26
Figura 4	– Form di richiesta per i log delle ricevute.....	32

## Indice delle Tabelle

Tabella 1	– Corrispondenza Normativa - Manuale Operativo .....	10
Tabella 2	– Guasti e disservizi: contromisure e modalità di gestione .....	41

## 1 Introduzione

Register SpA con P.IVA./Codice fiscale 04628270482 iscritta dal 26.04.1995 al Registro delle Imprese di Firenze.

Register SpA (nel seguito anche “Register” o “la Società”) è leader storico in Italia nella fornitura di servizi di registrazione di domini, hosting, protezione del brand e pubblicità in rete.

Register si pone altresì sul mercato quale “Gestore di Posta Elettronica Certificata” (nel seguito, per semplicità, anche indicato con l’acronimo “PEC”), regolarmente iscritto all’elenco pubblico dei gestori PEC coordinato dall’Agenzia per l’Italia Digitale.

### 1.1 Scopo del documento

Tale documento costituisce il **Manuale Operativo** (nel seguito, per brevità, anche indicato come “Manuale”) del Gestore Register ai sensi del Decreto del Presidente della Repubblica 11 febbraio 2005, n. 68 – “Regolamento recante disposizioni per l’utilizzo della posta elettronica certificata” [4].

Scopo del presente Manuale è fornire in maniera esaustiva tutte le informazioni sulle caratteristiche e procedure adottate da Register relative all’erogazione e alla gestione del servizio di Posta Elettronica Certificata.

Il presente Manuale Operativo è stato predisposto in accordo alle richieste di cui al punto “2. *Requisiti tecnico-organizzativi*”, sottopunto “2.1 *Manuale Operativo*” della Circolare CNIPA n. 56 del 21 maggio 2009 “*Modalità per la presentazione della domanda di iscrizione nell’elenco pubblico dei gestori di Posta Elettronica Certificata (PEC) di cui all’articolo 14 del decreto del Presidente della Repubblica 11 febbraio 2005, n. 68*” [6].

### 1.2 Dominio di applicabilità

Oltre alle informazioni di carattere generale, tale Manuale contiene tutte le indicazioni necessarie alla spiegazione dell’offerta del servizio di Posta Elettronica Certificata erogato da Register in qualità di Gestore di Posta Elettronica certificata.

### 1.3 Definizioni abbreviazioni e termini tecnici

Al fine di facilitare la comprensione del presente Manuale Operativo e consentirne una corretta interpretazione, in questa sezione vengono definiti termini e acronimi usati comunemente in materia.

Termine – Acronimo	Definizione
<b>Agenzia per l'Italia Digitale</b>	Ente Nazionale per la Digitalizzazione della Pubblica Amministrazione.
<b>Antispam</b>	Software che consente di bloccare l'invio/inoltro indiscriminato di e-mail, spesso a carattere pubblicitario e/o commerciale; tale software è integrato nelle piattaforme che erogano il servizio di posta elettronica.
<b>Antivirus</b>	Software in grado di rilevare eventuale malware (virus, trojan, grayware) presenti su un sistema informatico, su una comunicazione mail o più in generale su un flusso di dati in transito. Qualora configurato opportunamente un sistema Antivirus è in grado di rimuovere il codice malevolo ripristinando lo stato di corretto funzionamento dei sistemi o sanizzando le comunicazioni.
<b>Avviso di mancata consegna</b>	Avviso, emesso dal sistema, per indicare l'anomalia al mittente del messaggio originale nel caso in cui il gestore di posta elettronica certificata sia impossibilitato a consegnare il messaggio nella casella di posta elettronica certificata del destinatario.
<b>Avviso di non accettazione</b>	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, recante la motivazione per cui non è possibile accettare il messaggio e l'esplicitazione che il messaggio non potrà essere consegnato al destinatario.
<b>Backup</b>	Copia di sicurezza o di riserva fatta per prevenire la perdita accidentale di dati informatici.
<b>Busta di trasporto</b>	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.
<b>Casella di Posta Elettronica Certificata</b>	Casella di posta elettronica posta all'interno di un dominio di posta elettronica certificata ed alla quale è associata una funzione che rilascia ricevute di avvenuta consegna al ricevimento di messaggi di posta elettronica certificata.
<b>Cliente</b>	Acquirente dei servizi erogati da Register.
<b>Dati di certificazione</b>	Dati, quali ad esempio data ed ora di invio, mittente, destinatario, oggetto, identificativo del messaggio, che descrivono l'invio del messaggio originale e sono certificati dal gestore di posta elettronica certificata del mittente; tali dati sono inseriti nelle ricevute e sono trasferiti al Titolare destinatario insieme al messaggio originale per mezzo di una busta di trasporto
<b>Destinatario</b>	Utente che si avvale del servizio di Posta Elettronica Certificata per la ricezione dei documenti prodotti mediante strumenti informatici.
<b>DNS (Domain Name System)</b>	Sistema d'identificazione basato sull'associazione e traduzione di nomi facilmente memorizzabili in indirizzi IP. Per esempio, inserendo il nome di un sito o il relativo indirizzo IP nella barra degli indirizzi del browser, si ottiene lo stesso risultato.
<b> dominio di Posta Elettronica Certificata</b>	dominio DNS dedicato alle caselle di posta elettronica degli utenti PEC.
<b>Firewall</b>	Componente di difesa perimetrale di una rete informatica.
<b>Firma del Gestore di Posta Elettronica Certificata</b>	Firma elettronica avanzata, basata su un sistema di chiavi asimmetriche, che consente di rendere manifesta la provenienza e di assicurare l'integrità e l'autenticità dei messaggi del sistema di posta elettronica certificata, generata attraverso una procedura informatica che garantisce la connessione univoca al gestore e la sua univoca identificazione, creata automaticamente con mezzi che garantiscano il controllo esclusivo da parte del gestore.
<b>Firma digitale</b>	Particolare tipo di firma elettronica avanzata basata su un certificato qualificato e su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al Titolare tramite la chiave privata e al destinatario tramite la chiave

Termine – Acronimo	Definizione
	pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici.
<b>Firma elettronica</b>	Insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di identificazione informatica.
<b>Firma elettronica avanzata</b>	Firma elettronica basata su un sistema di chiavi asimmetriche, consente di rendere manifesta la provenienza e di assicurare l'integrità e l'autenticità dei messaggi del sistema di posta elettronica certificata, generata attraverso una procedura informatica che garantisce la connessione univoca al gestore e la sua univoca identificazione, creata automaticamente con mezzi che garantiscano il controllo esclusivo da parte del gestore.
<b>FQDN (Fully Qualified Domain Name)</b>	Nome a dominio enunciato per esteso che identifica in modo univoco un server di rete.
<b>Gestore di Posta Elettronica Certificata</b>	Soggetto che presta servizi di trasmissione dei documenti informatici mediante la posta elettronica certificata.
<b>Gestore PEC</b>	Register in qualità di erogatore del servizio PEC.
<b>HTTPS (Hyper Text Transfer Protocol)</b>	Protocollo HTTP associato al protocollo SSL usato per garantire trasferimenti riservati di dati.
<b>IMAP/S (Internet Message Access Protocol)</b>	Protocollo per accedere alla lettura delle e-mail direttamente sul server senza che vengano scaricate sul proprio computer. In questo modo l'utente può decidere autonomamente quali e-mail scaricare, visualizzandone il mittente, l'oggetto e altre caratteristiche. L'adozione del layer di cifratura garantisce la sicurezza durante lo scambio di dati e credenziali di accesso.
<b>LDAP (Lightweight Directory Access Protocol)</b>	Protocollo standard per l'interrogazione e la modifica dei servizi di directory. In particolare con il termine LDAP è da intendersi il database di informazioni organizzate gerarchicamente interrogabili tramite il protocollo stesso.
<b>Log dei messaggi</b>	Registro informatico delle operazioni relative alle trasmissioni effettuate mediante posta elettronica certificata tenuto dal Gestore.
<b>Marca temporale</b>	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 del 27 aprile 2004, n. 98
<b>Messaggio di Posta Elettronica Certificata</b>	Documento informatico composto dal testo del messaggio, dai dati di certificazione e dagli eventuali documenti informatici allegati.
<b>PEC</b>	Posta Elettronica Certificata.
<b>POP3/S (Post Office Protocol 3)</b>	Protocollo utilizzato da server fornitori di accesso per trasmettere la posta elettronica. L'adozione del layer di cifratura garantisce la sicurezza durante lo scambio di dati e credenziali di accesso.
<b>Punto di accesso</b>	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.
<b>Punto di consegna</b>	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.
<b>Punto di ricezione</b>	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

Termine – Acronimo	Definizione
	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.
<b>Ricevuta di accettazione</b>	Ricevuta, sottoscritta con la firma del gestore di posta elettronica certificata del mittente, contenente i dati di certificazione, rilasciata al mittente dal punto di accesso a fronte dell'invio di un messaggio di posta elettronica certificata.
<b>Ricevuta di avvenuta consegna</b>	Ricevuta, sottoscritta con la firma del gestore di posta elettronica certificata del destinatario, emessa dal punto di consegna al mittente nel momento in cui il messaggio è inserito nella casella di posta elettronica certificata del destinatario
<b>Riferimento temporale</b>	Informazione contenente la data e l'ora che viene associata ad un messaggio di posta elettronica certificata
<b>Selfcare</b>	Area di gestione della PEC
<b>Spazio mailbox</b>	Spazio di archiviazione riservato dal server alle e-mail in arrivo e inviate.
<b>SSL (Secure Socket Layer)</b>	Protocollo crittografico che permette una comunicazione sicura e l'integrità dei dati.
<b>Storage</b>	Dispositivi hardware, supporti, infrastrutture e software dedicati alla memorizzazione di grandi quantità di informazioni in formato elettronico.
<b>Titolare PEC</b>	Soggetto a cui è assegnata una casella di posta elettronica Certificata.
<b>Token di accesso (sicuro)</b>	Credenziale applicativa generata tramite Selfcare che consente l'autenticazione ai servizi PEC in alternativa alla password tradizionale.
<b>Utente PEC</b>	La persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi ente, associazione o organismo, nonché eventuali unità organizzative interne ove presenti, che sia mittente o destinatario di posta elettronica certificata.
<b>WebMail</b>	Servizio che consente di consultare la propria casella di posta accedendo ad essa dal sito del gestore, inserendo il proprio username e password. In questo modo tutta la corrispondenza è disponibile da qualunque PC connesso a Internet, per la consultazione on-line.
<b>Client di posta elettronica</b>	Un client di posta elettronica è un software che viene installato sul computer e che permette di comporre, inviare e ricevere messaggi email collegandosi ai server di posta elettronica (SMTPS) per la spedizione e (POP3s) per la ricezione.

## 2 Dati identificativi del Gestore

Il servizio di Posta Elettronica Certificata è erogato da Register SpA.

Di seguito le informazioni identificative del Gestore.

<b>Ragione sociale:</b>	Register SpA
<b>Legale rappresentante</b>	Claudio Corbetta
<b>Sede legale:</b>	Firenze, Viale della Giovine Italia, 17
<b>Sedi operative:</b>	<ul style="list-style-type: none"><li>• Firenze, Viale della Giovine Italia, 17</li><li>• Bergamo, Viale Giulio Cesare, 29</li></ul>
<b>Data Center:</b>	c/o BT Italia S.p.A., I.NET Building, Via Darwin 85, Settimo Milanese (MI)
<b>Partita IVA:</b>	04628270482
<b>Iscrizione Registro Delle Imprese:</b>	04628270482
<b>REA:</b>	FI-467460
<b>Capitale sociale:</b>	€ 5.108.619,32
<b>Sito Web:</b>	<a href="http://www.register.it">www.register.it</a>
<b>Email:</b>	<a href="mailto:gestorepec@pec.register.it">gestorepec@pec.register.it</a>

## 2.1 Organizzazione del personale

Al fine di rispondere in modo efficace alle specifiche esigenze che il servizio PEC richiede, è stata costituita una struttura organizzativa interna con il compito di gestire e monitorare gli aspetti previsti dalla normativa [2]:

- Registrazione dei Titolari;
- Servizi Tecnici;
- Verifiche e Ispezioni Interne;
- Sicurezza;
- Sicurezza dei Log dei Messaggi;
- Sistema di Riferimento Temporale.

A presidio di ciascuna delle funzioni identificate, in accordo a quanto richiesto dalla normativa di riferimento [2], Register ha identificato specifici soggetti responsabili. Tali responsabili, per lo svolgimento delle funzioni di loro competenza, possono avvalersi di addetti ed operatori dipendenti di Register ed, in casi di emergenza, anche di personale del fornitore BT Italia S.p.A. appositamente incaricato<sup>1</sup>.

---

<sup>1</sup> BT Italia S.p.A: è fornitore per Register del servizio di connettività e housing dell'architettura del servizio PEC. Per servizio di housing si intende un servizio che prevede la concessione in locazione di uno spazio fisico dedicato esclusivamente agli apparati Register all'interno di un data center, ove sono collocati i rack della PEC, accessibili ai soli operatori di Register o, in casi straordinari definiti e autorizzati da Register stessa, al personale del fornitore. Register ha la gestione diretta del servizio PEC ed il controllo delle sue varie fasi e degli apparati tecnologici che forniscono il servizio PEC ed è l'unico soggetto in grado di accedere ai dati ed alle informazioni relative al servizio PEC contenute negli apparati collocati presso la sede di BT Italia. Il rapporto tra Register e BT Italia è disciplinato da un contratto che garantisce i livelli di servizio ed il controllo di Register sui singoli servizi forniti da BT Italia. Register provvede alla gestione e soluzione di eventuali guasti o malfunzionamenti attraverso il proprio personale. In caso di necessità, Register può avvalersi del personale incaricato di BT Italia per effettuare operazioni fisiche sui server PEC quali ad esempio sostituzione di parti guaste ed interventi di ripristino di emergenza; tali interventi sono garantiti da BT Italia S.p.A. a Register dal servizio di assistenza "Eyes&hands", che prevede l'intervento di un tecnico nel Data Center su richiesta esplicita di Register, entro due ore dalla richiesta stessa al fine di velocizzare eventuali interventi di ripristino. I singoli servizi forniti da BT Italia, inclusi gli interventi di assistenza, sono controllati da Register. Tutti gli accessi ai rack della PEC sono controllati tramite badge identificativi, rilasciati e gestiti da Register.

## 3 Struttura e storia del Manuale Operativo

### 3.1 Reperibilità del Manuale Operativo

Il presente Manuale è un documento *pubblico*, secondo le disposizioni del Decreto del Presidente della Repubblica 11 febbraio 2005, n. 68 – “Regolamento recante disposizioni per l’utilizzo della posta elettronica certificata” [4], e delle normative attuative, che ha il fine di costituire garanzia di affidabilità del servizio di erogazione della PEC nei confronti degli utilizzatori finali. Il Manuale Operativo è accessibile e scaricabile:

- dal sito di Register nella sezione dedicata alla PEC <http://www.register.it/pec>
- dal Pannello di controllo messo a disposizione da Register agli utenti registrati <https://controlpanel.register.it/index.html>

La versione del Manuale Operativo, resa disponibile e pubblicata agli indirizzi citati, è l’ultima rilasciata e approvata dalla Società.

### 3.2 Versione e storia del Manuale Operativo

La versione corrente del Manuale Operativo è esclusivamente la versione in formato elettronico disponibile agli indirizzi citati [si veda il paragrafo 3.1 del presente Manuale].

Versione del Manuale e storia delle modifiche			
Versione	Data	Paragrafo	Note sui cambiamenti
1.0	01 Maggio 2019	N.A.	Prima versione del documento
1.1	30 Settembre 2019	7.3, 7.5, 8.5.3	Modifiche layout generale MO; visualizzazione stato casella pec; aggiornamento canale assistenza; aggiornamento richiamo decreto privacy
1.2	25 Novembre 2019	8.5	Aggiornamento ed ottimizzazione comunicazione al Titolare norme protezione dati personali
1.3	20 gennaio 2020	9.4	Inclusione della colpa lieve nel risarcimento danni; in linea con quanto richiesto dal CAD ai gestori di servizi fiduciari.
2.0	22 aprile 2020	6.4.1, 5.2.1 – 7.3	Inclusione login webmail con SpidItalia; Rafforzamento sicurezza login webmail – Inclusione servizio di Conservazione a norma dedicato alla casella PEC.
2.1	15 giugno 2020	5.2.1, 7.3	Acquisto e rinnovo spazio aggiuntivo di conservazione
2.2	24 settembre 2022	1.3, 4.1, 5.2.2, 6.4.1, 7.3, 7.4	Cambio Responsabile del MO; dettaglio su record SPF; esplicitate informazioni su trasferimento casella pec; pec sui domini @registerpec.it, @dadapec.com, @pec-mail.it importate su nostra piattaforma; dettaglio richiesta log da webmail in pdf.
3.0	28 novembre 2023	7.3	Anticipo della decertificazione del dominio PEC
4.0	15 gennaio 2024	7.1.1	Possibilità di registrazione PEC utilizzando credenziali SPID
4.1	05 luglio 2024	2	Cambio indirizzo sede di Bergamo
5.0	19 novembre 2024	5.4	Autenticazione forte

Versione del Manuale e storia delle modifiche			
Versione	Data	Paragrafo	Note sui cambiamenti
6.0	19 novembre 2025	Figura 2, 6.4.1*, 7*	Nuova Login e Selfcare
6.1	08 gennaio 2026	7.4, 7.2	Possibilità di revoca da Selfcare
6.2	09 marzo 2026	1.3, 6.3, 6.4*, 7.1, 7.2, 7.5, 8.5, 9.2	Nuova funzionalità di gestione Token di accesso sicuro.

### 3.3 Convenzioni utilizzate

Si riportano di seguito le diciture e le convenzioni lessicali e tecniche correntemente utilizzate nel presente Manuale, fornendone relativa connotazione interpretativa.

Quando viene utilizzata la dicitura “*deve*”, “*occorre*”, “*è necessario*” (ed altre varianti di egual e paritario valore) è sotto intesa l’obbligatorietà di quanto riportato; l’oggetto della frase è condizione *sine qua non* per la corretta interpretazione della valenza di quanto riportato o il corretto funzionamento di quanto specificato.

Quando viene utilizzata la dicitura “*è consigliato*”, “*è opportuno*” (ed altre varianti di egual e paritario valore) si fa rimando all’interpretazione del lettore in merito alla valenza di quanto riportato o al corretto funzionamento di quanto specificato.

Con il termine “Manuale Operativo” si fa sempre riferimento alla versione corrente del Manuale Operativo [si veda il paragrafo 3.2 del presente Manuale].

### 3.4 Riferimenti normativi per la verifica dei contenuti

Il servizio PEC erogato da Register e il presente Manuale Operativo sono stati sviluppati in ottemperanza alla vigente normativa, specifica in materia, e ad altre normative cogenti. Di seguito si riporta l’elenco delle normative prese in considerazione.

- [1] Decreto del Presidente del Consiglio dei Ministri 6 maggio 2009 – “*Disposizioni in materia di rilascio e di uso della casella di posta elettronica certificata assegnata ai cittadini*”.
- [2] Decreto Ministeriale 2 novembre 2005 – “*Regole Tecniche del servizio di trasmissione dei documenti informatici tramite Posta Elettronica Certificata*” e relativo allegato; sue successive note ed integrazioni.
- [3] Decreto Legislativo, 7 marzo 2005 n. 82 – “*Codice dell’Amministrazione Digitale*” (CAD); versione vigente.

- [4] Decreto del Presidente della Repubblica 11 febbraio 2005, n. 68 – *“Regolamento recante disposizioni per l’utilizzo della posta elettronica certificata”*.
- [5] Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 – *“Disposizioni legislative in materia di documentazione amministrativa”*.
- [6] Circolare CNIPA 21 maggio 2009, n. 56 – *“Modalità per la presentazione della domanda di iscrizione nell’elenco pubblico dei gestori di posta elettronica certificata (PEC) di cui all’articolo 14 del decreto del Presidente della Repubblica 11 febbraio 2005, n. 68”*.
- [7] Circolare CNIPA 7 dicembre 2006, n. 51 – *“Espletamento della vigilanza e del controllo sulle attività esercitate dagli iscritti nell’elenco dei gestori di posta elettronica certificata (PEC), di cui all’articolo 14 del decreto del Presidente della Repubblica 11 febbraio 2005, n. 68, «Regolamento recante disposizioni per l’utilizzo della posta elettronica certificata, a norma dell’articolo 27 della legge 16 gennaio 2003, n. 3».”*
- [8] Decreto Legislativo 30 giugno 2003, n. 196 – *“Codice in materia di protezione dei dati personali”* e successive modificazioni ed integrazioni.
- [9] Provvedimento Garante Privacy, 17 gennaio 2008 – *“Sicurezza dei dati di traffico telefonico e telematico”* e successive modificazioni ed integrazioni.
- [10] Provvedimento Garante Privacy, 27 novembre 2008 – *“Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema”*.
- [11] Regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio del 23 luglio 2014 in materia di *identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno* pubblicato in Gazzetta ufficiale dell’Unione europea serie L257 del 28 agosto 2014.
- [12] 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).

L’elenco è da considerarsi non esaustivo; si è fatto ad ogni modo riferimento a quanto pubblicato sul sito dell’Agenzia per l’Italia Digitale, con aggiornamento alla data di redazione del presente Manuale.

### 3.5 Tabella di corrispondenza Normativa – Manuale Operativo

Contenuto in relazione alla circolare CNIPA/CR/56 Manuale Operativo	Capitolo / paragrafo del Manuale Operativo
Dati identificativi del Gestore	2
Responsabile del Manuale Operativo	4.1
Riferimenti normativi per la verifica dei contenuti	3.4
Indirizzo del sito web del Gestore ove è pubblicato e scaricabile il Manuale Operativo	3.1
Procedure e standard tecnologici e di sicurezza	8
Definizioni, abbreviazioni e termini tecnici	1.3
Descrizione sintetica del servizio offerto	5.2
Contenuto e modalità di offerta	5
Modalità di accesso al servizio	6.4
Descrizione delle modalità di reperimento e di presentazione delle informazioni presenti nei log dei messaggi	7.4
Indicazione dei livelli di servizio	9.3
Indicazione delle condizioni di fornitura	9
Indicazione delle modalità di protezione dei dati dei titolari	8.5
Obblighi, responsabilità e limitazioni in sede di indennizzo	9.1; 9.2; 9.4
Procedure operative in caso di cessazione dell'attività di Gestore di posta elettronica certificata	9.6
Versione del Manuale Operativo	Frontespizio

Tabella 1 – Corrispondenza Normativa - Manuale Operativo

## 4 Procedure per l'aggiornamento del Manuale Operativo

### 4.1 Responsabile del Manuale Operativo

Register ha individuato nella persona di Silvia Mazzanti il Responsabile del presente Manuale Operativo.

Per informazioni, domande e chiarimenti, l'utente può contattare il Responsabile del Manuale Operativo seguendo le istruzioni pubblicate al paragrafo 2.

### 4.2 Revisione del Manuale Operativo ed approvazione delle modifiche

Register si impegna a mantenere costantemente allineato il contenuto del presente Manuale all'offerta PEC messa a disposizione sul sito.

La versione corrente del Manuale Operativo è conforme alle caratteristiche del sistema di gestione ed erogazione PEC adottato, in accordo ai requisiti previsti a livello normativo [2].

Il contenuto del presente Manuale può essere oggetto di aggiornamento a seguito di:

- variazioni nei contenuti e nelle modalità di fruizione del servizio PEC;
- variazioni del sistema di gestione ed erogazione del servizio PEC, a seguito di:
  - modifiche o ottimizzazioni del sistema stesso, previste da Register;
  - modifiche delle normative esistenti o pubblicazione di nuove normative emesse da parte degli organi competenti.

Nel caso in cui si ravveda necessità di aggiornamento del contenuto, il Manuale stesso sarà verificato e approvato internamente, a cura del Responsabile sopra identificato, e sarà sottoposto a validazione a cura dell'Agenzia per l'Italia Digitale, in accordo ai casi previsti dalla normativa vigente [2].

## 5 Contenuto e modalità di offerta

### 5.1 Introduzione al servizio di Posta Elettronica Certificata

La Posta Elettronica Certificata (PEC) è un'estensione della posta elettronica che fornisce al mittente la documentazione, con valore legale, dell'invio e della consegna di documenti informatici, qualora il destinatario utilizzi anch'esso un servizio PEC.

Ogni messaggio PEC inviato viene catalogato con un codice identificativo [si veda il paragrafo 7.5 del presente Manuale] Ed i relativi log conservati per trenta mesi secondo le disposizioni di legge [2].

La PEC fornisce al processo di trasmissione delle informazioni e dei documenti informatici valore equivalente a quello della notifica a mezzo posta raccomandata in tutti i casi e nei limiti previsti dalla legge. Il servizio PEC erogato da Register è stato sviluppato in accordo a quanto richiesto dalla vigente normativa [si veda il paragrafo 3.4 del presente Manuale], pertanto i messaggi e-mail inviati mediante caselle PEC Register sono dotati di valore legale nei casi previsti dalla legge.

Il servizio di Posta elettronica certificata (PEC) fornito da Register è conforme alle regole tecniche richiamate dal DM 2 novembre 2005 e dal suo allegato e alle sue successive note e integrazioni [2], ed ha conseguito la certificazione ISO 9001:2015 ed ISO27001:2022.

### 5.2 Tipologie di servizio offerte (Funzionalità, dimensioni casella e messaggi)

A fronte dell'invio di una e-mail da account PEC, il Titolare PEC riceve ricevuta di accettazione e successiva ricevuta di avvenuta consegna.

Le ricevute di avvenuta consegna possono essere di tre tipologie: ricevuta completa (che contiene in allegato i dati di certificazione ed il messaggio originale), ricevuta breve (che contiene i dati di certificazione ed un estratto del messaggio originale) o sintetica (che contiene i dati di certificazione).

La tipologia di ricevuta è scelta dall'utente al momento dell'invio del messaggio PEC. Le citate ricevute attestano, rispettivamente, l'avvenuto invio del messaggio e l'avvenuta consegna nella casella PEC di un altro utente PEC. Register, in qualità di Gestore PEC, conserva i log contenenti i dati identificativi del messaggio [si veda il paragrafo 7.5 del presente Manuale] per un periodo di trenta mesi, come previsto dalla legge [2; 4].

Tutte le tipologie di caselle consentono anche la ricezione di messaggi e-mail standard (e-mail non certificate PEC).

Oltre alle funzionalità proprie del servizio PEC, Register mette a disposizione anche la seguente componente, facente parte del servizio stesso:

- Notifica sms a seguito di ricezione di una e-mail PEC (configurabile da parte del Titolare).
- Spazio di Conservazione a norma dedicato alla casella PEC

Il servizio PEC Register è messo a disposizione sia mediante accesso WebMail (tramite i principali browser internet) che mediante configurazione di client di posta elettronica (ad esempio Microsoft Outlook) del Titolare PEC.

#### Funzionalità standard

Le principali funzionalità offerte dal servizio PEC fornito da Register, in linea con quanto richiesto dalla normativa vigente, sono:

- invio e ricezione messaggi certificati;
- ricezione messaggi non certificati: questi verranno contrassegnati come messaggi NON PEC nella WebMail;
- autenticazione dell'utente tramite UserID e password o tramite certificati digitali;
- certificazione dell'invio messaggi;
- garanzia di integrità del messaggio PEC;
- certificazione della consegna messaggi;
- firma elettronica delle buste di consegna;
- servizio antivirus.

#### Funzionalità aggiuntive

Le funzionalità aggiuntive offerte dal servizio PEC di Register sono:

- filtro impostare la ricezione di soli messaggi PEC;
- filtri per l'archiviazione automatica dei messaggi e delle ricevute;
- rubrica contatti online;
- archivio;
- calendario online;
- supporto drag & drop per la gestione delle e-mail e dei contatti;

- editor per invio e-mail in HTML;
- servizio di Antispam;
- servizio notifica via SMS che permette di controllare l'arrivo di nuova posta PEC.

Gli SMS di notifica vengono inviati giornalmente in una fascia di orario prestabilito da parte dell'utente ed in modo aggregato nel caso di possesso di un numero maggiore di pec.

- servizio di notifica via email che permette di facilitare il Cliente nella gestione della propria casella PEC. Tali email comunicano eventi come l'approssimarsi della scadenza del prodotto PEC.

**Il Gestore si riserva la facoltà di inibire l'accesso al servizio in caso di superamento dei limiti sopra indicati o dove si verificassero situazioni che possano compromettere la sicurezza della casella o del servizio**, come indicato nel § 8. Eventuali esigenze specifiche troveranno soluzione in un accordo contrattuale che, partendo dalle caratteristiche elencate garantite a tutti gli utenti, potrà offrire maggiori servizi e/o volumi.

### 5.2.1 Servizio di conservazione a norma dedicato alla casella PEC

Ad ogni casella PEC è associato uno spazio di Conservazione a norma, così da poter conservare la corrispondenza della casella PEC, garantendo autenticità, integrità, affidabilità, leggibilità e reperibilità.

Il servizio è strettamente legato alla casella PEC, pertanto ne segue il ciclo di vita in termini di durata e scadenza [vedi paragrafo 7.4].

Il servizio richiede una esplicita attivazione (affidamento): può essere attivato dal Tab Conservazione all'interno della webmail [per accedere alla webmail vedi 6.4.1] in pochi semplici passi, affidando a Register il ruolo di Conservatore.



Una volta attivato, sarà possibile inviare in conservazione ogni singolo messaggio di posta certificata e/o messaggi non certificati ricevuti o inviati, utilizzando la voce **“Invia in conservazione”** presente sul menù di lettura messaggio. In Conservazione viene inviata un duplicato del messaggio originale; il messaggio originale rimane nella casella PEC.

I messaggi inviati in Conservazione non potranno più essere rimossi.

Lo spazio di Conservazione associato alla casella PEC viene indicato in fase di offerta come indicato di seguito. In caso di esaurimento dello spazio messo a disposizione ed incluso nell'offerta PEC, è possibile acquistare spazio aggiuntivo di Conservazione dall'area Conservazione all'interno della webmail PEC.

Per maggiori informazioni sul servizio di Conservazione si rimanda alla documentazione specifica: <https://www.register.it/assistenza/cat/conservazione/>

Il servizio di Conservazione di Register ha conseguito ed è soggetto alla certificazione ISO9001:2015 ed ISO27001:2013.

### 5.2.2 Offerta PEC di Register SpA

L'offerta PEC di register è costituita da due tipologie di prodotto:

- **PEC attivata su dominio condiviso Register (PEC Agile)**

La casella PEC è attivata, a scelta del Cliente, sul terzo livello di uno dei domini gestiti da Register e messi a disposizione degli utenti PEC (per esempio dedicati agli ordini professionali). Si rimanda al sito di Register per informazioni aggiornate sulle caratteristiche delle stesse: <https://www.register.it/pec/>

Le caselle PEC di tale tipologia includono, fra le altre: Accesso alla WebMail; Configurazione Client POP3/S e IMAP/S; Servizio Antivirus / Antispam; Servizio di notifica via email che permette di facilitare il Cliente nella gestione della propria casella PEC. Tali email comunicano eventi come l'approssimarsi della scadenza del prodotto PEC; Spazio di Conservazione a norma dedicato alla casella PEC.

- **PEC attivata su dominio di un Cliente (PEC Unica)**

Si tratta di una casella PEC attivata sul terzo livello di un dominio di proprietà del Cliente.

Si rimanda al sito di Register per informazioni aggiornate sulle caratteristiche delle stesse: <https://www.register.it/pec/>

Le caselle PEC di tale tipologia includono, fra le altre:

Accesso alla WebMail; Configurazione Client POP3/S e IMAP/S; Servizio Antivirus / Antispam; Servizio di notifica via email che permette di facilitare il Cliente nella gestione della propria casella PEC. Tali email comunicano eventi come l'approssimarsi della scadenza del prodotto PEC; Spazio di Conservazione a norma dedicato alla casella PEC.

Affinché il servizio PEC possa funzionare correttamente il dominio deve appartenere alla piattaforma Register: solo così il Gestore avrà la possibilità di configurare senza errori in modo del tutto automatico il record MX (dei servizi DNS), verso mx.pec-email.com: base del funzionamento del servizio stesso.

Il Cliente è l'unico responsabile della corretta configurazione DNS. Qualora i record MX vengano variati, ripristinati o subiscano anomalie, il Cliente sarà tenuto a contattare il Customer Care per riattivare il servizio. Il corretto funzionamento del servizio PEC dipende dalla validità temporale del dominio a cui è associato.

Nel caso in cui il Cliente volesse implementare SPF sulla sua PEC, deve configurare, sul DNS del dominio PEC, un record TXT contenente il testo (comprese le virgolette):

```
"v=spf1 include:spf.pec-email.com ~all"
```

**Il record SPF deve essere aggiunto al record DNS relativo al dominio PEC** (esempio pec.nomedominio.tld), NON al dominio di secondo livello (esempio nomedominio.tld). Tale attività è a suo carico.

Le caselle PEC possono essere vendute singolarmente o in pacchetti cumulativi secondo le offerte online/offline.

I prezzi delle caselle sono presenti sulla pagina di riferimento del sito della Società e possono subire variazioni e scontistiche in base ad elementi di vario genere: si rimanda al sito Register per informazioni aggiornate in merito visitare la pagina: <http://www.register.it/pec/>

Il Titolare è tenuto a verificare periodicamente lo stato di riempimento della propria casella PEC al fine di evitare la mancata ricezione dei messaggi.

### 5.3 Interoperabilità gestori

In ottemperanza a quanto previsto dalla normativa vigente [4], Register garantisce l'interoperabilità con gli altri gestori in conformità alle specifiche tecniche di cui all'allegato del Decreto 2 novembre 2005 [2].

Register verificherà periodicamente l'invio e la ricezione di messaggi di Posta Elettronica Certificata verso gli altri gestori accreditati.

### 5.4 Modalità elaborazione dei messaggi

Il funzionamento del servizio PEC prevede le seguenti fasi:

- 1 invio di un messaggio da parte del mittente;

- 2 controllo sul messaggio effettuato dal server PEC del mittente (Punto di accesso) ed invio al mittente di una ricevuta di accettazione da parte del suo Gestore;
- 3 creazione della busta di trasporto;
- 4 invio della ricevuta di presa in carico dal server PEC del destinatario (Punto di Ricezione) al Punto di Accesso;
- 5 invio della busta di trasporto al dominio del destinatario;
- 6/7 invio della ricevuta di consegna al mittente.

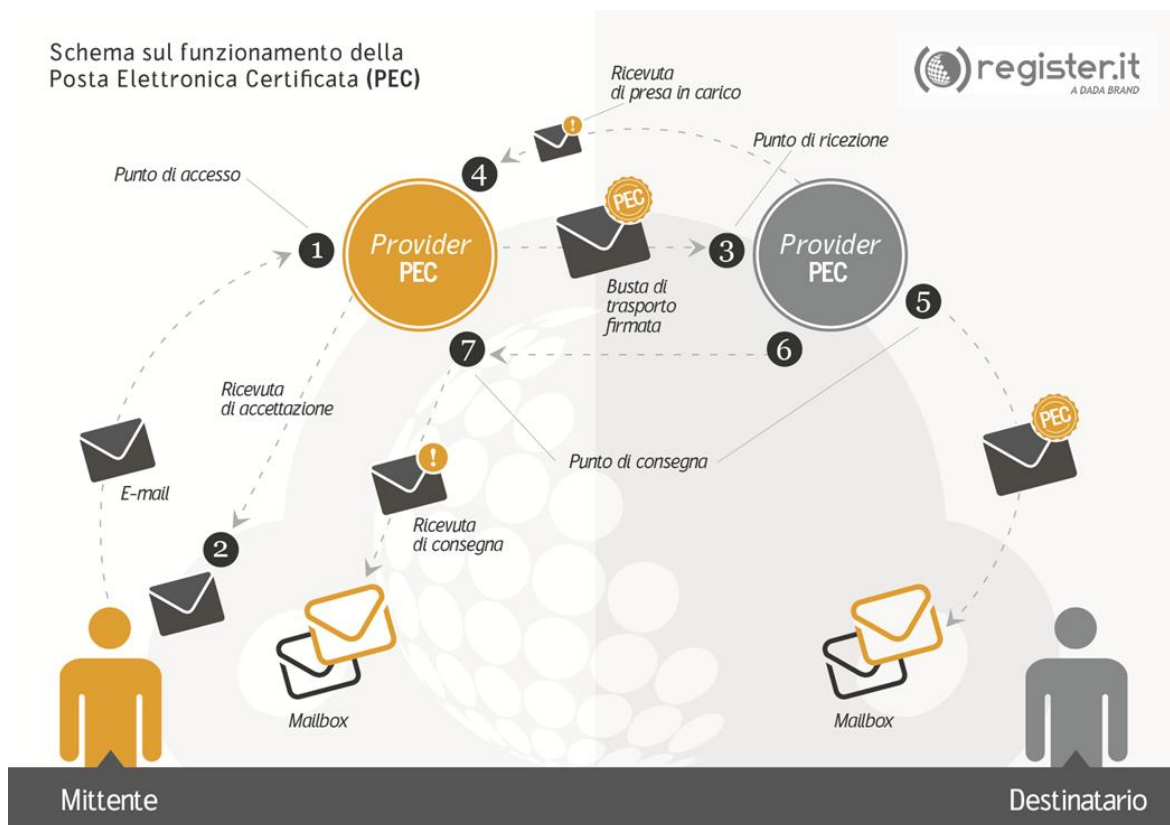


Figura 1 – Flusso End to End in caso di invio positivo del messaggio di PEC

Il flusso sopra descritto si riferisce alle comunicazioni da mittente munito di PEC verso destinatario munito di PEC.

Nel caso in cui il destinatario di un messaggio PEC non appartenga a un dominio PEC il processo di consegna del messaggio si svolge nel seguente modo:

- 1 invio di un messaggio da parte del mittente;
- 2 controllo sul messaggio effettuato dal server PEC del mittente (Punto di accesso);

- 3 invio al mittente di una ricevuta di accettazione da parte del suo server;
- 4 creazione della busta di trasporto;
- 5 invio della busta di trasporto al dominio del destinatario.

Qualora il gestore del mittente fosse impossibilitato ad accettare il messaggio in ingresso invierà al mittente stesso una ricevuta di mancata accettazione con la motivazione per cui non è stato possibile accettare il messaggio.

Qualora il gestore del destinatario sia impossibilitato a consegnare il messaggio di posta elettronica certificata (ad es: casella piena), il sistema invierà al mittente una ricevuta di mancata consegna. Tale comunicazione viene inviata dal gestore in due momenti specifici. Dopo 12 ore dall'invio del messaggio avviene la prima comunicazione di mancata consegna in cui si avvisa che il gestore del destinatario potrebbe non essere in grado di consegnare il messaggio. Dopo 24 ore avviene la seconda comunicazione in cui si avvisa della mancata consegna per il superamento dei tempi massimi.

Nel caso in cui una mail certificata PEC contenga un virus (sia nel testo che negli allegati) si presentano i seguenti scenari:

- qualora il virus venga intercettato dal gestore mittente viene inviato al mittente del messaggio un "avviso di non accettazione per virus informatico";
- se, diversamente, fosse il gestore destinatario a rilevare il virus, esso invierà un avviso di rilevazione virus al punto di ricezione il quale provvederà a consegnare al proprio utente (mittente del messaggio originale) un "avviso di mancata consegna per virus".

Nota: i log dei messaggi contenenti virus vengono comunque conservati dal gestore per il periodo di trenta mesi previsti dalla legge.

## 5.5 Modalità di archiviazione dei messaggi

L'archiviazione dei messaggi è un sistema che permette di conservare la posta in arrivo e di mantenerla organizzata mediante la creazione di specifiche cartelle.

Le modalità di archiviazione dei messaggi sono due:

- mediante client di posta (software per scaricare la posta elettronica sul proprio Personal Computer);
- mediante WebMail (archiviazione sui server PEC di Register).

## 5.6 Conservazione dei Log delle ricevute dei messaggi PEC

Tutte le ricevute delle e-mail inviate tramite la piattaforma certificata PEC (accettazione, avvenuta consegna, etc.) vengono salvate automaticamente dal sistema nella mailbox del Titolare PEC. Nel caso in cui il Titolare abbia la necessità di richiedere i log contenenti le ricevute PEC di uno specifico arco temporale, è possibile utilizzare la funzione di richiesta nel pannello di controllo della PEC. La procedura è descritta nel paragrafo 7.5 del presente Manuale Operativo.

Alla scadenza dei trenta mesi previsti dalla legge per la conservazione dei log delle ricevute, i log vengono fisicamente eliminati dai database del Gestore.

## 6 Guida all'uso dei Servizi PEC Register

### 6.1 Requisiti tecnici minimi per l'utilizzo del servizio

I requisiti tecnici minimi per utilizzare il servizio PEC fornito da Register sono:

- PC idoneo alla navigazione internet;
- connessione internet;
- programma che consente di usufruire dei servizi di connettività in rete e di navigare sul Web (browser).

Si consiglia di aggiornare le versioni del Browser al fine di non avere problemi di funzionalità.

### 6.2 Connettività e configurazione browser e software di posta elettronica

Dopo aver installato un browser o un software per scaricare la posta elettronica sul proprio Personal Computer, è necessario effettuare la procedura di configurazione affinché tali strumenti funzionino correttamente. In molti casi viene usata una configurazione predefinita.

Per utilizzare correttamente le varie applicazioni browser sono previste impostazioni specifiche in relazione alla versione del sistema operativo usato. Generalmente i settaggi vengono indicati durante la fase di installazione dell'applicazione.

Sul sito di Register, nella sezione *Manuali Email*, all'interno del canale *Assistenza*, è possibile trovare tutte le informazioni utili per la configurazione dei principali client di posta elettronica: <https://www.register.it/help/>

### 6.3 Gestione della password

Il sistema PEC di Register prevede che per accedere al servizio tutti gli utenti si debbano autenticare con username e password personali sia per l'invio sia per la ricezione di messaggi, al fine di evitare che informazioni riservate vengano trattate, consultate od usate impropriamente da persone non autorizzate.

Tramite Selfcare della PEC è possibile modificare la password ogni volta si presenti l'esigenza. Si consiglia di cambiare la password periodicamente.

In caso di smarrimento della password di accesso alla casella di Posta Elettronica Certificata, il Titolare PEC può procedere al recupero tramite un flusso sicuro che prevede due alternative:

1. la risposta alla domanda segreta precedentemente specificata dall'utente (in fase di attivazione);
2. la procedura di recupero password presente sulla pagina di login.

## 6.4 Modalità di accesso alla casella PEC

Il Titolare PEC può accedere alla propria casella in due modi:

- via WebMail;
- via client di posta elettronica.

### 6.4.1 Accesso via WebMail

Per accedere al servizio è necessario avere un Personal Computer dotato di un browser con livello di codifica a 128 bit o superiore. Per utilizzare le funzionalità complete di firma, è necessario utilizzare un browser che supporti la crittografia tramite il protocollo sicuro https.

Si accede alla Webmail dalla pagina <https://www.pec.net/>, seguendo 2 modalità:

- Autenticazione ad un solo fattore;
- Autenticazione forte a due fattori, utilizzando le credenziali Spid.

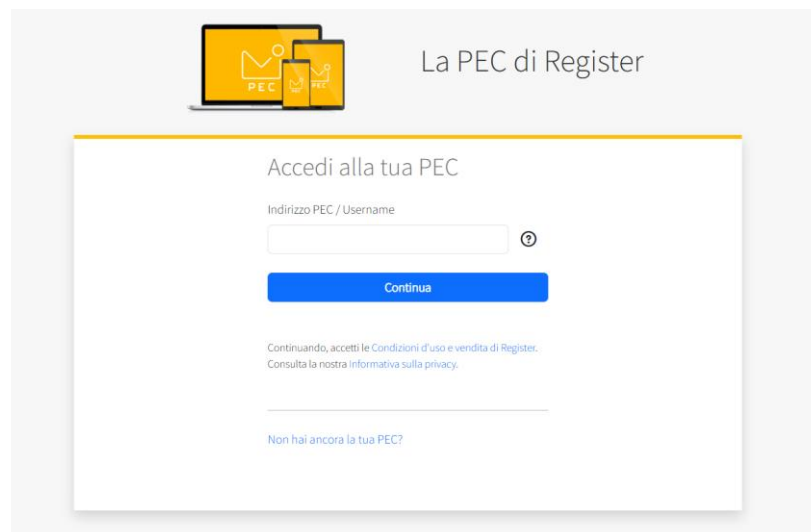


Figura 2 – Login Webmail PEC

Entrambe le modalità conducono all'area Selfcare della PEC, attraverso la quale è possibile accedere alla Webmail.

Per maggiori dettagli sull'area Selfcare, si rimanda al paragrafo dedicato [si veda il paragrafo 7.2 del presente Manuale].

#### *6.4.1.1 Accesso via WebMail: accesso a singolo fattore*

Per accedere alla propria casella PEC via WebMail è sufficiente inserire il proprio indirizzo PEC e seguire le indicazioni: l'autenticazione avviene mediante inserimento, negli appositi spazi, delle proprie credenziali (username e password, scelte in fase attivazione).

L'accesso via WebMail avviene attraverso l'utilizzo di un comune browser internet e non richiede alcuna attività di configurazione.

#### *Principali browser supportati*

Ai fini dell'utilizzo della WebMail, si consiglia il ricorso alle seguenti versioni di browser:

- Microsoft Edge: ultima versione o quella subito precedente;
- Firefox: ultima versione o quella subito precedente;
- Chrome: ultima versione o quella subito precedente;
- Safari: ultima versione o quella subito precedente.

Al fine di incrementare il livello di sicurezza dell'accesso alla casella PEC, è stato implementato un meccanismo che blocca temporaneamente l'accesso dalla webmail nel caso in cui il sistema rilevi un numero eccessivo di tentativi di login falliti e ravvicinati tra loro nel tempo.

**L'accesso a singolo fattore è garantito a tutte le PEC, siano esse intestate a persona fisica o giuridica, ad eccezione delle PEC che abbiano scelto di allinearsi agli standard europei**

#### *6.4.1.2 Accesso via WebMail: Autenticazione con credenziali SPID*

Register, in qualità di SP accreditato, offre la possibilità di accedere alla propria casella PEC via WebMail anche utilizzando le proprie credenziali Spid livello 2 (Level of Assurance 3 dello standard ISO/IEC DIS 29115 che si basa su un sistema di autenticazione a due fattori non necessariamente basato su certificati digitali).

E' sufficiente collegarsi all'indirizzo sicuro <https://www.pec.net/>, inserire il proprio indirizzo PEC, scegliere la voce '**Entra con Spid**', selezionare l'IdP con cui si hanno le credenziali e procedere all'autenticazione seguendo le indicazioni del provider Spid di riferimento. Dopo aver concluso

positivamente l'autenticazione si viene indirizzati al proprio Selfcare attraverso il quale è possibile accedere alla Webmail.

**Il servizio è attualmente disponibile solo per le PEC intestate a Persone Fisiche che abbiamo accettato di allinearsi allo standard europeo o che abbiano i requisiti per farlo.** Nel caso di accettazione, l'accesso tramite user e password non sarà più attivo e si potrà accedere solo in modalità sicura.

#### 6.4.2 Accesso via client di posta elettronica

Per poter accedere alla propria casella PEC è necessario aver installato un software per scaricare la posta elettronica (di seguito client) sul proprio Personal Computer.

E' necessario inoltre configurare opportunamente il client di posta elettronica con i parametri corretti per identificare, ad esempio, il tipo di server di posta a cui collegarsi per eseguire le operazioni di autenticazione della casella PEC.

Per potersi collegare al server di posta in arrivo verrà utilizzata una connessione protetta. Sarà infatti necessario configurare il protocollo POP3S o IMAPS e SMTP per la connessione SSL.

E' altresì possibile gestire i messaggi di posta elettronica dalla propria casella PEC nelle due seguenti modalità:

**POP3:** da utilizzare se si desidera salvare i messaggi ed inviarli dal proprio computer. La configurazione sarà impostata con l'ausilio del protocollo **pop3/s** (porta **995**) e **smpts** (porta **465**);

**IMAPS:** da utilizzare se si ha la necessità di leggere e inviare la posta da diverse postazioni. La configurazione sarà impostata utilizzando il protocollo **imaps** (porta **993**) e **smpts** (porta **465**).

#### I client di posta elettronica più diffusi sono:

- Microsoft Outlook 5.5 o superiore;
- Mozilla Thunderbird;
- Eudora;
- Lotus Notes;
- Kmail (sistema operativo Linux).

Online le guide per la corretta configurazione: <https://www.register.it/assistenza/cat/configurazione-pec/>

Rimane a cura del Titolare verificare costantemente l'aggiornamento della propria strumentazione rispetto ai criteri di sicurezza da adottare sia in termini di antivirus (per evitare di essere una fonte di contaminazione) sia in termini di sistemi operativi (utilizzando solo quelli che prevedono un costante aggiornamento di prevenzione alla contaminazione).

In alternativa alla password tradizionale, il Titolare può utilizzare un token di accesso sicuro generato area Selfcare, secondo quanto descritto al paragrafo 6.4.3. Tuttavia, per le PEC conformi agli standard europei, l'uso di questo metodo è obbligatorio.

### 6.4.3 Accesso tramite Token di accesso sicuro

Register rende disponibile, all'interno dell'area Selfcare PEC, una funzionalità di generazione e gestione di token di accesso sicuro per l'autenticazione ai servizi PEC.

Il token costituisce una credenziale applicativa alternativa alla password ordinaria e può essere utilizzato per l'accesso alla casella PEC tramite client di posta elettronica configurati con protocolli standard (IMAP, POP3, SMTP) nonché per ulteriori modalità di integrazione eventualmente previste.

Il token:

- è generato su iniziativa del Titolare della casella tramite area Selfcare;
- è univocamente associato alla specifica casella PEC;
- può essere revocato in qualsiasi momento dal Titolare;
- può essere rinnovato secondo le modalità rese disponibili dal sistema;
- non consente l'accesso all'area Selfcare, salvo diversa indicazione tecnica.

L'utilizzo del token consente di rafforzare la sicurezza delle credenziali di accesso e di favorire l'utilizzo della casella PEC anche in contesti conformi a standard europei di autenticazione sicura.

Il Titolare è responsabile della custodia e del corretto utilizzo dei token generati.

All'interno dell'area Selfcare, nella sezione dedicata alla Sicurezza, il Titolare può gestire i token di accesso sicuro relativi alle proprie caselle PEC. Sono disponibili le seguenti funzionalità:

- **Generazione del token:** creazione di token sicuro di accesso per l'accesso ai servizi PEC;
- **Revoca del token:** disabilitazione immediata del token precedentemente generato;
- **Rinnovo del token:** generazione di un nuovo token in sostituzione di uno precedente.

Il sistema registra le operazioni di generazione, rinnovo e revoca ai fini di tracciabilità e sicurezza.

## 7 Modalità di erogazione del servizio e procedure di gestione

### 7.1 Attivazione del servizio

La procedura di attivazione del servizio PEC si compone di due fasi: la fase d'acquisto e la fase di attivazione della casella PEC.

#### *Fase di Acquisto*

Il Cliente dà inizio alla fase di acquisto dopo aver selezionato sul sito di Register il prodotto PEC che preferisce [si veda il paragrafo 5.1 del presente Manuale].

Il servizio è disciplinato e fornito in conformità con la normativa vigente [2; 4] e con quanto previsto dalla documentazione fornita al Cliente di seguito elencata:

- Condizioni Generali di Servizio: <https://www.register.it/company/legal/>
- Ordine di Servizio PEC contenente le condizioni contrattuali particolari del servizio di Posta Elettronica Certificata: <https://www.register.it/company/legal/>
- il presente Manuale Operativo: [http://www.register.it/pec/Manuale\\_Operativo\\_PEC\\_Register\\_it.pdf](http://www.register.it/pec/Manuale_Operativo_PEC_Register_it.pdf)
- informativa sulla Privacy: <http://www.register.it/company/privacy.html>

Al termine della fase di acquisto il sistema genera il Pannello di controllo del Cliente.

#### *Fase di Attivazione*

La procedura di attivazione della casella PEC si esegue dal Pannello di controllo ed inizia con la scelta, da parte del Cliente, dell'indirizzo della casella stessa: il Cliente può, infatti, scegliere una casella PEC ospitata su un dominio di sua proprietà oppure su di un dominio condiviso Register [si veda il paragrafo 5.1 del presente Manuale].

Si precisa che il nome della casella non costituisce un elemento esaustivo di identificazione del Titolare.

Register, a sua discrezione, si riserva la facoltà di rifiutare l'attivazione di caselle per motivi tecnici (es: nomi troppo lunghi) o legali (es: nomi lesivi dei diritti dei terzi).

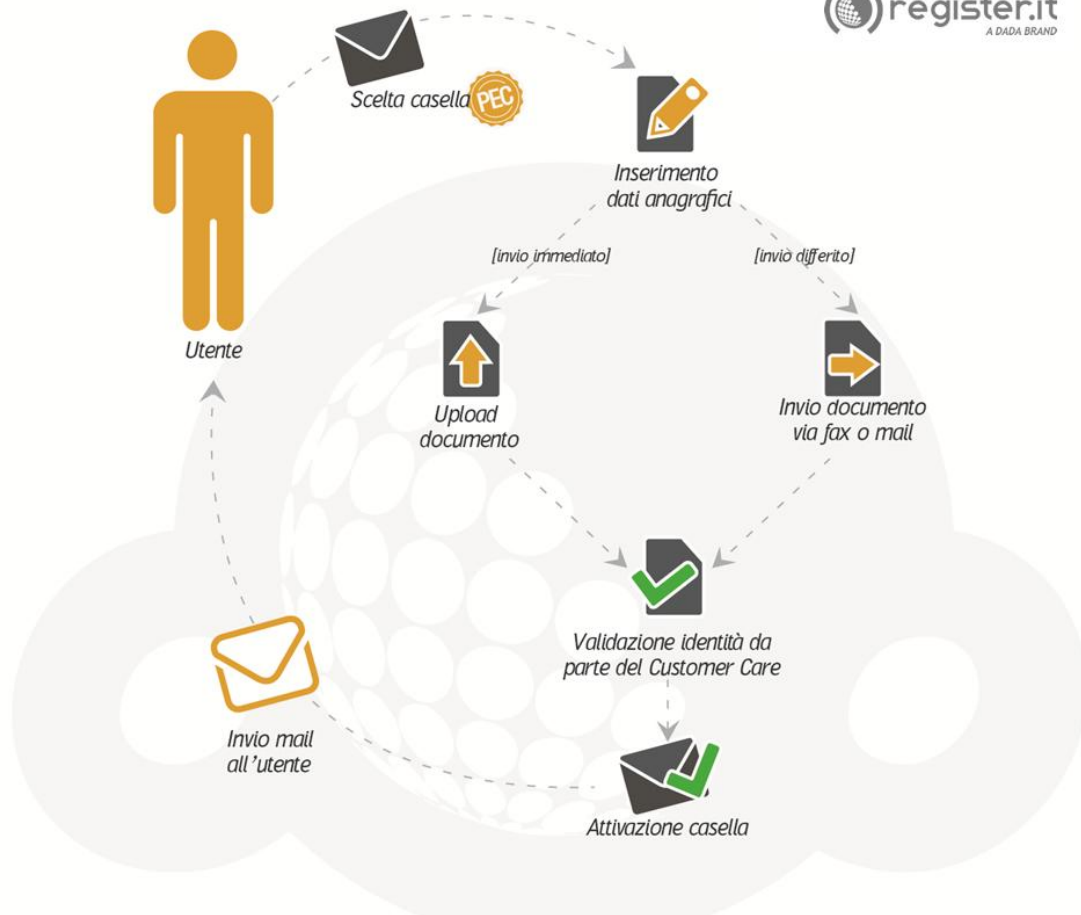


Figura 3 – Processo di attivazione della casella PEC

Una volta scelto l'indirizzo della casella PEC, il Titolare PEC la può attivare dal proprio Pannello di Controllo. L'attivazione prevede i seguenti quattro passaggi.

1 *Compilazione del "form di raccolta dati utente"*

Il Titolare PEC inserisce i propri dati anagrafici, un indirizzo e-mail valido esistente (come email di contatto per eventuali comunicazioni, da aggiornarsi a cura del Titolare), la password che intende utilizzare per l'accesso alla casella PEC e la risposta alla domanda di sicurezza (da utilizzare in caso di perdita della password).

2 *Invio della copia documento di identità e tessera sanitaria*

Il Titolare PEC compila ed invia al Customer Care Register la Richiesta di attivazione, insieme ad una copia fronte/retro del proprio documento di identità (carta di identità o documenti equipollenti ai sensi dell'art. 35 comma 2 DPR445/2000) e copia fronte/retro della tessera sanitaria al fine di poter

attivare il servizio PEC. L'invio dello stesso può essere fatto attraverso varie modalità fra cui: fax, e-mail, form di upload (i cui riferimenti sono presenti all'interno del pannello di controllo).

### 3 *Verifica dati*

Un operatore del Customer Care di Register verifica la corrispondenza tra i dati presenti sui documenti inviati dal Titolare PEC e i dati anagrafici del Titolare immessi nel form di attivazione e riportati nel PDF generato automaticamente.

### 4 *Attivazione*

Il servizio PEC viene attivato se la verifica di cui al punto 3 ha esito positivo. Il Titolare riceverà una email al suo indirizzo di contatto che conferma l'avvenuta attivazione. In caso contrario (es: documenti inviati errati o illeggibili, differenze tra i dati dei documenti e l'anagrafica inserita online, etc.), il Customer Care Register provvederà a comunicare al Cliente il fallimento della procedura di attivazione, che dovrà essere messa nuovamente in atto (punto 1).

Il Customer Care Register si riserva di impiegare massimo 3 giorni lavorativi per effettuare la verifica della congruenza tra dati inseriti e il documento di identità del Titolare e comunicarne l'esito.

#### **Note:**

- a) Durante il periodo di tempo che intercorre fra l'acquisto e l'attivazione del servizio PEC, l'utente ha la possibilità di modificare i dati inseriti nel punto 1 (per poter correggere eventuali errori) accedendo ad un form apposito presente all'interno del Pannello di Controllo PEC.
- b) Durante il periodo di tempo che intercorre fra l'acquisto e l'attivazione del servizio PEC, l'utente ha la possibilità di controllare lo stato di attivazione del servizio PEC (es: documentazione in attesa di essere ricevuta, documentazione ricevuta ma non ancora validata) dal Pannello di Controllo PEC.

#### **7.1.1 Attivazione PEC con credenziali SPID**

Register SpA offre il servizio di recapito elettronico certificato mediante una procedura ancora più sicura, facile, veloce e vicina agli standard europei.

Attualmente limitato alla registrazione delle pec per persona fisica, il Titolare ha la possibilità di effettuare la registrazione utilizzando le credenziali SPID rendendo il processo più sicuro e velocizzando l'attivazione.

Nell'ottica europea di identificazione certa del mittente del messaggio di posta certificata, includendo questa modalità di attivazione la PEC di Register sta andando verso il recapito qualificato internazionale rispetto al Regolamento eIDAS e allo standard REM, identificando in modo forte il Titolare.

L'utilizzo della casella non cambia e segue quanto indicato nel paragrafo 6.4

## 7.2 Area Selfcare PEC

L'area Selfcare è la sezione a cui si accede immediatamente dopo l'autenticazione e rappresenta il punto di controllo principale della propria PEC. Da questa area è possibile gestire in autonomia le funzionalità rese disponibili sul servizio, fra cui:

- accedere alla webmail;
- visualizzare in modo chiaro i dati della casella e del relativo titolare;
- revocare in modo definitivo la casella PEC
- gestire la password;
- gestire i token di accesso sicuro.

## 7.3 Modifica del Titolare assegnatario di casella PEC attiva e riassegnazione di casella PEC disattivata

### 7.3.1 Modifica del Titolare assegnatario di casella PEC attiva:

La modifica del Titolare di una casella PEC attiva è consentita esclusivamente in favore di soggetti, persone fisiche o giuridiche, che abbiano lo stesso codice fiscale o lo stesso numero di partita iva del precedente Titolare.

Il processo di modifica di titolarità della casella PEC potrà essere gestito in modo autonomo all'interno della webmail dove sono presenti voci di gestione della casella stessa. Tutti i dettagli all'interno dell'area online di assistenza: <https://www.register.it/assistenza/cat/pec/>

Rimane in carico al Titolare:

- di aver effettuato lui stesso la pulizia e la cancellazione dei messaggi presenti nella casella PEC;
- di assumersi la responsabilità di lasciare visibili al nuovo Titolare PEC solo le e-mail che è interessato a condividere;
- di sollevare Register da ogni responsabilità circa la presenza di messaggi di posta elettronica nella casella PEC dopo il cambio di titolarità.

Il documento richiesto dovrà essere inviato al Customer Care (seguendo le indicazioni presenti in procedura) unitamente alla copia dei documenti di identità (carta di identità o documenti equipollenti ai sensi dell'art. 35 comma 2 DPR445/2000) possibilmente di entrambi i Titolari PEC (attuale e nuovo).

Il Customer Care, una volta effettuate le verifiche con esito positivo, processerà la richiesta di variazione del Titolare della casella PEC modificando l'anagrafica e comunicherà ad entrambi i soggetti l'avvenuta modifica, inviando una email agli indirizzi di contatto del precedente e dell'attuale Titolare. Se invece la richiesta di cambio titolare viene respinta, l'attuale Titolare riceverà una email all'indirizzo di contatto contenente il motivo del rifiuto.

Register conserverà comunque un riferimento al vecchio Titolare al fine di permettere la ricerca e la fornitura, su richiesta del vecchio Titolare al Customer Care, dei log delle ricevute [si veda il paragrafo 7.5 del presente Manuale] per un periodo di trenta mesi (come richiesto dalla normativa [2]).

### 7.3.2 Riassegnazione di casella PEC disattivata

La richiesta di attivazione di una casella di posta elettronica certificata avente il nome identico ad una casella di posta già attivata in passato che ha cessato il proprio ciclo di vita, (cd. riassegnazione di una casella pec disattivata), è possibile esclusivamente a condizione che il nuovo Titolare, sia esso persona fisica o persona giuridica, sia lo stesso del precedente pertanto viene assunto che abbia codice fiscale o il numero di partita iva uguale al precedente Titolare.

A tal proposito, una volta espletata la fase di acquisto, in cui viene chiesto di indicare il nome della casella che si intende attivare, la richiesta di attivazione viene esaminata dal Customer care seguendo il criterio sopra indicato. In casi di rigetto della domanda, il Cliente riceverà debita comunicazione di esito negativo.

### 7.4 Rinnovo e disattivazione di una casella PEC

Il Titolare di una casella PEC può rinnovare il prodotto in scadenza in qualsiasi momento prima della scadenza del servizio stesso. Per fare ciò è necessario che lo stesso acceda alla pagina dedicata al rinnovo del prodotto dal proprio Pannello di Controllo di Register. Una volta effettuato il rinnovo, il servizio PEC rimane attivo fino alla successiva scadenza (ad es. una casella in scadenza il 15 maggio 2014, se rinnovata il 10 maggio 2014 avrà la successiva data di scadenza il 15 maggio 2015). Il Cliente riceve comunicazione alla email di contatto sull'approssimarsi della scadenza del prodotto PEC 30, 15 e 5 giorni prima, il giorno stesso della scadenza e 5 giorni dopo la scadenza stessa.

Con il rinnovo del servizio PEC viene rinnovato anche il servizio di Conservazione a norma dedicato alla casella PEC (1GB incluso nella casella).

Lo stato del servizio di Posta Elettronica Certificata può essere facilmente visibile direttamente dal Pannello di gestione della PEC all'interno della WebMail.

Una volta effettuato il pagamento, il Cliente riceve una email di conferma dell'avvenuto rinnovo.

Diversamente è possibile disattivare il servizio in due modi:

- **Naturale scadenza del prodotto:** non rinnovando il prodotto entro la data di scadenza. La casella PEC rimane in stato di sola lettura per un tempo massimo di 30 giorni durante i quali l'utente PEC può rinnovare il servizio senza perdita di dati. Allo scadere dei 30 giorni la casella viene revocata in modo irreversibile; in caso di mancato rinnovo di una casella esistente su dominio personalizzato (pec Unica), oltre alla revoca della casella pec si ha la decertificazione del dominio pec. L'operazione di decertificazione del dominio ha esito positivo solo se non ci sono altre caselle attive/in attivazione sullo stesso dominio. Allo scadere dei 35 giorni successivi alla data di scadenza Register elimina definitivamente la casella PEC, il suo contenuto e tutta la corrispondenza inviata in Conservazione;
- **Disattivazione anticipata:** revoca anticipata ed immediata rispetto alla data di scadenza. La casella pec viene immediatamente revocata. In caso di disattivazione anticipata di una casella esistente su dominio personalizzato (pec Unica) si ha immediata decertificazione anche del dominio pec. Il dominio viene decertificato solo se non ci sono altre caselle attive/in attivazione sullo stesso dominio. Tale azione è irreversibile. La disattivazione anticipata non può essere associata ai documenti messi in Conservazione che manterranno la scadenza originaria.

**Il Titolare deve revocare la propria PEC autonomamente cliccando sulla voce Revoca all'interno della sua area Selfcare.**

Solo in casi eccezionali, individuati a insindacabile giudizio di Register, il Titolare del servizio potrà richiedere la disattivazione contattando il Customer Care all'indirizzo [disattivazioni@pec-email.com](mailto:disattivazioni@pec-email.com). In tal caso, la richiesta dovrà essere trasmessa esclusivamente mediante invio di un messaggio di posta elettronica certificata (PEC) dalla casella oggetto di disattivazione, indicando e allegando le informazioni di seguito specificate:

- il proprio nome e cognome;
- l'indirizzo della casella di PEC da eliminare;
- un indirizzo e-mail valido (su cui comunicare l'effettiva disattivazione del servizio).

Questo un testo di esempio consigliato:

"OGGETTO: Disattivazione casella PEC .....@.....";

Testo della comunicazione: "Il/la sottoscritto/a \_\_\_\_\_, titolare della casella PEC

.....@..... richiede la disattivazione anticipata della stessa. Si prega di comunicare

l'avvenuta disattivazione all'indirizzo email: \_\_\_\_\_”

**Note:** per esercitare il diritto di recesso ex art. 64 e ss. del D.Lgv. 206/2005, applicabile solo ai “consumatori”, così come definiti all’art. 3 lett. “a” del citato decreto legislativo, si prega di fare riferimento a quanto indicato all’art. 2 delle Condizioni Generali di Servizio pubblicate nella homepage del sito di Register.

**Solo per le pec esistenti su dominio personalizzato: il mancato rinnovo del dominio o il trasferimento del dominio ad altro gestore alla scadenza comporta la disattivazione della/e casella/e pec ad esso associata/e e la cancellazione del relativo contenuto. Mancato rinnovo o trasferimento ad altro gestore sono assimilabili alla richiesta di disattivazione anticipata e nessuna ulteriore attività è in capo a Register.**

Il Titolare potrà avere evidenza dello stato di vita della propria casella accedendo al Pannello di controllo. La disattivazione della casella PEC viene confermata tramite e-mail all’indirizzo di contatto associato alla PEC stessa.

**Register non assume nessun onere di salvataggio preventivo dei contenuti delle caselle, che è invece demandata al cliente. Si consiglia, pertanto, di effettuare una copia di salvataggio dei messaggi pec giacenti prima di procedere o comunque entro i termini di decertificazione del dominio sopra indicati.**

**A seguito della disattivazione della PEC vengono disattivati tutti i servizi ad essa associati, inclusa la conservazione.**

Anche dopo la disattivazione di una casella PEC, il Titolare potrà comunque richiedere copia dei log delle ricevute di consegna PEC per i trenta mesi successivi alla ricezione dell’ultima notifica, come da procedura prevista [si veda il paragrafo 7.5 del presente Manuale].

Nel caso fosse stato acquistato spazio aggiuntivo di conservazione, dovrà essere anch’esso rinnovato al fine di poterlo continuare ad utilizzare, secondo quanto disposto nel Manuale della Conservazione e nell’ordine di servizio PEC. **Invitiamo a rinnovare lo spazio aggiuntivo per un periodo uguale a quello della casella PEC così da mantenere allineata la scadenza, poiché ad essa collegata.**

Nel caso in cui il Cliente o, se diverso, l’Utilizzatore abbia acquistato Spazio Aggiuntivo, egli potrà:

- non rinnovare lo Spazio Aggiuntivo. In tal caso tutta la Corrispondenza PEC versata in conservazione fino a tale momento verrà cancellata secondo quanto previsto dal Manuale della Conservazione. Rimarrà associato alla casella PEC lo spazio vuoto di 1 GB incluso nella casella stessa;
- rinnovare tutto lo Spazio Aggiuntivo acquistato, ma non rinnovare la casella PEC. In tal caso l’Utilizzatore può SOLO accedere alla Corrispondenza PEC conservata fino a quel momento nello spazio

gratuito di 1 GB e/o nello Spazio Aggiuntivo acquistati esclusivamente tramite il servizio di assistenza clienti. Per maggiori dettagli si rimanda al Manuale della Conservazione.

## 7.5 Richiesta dei Log contenenti le ricevute PEC

Le ricevute delle e-mail inviate tramite la piattaforma certificata PEC vengono salvate automaticamente nella mailbox del Titolare PEC. Anche in caso di cancellazione delle ricevute da parte del Titolare stesso, è possibile recuperare i log direttamente dal Pannello di controllo PEC (a meno di eccezioni particolari comunicate direttamente sul pannello) dopo un tempo indicativo di 14 ore dall'invio del messaggio PEC di cui si vuole i log.

Sarà così possibile scaricare sul proprio computer i log richiesti delle mail certificate PEC di cui il Titolare PEC è mittente o destinatario. Di seguito è riportata la figura relativa al form presente sul Pannello di Controllo per la richiesta dei log all'interno di un determinato range temporale.



Figura 4 – Form di richiesta per i log delle ricevute

I dati registrati dal Gestore ed indicati nei log come previsto dalla normativa, sono i seguenti:

- codice identificativo univoco assegnato al messaggio originale;
- data e l'ora dell'evento;
- mittente del messaggio originale;
- destinatari del messaggio originale;
- oggetto del messaggio originale;
- tipo di evento (accettazione, ricezione, consegna, emissione ricevute, errore, etc.);
- il codice identificativo dei messaggi correlati generati (ricevute, errori, ecc.);
- il gestore mittente.

Nei casi previsti dalla legge la richiesta di visualizzazione dei Log potrà essere avanzata anche dall'Autorità Giudiziaria

In caso di necessità di Log di valore legale per gli usi previsti dalla legge, in mancanza delle ricevute PEC originali, sarà possibile fare una richiesta al Customer Care del Gestore Register presentando la documentazione ufficiale.

## 7.6 Richiesta di assistenza (canali e tempistiche)

I Titolari di caselle PEC Register possono richiedere assistenza e informazioni mediante i seguenti canali:

### Form Online

Il Cliente può contattare l'assistenza clienti utilizzando il form "Richiedi Assistenza" presente nel Pannello di Controllo di Register.

### "Register Chat"

Il Cliente può contattare l'assistenza clienti utilizzando anche la funzione di "Live Chat" presente sul sito di Register

### Assistenza Guide e Telefonica

Il servizio di assistenza prevede il supporto tecnico ai clienti che utilizzano caselle di posta Elettronica Certificata fornite dal Gestore Register SpA.

Il servizio potrebbe essere a pagamento. Tutti i dettagli sono consultabili sulla pagina: <https://www.register.it/assistenza/cat/pec/>

## 8 Procedure e standard tecnologici e di sicurezza

Register, in accordo ai requisiti normativi, si pone l'obiettivo di assicurare un adeguato livello di qualità nell'erogazione del servizio PEC, garantendo altresì un appropriato livello di protezione delle informazioni.

Per salvaguardare i dati e gli asset che costituiscono il patrimonio informativo aziendale, Register ha adottato una serie di misure tecniche, organizzative e procedurali fondate sul rispetto dei seguenti principi cardine:

- *Riservatezza*: garantire l'accessibilità dell'informazione solamente a coloro che hanno l'autorizzazione ad accedervi;
- *Integrità*: garantire l'accuratezza e la completezza dell'informazione e dei metodi di elaborazione;
- *Disponibilità*: garantire l'accessibilità dell'informazione da parte degli utenti autorizzati, quando vi è necessità.

Il Gestore si riserva la facoltà di mettere in atto azioni sulle caselle e sull'accesso al servizio, dove si verificassero situazioni che possano compromettere la sicurezza delle caselle o del servizio stesso (esempio invii massivi che superano il numero di 500 invii al giorno).

### 8.1 Standard e procedure di riferimento

Ai fini dello sviluppo della piattaforma di erogazione del servizio PEC, Register ha fatto ricorso ad un approccio orientato alla Sicurezza delle Informazioni, prendendo in considerazione i principali standard internazionali, metodologie e best practices specifiche di settore (e.g. lo standard *ISO/IEC 27002*).

Inoltre, per la gestione dei processi di erogazione del servizio PEC, Register si attiene ai principi previsti dalle norme di riferimento di settore per l'implementazione di un Sistema di Gestione della Qualità, finalizzato al miglioramento continuo dell'efficacia e dell'efficienza nella realizzazione del prodotto e nell'erogazione del servizio, con lo scopo di ottenere e incrementare la soddisfazione del Cliente (norma UNI EN ISO 9001).

Il rispetto dei requisiti di sicurezza adottati per lo sviluppo della piattaforma e la gestione dei processi di erogazione del servizio PEC vengono costantemente controllati attraverso opportune verifiche ispettive interne, al fine di individuare eventuali punti vulnerabili e attuare azioni di miglioramento continuo dei livelli di sicurezza e gestione.

Nel seguito sono esplicitati alcuni processi relativi alla gestione operativa del servizio di Posta Elettronica Certificata adottati dalla Società.

## 8.2 Procedure di gestione dei sistemi

La Società ha adottato opportune misure e procedure finalizzate sia alla supervisione del regolare funzionamento dei sistemi appartenenti all'architettura PEC sia alla corretta gestione del sistema di erogazione del servizio PEC.

In particolare, Register ha implementato appositi strumenti per il monitoraggio dei sistemi ed il controllo dei messaggi di posta elettronica, nonché appropriate procedure per il salvataggio periodico dei dati.

### 8.2.1 Monitoraggio dei sistemi

Per verificare la disponibilità del servizio di Posta Elettronica Certificata sono state attivate sonde e strumenti per il controllo dei singoli elementi che compongono l'architettura del sistema PEC e per la verifica dei vari servizi che la piattaforma PEC eroga. I controlli agiscono a livello di singolo modulo di sistema e servizio, in modo tale da rilevare i malfunzionamenti in tempo reale e prevenire eventuali interruzioni del servizio stesso.

Nel caso in cui venga rilevato un malfunzionamento, il sistema di monitoraggio invia una e-mail ai tecnici addetti alla manutenzione del sistema informatico affinché vengano attivate le necessarie procedure di intervento.

Il sistema di erogazione del servizio PEC è attivo 24 ore su 24, 7 giorni su 7.

### 8.2.2 Antivirus e contrasto allo SPAM

Gli applicativi di controllo antivirus operano sulle e-mail certificate e non certificate. L'antivirus utilizzato da Register impedisce quanto più possibile il trasporto di virus all'interno dei messaggi di posta elettronica. La configurazione dell'antivirus, secondo quanto previsto a livello normativo [2], consente la gestione dei messaggi contenenti potenziali minacce in modo tale da permettere la valutazione dell'opportunità di consegnare un messaggio di mancata consegna per rilevazione di malware informatici o respingere/cancellare il messaggio contenente tale minaccia.

Il sistema antivirus effettua automaticamente, con cadenza oraria, controlli per verificare la presenza di aggiornamenti delle definizioni delle firme di riconoscimenti del malware e se disponibili le rende immediatamente operative; ciò consente alla piattaforma antivirus di essere efficace nella protezione di minacce malware anche se appena diffuse.

Il servizio offre un sistema di Antispam che opera esclusivamente sui messaggi non certificati. Tutti i messaggi vengono marcati secondo tre livelli: spam, spam sospetto e non spam. Nel caso risultasse che una casella sta inviando SPAM, tale casella verrà bloccata modificando la sua password. La nuova password verrà comunicata all'utente tramite una mail all'indirizzo di contatto alternativo fornito dal Titolare, oppure ad altro dei suoi riferimenti di contatto.

Con questa operatività si vuole contrastare gli invii di SPAM eseguiti grazie al furto di credenziali operato tramite phishing o malware.

Le caselle possono essere bloccate tramite modifica della password anche nel caso di rilevazione di attività sospetta o di furto d'identità quali, per esempio, l'invio ad intervalli regolari di messaggi vuoti o dal contenuto irrilevante per il monitoraggio della validità delle credenziali acquisite.

### 8.2.3 Backup dei dati

Per prevenire la perdita parziale o totale dei dati archiviati sono state previste specifiche modalità di backup: ogni qual volta un dato viene creato o modificato, esso viene automaticamente e contestualmente replicato su un sistema di archiviazione gemello. Il sistema di archiviazione risulta quindi in Alta Affidabilità ed è situato nelle sale dedicate alla sola Register ad accesso controllato e limitato site all'interno del Data Center presso BT Italia S.p.A. a Settimo Milanese. BT garantisce inoltre la continuità della fornitura elettrica, connettività, sistema di condizionamento e antincendio, in modo tale da ovviare in maniera tempestiva ad un'eventuale indisponibilità del servizio.

Sono previste le seguenti modalità di backup:

- Metrocluster: ogni volta che un dato viene scritto su filer, lo stesso viene automaticamente replicato sui dischi del secondo controller in modo da poter ovviare in maniera rapida alla mancata disponibilità dello storage stesso. L'adozione dell'architettura metrocluster preserva dal rischio di perdita dati in caso di distruzione di un raidgroup.
- Snapshot dei volumi: a cadenza oraria, giornaliera e settimanale vengono eseguite delle snapshot del contenuto, ovvero delle "fotografie" dello stato e dei dati contenuti, che consentono di ripristinare in qualsiasi momento il singolo dato riportandolo allo stato in cui si trovava al momento della creazione dello snapshot.

La gestione dei dati di backup, così come l'eventuale ripristino dei dati stessi qualora si riveli necessario, è di esclusiva competenza del personale autorizzato Register. Tutte le trasmissioni e repliche di dati avvengono attraverso canali sicuri ed esclusivamente all'interno delle architetture PEC di proprietà di Register.

Tutti i volumi della piattaforma sono replicati nel datacenter di disaster recovery (Caldera) tramite la tecnologia snapmirror del fornitore dei filer, che permette di avere una replica geografica dei dati soddisfacendo i criteri di RPO/RTO.

### 8.3 Gestione della continuità operativa

Unitamente agli strumenti di monitoraggio dei sistemi e dei messaggi di posta elettronica e le procedure per il salvataggio periodico dei dati, Register ha altresì adottato appositi sistemi per assicurare la continuità di erogazione del servizio e definito specifiche procedure per la gestione di eventuali rischi, guasti / disservizi e disastri. In particolare, oltre ai backup di tutti i dati relativi all'infrastruttura IT del servizio di Posta Elettronica Certificata, i log generati sono soggetti ad una ulteriore duplicazione per esigenze di conservazione a norma come richiesto da normativa. Il flusso di archiviazione dei log generati è il seguente:

- Merge dei file generati dalle istanze dei vari nodi PEC;
- Marcatura temporale del file ottenuto tramite il servizio di Time Stamp Authority Certificata interno di Register, per garantirne l'integrità;
- Spostamento del file su piattaforma interna di Conservazione a norma.

#### 8.3.1 Sistemi di continuità/backup

Allo scopo di garantire i livelli di servizio richiesti dalla normativa vigente [2], Register ha organizzato la propria infrastruttura tecnologica per l'erogazione del servizio PEC con le modalità che vengono di seguito elencate:

- server ridondati con macchine secondarie in standby che subentrano automaticamente nel caso fault del sistema principale;
- gruppi di continuità distinti che servono i sistemi ridondati;
- generatore autonomo di elettricità, nel caso in cui la mancanza di tensione della rete elettrica si prolunghi nel tempo;
- monitoring esterno continuo dei servizi con allarmi verso la struttura tecnica di gestione per l'implementazione di interventi di ripristino immediati;
- firewall ridondati che permettono l'accesso ai servizi in modalità sicura, come definito dalla normativa tecnica in vigore. Il collegamento per la gestione avviene attraverso connessioni criptate sicure da indirizzi autorizzati;
- generazione di copie di backup come precedentemente indicato;

- replica geografica dei dati e dei servizi essenziali alla consultazione, sul Data Center di Disaster Recovery.

### 8.3.2 Procedure di ripristino

Register ha provveduto a definire apposite procedure finalizzate alla gestione di situazioni derivanti dalla manifestazione di taluni rischi, quali:

#### *Indisponibilità di una sede operativa*

L'erogazione del servizio di Posta Elettronica Certificata è assicurata mediante l'attivazione del personale coinvolto nell'erogazione del servizio PEC attraverso un canale cifrato (da remoto).

#### *Manomissione / furto degli elaboratori di dati*

In caso di manomissione / furto degli elaboratori di dati, Register sporge regolare denuncia alle Autorità competenti, assicura l'inibizione degli accessi logici attivi connessi allo specifico elaboratore e pone in essere attività volte a tutelare gli utenti della PEC eventualmente danneggiati dall'evento.

#### *Alterazione, manomissione, furto o utilizzo improprio di dati*

In caso di alterazione / manomissione / furto o utilizzo improprio dei dati, Register sporge regolare denuncia alle Autorità competenti, assicura l'inibizione degli accessi logici delle persone coinvolte ai sistemi, attua le necessarie azioni correttive per il ripristino della situazione e pone in essere attività volte a tutelare gli utenti della PEC eventualmente danneggiati dall'evento.

#### *Carenze di sicurezza*

I reparti tecnici effettuano un monitoraggio 24 ore su 24 dello stato dei sistemi, in modo da rilevare eventuali minacce di sicurezza/integrità dei sistemi PEC e applicare tempestivamente le opportune modifiche seguendo i flussi previsti per gli aggiornamenti di sicurezza.

#### *Incidenti sulla rete (Data Center)*

Un presidio sistemistico controlla costantemente il sistema; al verificarsi di eventuali allarmi vengono effettuate le opportune azioni correttive. L'architettura implementata prevede una ridondanza dei sistemi nel DC di produzione in due sale separate e presso due data center distinti completamente indipendenti anche da un punto di vista di connettività; in questo modo, nel caso in cui si verificano eventuali problematiche, è possibile attivare il sistema di DR.

### 8.3.3 Gestione guasti / disservizi e disastri

La prima categoria di interruzioni del servizio è riferibile ai guasti od ai disservizi che potrebbero interessare i servizi fiduciari e le sue componenti; essi sono raggruppabili come segue:

- Problemi legati alle infrastrutture;
- Guasti hardware (server);
- Disservizi legati al software;
- Disservizi legati ai dati.

Come riportato in precedenza, l'architettura di gestione ed erogazione dei servizi è fisicamente e logicamente ridondata presso due sale separate ed ubicate presso il fornitore BT Italia S.p.A. di Settimo Milanese e il datacenter di Disaster Recovery Irideos geograficamente separato ubicato a Caldera Milano. Ciò consente di ridurre al minimo la possibilità di down totale del servizio causata da una problematica logistico-architetturale.

Nella seguente tabella si riportano le casistiche di guasti presi in considerazione per ciascuna categoria sopracitata, una breve descrizione delle contromisure e delle modalità di gestione applicate e l'indicazione del tempo di intervento stimato per la gestione dell'evento.

Evento	Contromisure e modalità di gestione
<b>Problemi legati alle infrastrutture</b>	
Indisponibilità totale degli apparati di un solo compartimento del Data Center	Il flusso dati viene reindirizzato sugli apparati e i server del secondo compartimento, che prende in carico l'erogazione del servizio fino al ripristino del compartimento indisponibile.
Indisponibilità di un Virtual Server	In caso un Virtual Server risulti non disponibile, il Virtual Server presente nel secondo compartimento consentirà la gestione della totalità del servizio.
Guasto di uno switch (SWN/SWS)	Se uno dei due switch del compartimento risulta non disponibile, la connettività viene garantita automaticamente dallo switch di backup. Le interfacce di rete dei singoli server sono configurate in maniera tale da essere collegate ad entrambi gli switch.
Indisponibilità del server DBM	Occorre utilizzare lo slave di backup come nuovo master. Durante l'operazione di switch non risulterà possibile creare/rimuovere/modificare gli account e i domini PEC; la continuità di erogazione del servizio è comunque garantita.
Indisponibilità dell'HSM	L'architettura PEC è stata sviluppata prevedendo la presenza di due HSM, uno per compartimento. Il sistema è progettato in maniera tale da consentire a un HSM di prendere in carico la gestione dell'intero flusso in caso di indisponibilità dell'altro HSM.
Guasto al controller del filer	In caso di guasto al controller dei dischi del filer di un compartimento, l'architettura di storage adottata prevede che la testa del filer del secondo compartimento si prenda in carico anche la gestione dei dischi di questo compartimento, garantendo così la continuità di erogazione del servizio.
Guasto di un disco del filer	Il guasto del disco di un filer è automaticamente gestito dall'architettura adottata.
Guasto/indisponibilità dei dischi del filer	L'architettura metrocluster prevede una replica del contenuto dei dischi di un compartimento sui dischi del secondo compartimento.
Crash/indisponibilità totale del nodo PEC	L'architettura prevede la presenza di "n" nodi PEC replicati: nel caso uno di essi risultasse indisponibile, il balancer lo escluderà automaticamente, smistando le richieste sugli altri nodi.
Indisponibilità di uno o più servizi del nodo PEC	L'architettura prevede la presenza di "n" nodi PEC replicati: nel caso uno di essi risultasse indisponibile, il balancer lo escluderà automaticamente, smistando le richieste sui rimanenti nodi attivi.
Crash/indisponibilità di NTP client	Il nodo non si può considerare più attivo ai fini dell'erogazione del servizio, in quanto non è più possibile garantire la correttezza della data di sistema e quindi della marcatura temporale. In questo caso il balancer provvede a escludere l'intero nodo e a smistare le richieste sui rimanenti nodi attivi.
Crash/indisponibilità del server NTP	Per poter garantire la correttezza della data dei sistemi, è prevista la ridondanza per questo server: in caso di indisponibilità di questo server, il servizio di sincronizzazione NTP sarà fornito dal sever NTP di backup del secondo compartimento.
Crash/indisponibilità di LDAP slave	In tale caso, non è possibile per il modulo OpenPEC del nodo PEC individuare i domini PEC per stabilire se una e-mail è PEC o normale, quindi il nodo non può essere considerato attivo ai fini dell'erogazione del servizio. Il balancer provvederà a considerare il nodo in questione offline e a smistare quindi le connessioni sui rimanenti nodi attivi.

Evento	Contromisure e modalità di gestione
Crash/indisponibilità del master LDAP	<p>Per poter garantire la sincronizzazione dell'elenco dei gestori PEC con quello ufficiale dell'Agenzia per l'Italia Digitale, è previsto un server LDAP secondario che si attiva in caso di non disponibilità del master LDAP e che si fa carico delle operazioni di sincronizzazione dell'elenco gestori PEC.</p> <p>Inoltre, in caso di non disponibilità del master LDAP, il server di backup si fa carico anche della gestione del database LDAP per il controllo degli accessi ai server.</p>
Crash/indisponibilità di balancer	Sono previsti due server balancer, dei quali uno rimane attivo, l'altro resta in stand-by. In caso di problemi sul balancer attivo che ne impediscano il funzionamento, viene attivato il balancer secondario che si prenderà in carico la gestione di tutti i VIP (Virtual IP) e di tutto il bilanciamento dei servizi, garantendo così la continuità dell'erogazione del servizio.
Crash/indisponibilità di uno slave DB	In caso un'istanza slave del DB (su uno dei nodi PEC) risulti non disponibile, il balancer considererà l'intero nodo non disponibile e provvederà automaticamente ad escluderlo dal bilanciamento, reindirizzando tutto il traffico sui rimanenti nodi attivi.
Indisponibilità di uno o più servizi del nodo PEC	In caso di indisponibilità di uno o più servizi del nodo PEC, il nodo stesso dovrà considerarsi non più affidabile. Quindi il balancer provvederà a escluderlo dal cluster e, automaticamente, smistare le connessioni e le richieste sui rimanenti nodi attivi.
Problemi su tabelle database slave	In caso si verificano problemi sulle tabelle di un database slave, tale database dovrà essere messo offline (in maniera automatica) in modo da non compromettere l'integrità dei dati. Quindi l'intero nodo sarà disabilitato dal balancer e il traffico rediretto automaticamente sui restanti nodi attivi.
Problemi su tabelle database master	In caso si verificano problemi sulle tabelle del database master lo stesso DB sarà da considerarsi non più attendibile fino a quando verrà effettuato un controllo sull'integrità dei dati; occorre utilizzare lo slave di backup come nuovo master. Durante l'operazione di switch non risulterà possibile creare/rimuovere/modificare gli account e i domini PEC; la continuità di erogazione del servizio è comunque garantita.
LDAP bloccato (client)	L'intero nodo PEC verrà disattivato automaticamente dal bilanciatore e il traffico reindirizzato sui rimanenti nodi attivi.
Perdita dati su storage	In caso di perdita dati sullo storage, sia per danno accidentale che per malfunzionamento, è necessario l'intervento manuale di un amministratore per il ripristino dei dati dai backup.

Tabella 2 – Guasti e disservizi: contromisure e modalità di gestione

## 8.4 Standard tecnologici e di sicurezza

Register ha sviluppato ed adottato misure tecniche e di sicurezza finalizzate alla gestione delle infrastrutture tecnologiche utilizzate per l'erogazione del servizio PEC, con particolare riguardo alla protezione dei dati generati dai sistemi di trasmissione di posta elettronica.

Al fine di identificare le misure di sicurezza più opportune, Register ha condotto una specifica analisi dei rischi.

### 8.4.1 Analisi dei rischi

L'analisi dei rischi è stata condotta sulla base della seguente metodologia:

- 1 In primo luogo è stato identificato il perimetro di applicazione dell'analisi, individuando le sedi dalle quali viene erogato il servizio PEC e individuando gli asset e le informazioni inerenti il servizio PEC;
- 2 Successivamente sono individuate le minacce potenzialmente impattanti, prendendo in considerazione minacce legate al contesto fisico/ambientale, minacce generate dal comportamento umano e minacce legate al contesto tecnologico;
- 3 Sono definite le metriche di riferimento ed effettuata l'analisi del rischio relativo alla sicurezza delle informazioni, determinando la verosimiglianza di un evento dannoso e le potenziali conseguenze che lo stesso potrebbe causare;
- 4 Infine, sono identificate e implementate le necessarie contromisure, atte ad assicurare un adeguato livello di sicurezza.

### 8.4.2 Soluzioni tecniche adottate

L'architettura della piattaforma PEC è bilanciata (strutturata in modo da soddisfare carichi di connessione elevati) e ridondata (strutturata in modo da garantire la continuità del servizio in caso di malfunzionamenti del server).

Il sistema si avvale di un server HSM per la verifica e apposizione della firma digitale.

Infine, un firewall filtra e blocca flussi di dati in base a specifiche direttive di sicurezza.

L'infrastruttura PEC è collegata ad internet tramite un'attestazione GigaEthernet e si basa su un canale ridonato con banda da 1 Gbps (o superiore) ciascuno e strutturati per garantire una banda adeguata alla tipologia di servizio offerto.

Le ricevute PEC vengono conservate in un apposito storage che ne garantisce l'archiviazione sicura e la possibilità di consultazione.

### 8.4.3 Misure di sicurezza per la protezione di dati e architetture

Di seguito si riporta un breve riassunto delle misure di sicurezza adottate da Register in relazione alle categorie di minacce sopra citate.

#### *Misure a presidio di minacce legate al contesto fisico - ambientale*

A fronte di minacce quali eventi naturali (alluvione, grandinata, fulmini, terremoto, etc.) o eventi impattanti le strutture (allagamento, blackout energetici, crolli o esplosioni accidentali, incendio, accessi non autorizzati alle strutture, etc.), pur tenendo conto dei trend storici di manifestazione degli eventi stessi e della bassa incidenza dei fenomeni considerati nell'arco storico di operatività delle sedi a perimetro, la Società ha comunque fatto ricorso a apposite contromisure specifiche per le varie sedi di erogazione del servizio:

- utilizzo di sistemi parafulmine e dispositivi di messa a terra, al fine di prevenire eventuali interruzioni di operatività a seguito di sovraccarichi della rete elettrica e conseguente danneggiamento delle apparecchiature elettroniche e di eventuali danni collaterali quali incendi;
- adozione di impianti di rilevazione fumi ed estintori/idranti a mano a norma di legge, per prevenire e fronteggiare minacce di incendio o esplosioni accidentali;
- installazione di gruppi di continuità (sistema UPS), per governare fenomeni di black out energetici o guasti agli impianti di distribuzione interna dell'energia elettrica;
- ricorso a sistemi di accesso controllato agli edifici, per prevenire accessi non autorizzati e per monitoraggio costante della sicurezza delle sedi.

#### *Data Center:*

La collocazione geografica dei Data Center (DC) presso cui sono ubicate le architetture di erogazione del servizio PEC di produzione è ottimale dal punto di vista del rischio sismico, del rischio inondazione e dei rischi dovuti alla vicinanza di impianti industriali pericolosi.

Tutti i sistemi di contromisura sotto descritti sono, tranne ove specificatamente indicato, demandati alla gestione di BT Italia (DC primario) e Irideos (DC di disaster recovery). Tali contromisure sono garantite e regolate dal contratto di housing tra Register ed i fornitori di data center.

Sulla base delle condizioni di fornitura del servizio contrattualizzate, il fornitore è responsabile anche di assicurare il corretto funzionamento, o nel caso gli opportuni interventi, in caso di indisponibilità del Service Provider o di malfunzionamento o guasto delle linee di telecomunicazione. Inoltre il fornitore fornisce, su richiesta, opportuni report post-incidente che indichino l'accaduto e le contromisure apportate in caso di incidente.

### *Misure a presidio di minacce generate dal comportamento umano*

Per prevenire eventuali rischi generati da azioni e atteggiamenti messi in atto dal personale di Register o da soggetti terzi, sia intenzionali che accidentali, la Società ha ritenuto opportuno adottare accorgimenti quali:

- Selezione di personale adeguatamente competente;
- Promozione di attività per lo sviluppo delle conoscenze e delle competenze del personale;
- Diffusione di apposito materiale con regole comportamento;
- Adozione di misure logiche di protezione dei dati e delle informazioni presenti sui sistemi e sulle postazioni di lavoro.

### *Misure a presidio di minacce legate al contesto tecnologico*

Al fine di prevenire la manifestazione di tale categoria di minacce, Register ha implementato specifiche contromisure sia sulle postazioni di lavoro del personale sia sui sistemi dell'architettura PEC, ubicata presso il fornitore BT Italia.

Limitatamente alle postazioni di lavoro utilizzate da personale Register impiegato nell'erogazione del servizio PEC (sia per servizi a supporto del Cliente sia per gestione operativa delle architetture IT) la Società ha implementato, a livello tecnologico, le seguenti misure di sicurezza:

- Adozione di un sistema di autenticazione ed autorizzazione a livello informatico, basato su profili di accesso differenziati sulla base delle attività lavorative richieste in accordo alle mansioni attribuite e del livello professionale ricoperto. Tale contromisura, nello specifico, è stata implementata non solo in riferimento all'erogazione del servizio PEC, ma anche in accordo alla vigente normativa in materia di protezione dei dati personali;
- Adozione di una piattaforma di riferimento per le postazioni di lavoro dotata di sistemi antivirus (ove applicabile) e di aggiornamento periodico del livello di sicurezza delle postazioni (patch management) e di sistemi di esecuzione automatica dei backup;
- Configurazione a livello network di reti virtuali private (VLAN e VPN) per l'accesso ai sistemi e alla rete di gestione delle architetture IT e gestione del servizio ed adozione di misure di

protezione delle trasmissioni mediante sistemi di cifratura dei flussi dati (protocolli di autenticazione cifrati).

La gestione dei server per l'erogazione del servizio PEC, dislocati presso Settimo Milanese, è a cura del personale Register. A tal proposito, la gestione delle contromisure a presidio di potenziali rischi, quali: la contaminazione dei sistemi da virus informatico, gli attacchi informatici, l'accesso logico non autorizzato ai dati, furto/sottrazione di credenziali di autenticazione, etc, è effettuata a cura di amministratori di sistema della Società. Le misure di sicurezza implementate includono:

- Sistema di autenticazione e autorizzazione a livello informatico; password policy (e.g. scadenza periodica, regole sulla composizione, etc.); gestione dei profili utenti e del ciclo di vita delle utenze (disattivazione immediata in caso di cessazione delle necessità di accesso);
- Modalità di controllo accessi fisici regolato da badge personali ad accesso limitato e tracciamento accessi;
- Adozione di sistemi di logging remoto delle attività e degli accessi;
- Sistemi antivirus e di aggiornamento periodico del livello di sicurezza (patch management);
- Backup periodici dei dati e duplicazione in real time dei dati tra i sistemi presenti nelle due sale;
- Configurazione di reti virtuali separate per il trasferimento dei dati, al fine di poter isolare porzioni di rete o canali di trasmissione interi in caso di esigenze derivanti da compromissione delle trasmissioni;
- Comunicazioni cifrate con protocolli sicuri;
- Monitoraggio continuo dei sistemi per individuare tempestivamente degradazioni/interruzioni dei servizi o delle funzionalità dei singoli elementi che costituiscono l'infrastruttura PEC. Tramite l'utilizzo di software di monitoraggio, è possibile infatti monitorare in tempo reale i nodi, le reti e i servizi specifici per la PEC e in caso di interruzione o di degrado, il sistema genera un alert verso il personale di presidio IT h24/7 per consentire un tempestivo intervento. Il sistema di monitoraggio consente inoltre di avere informazioni aggiornate sui livelli di carico dei server coinvolti nell'erogazione del servizio PEC (ad es. % carico CPU, RAM utilizzata, traffico di rete generato, etc.) al fine di poter tempestivamente intervenire qualora si profilino situazioni di eccessivo carico che potrebbero causare un degradamento del servizio;
- Modalità di controllo accessi fisici, sia presso le sedi della Società ove sono presenti le postazioni di lavoro dei dipendenti, sia presso il Data Center.

## 8.5 Indicazione delle modalità di protezione dei dati dei titolari

I dati dei Titolari PEC vengono salvati in uno storage all'interno dell'area certificata PEC. Per garantire livelli massimi di protezione, in tutti quei casi di disservizio del sistema, i dati dei Titolari sono replicati su un server di backup, utile al ripristino dei dati stessi. L'accesso ai dati dei Titolari avviene in modalità sicura e solo dal personale autorizzato Register.

Per ulteriori informazioni relative alle attività di trattamento di dati personali effettuate da Register in qualità di titolare del trattamento in ambito PEC, si rinvia alla specifica "Informativa sul trattamento dei dati personali resa ai sensi dell'art. 13 del Regolamento UE 2016/679 ("GDPR"), con riferimento al servizio PEC di Register S.p.A.", pubblicata sul sito [www.register.it](http://www.register.it).

### 8.5.1 Gestione delle credenziali applicative (Token)

Il Gestore adotta misure tecniche e organizzative volte a garantire la generazione sicura, l'associazione univoca e la revocabilità dei token di accesso.

I token:

- sono generati mediante procedure automatizzate sicure;
- sono memorizzati in forma di hash crittografico nei sistemi del Gestore, pertanto non recuperabili in chiaro;
- possono essere revocati in ogni momento dal Titolare;
- vengono revocati a fine scadenza dal sistema;
- cessano di produrre effetti a seguito di revoca o sostituzione.

Il Gestore prevede politiche di durata e rinnovo dei token coerenti con i livelli di sicurezza del servizio.

## 9 Indicazione delle condizioni di fornitura

### 9.1 Obblighi e responsabilità del Gestore per l'erogazione del servizio PEC

Register fornisce il servizio di Posta Elettronica Certificata conformemente a quanto previsto dalla vigente normativa in materia [2; 4], dalle Condizioni Generali di Servizio [si veda il paragrafo 7.1 del presente Manuale] e dall'Ordine di Servizio PEC, nelle modalità descritte nel presente Manuale.

In particolare, Register si impegna a:

- predisporre ogni misura idonea ad assicurare l'interoperabilità dei servizi offerti, secondo quanto previsto dalle regole tecniche di cui all'art. 17 del Decreto del Presidente della Repubblica 11 febbraio 2005, n. 68 – *“Regolamento recante disposizioni per l'utilizzo della posta elettronica certificata”* [4];
- firmare le ricevute e le buste di trasporto con firma elettronica che garantisce la provenienza, l'integrità e l'autenticità del messaggio di posta elettronica certificata secondo le modalità previste dalle regole tecniche di cui all'art. 17 del Decreto del Presidente della Repubblica 11 febbraio 2005, n. 68 – *“Regolamento recante disposizioni per l'utilizzo della posta elettronica certificata”* [4];
- fornire al mittente la ricevuta di accettazione entro 30 minuti nel periodo di disponibilità del servizio (calcolato al netto della durata della trasmissione del messaggio con relativi allegati);
- fornire al mittente la ricevuta di avvenuta consegna o, entro le 24 ore successive all'invio, l'avviso di mancata consegna qualora il messaggio di Posta Elettronica Certificata non risulti consegnabile;
- apporre un riferimento temporale su ogni messaggio, nonché una marca temporale sui log dei messaggi generati da sistema; tali marche temporali vengono automaticamente apposte sui log almeno una volta al giorno utilizzando un servizio di marcatura temporale certificato (TSA), ai sensi della normativa vigente [2];
- trasmettere integralmente il messaggio di Posta Elettronica Certificata dal mittente al destinatario, includendolo nella busta di trasporto;
- mantenere traccia delle operazioni di trasmissione del messaggio su un apposito Registro dei log dei messaggi;
- conservare i dati del registro dei log dei messaggi [si veda il paragrafo 7.5 del presente Manuale] per trenta mesi, ai sensi della normativa vigente [2];

- adottare adeguate misure per garantire segretezza della corrispondenza, l'integrità e la sicurezza del servizio di posta elettronica certificata;
- adottare opportune soluzioni tecniche ed organizzative che garantiscano la riservatezza, la sicurezza, l'integrità e l'inalterabilità nel tempo delle informazioni contenute nel registro del log dei messaggi;
- prevedere l'esistenza di servizi di emergenza che assicurano il completamento della trasmissione ed il rilascio delle ricevute, salvo in caso di eventi improvvisi dagli esiti disastrosi (terremoto, attentato, etc.);
- non accettare messaggi con virus informatici, informare tempestivamente il mittente dell'impossibilità di dar corso alla trasmissione e conservare detti avvisi per trenta mesi;
- rilasciare un avviso di non accettazione per eccezioni formali, nonché di rilevazione di virus informatici o di mancata ricezione della ricevuta di presa in carico o di avvenuta consegna per superamento dei tempi massimi previsti, ai sensi della normativa vigente [2] ;
- assicurare i livelli minimi di esercizio previsti dalle regole tecniche di cui all'art. 17 del Decreto del Presidente della Repubblica 11 febbraio 2005, n. 68 – *“Regolamento recante disposizioni per l'utilizzo della posta elettronica certificata”* [4]; agire nel rispetto delle norme previste dal Decreto Legislativo 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali), sue successive modifiche e integrazioni [8] e provvedimenti dell'Autorità Garante per la Privacy emessi in materia [9; 10].

Register si riserva il diritto di modificare le modalità tecniche e contrattuali di erogazione del servizio al fine di adeguarlo alle offerte commerciali, all'evoluzione tecnologica e alle disposizioni normative eventualmente emanate, impegnandosi ad aggiornare il presente Manuale Operativo.

## 9.2 Obblighi del Titolare della casella, contraente del servizio

Il Titolare della casella PEC assume gli obblighi e le responsabilità previste dalla normativa vigente, dalle Condizioni Generali di Servizio e dall'Ordine di servizio PEC.

Inoltre, egli assume l'obbligo di:

- consultare preventivamente il presente Manuale Operativo;
- fornire al Gestore tutte le informazioni necessarie ad identificare la persona ed attivare il servizio, garantendo, sotto la propria responsabilità, la veridicità dei dati comunicati e l'aggiornamento degli stessi;

- conservare i codici di accesso al servizio con modalità idonee ad impedire tale accesso a terzi non autorizzati;
- informare le persone abilitate a utilizzare le caselle di posta sulle tematiche di sicurezza concernenti il loro uso;
- adottare misure atte ad evitare l'inserimento di codici eseguibili dannosi nei messaggi (virus);
- utilizzare, per accedere al servizio, la WebMail messa a disposizione dal Gestore o i client di posta da esso indicati;
- sollevare il Gestore da ogni responsabilità in merito ai contenuti dei messaggi;
- prestare, ove richiesto, il consenso al trattamento dei dati personali ai sensi del Reg. (UE) 679/2016 (Codice in materia di protezione dei dati personali), sue successive modifiche e integrazioni [8]. Si precisa che il mancato conferimento del consenso a Register circa il trattamento dei dati personali comporta l'impossibilità di erogare il servizio.
- assicurare un adeguato livello di sicurezza della propria strumentazione, in particolare attraverso la presenza di un antivirus costantemente aggiornato e l'aggiornamento dei software installati (per esempio attivando gli aggiornamenti e il patching automatico).
- Il Titolare è tenuto a custodire con la massima diligenza i token di accesso sicuro generati tramite area Selfcare ed a procedere tempestivamente alla loro revoca in caso di sospetta compromissione.

### 9.3 Indicazione dei livelli di servizio





Register garantisce agli utenti che usufruiscono del servizio PEC un servizio di invio messaggi in conformità con quanto previsto dall'articolo 12 comma 2 del Decreto Ministeriale 2 novembre 2005 – *“Regole Tecniche del servizio di trasmissione dei documenti informatici tramite Posta Elettronica Certificata”* e relativo allegato; sue successive note ed integrazioni [2]:

- Numero massimo di destinatari contemporanei accettati: 300;
- La Dimensione massima garantita di ogni singolo messaggio, ottenuta moltiplicando il numero dei destinatari per la dimensione del messaggio, è di 100MB (ad es. se l'email inviata ha dimensioni pari a 50 MB, il numero massimo dei destinatari è 2, poiché 50MB x 2 destinatari = 100MB). Nel caso in cui il prodotto così ottenuto superi il valore di soglia, il sistema non accetterà il messaggio notificando l'evento all'utente tramite il relativo messaggio di 'Avviso di

non accettazione'.

Rimane a cura del Titolare verificare che il *client di posta elettronica* (rif. § 1.3 del presente manuale operativo) utilizzato supporti l'invio di messaggi da 100MB.

Fare riferimento alla tabella sottostante.

Client di riferimento	Dimensione allegato	Esito	Note
Windows Live Mail	100MB		Non sono stati riscontrati problemi
Outlook 2010	100MB		Limite di Sistema del software a 20MB
Outlook 2013	100MB		Limite di Sistema del software a 20MB
Outlook 2007	100MB		Limite di Sistema del software a 20MB
Mozilla Thunderbird	100MB		Non sono stati riscontrati problemi

*Nota: La presente tabella è stata elaborata a puro titolo esemplificativo e senza pretesa di esaustività. Viene pubblicata al solo scopo di agevolare la comprensione dei limitazioni tecniche dei client di posta elettronica.*

Per una esperienza ottimale si consiglia come dimensione di ogni singolo messaggio: 20MB, compatibile con i maggiori programmi di posta e la *Webmail* (rif. § 1.3 del presente manuale operativo). E' cura del Titolare verificare sempre la ricezione della ricevuta di consegna, unico documento che garantisce la consegna al destinatario.

Limitazioni tecniche dei Browser impediscono l'invio e la lettura di messaggi (o di allegati) di dimensione superiori a 30MB tramite *Webmail*.

Prima di spedire un messaggio di dimensioni significative, è buona norma e responsabilità del Titolare verificare di avere spazio sufficiente per ricevere tutte le ricevute di consegna: se il messaggio viene inviato (in "TO (A)") a molti destinatari di posta elettronica certificata e la dimensione del messaggio è significativa si deve infatti considerare che ogni ricevuta di consegna ha in allegato tutto il messaggio inviato, a meno di disposizioni contrarie da parte del mittente. In caso di mancanza di spazio, le ricevute eccedenti la dimensione della casella non saranno recapitate.

Per il servizio PEC, Register garantisce la disponibilità 24 ore su 24, 7 giorni su 7, salvo i fermi per manutenzione programmata.

Nel periodo temporale di riferimento, che è pari ad un quadrimestre, il funzionamento del servizio è garantito per il 99.8%.

Ogni singolo evento di non disponibilità del servizio non supera il 50% del totale previsto nel periodo di tempo di riferimento suddetto.

Le ricevute destinate ai mittenti di messaggi PEC, durante il normale periodo di disponibilità del servizio, pervengono nei tempi previsti dalla normativa vigente [2].

Il servizio PEC descritto si riferisce ai sistemi di Register fino al collegamento ad Internet, escludendo quindi la rete esterna il cui servizio è di competenza del provider del Cliente.

#### 9.4 Limitazioni ed indennizzi

Il Gestore non può in alcun modo essere considerato destinatario di un obbligo di controllo, mediazione o vigilanza sui contenuti dei messaggi inviati.

Fermo restando quanto previsto dalla vigente normativa, Register non assume alcun obbligo riguardo la conservazione dei messaggi inviati e trasmessi attraverso le proprie caselle di PEC. Tale responsabilità viene assunta unicamente dal Titolare.

Il Gestore di posta elettronica certificata è responsabile dei danni causati, con dolo o colpa, a qualsiasi persona fisica o giuridica in seguito al mancato adempimento degli obblighi contrattuali e di quelli previsti dalla normativa vigente.

Fatti salvi i casi di mancato adempimento da parte di Register dei propri obblighi contrattuali o di quelli previsti dalla normativa vigente, contrassegnato da dolo o colpa, anche lieve, Register non assume alcuna responsabilità per i danni diretti o indiretti, di qualsiasi natura ed entità, che dovessero derivare al Titolare della casella, agli Utilizzatori e/o a terzi, in conseguenza di circostanze loro imputabili, quali – a titolo esemplificativo e non esaustivo – l'uso, il mancato uso e/o l'uso improprio o illecito del servizio di Posta Elettronica Certificata.

Allo stesso modo, Register non assume alcuna responsabilità circa la mancata esecuzione delle obbligazioni contrattuali assunte, qualora tale mancata esecuzione sia dovuta a cause ad essa non imputabili, quali – a titolo esemplificativo e non esaustivo – manomissioni o interventi sul servizio o sui dispositivi effettuati dal Titolare e/o dagli utilizzatori e/o da terzi non autorizzati da Register, eventi naturali, caso fortuito o forza maggiore e/o eventi comunque imputabili a terzi (quali – a titolo esemplificativo – guasti imputabili ai gestori di reti di telecomunicazione, agli altri Gestori di Posta Elettronica Certificata, scioperi, etc.).

Register non assume inoltre alcuna responsabilità per i danni diretti o indiretti, di qualsiasi natura ed entità, che dovessero derivare al Titolare della casella, agli Utilizzatori e/o a terzi, in conseguenza di errori o malfunzionamenti verificatisi nei periodi di indisponibilità del servizio indicati al precedente paragrafo 9.3, non sussistendo in relazione a detti periodi alcun inadempimento degli obblighi contrattuali assunti Register.

Eventuali contestazioni del Titolare relative all'erogazione del servizio dovranno pervenire al Gestore, a pena di decadenza, entro 30 giorni dalla data dell'evento mediante raccomandata a/r.

### 9.5 Polizza assicurativa

Register, nell'ambito della propria attività di Gestore di Posta Elettronica Certificata è dotato di polizza assicurativa a copertura dei rischi dell'attività e dei danni causati a terzi (art. 14 comma 6 lett. i del Decreto del Presidente della Repubblica 11 febbraio 2005, n. 68 – *“Regolamento recante disposizioni per l'utilizzo della posta elettronica certificata”* [4]) che ha come massimale:

- € 2.500.000 per singolo sinistro;
- € 5.000.000 per annualità.

### 9.6 Procedura prevista in caso di cessazione di erogazione del servizio PEC da parte di Register

In caso di cessazione dell'attività, Register provvederà a informare debitamente l'Agenzia per l'Italia Digitale con adeguato preavviso così come previsto dalla normativa vigente, nonché ad avvisare anticipatamente, almeno 60 giorni prima, i Titolari rispetto alla data prevista di effettiva cessazione. Lo stesso avviso di cessazione del servizio verrà diffuso tramite il sito internet di Register.

Register provvederà a sincronizzarsi con il nuovo Gestore che prenderà in carico i domini e le caselle PEC da questa precedentemente gestiti. In alternativa, i Titolari potranno chiedere a Register la disattivazione immediata della casella PEC (fare riferimento al paragrafo 7.4 del presente documento).

Qualora non venga indicato alcun Gestore alternativo, si provvederà ad avvisare sul sito internet e a comunicare espressamente ai Clienti che alla data di prevista cessazione il servizio verrà disattivato. Dopo la data di prevista cessazione del servizio il Titolare della casella avrà la facoltà di ricevere messaggi per ulteriori 30 giorni (senza la possibilità di invio) e, alla scadenza di questi, di visionare la propria casella per ulteriori 10 giorni.

Register provvederà altresì ad informare i Clienti circa le modalità di ottenimento del rimborso della parte di Servizio non usufruito a causa della cessazione dell'attività di Gestore di Posta Elettronica Certificata.

In ogni caso, Register, o una entità fidata opportunamente coinvolta, conserverà il registro dei log delle ricevute per un periodo di trenta mesi successivi alla data di cessazione delle attività, secondo le disposizioni di legge [2] che potranno essere richieste al Customer Care secondo le modalità previste.