ReeVo S.p.A.

MANUALE OPERATIVO
POSTA ELETTRONICA CERTIFICATA (PEC)

Manuale Operativo Servizio PEC
Versione: 11.2
Data aggiornamento: 2 novembre 2026
Approvato da: Davide Altea
Classificazione documento: pubblico

(Firmato Digitalmente)

DAVIDE
ALTEA
02.11.2026
16:27:11
GMT+01:00

STORICO REVISIONI

Revisione numero	Oggetto della revisione	Data
1.0	Prima emissione.	26.01.2006
1.1	Aggiornamento dei riferimenti per “Archiviazione Manuale; Aggiornamento del Responsabile del Manuale; Aggiornamento del Responsabile del Trattamento dei Dati”.	15.06.2006
1.2	Aggiornamento dei dati identificativi del Gestore (ex pgr.1. 2. 1).	31.07.2007
1.3	Revisione generale del Manuale Operativo.	11.07.2008
1.4	Aggiornamento modalità di vendita; Migliore descrizione delle attività formative sul personale.	06.03.2009
1.5	Aggiornamento dello strumento utilizzato per apporre le marche temporali ai log. Adeguamento alla circolare CNIPA/ CR/56 – Circolare CNIPA 21 maggio 2009, n. 56.	22.03.2010
1.6	Revisione annuale “Aggiornamento del Responsabile del Manuale”; Descrizione nuove funzionalità”; Aggiornamenti dovuti alla installazione di una nuova release del SW PEC.	28.02.2011
2.0	Aggiornamento dei dati identificativi del Gestore.	24.11.2011
2.1	Aggiornamento logo. “Aggiornamento dei dati identificativi del Gestore” – “Aggiornamento riferimenti per Privacy”.	28.02.2013
3.0	Aggiornamento Sede Legale. Aggiornamento elenco Data Center.	03.12.2013
4.0	Adeguamento alla circolare AgID sulla riassegnazione delle caselle PEC.	12.03.2014
4.1	Aggiornamento Canali di comunicazione con il Gestore.	14.04.2014
4.2	Aggiornamento Amministratore Delegato IT NET S.r.l. Aggiornamento dei dati identificativi del Gestore.	26.05.2014
5.0	Revisione annuale.	02.03.2015
5.1	Aggiornamento Amministratore Delegato IT NET S.r.l. Aggiornamento indirizzo Servizio Clienti.	10.06.2015
5.2	Aggiornamento della dimensione massima dei messaggi.	12.05.2016
6.0	Aggiornamento Amministratore Delegato IT NET S.r.l. Aggiornamento descrizione infrastruttura di esercizio PEC.	22.05.2017
6.1	Nuova infrastruttura per il Disaster Recovery del servizio PEC.	15.09.2017
7.0	Revisione annuale “Adeguamento alla nuova organizzazione aziendale” ; “Adeguamento alla versione 2015 della norma ISO 9001”.	14.03.2018
8.0	Revisione periodica “Adeguamento alla nuova organizzazione aziendale”; “Aggiornamento assunzione di responsabilità per danni causati da dolo o colpa del Gestore”.	31.01.2020
9.0	Revisione periodica “Adeguamento alla nuova organizzazione aziendale”.	30.09.2022
10.0	Revisione periodica.	28.12.2023
11.0	Revisione in seguito a Fusione per Incorporazione di IT NET S.r.l. in ReeVo S.p.A. Aggiornamento URL portale di ticketing.	01.06.2025
11.1	Revisione periodica e Adeguamento alla nuova organizzazione aziendale.	14.11.2025
11.2	Revisione periodica. Aggiornamento organizzazione. Aggiornamento riferimento portale di ticketing e inserimento Manuale Utente.	02.11.2026

Sommario

1 Introduzione....5
1.1 Generalità del documento e dati identificativi del Gestore....5
1.2 Scopo e campo di applicazione....5
1.3 Identificazione del documento e gestione delle modifiche....6
1.4 Responsabile del manuale e canali di comunicazione....6
1.5 Definizioni, abbreviazioni e acronimi....6
1.5.1 Definizioni....6
1.5.2 Abbreviazioni e acronimi....9
1.6 Riferimenti Normativi....10
1.7 Tabella di corrispondenza....12
1.7.1 Generalità del gestore....12
1.7.2 Canali di comunicazione con il Gestore....12
1.7.3 Accessi sito Web del Gestore....13
1.8 Standard di sicurezza, qualità e tecnologici....13
1.8.1 Standard di sicurezza, qualità....13
1.8.2 Standard tecnologici....13
2 Generalità – Servizio Posta Elettronica Certificata....15
2.1 Funzionamento del servizio....15
2.2 Funzionamento del servizio - problemi di consegna....16
2.2.1 Descrizione del funzionamento in caso di messaggi non consegnati....17
2.2.2 Descrizione del servizio in presenza di virus....17
2.3 Caratteristiche delle ricevute e delle buste di trasporto....17
2.3.1 Firma elettronica delle ricevute e delle buste di trasporto....17
2.3.2 Riferimento temporale....17
2.3.3 Tipologia delle Ricevute di avvenuta consegna....18
3 Servizio Posta Elettronica Certificata ReeVo S.p.A....19
3.1 Tipologia del servizio offerto....19
3.1.1 Profilo base....19
3.1.2 Profilo Plus....19
3.1.3 Profilo offerta Multidominio....20
3.1.4 Gestione dei domini di Posta Elettronica Certificata....21
3.2 Accesso al servizio....21
3.2.1 Interfaccia Web....22
3.2.2 Client di Posta Elettronica....22
3.2.3 Credenziali di accesso e parametri configurazione del servizio....23
3.2.4 Raccomandazioni gestione utenza....23
3.2.5 Adeguamento del servizio PEC ai nuovi standard europei....23
4 Livelli di servizio – Indicatori di qualità....24
5 Condizioni di fornitura....25
5.1 Canali di vendita, proposta e documentazione del servizio....25
5.1.1 Attivazione diretta del servizio....25
5.1.2 Attivazione del servizio tramite Rivenditore (Reseller)....25
5.1.3 Attivazione del servizio tramite Rivenditore (Reseller) - Offerta Multidominio....25
5.1.4 Modalità alternative per l'attivazione del servizio....28
5.2 Attivazione del servizio....28
5.2.1 Gestione aggiornamento informazioni - Titolari - Caselle PEC....28
5.3 Disdetta del contratto....28
5.4 Corrispettivo economico....29
5.5 Descrizione generale degli elementi del contratto....29
5.6 Obblighi e responsabilità....29
5.6.1 Obblighi del Gestore....29
5.6.2 Obblighi del Titolare del Servizio....30

6 Sistemi Tecnologici....32
6.1 Infrastruttura, Affidabilità, Sicurezza, Scalabilità, Connettività....32
6.2 Data Center – caratteristiche principali....35
6.2.1 Caratteristiche comuni in uso tra i Data Center....35
6.2.2 Sito di Siziano (Stack EMEA)....35
6.2.3 Sito di Roma....36
6.3 Precisione del riferimento temporale....36
6.4 Gestione dei log dei messaggi....37
6.4.1 Gestione dei log Servizio di Posta Elettronica Certificata....37
6.4.2 Diritto alla portabilità dei dati....37
6.4.3 Archiviazione e Conservazione....37
6.4.4 Reperimento e presentazione log....38
7 Interoperabilità tra gestori....40
8 Misure di sicurezza, monitoraggio, continuità del servizio....41
8.1 Organizzazione del personale....41
8.2 Approccio organizzativo....41
8.3 Approccio tecnologico....42
8.3.1 Firma....42
8.3.2 Autenticazione....42
8.3.3 Colloquio sicuro....43
8.3.4 Sistema Antivirus e Antispam....43
8.3.5 Data Center - Standard di Sicurezza....43
8.3.6 Back up dei dati....43
8.3.7 Monitoraggio....44
8.3.8 Gestione delle emergenze....44
9 Piano di cessazione....46
10 Protezione dati personali....47
10.1 Informativa....47
10.2 Procedura di riferimento....48
10.3 Misure di sicurezza per la protezione dei dati personali....49
10.3.1 Trasmissione e accesso ai dati da parte dell'utente....50
10.3.2 Misure di sicurezza per la protezione dei dati....50

1 Introduzione

1.1 Generalità del documento e dati identificativi del Gestore

ReeVo S.p.A. è il Gestore del Servizio di Posta Elettronica Certificata (PEC), qualificato ai sensi dell'art. 29 del Decreto Legislativo 7 marzo 2005, n. 82 e successive modificazioni e integrazioni (Codice dell'Amministrazione Digitale – CAD), e iscritto nell'elenco dei gestori PEC pubblicato dall'Agenzia per l'Italia Digitale (AgID). Il servizio è disciplinato dal Decreto del Presidente della Repubblica 11 febbraio 2005, n. 68, e dal Decreto del Ministro per l'Innovazione e le Tecnologie 2 novembre 2005, recante «Regole tecniche per la formazione, la trasmissione e la validazione, anche temporale, della posta elettronica certificata», nonché dalle ulteriori disposizioni normative e tecniche applicabili.

Il Gestore garantisce l'erogazione del servizio nel rispetto dei requisiti tecnici, organizzativi e di sicurezza previsti dalla normativa e dalle disposizioni applicabili in materia di PEC, assicurando in particolare la disponibilità, l'integrità, l'autenticità e la tracciabilità delle comunicazioni gestite attraverso il servizio.

Nell'ambito dell'erogazione del servizio, il Gestore assicura le funzionalità necessarie a garantire la corretta trasmissione dei messaggi PEC, nonché la produzione e la conservazione delle ricevute e delle evidenze associate alle operazioni effettuate. Tali evidenze consentono di attestare, secondo le modalità previste dalla normativa, l'invio, la consegna e gli eventuali esiti della trasmissione dei messaggi.

Il Gestore adotta inoltre adeguate misure tecniche e organizzative volte a garantire la continuità operativa del servizio, la protezione dei dati trattati e la sicurezza delle infrastrutture e dei sistemi utilizzati per l'erogazione della PEC.

L'erogazione del servizio è effettuata secondo procedure documentate e sottoposte a periodiche attività di controllo, aggiornamento e verifica, in coerenza con i requisiti previsti dalla normativa vigente e con le disposizioni emanate dalle Autorità competenti.

Dati identificativi del gestore	
Ragione Sociale	ReeVo S.p.A.
Sede Legale	Foro Buonaparte, 57 20121 Milano (MI) - Italia
Partita IVA	03888200965
Iscrizione registro delle Imprese	03888200965
REA	1710741
Capitale Sociale	€ 1.122.816,00
Siti Web	www.reevo.it
E-mail	info@reevo.it

1.2 Scopo e campo di applicazione

Il presente documento è stato redatto con l'obiettivo di descrivere le caratteristiche, le modalità operative e le procedure adottate dal Gestore ReeVo S.p.A. per l'erogazione del Servizio di Posta Elettronica Certificata (PEC).

Il manuale contiene, oltre alle informazioni di carattere generale, tutte le indicazioni necessarie a fornire una descrizione completa del servizio di Posta Elettronica Certificata offerto dal Gestore.

Il documento tiene, inoltre, conto degli adeguamenti organizzativi e operativi intervenuti a seguito della fusione per incorporazione di IT NET S.r.l., avvenuta nel mese di dicembre 2024, disciplinando,

per quanto di competenza, le modalità di erogazione del servizio nell'attuale configurazione societaria.

1.3 Identificazione del documento e gestione delle modifiche

Denominazione documento: Manuale Operativo - Posta Elettronica Certificata.

Versione numero 11.2.

ReeVo S.p.A. è responsabile della definizione, pubblicazione e aggiornamento del documento.

Il Manuale Operativo è pubblicato sul sito Web del gestore ed è scaricabile e consultabile su: https://www.reevo.it/it/manuale-operativo-servizio-pec.

ReeVo S.p.A. garantisce che la versione pubblicata sul sito è l'ultima aggiornata.

Il Manuale Operativo è articolato in 10 (dieci) capitoli, ciascuno dei quali tratta tematiche specifiche e chiaramente definite, al fine di consentire all'Utente un agevole orientamento e una rapida consultazione del documento.

Eventuali modifiche al presente documento, tali da comportare l'emissione di una nuova versione, saranno sottoposte a un apposito ciclo di validazione interna, comprendente le fasi di verifica e approvazione, e saranno comunicate, ove previsto, agli organi competenti, tra cui l'Agenzia per l'Italia Digitale (AgID).

Gli aggiornamenti terranno conto delle modifiche intervenute nel quadro normativo e regolamentare di riferimento sul quale si basa il presente Manuale Operativo.

Tali modifiche potranno intervenire a fronte di ottimizzazioni procedurali, evoluzioni dell'offerta o anche per esigenze tecniche.

ReeVo S.p.A. si impegna ad effettuare un controllo con cadenza annuale sui contenuti del documento al fine di garantire la coerenza e l'aggiornamento dello stesso.

1.4 Responsabile del manuale e canali di comunicazione

Il responsabile del presente Manuale Operativo individuato da ReeVo S.p.A. è Davide Altea, a cui ogni utente può rivolgersi per informazioni, domande e chiarimenti riguardanti il presente manuale, contattandolo ai seguenti recapiti:

Ruolo: Resp. del manuale operativo e del sistema di riferimento temporale ReeVo S.p.A.

Davide Altea

E-mail: Davide.Altea@reevo.it

Telefono: (+39) 039 2873925

Sede: Via Energy Park, 22 (Ed 4) - 20871 Vimercate (MB)

1.5 Definizioni, abbreviazioni e acronimi

1.5.1 Definizioni

Di seguito si riportano le definizioni dei termini utilizzati nel presente Manuale Operativo

Definizione	Descrizione
Avviso di mancata consegna	L'avviso, emesso dal sistema, per indicare l'anomalia al mittente del messaggio originale, nel caso in cui il gestore di Posta Elettronica Certificata sia impossibilitato a consegnare il messaggio nella casella di Posta Elettronica Certificata del destinatario.

Definizione	Descrizione
Avviso di non accettazione	L'avviso sottoscritto con la firma del gestore di Posta Elettronica Certificata del mittente, che viene emesso quando il gestore del mittente è impossibilitato ad accettare il messaggio in ingresso, recante le motivazioni per cui non è possibile accettare il messaggio e l'esplicitazione che il messaggio non potrà essere consegnato al destinatario.
Busta di anomalia	La busta sottoscritta con la firma del gestore di Posta Elettronica Certificata del destinatario nella quale è inserito un messaggio errato ovvero non di Posta Elettronica Certificata e consegnata ad un titolare per evidenziare al destinatario detta anomalia.
Busta di trasporto	La busta creata dal punto di accesso e sottoscritta con la firma del gestore di Posta Elettronica Certificata del mittente, all'interno della quale sono inseriti i messaggi originali inviati dal Titolare di Posta Elettronica.
Casella di Posta Elettronica Certificata	È una casella di posta elettronica all'interno di un dominio di Posta Elettronica Certificata alla quale è associata una funzione che rilascia delle ricevute di avvenuta consegna al ricevimento di messaggi di Posta Elettronica Certificata.
Data Center	I Data Center utilizzati da ReeVo S.p.A. sono dislocati a Roma (RM) e Siziano (PV). Il servizio di Posta Elettronica Certificata è erogato dal Data Center di Siziano.
Dati di certificazione	I dati, quali ad esempio data e 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 varie ricevute e sono trasferiti al titolare destinatario insieme al messaggio originale per mezzo di una busta di trasporto.
Destinatario	Utente che si avvale del servizio di Posta Elettronica Certificata per la ricezione dei documenti prodotti mediante strumenti informatici.
Dominio di Posta Elettronica Certificata	Dominio di Posta Elettronica Certificata che contiene unicamente caselle di Posta Elettronica Certificata.
Firma del Gestore di Posta Elettronica Certificata	La firma elettronica avanzata, basata su un sistema di chiavi asimmetriche, che consente di rendere manifesta la provenienza e di assicurare l'integrità e l'autenticità dei messaggi del sistema di Posta Elettronica Certificata, generata attraverso una procedura informatica che garantisce la connessione univoca al gestore e la sua univoca identificazione, creata automaticamente con mezzi che garantiscono il controllo esclusivo da parte del Gestore.
Firma digitale	Particolare tipo di firma elettronica qualificata basata 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 pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici, ai sensi dell'art. 1, comma 1, lett. s), del Decreto Legislativo 7 marzo 2005, n. 82 (Codice dell'Amministrazione Digitale).
Firma Elettronica (categoria generale)	Dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati elettronici e utilizzati dal firmatario per firmare, ai sensi dell'art. 3, punto 10, del Regolamento (UE) n. 910/2014 (eIDAS).
Firma Elettronica qualificata (FEQ)	Firma elettronica avanzata basata su un certificato qualificato e creata mediante un dispositivo qualificato per la creazione della firma, avente valore giuridico equivalente alla firma autografa nei casi previsti dalla normativa vigente.
Firma Elettronica avanzata (FEA)	Firma elettronica che soddisfa i seguenti requisiti: è connessa unicamente al firmatario; è idonea a identificare il firmatario; è creata mediante dati per la creazione di una firma elettronica che il firmatario può, con un elevato livello di sicurezza, utilizzare sotto il proprio esclusivo controllo; è collegata ai dati sottoscritti in modo da consentire l'identificazione di ogni successiva modifica di tali dati, ai sensi dell'art. 26 del Regolamento (UE) n. 910/2014 (eIDAS).
Gestore di Posta Elettronica Certificata	È il soggetto che gestisce uno o più domini di Posta Elettronica Certificata con i relativi punti di accesso, di ricezione e di consegna. È titolare della chiave usata per la firma delle ricevute e delle buste nel rispetto della normativa vigente. Si interfaccia con altri gestori di Posta Elettronica Certificata per l'interoperabilità con altri titolari.

Definizione	Descrizione
Gestore mittente	Soggetto che, tramite il servizio PEC, gestisce e trasmette messaggi di posta elettronica certificata per conto del mittente, garantendone la corretta gestione e trasmissione secondo la normativa vigente.
Gestore destinatario	Soggetto che gestisce la casella PEC del destinatario e provvede alla ricezione e alla consegna del messaggio di posta elettronica certificata, secondo quanto previsto dalla normativa vigente.
Indice dei Gestori di Posta Elettronica Certificata (INI PEC)	Sistema che contiene l'elenco dei domini e dei Gestori di Posta Elettronica Certificata, nonché i relativi certificati corrispondenti alle chiavi utilizzate per la firma delle ricevute, degli avvisi e delle buste di trasporto. L'Indice costituisce la struttura tecnica di riferimento per l'interoperabilità tra i Gestori PEC.
Rivenditore (Reseller)	Soggetto che, sulla base di uno specifico accordo con il Gestore di Posta Elettronica Certificata, provvede alla commercializzazione e alla distribuzione del Servizio PEC per conto del Gestore. Il Rivenditore può integrare il Servizio PEC con servizi aggiuntivi propri, fermo restando che l'erogazione del servizio PEC e le relative responsabilità previste dalla normativa rimangono in capo al Gestore qualificato. Le modalità di commercializzazione, registrazione e gestione delle utenze tramite il Rivenditore sono disciplinate dal Gestore nel proprio Manuale Operativo.
Log dei messaggi	Registro informatico delle operazioni relative alle trasmissioni effettuate mediante la Posta Elettronica Certificata tenuto e monitorato dal Gestore.
Marca Temporale	Evidenza informatica con cui si attribuisce a uno o più documenti informatici un riferimento temporale opponibile ai terzi, secondo quanto previsto dalla normativa vigente, anche in conformità alle disposizioni del Regolamento (UE) n. 910/2014 (eIDAS) in materia di validazione temporale elettronica e validazione temporale elettronica qualificata.
Messaggio di Posta Elettronica Certificata	È un documento informatico composto dal testo del messaggio, dai dati di certificazione e dagli eventuali documenti informatici allegati.
Messaggio originale	È il messaggio inviato da un Utente di Posta Elettronica Certificata prima del suo arrivo al punto di accesso e consegnato al titolare destinatario per mezzo di una busta di trasporto che lo contiene.
Mittente	Utente che si avvale del Servizio di Posta Elettronica Certificata per l'invio di documenti prodotti mediante strumenti informatici.
Posta elettronica Certificata (PEC)	Ogni sistema di posta elettronica nel quale è fornita al mittente documentazione elettronica attestante l'invio e la consegna di documenti informatici, ai sensi dell'art. 1, comma 1, lett. g), del Decreto del Presidente della Repubblica 11 febbraio 2005, n. 68.
Punto di accesso	Il sistema che fornisce i servizi di accesso per l'invio e la lettura di messaggi di Posta Elettronica Certificata, nonché i servizi di identificazione ed accesso dell'Utente, di verifica della presenza di un virus informatico all'interno del messaggio, di emissione della ricevuta di accettazione e di imbustamento del messaggio originale nella busta di trasporto.
Punto di consegna	Il sistema che esegue la consegna del messaggio nella casella di Posta Elettronica Certificata del destinatario titolare e 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.
Punto di ricezione	Il sistema che riceve il messaggio all'interno di un dominio di Posta Elettronica Certificata effettua controlli sulla provenienza e sulla correttezza del messaggio ed emette la ricevuta di presa in carico, imbusta i messaggi errati in una busta di anomalia e verifica la presenza di virus informatici all'interno dei messaggi di posta ordinaria e della busta di trasporto.
REM / Registered Electronic Mail	Servizio di recapito elettronico qualificato che consente l'invio e la ricezione di comunicazioni elettroniche con garanzie di identificazione del mittente e del destinatario, integrità dei dati, prova dell'invio e della consegna.
Ricevuta breve di avvenuta consegna	La ricevuta nella quale sono contenuti i dati di certificazione ed un estratto del messaggio originale.
Ricevuta completa di avvenuta consegna	La ricevuta nella quale sono contenuti i dati di certificazione ed il messaggio originale.

Definizione	Descrizione
Ricevuta di accettazione	La ricevuta, sottoscritta con la firma del gestore di Posta Elettronica Certificata del mittente, contenente i dati di certificazione rilasciata al mittente dal punto di accesso a fronte dell'invio di un messaggio di Posta Elettronica Certificata.
Ricevuta di avvenuta consegna	La ricevuta sottoscritta con la firma del gestore di Posta Elettronica Certificata del destinatario, emessa dal punto di consegna al mittente nel momento in cui il messaggio è inserito nella casella di Posta Elettronica Certificata del destinatario.
Ricevuta di presa in carico	La ricevuta sottoscritta con la firma del gestore di Posta Elettronica Certificata del destinatario emessa dal punto di ricezione nei confronti del gestore di Posta Elettronica Certificata del mittente per attestare l'avvenuta presa in carico del messaggio da parte del sistema di Posta Elettronica Certificata del destinatario recante i dati di certificazione per consentirne l'associazione con il messaggio a cui si riferisce.
Ricevuta sintetica di avvenuta consegna	La ricevuta che contiene i dati di certificazione.
Servizio elettronico di recapito certificato (SERC)	Servizio che consente la trasmissione elettronica di dati tra terzi, fornendo garanzie di integrità dei dati, identificazione del mittente e del destinatario e prova della corretta trasmissione e ricezione.
Servizio elettronico di recapito certificato qualificato (SERCQ)	Servizio elettronico di recapito certificato che soddisfa i requisiti previsti dalla normativa europea e che è erogato da un prestatore di servizi fiduciari qualificato, garantendo l'identificazione delle parti, l'integrità dei dati e la prova dell'invio e della consegna.
Titolare della casella PEC	Il soggetto a cui sono assegnate una o più Caselle di Posta Elettronica Certificata. All'interno del presente documento si identifica come Titolare il soggetto al quale viene erogato il servizio di PEC.
Titolare del trattamento dei dati	La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento dei dati personali e assicura il rispetto degli obblighi previsti dalla normativa applicabile in materia di protezione dei dati personali, ai sensi dell'art. 4, punto 7, del Regolamento (UE) 2016/679 (GDPR).
Utente di Posta Elettronica Certificata	La persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi ente, associazione o organismo, nonché eventuali unità organizzative interne, che sia mittente o destinatario di Posta Elettronica Certificata.
Virus Informatico	Un programma informatico avente per scopo o per effetto il danneggiamento di un sistema informatico o telematico, dei dati e dei programmi in esso contenuti o ad esso pertinenti, ovvero l'interruzione, totale o parziale o l'alterazione del suo funzionamento.

1.5.2 Abbreviazioni e acronimi

Di seguito si riportano le abbreviazioni e gli acronimi utilizzati nel presente Manuale Operativo.

Abbreviazioni	Significato
ACN	Agenzia per la Cybersicurezza Nazionale
AgID	Agenzia per l'Italia Digitale: istituita con D.L. 22 giugno 2012, n.83, convertito nella legge del 7 agosto 2012, n. 134.
AHU	Air Handling Unit (Unità Trattamento Aria – UTA)
CAD	Codice dell'Amministrazione digitale (Decreto Legislativo 7 marzo 2005 n. 82)
CMS	Cryptographic Message Syntax
CNIPA	Centro Nazionale per l'Informatica nella Pubblica Amministrazione
CRL	Certificate Revocation List
CRL DP	Certificate Revocation List Distribution Point
DigitPA	A decorrere dal 29 dicembre 2009 a seguito del decreto del 1° dicembre 2009, n. 177 il CNIPA viene riordinato con nuova denominazione DigitPA
DNS	Domain Name System
DPR	Decreto del Presidente della Repubblica

Abbreviazioni	Significato
eIDAS 2.0	Electronic, IDentification, Authentication and trust Services
ETSI	European Telecommunications Standards Institute
FEA	Firma Elettronica Avanzata
FEQ	Firma Elettronica Qualificata
FQDN	Fully Qualified Domain Name
GDPR	*General Data Protection Regulation* - Regolamento generale per la Protezione dei Dati
HSM	Hardware Security Module – modulo HW per la Sicurezza
HTTPS	HyperText Transfer Protocol Secure
INI PEC	Indice Nazionale degli Indirizzi di Posta Elettronica Certificata
IMAP	Internet Message Access Protocol
INRiM	Istituto Nazionale di Ricerca Metrologica
LDAP	Lightweight Directory Access Protocol
LDIF	LDAP Data Interchange Format
MFA	Multi Factor Authentication
MIME	Multipurpose Internet Mail Extensions
NTP	Network Time Protocol
PEC	Posta Elettronica Certificata
PDU	Power Distribution Unit
POP3	Post Office Protocol version 3
PUE	Power Usage Effectiveness – Indice di efficienza energetica
REM	Registered Electronic Mail
RFC	Request for Comments
RPP	Remote Power Panels
RSA	Rivest–Shamir–Adleman
SAN	Storage Area Network
SERC	Servizio Elettronico di Recapito Certificato
S/MIME	Secure/MIME
SMTP	Simple Mail Transfer Protocol
TLS	Transport Layer Security
TSA	Time Stamping Authority
UPS	Uninterruptible Power System – Gruppi di continuità
UTC	Coordinated Universal Time
XML	eXtensible Markup Language
VA/PT	Vulnerability Assessment / Penetration Test

1.6 Riferimenti Normativi

Il presente Manuale Operativo è redatto in conformità alla normativa nazionale ed europea applicabile al servizio di Posta Elettronica Certificata (PEC), alle relative regole tecniche e alle disposizioni emanate dall'Agenzia per l'Italia Digitale (AgID).

- **Normativa nazionale**

[1] Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 e successive modificazioni e integrazioni – Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa, per gli aspetti applicabili alla formazione, trasmissione e validità dei documenti informatici.

[2] Decreto Legislativo 30 giugno 2003, n. 196 e successive modificazioni e integrazioni – Codice in materia di protezione dei dati personali, coordinato con il Regolamento (UE) 2016/679.

[3] Decreto Legislativo 7 marzo 2005, n. 82 e successive modificazioni e integrazioni – Codice dell'Amministrazione Digitale (CAD).

[4] 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, e successive modificazioni e integrazioni.

[5] Decreto del Ministro per l'innovazione e le tecnologie 2 novembre 2005 – Regole tecniche per la formazione, la trasmissione e la validazione, anche temporale, della posta elettronica certificata, e successive modificazioni e integrazioni.

[6] Decreto-legge 29 novembre 2008, n. 185, convertito, con modificazioni, dalla Legge 28 gennaio 2009, n. 2, e successive modificazioni e integrazioni, per le disposizioni applicabili alla Posta Elettronica Certificata e al domicilio digitale.

- **Normativa europea**

[7] Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 (General Data Protection Regulation – GDPR) – relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali e alla libera circolazione di tali dati.

[8] Regolamento (UE) n. 910/2014 del Parlamento Europeo e del Consiglio del 23 luglio 2014 (Regolamento eIDAS) – in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno, per quanto applicabile al servizio.

[9] Regolamento (UE) 2024/1183 del Parlamento Europeo e del Consiglio dell'11 aprile 2024, recante modifica del Regolamento (UE) n. 910/2014 per quanto riguarda l'istituzione del quadro europeo relativo a un'identità digitale (eIDAS 2.0), per gli aspetti applicabili ai servizi di recapito elettronico certificato e alla relativa evoluzione verso i servizi qualificati.

- **Regole tecniche e disposizioni AgID**

[10] Agenzia per l'Italia Digitale (AgID) – Regole tecniche per la Posta Elettronica Certificata, costituite dal Decreto del Ministro per l'innovazione e le tecnologie 2 novembre 2005 e dai relativi allegati tecnici, nonché dalle successive disposizioni e indicazioni AgID applicabili al servizio.

[11] Agenzia per l'Italia Digitale (AgID) – Linee guida per la vigilanza sui gestori di Posta Elettronica Certificata, per quanto applicabili alle attività del Gestore.

[12] Agenzia per l'Italia Digitale (AgID) – disposizioni, comunicazioni tecniche, specifiche operative, note operative e ulteriori provvedimenti applicabili ai gestori PEC pubblicati dall'Agenzia nel corso di validità del presente Manuale Operativo.

[13] Agenzia per l'Italia Digitale (AgID) – REM SERVICES – Criteri di adozione degli standard ETSI – Policy IT (REM-Policy-IT), versione 2.0, per gli aspetti applicabili all'eventuale erogazione o evoluzione del servizio verso servizi elettronici di recapito certificato qualificato.

[14] Agenzia per l'Italia Digitale (AgID) – Determinazione n. 233 del 9 agosto 2022 – Adozione delle Regole tecniche per i servizi di recapito certificato a norma del Regolamento eIDAS n. 910/2014 – Criteri di adozione standard ETSI – REM-Policy-IT, nella versione e nei limiti di applicabilità al servizio.

- Standard tecnici ETSI

[15] Standard tecnici ETSI e IETF espressamente richiamati dalle regole tecniche PEC, dalla REM-Policy-IT e dalle disposizioni AgID applicabili al servizio, nelle versioni applicabili alla specifica implementazione del Gestore.

- **Ulteriori riferimenti**

[16] Eventuali ulteriori disposizioni normative, regolamentari, tecniche e di vigilanza emanate dalle competenti Autorità nazionali ed europee successivamente alla pubblicazione o all'aggiornamento del presente Manuale Operativo, ove applicabili al servizio.

1.7 Tabella di corrispondenza

1.7.1 Generalità del gestore

Contenuto della Circolare CNIPA/CR/56 e successive modifiche e integrazioni (AgID.gov.it/it/piattaforme/posta-elettronica-certificata)	Inserimento nel Manuale Operativo
Dati identificativi del gestore	ReeVo S.p.A.
Nominativo del responsabile del Manuale operativo	Davide Altea
Indirizzo del sito Web del gestore ove è pubblicato e scaricabile	https://www.reevo.it
Indicazione delle procedure nonché degli standard tecnologici e di sicurezza utilizzati dal gestore nell'erogazione del servizio	Secondo linee guida Regolamento ACN / REM/ eIDAS 2.0
Le definizioni relative alle abbreviazioni e ai termini tecnici che figurano nel manuale	Responsabile: Cap.1.1 Sito: Capp. 1.3 e 1.7.3 Standard: Cap. 1.8 Definizioni: Cap. 1.5
Descrizione del servizio offerto	Capp. 2 e 3
Descrizione delle modalità di reperimento e di presentazione dei log dei messaggi	Cap 6.4.4
Indicazione modalità di accesso e fornitura del servizio	Capp. 3.2 e 5
Livelli di servizio e relativi indicatori di qualità di cui all'articolo 12 del Decreto del Ministro per l'innovazione e le tecnologie 2 novembre 2005	Cap. 4
Indicazione delle modalità di protezione dei dati dei Titolari delle caselle, gli obblighi e delle responsabilità che ne discendono e le eventuali limitazioni in caso di indennizzo relativamente ai soggetti previsti all'articolo 2 del Decreto del Presidente della Repubblica n. 68/2005	Capp. 5.6 e 10
Procedure operative da attuare nel caso di cessazione dell'attività di posta elettronica certificata	Cap..9

1.7.2 Canali di comunicazione con il Gestore

I seguenti canali, attraverso cui è possibile effettuare segnalazioni di natura tecnica o amministrativa 24 ore su 24, 365 giorni all'anno, sono disponibili sia per i Titolari delle caselle PEC sia per i partner commerciali:

- Per aprire una segnalazione, il Titolare o il Reseller può accedere al portale ticketing disponibile all' indirizzo helpdesk.reevo.eu, autenticarsi mediante username e password e compilare l'apposito form indicando la natura della problematica riscontrata.

  In alternativa, è possibile inviare la segnalazione all'indirizzo di posta elettronica servicedesk@reevo.it.
- Per le istruzioni relative all'utilizzo del portale ticketing helpdesk.reevo.eu, si rimanda al Manuale Utente HALO.
- Casella di posta elettronica certificata: reevo@pec.it per comunicazioni ufficiali (disdetta, modifica dati, …).

- Casella di posta elettronica certificata: richiestalog.pec@pec.reevo.it - eventuali richieste di log devono essere inviate dal Titolare tramite casella di Posta elettronica Certificata o Raccomandata A/R (su carta intestata debitamente firmata e allegando copia di un documento di riconoscimento) come indicato nel paragrafo 6.4.4 del presente manuale.
- Raccomandata A/R ReeVo S.p.A. Via Energy Park 22, Ed. 4 –20871 Vimercate Milano (MI)

1.7.3 Accessi sito Web del Gestore

Il sito https://www.reevo.it è il sito istituzionale di ReeVo S.p.A. attraverso il quale è possibile:

- consultare le informazioni relative al Gestore;
- prendere visione della sezione dedicata al servizio di Posta Elettronica Certificata;
- scaricare copia elettronica del presente Manuale Operativo.

1.8 Standard di sicurezza, qualità e tecnologici

1.8.1 Standard di sicurezza, qualità

ReeVo S.p.A. garantisce l'adeguatezza dei propri principali processi operativi e la corretta gestione delle informazioni circolanti in azienda, facendo riferimento agli standard ISO 9001 (per cui è certificata dal 2004) e allo standard ISO 27001 (certificazione ottenuta nel 2007, che ha sostituito la BS 7799 ottenuta nel 2005).

Gli standard, relativi alla qualità e alla sicurezza, cui l'azienda fa riferimento sono: UNI EN ISO 9001:2015 Sistemi di gestione per la qualità.

UNI ISO/IEC 27001:2022

UNI CEI EN ISO/IEC 27001:2024;

UNI ISO/IEC 27017:2015;

UNI ISO/IEC 27018:2019;

ISO/IEC 20000-1:2018;

ISO/IEC 27001-ISMS Requirements.

I certificati sono pubblicati sul sito aziendale https://www.reevo.it.

Tutta la documentazione operativa e di sistema è distribuita al personale ReeVo S.p.A. e pubblicata sulla intranet aziendale.

Nel presente manuale sono esplicitati alcuni processi relativi alla gestione operativa del servizio di Posta Elettronica Certificata e laddove necessario sono fatti espliciti riferimenti alle procedure interne.

1.8.2 Standard tecnologici

In relazione ai processi e alle applicazioni individuati nell'Allegato tecnico al Decreto del Ministro per l'innovazione e le tecnologie 2 novembre 2005 [5], il servizio di Posta Elettronica Certificata di ReeVo S.p.A. è conforme agli standard tecnologici di riferimento riportati nella tabella seguente.

Codice	Titolo
RFC 1847	Security Multiparts for MIME: Multipart/Signed and Multipart/Encrypted
RFC 1891	SMTP Service Extension for Delivery Status Notifications
RFC 1912	Common DNS Operational and Configuration Errors
RFC 2045	Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies
RFC 2049	Multipurpose Internet Mail Extensions (MIME) Part Five: Conformance Criteria and Examples

Codice	Titolo
RFC 2252	Lightweight Directory Access Protocol (v3): Attribute Syntax Definitions
RFC 2315	PKCS #7: Cryptographic Message Syntax Version 1.5
RFC 2633	S/MIME Version 3 Message Specification
RFC 2660	The Secure HyperText Transfer Protocol
RFC 2821	Simple Mail Transfer Protocol
RFC 2822	Internet Message Format
RFC 2849	The LDAP Data Interchange Format (LDIF) - Technical Specification
RFC 3207	SMTP Service Extension for Secure SMTP over Transport Layer Security
RFC 3280	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
RFC 6234	US Secure Hash Algorithms (SHA and SHA-based HMAC and HKDF)

2 Generalità – Servizio Posta Elettronica Certificata

Il servizio di Posta Elettronica Certificata (PEC) è la modalità di utilizzo della posta elettronica che consente al mittente di ottenere evidenza dell'invio e della consegna del messaggio e della relativa documentazione informatica quando la trasmissione avviene tra caselle di posta elettronica certificata, secondo le modalità previste dalla normativa vigente.

2.1 Funzionamento del servizio

Di seguito sono riportate le fasi previste per l'utilizzo dell'applicazione tra utenti di posta certificata:

Il mittente invia un messaggio attraverso il servizio di Posta Elettronica Certificata. Il server di posta certificata del mittente (Punto di Accesso) esegue i controlli formali previsti e prosegue:

- inviando al mittente una ricevuta di accettazione, con la quale conferma al mittente che il suo messaggio è stato accettato dal sistema, riportando data e ora specifiche. La ricevuta di accettazione è un messaggio di posta elettronica firmato dal gestore del mittente nel quale sono riportati data ed ora di accettazione, l'oggetto ed i dati del mittente e del destinatario;
- imbustando il messaggio originale in un messaggio di trasporto (Busta di trasporto) di tipo "S/MIME". Il messaggio di trasporto firmato dal gestore del mittente è un messaggio che contiene, come allegato, il messaggio originale e tutti i dati che ne certificano il trasporto;
- inviando il messaggio di trasporto al dominio destinatario (Punto di ricezione).

La trasmissione avviene sia tra caselle PEC associate allo stesso dominio sia tra caselle PEC associate a domini differenti.

Il messaggio è poi ricevuto dal punto di ricezione che esegue i controlli sulla provenienza e la correttezza del messaggio.

In particolare, viene verificata l'esistenza e la validità della firma del gestore che ha consegnato il messaggio del mittente.

Se le verifiche sono positive il punto di ricezione emette una ricevuta di presa in carico verso il gestore mittente e provvede all'inoltro del messaggio ricevuto verso il punto di consegna.

A seguito della consegna del messaggio di trasporto al destinatario (Punto di consegna), il server di Posta Certificata emette e invia al mittente una ricevuta di avvenuta consegna, attestante l'effettiva consegna del messaggio al destinatario indicato e certificante la data e l'ora dell'evento.

La ricevuta di avvenuta consegna è emessa contestualmente alla disponibilità del messaggio nella casella di posta elettronica del destinatario, indipendentemente dalla successiva lettura del messaggio da parte del destinatario.

La figura riassume il meccanismo di funzionamento del servizio di Posta Elettronica Certificata.

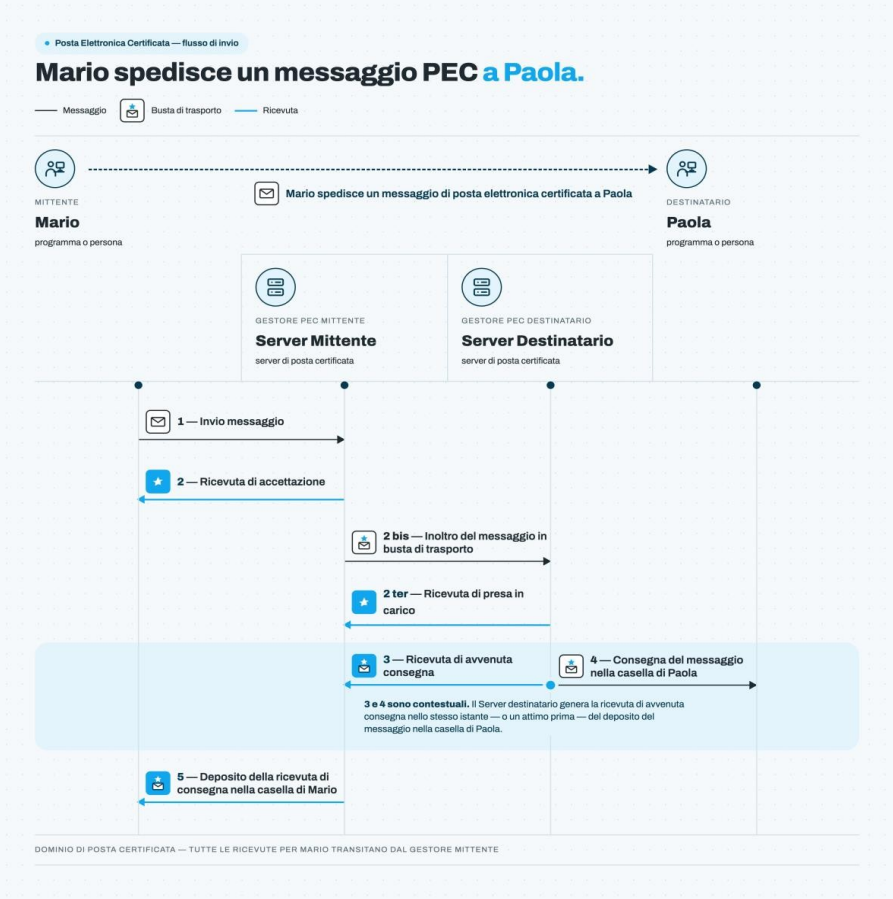


Figura 1

Nel caso in cui il destinatario di un messaggio di Posta Elettronica Certificata non appartenga ad un dominio PEC il processo di consegna del messaggio è previsto come di seguito descritto.

Il mittente invia un messaggio attraverso il servizio di Posta Elettronica Certificata.

Il server di posta certificata del mittente (Punto di accesso) esegue i controlli formali previsti e prosegue inviando al mittente una ricevuta di accettazione, con la quale conferma al mittente che il suo messaggio è stato accettato dal sistema, ad una data e ora specifiche.

- La ricevuta di accettazione è un messaggio di posta elettronica firmato dal gestore del mittente nel quale sono riportati data ed ora di accettazione, l'oggetto ed i dati del mittente e del destinatario.
- Nella ricevuta di accettazione è riportata la tipologia non PEC dei destinatari in modo da informare il mittente che il punto di accesso imbusta, quindi, il messaggio originale in un messaggio di trasporto (Busta di Trasporto) di tipo "S/MIME".

Il messaggio di trasporto firmato dal gestore del mittente è un messaggio che contiene, in allegato, il messaggio originale e tutti i dati che ne certificano il trasporto.

Il messaggio di trasporto viene quindi inviato al dominio destinatario attraverso il gestore di posta del dominio destinatario.

Al mittente non è emessa alcuna ricevuta di avvenuta consegna.

2.2 Funzionamento del servizio - problemi di consegna

Il processo descritto nel paragrafo precedente rappresenta il normale flusso di consegna.

Possono, tuttavia, verificarsi casi nei quali il messaggio di Posta Elettronica Certificata non può essere consegnato.

In tali casi, il flusso operativo è descritto di seguito.

2.2.1 Descrizione del funzionamento in caso di messaggi non consegnati

Il funzionamento del sistema prevede che:

- se il gestore del mittente non riceve dal gestore del destinatario, nelle dodici ore successive all'inoltro del messaggio, la ricevuta di presa in carico o di avvenuta consegna del messaggio inviato, allora il gestore del mittente comunica al mittente che il gestore del destinatario potrebbe non essere in grado di realizzare la consegna del messaggio;
- se entro ulteriori dodici ore, il gestore del mittente non riceve la ricevuta di avvenuta consegna del messaggio inviato, inoltra al mittente un ulteriore avviso relativo alla mancata consegna del messaggio entro le 24 ore successive all'invio.

2.2.2 Descrizione del servizio in presenza di virus

Il funzionamento del servizio di Posta Elettronica Certificata prevede specifiche attività a carico dei Gestori nel caso in cui siano rilevati virus informatici, secondo quanto previsto dalla normativa vigente e dalle disposizioni AgID applicabili.

- Qualora il Gestore del mittente rilevi la presenza di virus informatici nel messaggio in elaborazione, non procede alla sua accettazione e informa tempestivamente il mittente dell'impossibilità di dare corso alla trasmissione. Il Gestore del mittente conserva il messaggio ricevuto per un periodo di trenta mesi.
- Qualora il Gestore del destinatario rilevi la presenza di virus informatici nel messaggio, non procede al suo inoltro al destinatario e informa tempestivamente il Gestore del mittente, affinché quest'ultimo comunichi al mittente l'impossibilità di dare corso alla trasmissione. Il Gestore del destinatario conserva il messaggio ricevuto per un periodo di trenta mesi, secondo le modalità previste dalla normativa vigente.

In conformità alle "Istruzioni per la conservazione dei log dei messaggi e dei messaggi di Posta Elettronica Certificata con Virus", versione 1.0 del 5 luglio 2016, pubblicate da AgID, i log relativi ai messaggi contenenti virus sono conservati per un periodo di trenta mesi.

Nei casi sopra descritti, al mittente è trasmesso uno specifico avviso recante l'indicazione dei motivi che hanno impedito la trasmissione del messaggio.

2.3 Caratteristiche delle ricevute e delle buste di trasporto

2.3.1 Firma elettronica delle ricevute e delle buste di trasporto

Le ricevute e le buste di trasporto rilasciate dal Gestore sono sottoscritte dal Gestore stesso mediante Firma Digitale o Firma Elettronica Avanzata (FEA), quest'ultima generata automaticamente dal sistema di posta elettronica e basata su chiavi asimmetriche a coppia, una pubblica e una privata, che consente di renderne manifesta la provenienza e assicurarne l'integrità e l'autenticità.

2.3.2 Riferimento temporale

Per tutti gli eventi che costituiscono la transazione di elaborazione dei messaggi, quali la generazione delle ricevute e delle buste di trasporto, il Gestore appone un riferimento temporale in conformità all'art. 10 del D.P.R. 11 febbraio 2005, n. 68 [4].

2.3.3 Tipologia delle Ricevute di avvenuta consegna

Coerentemente con quanto previsto dalle Regole tecniche allegate al Decreto del Ministro per l'innovazione e le tecnologie 2 novembre 2005, il Gestore può emettere tre differenti tipologie di ricevute di avvenuta consegna, volte a soddisfare differenti esigenze dell'utenza, di seguito riepilogate.

- Ricevuta di avvenuta consegna completa è costituita da un messaggio di posta elettronica inviato al mittente che riporta in formato leggibile i dati di certificazione (mittente, destinatario, oggetto, data e ora di avvenuta consegna, codice identificativo del messaggio). Gli stessi dati sono inseriti all'interno di un file XML allegato alla ricevuta. Per le consegne relative ai destinatari primari del messaggio (che sono i destinatari diretti del messaggio diversi dai destinatari riceventi in copia), la ricevuta di avvenuta consegna contiene anche il messaggio originale, testo ed eventuali allegati;
- Ricevuta di avvenuta consegna breve ha lo scopo di ridurre i flussi di trasmissione della Posta Elettronica Certificata, soprattutto in quei casi in cui la mole di documenti e di messaggi scambiati è molto consistente. Per quanto descritto tale ricevuta contiene il messaggio originale e gli hash crittografici degli eventuali allegati. Per permettere la verifica dei contenuti trasmessi, il mittente deve conservare gli originali non modificati degli allegati inseriti nel messaggio originale a cui gli hash fanno riferimento. La ricevuta breve può essere richiesta dal mittente utilizzando appositi client di posta capaci di formare il messaggio di Posta Elettronica Certificata, come specificato dall'allegato tecnico al DM 2 novembre 2005.
- Ricevuta di avvenuta consegna sintetica segue le regole di emissione della ricevuta completa solo che l'allegato contiene esclusivamente il file XML con i dati di certificazione descritti. La ricevuta sintetica è particolarmente utile per i servizi che includono la Posta Elettronica Certificata come strumento di trasporto a supporto di una forte automazione dei flussi di comunicazione. Anche questo tipo di ricevuta può essere richiesta dal mittente utilizzando un client di posta capace di formare il messaggio di Posta Elettronica Certificata come specificato dall'allegato tecnico al DM 2 novembre 2005.

3 Servizio Posta Elettronica Certificata ReeVo S.p.A.

In questo capitolo è descritta l'offerta di Posta Elettronica Certificata di ReeVo S.p.A. destinata alla titolarità delle Persone fisiche, alle Aziende (persone giuridiche) e agli Enti della Pubblica Amministrazione.

3.1 Tipologia del servizio offerto

ReeVo S.p.A. offre il servizio di Posta Elettronica Certificata secondo i profili di seguito indicati:

- Profilo Base.
- Profilo Plus.
- Profilo Multidominio.

3.1.1 Profilo Base

È l'offerta per i Clienti che desiderano utilizzare il servizio con il dominio predefinito: mailcert.it.

Il Titolare può richiedere una o più Caselle di Posta Elettronica Certificata del tipo "nome_utente@mailcert.it".

Il valore <nome_utente> sarà proposto dal richiedente.

ReeVo S.p.A. si riserva il diritto di rifiutare tale richiesta.

Alcune cause di tale rifiuto del <nome_utente> possono essere, a titolo esemplificativo e non esaustivo, casi di omonimia, nomi troppo lunghi, nomi simili a marchi noti o afferenti a Enti o Istituzioni Pubbliche.

In conformità alla prescrizione Agenzia per l'Italia Digitale (AgID) del 17 dicembre 2013, "Prescrizione sulla riassegnazione delle caselle di posta elettronica certificata" e in riferimento al "Practice Statement REM" (vd. documento del Prestatore / Gestore a garanzia del corretto **funzionamento e sicurezza del servizio REM)** che vieta al Gestore di riassegnare il medesimo indirizzo PEC a un soggetto diverso dal titolare originario, saranno automaticamente rifiutati gli identificativi di casella (<nome_utente>) già utilizzati in precedenza.

Ciascuna casella di Posta Elettronica Certificata ha dimensione standard minima di 50 MB.

Il dominio di Posta Elettronica Certificata mailcert.it è un dominio "aperto" e permette al Titolare di ricevere sia posta elettronica certificata sia posta elettronica ordinaria.

Ciascun Titolare ha la possibilità di decidere se gestire la posta elettronica ordinaria in ingresso direttamente sul proprio account PEC oppure reindirizzare tale tipo di posta elettronica su un account di posta elettronica ordinaria non appartenente al dominio mailcert.it.

A tal proposito il Titolare dispone di apposita sezione nella maschera "Impostazioni" atta ad abilitare l'inoltro della posta ordinaria (SPAM e NO SPAM) a un indirizzo di posta elettronica "esterno".

Dunque, i messaggi di posta elettronica ordinaria, eventualmente ricevuti sulla casella PEC, saranno reindirizzati alla casella indicata e poi eliminati dalla casella PEC.

Tali messaggi potranno essere consultati solo nella casella "esterna" di destinazione.

3.1.2 Profilo Plus

Profilo di offerta Plus

- Dominio personalizzato e scelto dal Titolare tra le tipologie di seguito elencate:

  - nuovo dominio di 2° livello. In questo caso la registrazione del dominio verrà effettuata da ReeVo S.p.A. per conto del Titolare stesso una volta ricevuta la documentazione correttamente compilata;
  - dominio di 3° livello a fronte di un dominio già registrato. In questo caso non è necessaria alcuna registrazione;
  - dominio di 3° livello del tipo nome_Titolare.mailcert.it dove <nome_Titolare> è scelto dal Titolare. In questo caso ReeVo S.p.A. si riserva la facoltà di rifiutare tale scelta. Cause di rifiuto del <nome_Titolare> possono essere, a titolo esemplificativo e non esaustivo, casi di omonimia, nomi troppo lunghi, nomi simili a marchi noti o afferenti a Enti o Istituzioni Pubbliche.
- Possibilità di scelta del numero di caselle.
- Possibilità di scelta dello spazio disco totale da associare, successivamente, a ciascuna casella in base alle proprie e specifiche esigenze.
- Definire l'amministrazione delle caselle delegata al Titolare, tramite interfaccia Web. Il Titolare si impegna ad agire in conformità a quanto indicato nella comunicazione AgID del 17.12.2013 con oggetto "Prescrizione sulla riassegnazione delle caselle di posta elettronica certificata" in cui "è posto, con decorrenza immediata, il divieto al Gestore di posta elettronica certificata, con riferimento agli indirizzi PEC dallo stesso gestiti, di riassegnare il medesimo indirizzo di posta elettronica certificata a soggetto diverso dal titolare originario".
- Il dominio aperto generato è abilitato a ricevere sia posta elettronica certificata sia posta elettronica ordinaria. Il Titolare ha la facoltà di modificare questo tipo di configurazione avvalendosi di apposito "check box" nel pannello di amministrazione del dominio stesso.

  Il Titolare di ogni casella ha la possibilità di decidere se gestire la posta elettronica ordinaria in ingresso direttamente sul proprio account PEC, inoltre, reindirizzare tale tipologia di posta elettronica su un account di posta elettronica ordinaria non appartenente al dominio stesso.
- Il servizio dispone di interfaccia Web (Web mail).

3.1.3 Profilo offerta Multidominio

Il "profilo Multidominio" è una tipologia di offerta solitamente riservata ai Reseller: il Rivenditore (Reseller) di ReeVo S.p.A. può offrire il servizio PEC ai propri clienti finali consentendo l'amministrazione delegata dei domini di Posta Elettronica Certificata.

La gerarchia di amministrazione del servizio prevede quindi le seguenti figure:

- Amministratore ReeVo S.p.A. - gestisce la piattaforma e configura il servizio "Multidominio" di Posta Elettronica Certificata al proprio cliente (Reseller);
- Amministratore del servizio Profilo Multidominio - configura il servizio ai propri clienti finali, in particolare, associa ad ogni suo cliente un dominio di Posta Elettronica Certificata e per ciascun dominio associa il numero di caselle, lo spazio disco ed eventuali funzionalità aggiuntive (ad es. se il dominio è "chiuso" o "aperto" rispetto alla posta elettronica ordinaria);
- Amministratore di dominio – può creare/modificare/cancellare gli utenti relativi al proprio dominio associando a ciascuno le funzionalità disponibili. Nel compiere questa attività l'amministratore di dominio si impegna ad agire in conformità a quanto indicato nella comunicazione AgID del 17.12.2013 con oggetto "Prescrizione sulla riassegnazione delle caselle di Posta Elettronica Certificata" in cui "è posto, con decorrenza immediata, il divieto al Gestore di posta elettronica

certificata, con riferimento agli indirizzi PEC dallo stesso gestiti, di riassegnare il medesimo indirizzo di posta elettronica certificata a soggetto diverso dal titolare originario".

- utente – utente del servizio di Posta Elettronica Certificata (tipicamente un cliente del Rivenditore (Reseller)).
- Con il "Profilo Multidominio" potranno essere utilizzati nomi a dominio appartenenti ad una delle tre tipologie elencate di seguito:
  - nuovo dominio di 2° livello: in questo caso la registrazione del dominio verrà effettuata da ReeVo S.p.A. per conto del Titolare stesso una volta ricevuta la documentazione correttamente compilata;
  - dominio di 3° livello: a fronte di un dominio già registrato. In questo caso non è necessaria alcuna registrazione;
  - dominio di 3° livello: del tipo nome_Titolare.mailcert.it dove <nome_Titolare> è scelto dal Titolare. In questo caso ReeVo S.p.A. si riserva la facoltà di rifiutare tale scelta. Cause di rifiuto del <nome_Titolare> possono essere, a titolo esemplificativo e non esaustivo, casi di omonimia, nomi troppo lunghi, nomi simili a marchi noti o afferenti a Enti o Istituzioni Pubbliche.

3.1.4 Gestione dei domini di Posta Elettronica Certificata

Descrizione del processo:

- Il dominio di Posta Elettronica Certificata scelto dal Titolare potrà contenere solamente caselle di Posta Elettronica Certificata.
- Tutti i messaggi in uscita dalle caselle di posta configurate nel dominio certificato del Titolare sono trattati come scambi di messaggi di posta certificata. Per ogni messaggio inviato a utenti di Posta Elettronica Certificata, il mittente riceverà una ricevuta di accettazione ed una ricevuta di consegna per ciascuno dei destinatari ai quali il messaggio è stato inviato. In caso di problemi di consegna o anomalie nell'utilizzo del servizio il mittente riceverà i corrispondenti avvisi.
- Nel caso in cui la gestione del dominio/sottodominio sia a carico del Titolare allora si richiede al Titolare stesso che il gestore del suo dominio configuri opportunamente i server DNS al fine di assicurare la visibilità in rete dei server coinvolti nel processo di gestione della Posta Elettronica Certificata. La responsabilità della corretta configurazione del DNS è esclusiva competenza del Titolare come previsto nella specifica clausola contrattuale. I servizi relativi al dominio di Posta Elettronica Certificata verranno forniti dalla piattaforma di ReeVo S.p.A.
- ReeVo S.p.A. avrà l'onere dell'inserimento dei domini nell'indice dei gestori di Posta Elettronica Certificata che contiene la lista di tutti i domini di Posta Elettronica Certificata gestiti da ciascun operatore.
- ReeVo S.p.A. si riserva di non procedere alla registrazione di nomi dominio che non siano considerati conformi alla policy aziendale e che risultino violare i diritti di terzi in tema di proprietà industriale e intellettuale.

3.2 Accesso al servizio

Il servizio di Posta Elettronica Certificata è accessibile sia tramite interfaccia Web sia tramite client di posta elettronica.

3.2.1 Interfaccia Web

L'interfaccia Web (HTTPS) è disponibile all'indirizzo segnalato sul sito https://www.reevo.it e prevede le seguenti principali funzionalità in base al profilo dell'Utente:

- Profilo "Amministratore del servizio del Titolare" (disponibile solo per l'offerta Plus e Multidominio):
  - gestione degli utenti (creazione/modifica/cancellazione);
  - associazione a ciascuna casella dello spazio;
  - impostazione del dominio come "aperto" o "chiuso" alla posta elettronica ordinaria;
  - reset della password ad un valore impostato nel caso in cui un Utente abbia dimenticato la propria;
- Profilo "Utente" del servizio:
  - gestione dei messaggi in arrivo;
  - composizione di un nuovo messaggio;
  - selezione della tipologia di ricevuta di avvenuta consegna (completa, breve, sintetica). Il tipo di ricevuta previsto di default dal sistema è "completa";
  - organizzazione dei messaggi in cartelle;
  - ricerca dei messaggi;
  - nel caso di dominio "aperto" (in grado di ricevere messaggi di posta elettronica ordinaria oltre che quelli di tipo certificato) definire una casella a cui effettuare il reindirizzamento dei messaggi di posta elettronica ordinaria;
  - cambio della password.

3.2.2 Client di Posta Elettronica

L'accesso al servizio è consentito mediante l'utilizzo di qualsiasi client di Posta Elettronica che preveda l'uso dei seguenti protocolli:

Invio: SMTP/S;

Ricezione: POP3/S IMAP/S.

In tale accezione le funzionalità disponibili sono quelle tipiche dello specifico client utilizzato.

Per poter utilizzare il servizio è necessario configurare il client con i parametri relativi a:

- server di posta in arrivo (POP3/S o IMAP/S) e della relativa porta;
- server di posta in uscita (SMTP/S) e della relativa porta.

Tali informazioni sono fornite al Titolare attraverso la lettera di benvenuto (Welcome Letter).

La selezione della tipologia per la ricevuta di avvenuta consegna si ottiene facendo in modo che il client di posta inserisca nell'header del messaggio, inviato dal mittente, una delle righe seguenti:

- X-TipoRicevuta: breve se si vuole una ricevuta "breve";
- X-TipoRicevuta: sintetica se si vuole una ricevuta "sintetica".

La tipologia di ricevuta, prevista di default dal Sistema, è "completa".

3.2.3 Credenziali di accesso e parametri configurazione del servizio

Le credenziali di accesso al servizio sono trasmesse al Titolare all'interno della lettera di benvenuto (Welcome Letter), all'indirizzo di posta elettronica indicato all'interno della documentazione contrattuale.

A seconda della scelta eseguita dal Titolare:

- Profilo Base riceverà le credenziali per gli utenti richiesti su dominio mailcert.it;
- Profilo Plus oppure Profilo Multidominio riceverà le credenziali di accesso dell'Utente Amministratore.

Dopo aver eseguito il primo accesso è raccomandato sempre modificare la password.

3.2.4 Raccomandazioni gestione utenza

Al fine di garantire il corretto e sicuro utilizzo del servizio PEC, ReeVo S.p.A. raccomanda quanto di seguito indicato:

- procedere alla modifica della password, successivamente al primo accesso, tramite la funzionalità di modifica della password disponibile da interfaccia Web e di provvedere al cambiamento della password con cadenza periodica;
- il Titolare della casella è tenuto a consultare la propria casella di posta certificata con regolarità, poiché la disponibilità di un messaggio nella casella del destinatario determina la consegna dello stesso, indipendentemente dalla successiva lettura da parte del destinatario;
- archiviare periodicamente i messaggi sul proprio computer e successivamente cancellarli dal server di posta per evitare che venga occupato tutto lo spazio disponibile e quindi i messaggi successivi possano essere rifiutati;
- informare gli utilizzatori che la casella PEC consente di effettuare comunicazioni con gli effetti previsti dalla normativa vigente e deve, pertanto, essere utilizzata esclusivamente per le finalità proprie del servizio, quindi non come una casella di posta elettronica ordinaria;
- dotare le postazioni di lavoro di Antivirus costantemente aggiornato al fine di garantire maggiore sicurezza per quanto sia oggetto di spedizione e ricezione;
- anche se il servizio di Posta Elettronica Certificata di ReeVo S.p.A. è dotato di antivirus, non è sempre possibile controllare tutti i contenuti potenzialmente dannosi (a titolo di esempio si evidenzia che contenuti messaggi cifrati e/o compressi non possono essere sottoposti a controlli efficaci).

3.2.5 Adeguamento del servizio PEC ai nuovi standard europei

ReeVo S.p.A., nell'ambito del percorso di adeguamento del servizio PEC ai nuovi standard europei, sta introducendo specifici requisiti, volti a rafforzare l'affidabilità sull'identità dei Titolari delle caselle e sulla sicurezza nell'accesso del servizio. A tal fine, le persone fisiche saranno sottoposte a una procedura di identificazione certa, finalizzata alla verifica della loro identità; per le persone giuridiche e le P.A., la verifica riguarderà invece, l'identità e i poteri del soggetto legittimato ad agire per conto dell'organizzazione, secondo quanto previsto dal Regolamento (UE) n. 910/2014, come modificato dal Regolamento (UE) 2024/1183, e dai relativi standard tecnici ETSI applicabili ai servizi elettronici di recapito certificato qualificati. L'accesso alla casella è protetto mediante autenticazione a due fattori (MFA), basata sull'utilizzo di due distinti fattori di autenticazione appartenenti ad almeno due diverse categorie (conoscenza, possesso o inerenza), volta a ridurre il rischio di accessi non autorizzati e rafforzare la sicurezza del servizio, in conformità alla medesima disciplina europea.

4 Livelli di servizio – Indicatori di qualità

Il presente capitolo descrive i livelli di servizio e gli indicatori di qualità del servizio di Posta Elettronica Certificata (PEC), definiti in conformità al quadro normativo e tecnico di riferimento, con particolare riguardo al **D.P.R. 11 febbraio 2005, n. 68**, e al **D.M. 2 novembre 2005**, recante le regole tecniche per la formazione, la trasmissione e la validazione, anche temporale, della PEC. Si fa inoltre riferimento al **D.Lgs. 7 marzo 2005, n. 82 (Codice dell'Amministrazione Digitale – CAD)**, in particolare all'art. 48, relativo alla posta elettronica certificata.

La tabella seguente riporta i principali parametri di qualità e di servizio, utilizzati per monitorare le prestazioni, l'affidabilità e il rispetto dei livelli minimi previsti dalla normativa applicabile.

Numero Destinatari	
Numero massimo di destinatari per i messaggi originati da caselle di Posta Elettronica Certificata ReeVo S.p.A.	50
Dimensione messaggi	
La dimensione di ogni singolo messaggio che può essere accettata dal Servizio di Posta Elettronica Certificata di ReeVo S.p.A. per cui è garantita la trasmissione (intesa come prodotto del numero dei destinatari e delle dimensioni del messaggio stesso).	100 MB
Disponibilità servizio	
Il periodo temporale di riferimento per il calcolo della disponibilità/ indisponibilità del servizio.	Quattro mesi (1 quadrimestre)
La disponibilità del servizio nel periodo di riferimento sopra indicato.	99,80%
L'indisponibilità del servizio per il singolo fermo nel periodo sopra indicato.	≤ 50% del totale previsto per l'intervallo di tempo di riferimento
Tempi	
Tempo di consegna delle ricevute di accettazione nel periodo di disponibilità del servizio.	30 minuti

5 Condizioni di fornitura

5.1 Canali di vendita, proposta e documentazione del servizio

Il servizio di Posta Elettronica Certificata è commercializzato da ReeVo S.p.A.:

- Modalità diretta tramite propria forza di vendita autorizzata;
- tramite Rivenditore (Reseller).

Il servizio è disciplinato e fornito in conformità con la vigente normativa e con quanto previsto dalla documentazione, di seguito elencata, che sarà fornita al Titolare durante la fase di stipula contrattuale:

- Condizioni generali di contratto.
- Proposta di contratto contenente gli elementi del servizio, i valori economici e la richiesta di attivazione del servizio.
- Manuale Operativo.
- Informativa sulla privacy.

5.1.1 Attivazione diretta del servizio

Il personale del Customer Service di ReeVo S.p.A. accompagna il richiedente nelle diverse fasi di attivazione del servizio, raccogliendo le informazioni necessarie alla configurazione dell'offerta, quali il numero di caselle PEC, lo spazio complessivamente disponibile e gli eventuali servizi opzionali richiesti.

Il Customer Service provvede, inoltre, all'identificazione del richiedente, alla definizione delle condizioni contrattuali e alla verifica della completezza e correttezza della documentazione prevista per l'attivazione.

A tal fine, viene utilizzata la documentazione contrattuale predisposta da ReeVo S.p.A., nella quale sono riportate le condizioni e le caratteristiche del servizio richiesto dal Titolare.

Al ricevimento della documentazione prevista, ReeVo S.p.A. avvia le attività necessarie alla verifica e alla lavorazione della richiesta, fino alla successiva attivazione del servizio.

5.1.2 Attivazione del servizio tramite Rivenditore (Reseller)

Il Rivenditore (Reseller) è il soggetto autorizzato da ReeVo S.p.A. alla commercializzazione del servizio di Posta Elettronica Certificata (PEC); quindi, raccoglie le informazioni relative al servizio (numero caselle, spazio totale, eventuali servizi opzionali); procede all'identificazione del richiedente, alla definizione dell'accordo e alla firma del contratto verificandone la correttezza e la completezza.

Tutta la documentazione contrattuale è predisposta da ReeVo S.p.A. e contiene le condizioni del servizio che il Titolare richiede al Gestore.

Alla conclusione delle attività su indicate, il Reseller avvia la lavorazione del contratto inviando al punto di contatto indicato da ReeVo S.p.A. la documentazione idonea e completa al fine di garantire in tale fase il riconoscimento del richiedente del servizio.

ReeVo S.p.A. è integralmente responsabile della qualità del servizio nei confronti del Titolare.

5.1.3 Attivazione del servizio tramite Rivenditore (Reseller) - Offerta Multidominio

ReeVo S.p.A. può veicolare i propri servizi attraverso accordi di rivendita nel rispetto della normativa vigente e del presente Manuale Operativo.

Responsabilità del Gestore del servizio di Posta Elettronica Certificata

ReeVo S.p.A., in qualità di Gestore di Posta Elettronica Certificata qualificato e soggetto responsabile dell'erogazione del servizio, è integralmente responsabile della gestione e dell'erogazione del servizio PEC, nel rispetto della normativa vigente, delle regole tecniche applicabili e di quanto previsto dal presente Manuale Operativo.

In particolare, ReeVo S.p.A.:

- assicura l'erogazione del servizio di Posta Elettronica Certificata e ne garantisce la conformità ai requisiti normativi e tecnici applicabili;
- gestisce direttamente gli aspetti tecnici e operativi del servizio PEC;
- riceve e gestisce le richieste relative ai Log del servizio secondo le modalità indicate al paragrafo 6.4.4 del presente Manuale Operativo;
- assicura la gestione e la conservazione delle evidenze e delle informazioni previste dalla normativa applicabile;
- gestisce le segnalazioni e le richieste di assistenza tecnica che richiedono l'intervento del Gestore;
- garantisce la disponibilità dei propri sistemi e delle infrastrutture necessarie all'erogazione del servizio, secondo i livelli e le modalità previsti dalla documentazione applicabile;
- provvede alla registrazione e alla gestione dei dati dei Titolari necessari all'erogazione del servizio;
- rende disponibile il presente Manuale Operativo ai soggetti interessati secondo le modalità previste.

Responsabilità del Reseller

Il Reseller opera in qualità di soggetto commerciale incaricato della distribuzione del servizio PEC erogato da ReeVo S.p.A. e costituisce, ove previsto dal modello di servizio adottato, il punto di riferimento commerciale e di primo contatto per il Titolare.

Nell'ambito delle attività di propria competenza, il Reseller:

- raccoglie le richieste del cliente relative all'attivazione e alla gestione del servizio;
- raccoglie e verifica la documentazione necessaria alla sottoscrizione del servizio, secondo le procedure definite dal Gestore;
- fornisce al cliente le informazioni commerciali e operative relative al servizio;
- fornisce al cliente copia del presente Manuale Operativo;
- trasmette al Gestore i dati e la documentazione necessari alla registrazione e all'attivazione del Titolare, secondo le modalità definite dal Gestore;
- può fornire un servizio di assistenza amministrativa e di primo livello, limitatamente alle attività di propria competenza;
- raccoglie le eventuali segnalazioni tecniche del cliente e le trasmette al Gestore secondo le procedure e i canali definiti dal Gestore.

Il Reseller non assume la responsabilità dell'erogazione del servizio PEC, che rimane integralmente in capo a ReeVo S.p.A. in qualità di Gestore qualificato.

Dati e documentazione trasmessi al Gestore

Ai fini della registrazione e dell'attivazione del Titolare, il Reseller trasmette a ReeVo S.p.A., secondo le modalità e i canali definiti dal Gestore, i dati e la documentazione necessari alla corretta gestione del servizio.

In particolare, possono essere richiesti:

- nome e cognome del Titolare o ragione sociale;
- codice cliente;
- codice del contratto;
- dominio di Posta Elettronica Certificata;
- data di attivazione;
- copia del documento di identità;
- copia della documentazione contrattuale sottoscritta;
- informativa privacy sottoscritta;
- ulteriori dati e documenti necessari per l'erogazione del servizio e previsti dalla normativa applicabile.

La trasmissione dei dati e della documentazione al Gestore avviene secondo le modalità, i tempi e i requisiti di sicurezza stabiliti da ReeVo S.p.A.

ReeVo S.p.A. rimane integralmente responsabile del servizio nei confronti del Titolare.

Attività di audit sui Reseller

Nell'ambito delle proprie responsabilità quale Gestore qualificato del servizio di Posta Elettronica Certificata, ReeVo S.p.A. effettua periodicamente attività di audit e verifica nei confronti dei Reseller, secondo modalità e frequenza definite dal Gestore.

Le attività di audit sono finalizzate a verificare il corretto svolgimento delle attività affidate ai Reseller, il rispetto delle procedure e delle prescrizioni applicabili al servizio e il mantenimento degli standard di qualità richiesti, con particolare riferimento alle attività che possono incidere sull'erogazione del servizio PEC e sull'esperienza del Titolare.

Gli audit possono comprendere, a titolo esemplificativo, la verifica:

- delle modalità di acquisizione e gestione della clientela;
- della corretta raccolta e trasmissione al Gestore dei dati e della documentazione necessari all'attivazione e alla gestione delle caselle PEC;
- delle modalità di gestione delle richieste e delle segnalazioni dei Titolari;
- del rispetto delle procedure e delle istruzioni operative impartite da ReeVo S.p.A.;
- della corretta gestione delle informazioni e della documentazione relativa al servizio;
- dei livelli di servizio e di qualità assicurati nell'ambito delle attività di competenza del Reseller.

Gli esiti delle attività di audit sono documentati e, ove necessario, possono determinare l'adozione di azioni correttive e preventive, nonché ulteriori verifiche finalizzate ad accertarne l'effettiva attuazione.

Le attività di audit e di controllo sui Reseller non modificano né limitano la responsabilità di ReeVo S.p.A. quale Gestore qualificato del servizio PEC, che permane integralmente responsabile dell'erogazione del servizio e del rispetto dei requisiti normativi e tecnici applicabili. Le sessioni di

audit consentono di monitorare l'andamento del servizio al fine di garantire piena efficacia in termini di affidabilità, qualità, stabilità e reputazione.

5.1.4 Modalità alternative per l'attivazione del servizio

ReeVo S.p.A. si riserva la facoltà di fornire nuove modalità e flussi per la richiesta di nuove attivazioni. Le modalità oggi disponibili e quelle future garantiscono e garantiranno il rispetto delle norme relative alla privacy e alla normativa vigente relativa al servizio di Posta Elettronica Certificata.

5.2 Attivazione del servizio

I tempi di attivazione del Servizio sono tre (3) giorni lavorativi, da intendersi dalla data di ricezione della documentazione completa e necessaria, compresa la documentazione eventuale per la registrazione di un nuovo dominio.

L'attivazione del servizio viene comunicata al cliente inviando una lettera di benvenuto (Welcome Letter) all'indirizzo di posta indicato nella documentazione contrattuale contenente:

- il login e la password di accesso al servizio per l'Utente amministratore (nel caso di profilo Plus o Multidominio);
- Il login e la password di accesso alla casella su dominio mailcert.it (nel caso di profilo Base);
- la URL di accesso al servizio tramite interfaccia Web (Web mail);
- i parametri di configurazione del client di posta elettronica;
- i riferimenti del sito Web;
- indicazioni dei riferimenti per accedere ai servizi di Customer Care di ReeVo S.p.A. (caselle di posta elettronica per richiedere assistenza tecnica e amministrativa, le credenziali di accesso e l'indirizzo del portale per l'inoltro delle segnalazioni).

5.2.1 Gestione aggiornamento informazioni - Titolari - Caselle PEC

Il Gestore provvede alla gestione e all'aggiornamento delle informazioni relative ai Titolari e alle caselle di Posta Elettronica Certificata, in conformità alle disposizioni previste dal D.P.R. 11 febbraio 2005, n. 68 e dalle Regole tecniche allegate al D.M. 2 novembre 2005.

A ciascuna casella PEC, il Gestore associa almeno un codice identificativo del Titolare, abbinato a un sistema di autenticazione conforme ai requisiti previsti dalle Regole tecniche.

Il Gestore provvede all'aggiornamento delle informazioni relative al Titolare e alla casella PEC in occasione dell'attivazione, della modifica, della sospensione e della cessazione del servizio, secondo le procedure definite dal Gestore e nel rispetto della normativa applicabile.

Le operazioni di inserimento, modifica e cessazione delle informazioni sono effettuate esclusivamente da personale autorizzato e sono soggette a idonei controlli e misure di sicurezza, tali da garantire l'integrità, la riservatezza e la tracciabilità delle informazioni gestite.

Il Gestore assicura inoltre la disponibilità delle informazioni e della relativa documentazione alle Autorità competenti, nei casi e secondo le modalità previste dalla normativa vigente.

5.3 Disdetta del contratto

Il Titolare, opportunamente identificato, può richiedere la risoluzione del contratto per il servizio di Posta Elettronica Certificata inviando una PEC oppure una raccomandata A/R all'indirizzo indicato nel Manuale Operativo (cfr. 1.7.2). Il Gestore comunica al Titolare l'avvenuta disdetta/disattivazione. La disdetta sarà operativa entro trenta (30) giorni lavorativi a partire dalla data di risoluzione richiesta

dal Titolare. Le richieste di disdetta/disattivazione sono conservate da ReeVo S.p.A. per almeno trenta (30) mesi.

5.4 Corrispettivo economico

Il servizio di Posta Elettronica Certificata di ReeVo S.p.A. prevede un canone annuale dipendente dal numero dei domini/caselle di Posta Elettronica Certificata, dallo spazio totale richiesto e dalle funzionalità opzionali acquistate. Le condizioni economiche sono determinate dalla personalizzazione dell'offerta in termini di dimensionamento della richiesta del cliente e definite nell'accordo contrattuale.

5.5 Descrizione generale degli elementi del contratto

Sospensione del servizio:

ReeVo S.p.A. potrà sospendere temporaneamente il servizio per procedere alla manutenzione ordinaria e straordinaria degli impianti e delle apparecchiature necessarie all'erogazione del servizio dandone comunicazione al Titolare tramite e-mail con un preavviso di almeno 24 ore.

ReeVo S.p.A. potrà sospendere in ogni momento il Servizio, in tutto o in parte, anche senza preavviso, in caso di guasti alla rete e agli apparati di fornitura del Servizio, dipendenti da caso fortuito o forza maggiore, nonché nel caso di modifiche e/o manutenzioni straordinarie non programmabili e tecnicamente indispensabili.

Costituiscono casi di forza maggiore gli eventi al di fuori del ragionevole controllo di ReeVo S.p.A., quali, a titolo esemplificativo ma non esaustivo, attività e/o decisioni governative e/o della Pubblica Amministrazione, atti dell'Autorità Militare, limitazioni legali, catastrofi naturali, fulmini, incendi, esplosioni, sommosse, guerre, epidemie, e, purché siano su base nazionale, scioperi, mancanza di materie prime, energia, trasporti, ecc.

ReeVo S.p.A. potrà sospendere il Servizio anche in caso di violazione da parte del Titolare degli obblighi posti a suo carico in conformità a quanto previsto dal Manuale Operativo o dallo specifico accordo contrattuale, dandone comunicazione al Titolare tramite e-mail e fatta salva ogni eventuale azione di rivalsa nei riguardi del responsabile delle violazioni.

Risoluzione del contratto: ReeVo S.p.A. potrà procedere alla risoluzione del contratto:

- nel caso in cui il servizio sia utilizzato per finalità contrarie a leggi, regolamenti, disposizioni e normative;
- in caso di mancato pagamento entro giorni trenta (30) dalla data di scadenza del pagamento indicato in fattura.

La risoluzione contrattuale sarà comunicata al Titolare tramite Posta Elettronica Certificata.

In tale casistica, rimane l'obbligo da parte del Titolare al pagamento dei corrispettivi non pagati e onorare quanto previsto a livello contrattuale.

5.6 Obblighi e responsabilità

5.6.1 Obblighi del Gestore

ReeVo S.p.A. fornirà il Servizio conformemente a quanto stabilito dalla normativa vigente in materia, con le modalità indicate nel presente documento.

In particolare, ReeVo S.p.A. assume i seguenti obblighi:

- garantire la fornitura del servizio di Posta Elettronica Certificata in conformità con le normative vigenti;

- assicurare l'erogazione del Servizio secondo i livelli minimi di servizio previsti dalla normativa vigente e dal presente Manuale;
- assicurare l'interoperabilità del Servizio con gli altri operatori iscritti nell'elenco pubblico dei gestori PEC;
- rendere disponibili nei casi previsti dalla legge i log inerenti le trasmissioni tra caselle di Posta Elettronica Certificata.

ReeVo S.p.A. si riserva il diritto di modificare le specifiche tecniche di erogazione del Servizio in base all'evoluzione tecnologica e/o normativa, aggiornando il presente manuale operativo così come specificato al paragrafo 1.3 del presente documento.

5.6.2 Obblighi del Titolare del Servizio

Il Titolare assume i seguenti obblighi:

- fornire tutte le informazioni e la documentazione richiesta da ReeVo S.p.A., necessarie ad una corretta identificazione garantendone, sotto la propria responsabilità, l'attendibilità ai sensi del DPR n. 68/2005 [4] e successive modifiche ed integrazioni;
- prestare il consenso al trattamento dei dati personali, ai sensi del Regolamento GDPR (Reg. UE 2016/679), con il D.Lgs. 196/2003 come modificato dal D.Lgs. 101/2018;
- informare immediatamente ReeVo S.p.A. in caso risulti compromessa la riservatezza dei codici di accesso per l'utilizzo del Servizio.

Il Titolare assume inoltre i seguenti obblighi e si impegna ad estenderli agli Utenti del servizio:

- consultare in maniera preventiva il Manuale Operativo per conoscerne i contenuti;
- visionare la versione aggiornata del Manuale Operativo sul sito ReeVo al seguente link: https://www.reevo.it/it/manuale-operativo-servizio-pec;
- conservare con la massima riservatezza e diligenza i codici di accesso al Servizio;
- non utilizzare il Servizio con lo scopo di depositare, inviare, pubblicare, trasmettere e/o condividere applicazioni o documenti informatici che siano in contrasto o violino diritti di proprietà intellettuale, segreti commerciali, marchi, brevetti o altri diritti di proprietà di terzi.

Il Titolare prende atto che alla scadenza del contratto o in caso di sua risoluzione, non sarà più possibile accedere al Servizio e al suo contenuto e pertanto si impegna a darne informativa agli Utenti, sollevando ReeVo S.p.A. da ogni responsabilità derivante dal mancato accesso.

Responsabilità del Titolare

Il Titolare manleva ReeVo S.p.A. da ogni responsabilità, spesa, danno o pregiudizio, diretto od indiretto, di cui ReeVo S.p.A. fosse chiamata a rispondere nei confronti di terzi per fatto:

- riconducibile alla erronea o parziale indicazione dei dati forniti dal Titolare;
- imputabile al Titolare o all'Utente in relazione all'uso del Servizio.

Cessione del servizio

Il Titolare non potrà cedere a terzi in tutto o in parte il Servizio regolato dalle presenti condizioni, senza la preventiva autorizzazione scritta di ReeVo S.p.A.

Responsabilità, esclusioni e limitazione in sede di indennizzo

Il Gestore ReeVo S.p.A. 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.

ReeVo S.p.A. non sarà invece in alcun modo responsabile per danni di natura diretta od indiretta derivanti da:

- atti della Pubblica Autorità, caso fortuito, forza maggiore ovvero da altra causa non imputabile a ReeVo S.p.A. quali, in via puramente esemplificativa e non esaustiva, mancato o erroneo funzionamento di reti, apparecchiature o strumenti di carattere tecnico al di fuori della sfera di controllo di ReeVo S.p.A., interruzioni nella fornitura di energia elettrica, terremoti, esplosioni, incendi;
- erroneo utilizzo di codici identificativi da parte dell'Utente;
- mancato invio o mancata consegna dei messaggi al di fuori dei livelli di servizio previsti dalla normativa vigente, causati da anomalie segnalate al mittente o al destinatario, i quali non abbiano provveduto a riscontrare la comunicazione di anomalia inviata da ReeVo S.p.A.;
- impiego del Servizio al di fuori delle previsioni normative vigenti o dall'utilizzo di servizi di posta elettronica forniti da gestori non inclusi nell'elenco pubblico tenuto da AgID.

Si evidenzia inoltre che ReeVo S.p.A.:

- non assume alcuna responsabilità, salvo eventuale dolo o colpa, dei ritardi che i messaggi di posta elettronica possono subire nella loro trasmissione via Internet;
- è esonerata da ogni potere di controllo, di mediazione o di vigilanza sul contenuto dei messaggi inviati dagli Utenti e non assume nessuna responsabilità riguardo al loro contenuto illecito o contrario alla morale o all'ordine pubblico, non sussistendo alcun obbligo di vigilanza o di cancellazione in capo a ReeVo S.p.A. in riferimento al contenuto dei messaggi;
- non assume nessun obbligo, garanzia o responsabilità ulteriori rispetto a quelle scaturenti dal contratto di fornitura del Servizio per il tramite di ReeVo S.p.A. e dalla normativa vigente.

ReeVo S.p.A., nell'ambito della sua attività di Gestore di Posta Elettronica Certificata è dotata di tre polizze assicurative comprendenti la società italiana e le controllate estere, con coperture idonee per i rischi dell'attività e i danni causati a terzi.

6 Sistemi Tecnologici

6.1 Infrastruttura, Affidabilità, Sicurezza, Scalabilità, Connettività

Infrastruttura

La piattaforma tecnologica utilizzata per erogare il Servizio di Posta Elettronica Certificata è installata presso il Data Center utilizzato da ReeVo S.p.A. a Siziano (PV) e si basa su un'architettura progettata per garantire la massima disponibilità del servizio agli utenti.

Il core della piattaforma è rappresentato da un pool di server gestito dal sistema di virtualizzazione VMware che, attraverso le sue funzionalità, permette di raggiungere il livello di affidabilità richiesto dalla attuale normativa sul servizio di Posta Elettronica Certificata.

L'architettura logica del sistema, come descritto nella **figura 2** è così articolata:

- modulo Firewall: composto da una coppia di sistemi in mutuo failover garantisce il primo livello di protezione permettendo l'accesso ai soli protocolli utilizzati per l'erogazione del servizio;
- modulo Bilanciatore: permette di ridirigere il traffico diretto verso un dato servizio su più di un server del modulo di Front End e del modulo Web garantendo una corretta distribuzione del carico;
- modulo Front-End: composto da più Server, fornisce il punto di accesso agli Utenti attraverso vari protocolli (SMTP/S, POP3/S e IMAP/S) e si occupa dello scambio di corrispondenza con gli altri Gestori;
- modulo Web: implementato da più Server, permette di accedere al servizio tramite interfaccia Web (HTTPS) da cui si possono eseguire tutte le attività indicate al paragrafo 3.2.1;
- modulo Antivirus: composto da più Server per garantire ridondanza e performance adeguate, questo modulo fornisce il servizio di controllo e "pulizia" di eventuali virus informatici;
- modulo Back-End: composto di più Server fornisce i servizi di LDAP e di Message Store (Contenitore delle caselle di Posta). Ogni server di Back-End è interconnesso al modulo SAN attraverso una doppia connessione in fibra ottica;
- modulo database: mantiene le informazioni che si riferiscono alle transazioni di Posta Elettronica Certificata. Su questo modulo sono implementate le procedure per l'estrazione dei file di log e per la loro marcatura temporale;
- modulo HSM (Hardware Security Module): composto da una batteria di appliance dedicate che ospitano i processori crittografici intelligenti utilizzate per:
  - memorizzazione delle chiavi private di firma;
  - processo di firma digitale su Ricevute e Buste;
- modulo SAN (Storage Area Network): è il sistema su cui sono contenuti i dati acceduti da tutti i moduli che implementano il servizio di Posta Elettronica Certificata. È implementato da uno storage in configurazione HA (completamente ridondato in tutte le sue parti critiche: processore, controller, alimentazione, interfacce di rete, …) con dischi in configurazione Raid. La connessione tra i server di erogazione e lo storage è realizzata attraverso connessioni di rete ridondate.

Attraverso l'utilizzo di una soluzione di virtualizzazione ReeVo S.p.A. è in grado di garantire le seguenti funzionalità:

Affidabilità.

- In caso di fault di uno dei nodi del modulo Firewall il secondo nodo continua a gestire il traffico garantendo l'applicazione delle policy di sicurezza in accesso;
- in caso di fault di una macchina fisica del pool (o della necessità di un intervento di upgrading HW della macchina stessa) i server virtuali possono essere facilmente "spostati" su un altro nodo del pool (il software di gestione del pool supporta la funzionalità di Live Migration);
- le caselle di posta degli utenti risiedono sul modulo SAN accessibile dai server tramite connessioni di rete ridondate;

Sicurezza.

- La presenza del modulo Firewall, sul quale viene applicata la politica secondo cui tutto ciò che non è espressamente consentito è negato, unitamente all'utilizzo di sistemi di Load Balancing, volti a disaccoppiare il servizio erogato dai server fisici che lo ospitano, garantisce un elevato livello di protezione dell'intero sistema, riducendo i rischi connessi a eventuali attacchi informatici.
- I sistemi utilizzati per l'erogazione del servizio sono sottoposti ad interventi di hardening, con l'obiettivo di abilitare i soli servizi indispensabili al funzionamento della PEC e disabilitare tutti gli altri.
- Cybersecurity e controllo da parte del SOC di ReeVo, basato su tecnologie Splunk, Crowdstrike e Tenable.

La piattaforma è sottoposta a VA/PT periodici.

Scalabilità.

- L'utilizzo di un'architettura virtualizzata permette di scalare facilmente sia in modalità orizzontale sia in modalità verticale.
- A fronte del rilevamento di una crescita delle attività è sufficiente aumentare le risorse disponibili alle macchine virtuali o inserire nel pool nuovi nodi fisici e "ridistribuire" i server virtuali sui nuovi nodi fisici.

Interazione con l'HSM: la seguente **figura 2** mostra un bus di rete intermedio a cui sono collegati sia il FrontEnd/WEB sia l'HSM e il BackEnd. Le chiamate crittografiche verso l'HSM per la firma dei messaggi e delle ricevute sono gestite esclusivamente dal PEC Engine (Back End), garantendo la corretta segregazione dei livelli di sicurezza.

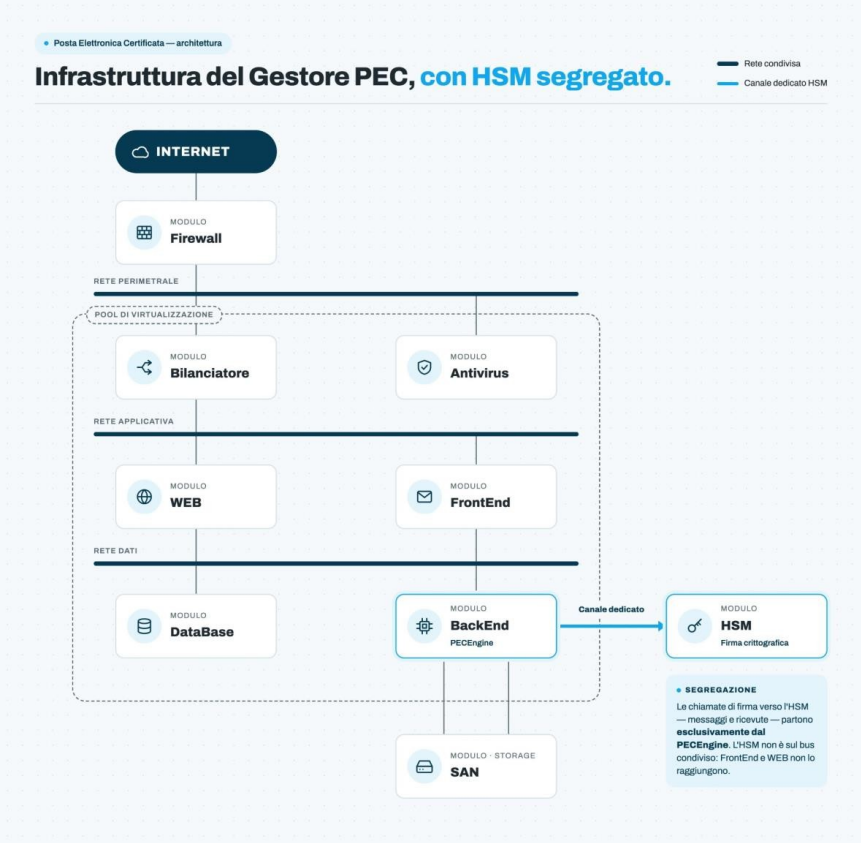


Figura 2

Connettività.

I Data Center utilizzati da ReeVo S.p.A. sono ubicati a Roma (RM) e Siziano (PV).

I Data Center sono interconnessi da circuiti in F.O. di ReeVo S.p.A. (2 x 10 Gb/sec tra Siziano e Roma).

Tale infrastruttura permette di annunciare l'Autonomous System di ReeVo S.p.A. (AS 3242) via BGP verso idonei carriers.

La tabella seguente riassume la capacità trasmissiva verso Internet:

Data Center	Banda verso Internet	Banda verso Mix
Roma	2 x 10 Gb/sec (Wind)	-
Siziano	4 x 10 Gb/sec (Multicarrier: FT, RETN, HE)	2 x 10 Gb/sec

Tali caratteristiche assicurano un'elevata connettività dei Data Center verso la rete Internet nazionale e internazionale, favorendo la continuità e l'accessibilità dei servizi erogati.

L'infrastruttura di erogazione primaria del servizio di Posta Elettronica Certificata è posizionata presso il Data Center utilizzato da ReeVo S.p.A. a Siziano.

Tale Data Center è connesso al servizio Blended IP multicarrier di Stack Emea con F.O. a 10 Gb/sec.

Sul sito di disaster recovery dislocato presso il Data Center utilizzato da ReeVo a Roma, l'infrastruttura ReeVo è connessa al POP Wind, presente nello stesso comprensorio, tramite connessioni multiple GigabitEthernet in fibra ottica terminate senza necessità di collegamenti WAN.

6.2 Data Center – caratteristiche principali

Al fine di garantire la continuità del servizio di Posta Elettronica Certificata, ReeVo S.p.A. ha affiancato al sito primario di erogazione (Siziano) un sito di disaster recovery (Roma) da cui, in caso di grave disservizio sul sito primario, continuare ad erogare il servizio ai Titolari.

Entrambi i siti rispondono alle più rigorose indicazioni in termini di sicurezza fisica (controllo accessi, alimentazione elettrica, condizionamento, …) e di sicurezza logica.

6.2.1 Caratteristiche comuni in uso tra i Data Center

Le infrastrutture presso le quali sono ubicati i Data Center sono dotate dei seguenti sistemi e misure di sicurezza:

- controllo degli accessi mediante badge e codice numerico, articolato su più livelli di sicurezza;
- sistemi di rilevamento delle intrusioni e servizio di vigilanza, attivo 24 ore su 24, 7 giorni su 7, 365 giorni all'anno;
- sistemi di videosorveglianza a circuito chiuso, con archiviazione digitale delle registrazioni nel rispetto della normativa vigente in materia di protezione dei dati personali;
- sistemi di rilevazione e gestione degli eventi di fumo, incendio e allagamento;
- collegamenti con gli altri Data Center finalizzati all'erogazione dei servizi di disaster recovery.

6.2.2 Sito di Siziano (Stack EMEA)

Alimentazione elettrica:

- il campus è alimentato da una linea ridondata in alta tensione da 132 kV.
- tutto il carico IT è protetto da un sistema UPS tri-ridondante in grado di assicurare il 100% di disponibilità (100% uptime);
- certificazione Tier4 (modalità "system + system" (2N+1));
- sistema basato su due impianti elettrici separati e totalmente indipendenti (Feed A e Feed B), ognuno dei quali può sostenere, in ogni momento, il carico dell'intera Facility;
- ogni impianto è dotato di un suo UPS (Uninterruptible Power Systems), System Bypass Modules, PDU (Power Distribution Units), RPP (Remote Power Panels) e altri componenti adeguati al livello di tiering;
- tutti i rack sono dotati di una doppia alimentazione, ognuna afferente a una "catena" di alimentazione (Feed A, Feed B).

Climatizzazione:

- l'impianto di raffreddamento si basa su un set modulare di AHU (Air Handling Unit) che sfruttano il principio del raffrescamento evaporativo indiretto tramite scambiatori aria-aria opportunamente raffreddati da sistemi ad acqua (esterni al DC);
- l'infrastruttura in acciaio, che sostiene il sistema T-SCIF, ha anche la funzione di volano termico, permettendo alla Facility di raggiungere livelli di resilienza superiori ai più elevati standard di settore.
- questi sistemi di ultima generazione permettono di misurare un PUE inferiore a 1,4.

Tali soluzioni consentono al DC di ospitare rack ad alta densità, fino a 40 kW, completamente raffrescati ad aria.

6.2.3 Sito di Roma

Alimentazione elettrica:

- l'alimentazione principale del Data Center è garantita da una fornitura a 20KV in singola via e doppio anello; ricevimento Media Tensione (M.T.) situato esternamente al corpo di fabbrica, in apposita struttura;
- gruppo elettrogeno da 1638 kVA in container, installato esternamente al fabbricato UPS (tempo di attivazione automatico < 10sec) con un serbatoio di stoccaggio carburante a doppia camera, avente una capacità di 10.000 litri;
- gruppi di continuità (UPS) ridondati al 100% garantiscono una potenza minima di continuità pari a 400kW. Sono in grado di fornire energia alle apparecchiature direttamente dalla rete elettrica, evitando il passaggio al raddrizzatore e alle batterie.

Climatizzazione:

- ciascun data Hall dispone di tre condizionatori perimetrali con potenzialità di 22,5 kW ciascuno per un totale di 67,5 kW frigoriferi;
- sono presenti due gruppi refrigeratori acqua in versione Freecooling per una potenza di 550 kW frigoriferi posti all'esterno degli edifici che ospitano il DC;
- in ogni Data Hall i rack sono stati disposti in file back-to-back realizzando così un'alternanza di corridoi caldi (quelli su cui si affaccia il retro dei rack) e corridoi freddi (quelli in cui gli apparati di ventilazione insufflano l'aria trattata).

6.3 Precisione del riferimento temporale

Gli eventi generati nell'ambito dei processi di elaborazione dei messaggi, delle ricevute e dei log, presso i punti di accesso, di ricezione e di consegna, sono corredati del relativo riferimento temporale. Gli eventi (generazione di ricevute, buste di trasporto, log, ecc.) che costituiscono la transazione di elaborazione del messaggio, presso i punti di accesso, ricezione e consegna, impiegano il riferimento temporale rilevato all'interno della transazione stessa. In questo modo l'indicazione dell'istante di elaborazione del messaggio è univoca all'interno dei log, delle ricevute, dei messaggi, ecc. generati dal server. Le indicazioni temporali rese disponibili all'Utente in formato leggibile sono espresse secondo l'ora italiana vigente (solare o legale) al momento cui si riferisce l'operazione. Il formato utilizzato per la data è "gg/mm/aaaa", mentre l'orario è espresso nel formato "hh:mm:ss", con indicazione delle ore secondo il sistema delle 24 ore. Al dato temporale è fatta seguire tra parentesi la "zona" ossia la differenza (in ore e minuti) tra l'ora legale e UTC. La rappresentazione di tale valore è in formato "[+|-] hhmm", dove il primo carattere indica una differenza positiva o negativa. Si considera come sorgente del riferimento temporale l'orologio di sistema, la cui precisione è garantita dalla sua sincronizzazione via NTP (Network Time Protocol) con INRiM (Istituto Nazionale di Ricerca Metrologica -http://rime.inrim.it/labtf/ntp/) che fornisce un servizio di sincronizzazione per sistemi informatici collegati alla rete Internet, basato su due server primari installati nel Laboratorio di Tempo e Frequenza Campione.

I server sono sincronizzati, tramite generatore di codice di data, dai campioni atomici a fascio di cesio utilizzati per generare la scala di tempo nazionale italiana UTC (IT). Lo scarto di tempo tra i server NTP e la scala di tempo nazionale italiana viene tenuto sotto controllo ed è normalmente inferiore ad alcuni millisecondi. La precisione di sincronizzazione ottenibile dipende dalla tipologia della rete e dalla distanza interposta tra il server (Network Time Protocol) e il calcolatore che si vuole sincronizzare; i valori di scarto tipici sono inferiori al millisecondo per sistemi appartenenti alla stessa rete e possono arrivare a qualche centinaio di millisecondi per reti remote.

Il Network Time Protocol (NTP) è uno dei metodi più accurati e flessibili per disseminare l'informazione di tempo e di data sulla rete Internet. Esso permette di sincronizzare e mantenere sincronizzati tra loro computer collegati tramite reti locali, metropolitane o addirittura mondiali (Internet) utilizzando una struttura di tipo gerarchico.

6.4 Gestione dei log dei messaggi

Il log dei messaggi è il registro informatico delle operazioni riguardanti le trasmissioni effettuate mediante Posta Elettronica Certificata che, come richiesto dalla normativa in vigore, è tenuto dal gestore.

6.4.1 Gestione dei log Servizio di Posta Elettronica Certificata

Nel presente paragrafo sono descritte le modalità di gestione dei log relativi al Servizio di Posta Elettronica Certificata (PEC).

Durante le fasi di trattamento dei messaggi presso i punti di accesso, di ricezione e di consegna, il sistema registra gli eventi e le operazioni rilevanti ai fini della tracciabilità del servizio.

Le informazioni relative agli eventi sono registrate nei sistemi di gestione dei log e comprendono, ove applicabile:

- 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;
- tipologia dell'evento (accettazione, ricezione, consegna, emissione di ricevute, errore, ecc.);
- codice identificativo dei messaggi correlati generati (ricevute, errori, ecc.);
- gestore mittente.

Le informazioni registrate nei singoli record sono determinate dalla tipologia di evento tracciato e dalle relative esigenze di elaborazione e tracciabilità del servizio.

6.4.2 Diritto alla portabilità dei dati

Ai sensi del Regolamento GDPR (cfr. cap. 10), l'interessato ha il diritto di ricevere i dati personali che lo riguardano, forniti al Titolare del trattamento e trattati nell'ambito dell'erogazione del servizio PEC, in un formato strutturato, di uso comune e leggibile da dispositivo automatico.

L'esercizio del diritto alla portabilità è consentito nei limiti e alle condizioni previste dall'art. 20 del GDPR e riguarda i dati personali trattati con mezzi automatizzati, qualora il trattamento sia basato sul consenso dell'interessato o sia necessario all'esecuzione di un contratto di cui l'interessato è parte.

Il diritto alla portabilità non si applica ai trattamenti necessari per l'esecuzione di un compito svolto nel pubblico interesse o connesso all'esercizio di pubblici poteri e non deve pregiudicare i diritti e le libertà altrui.

6.4.3 Archiviazione e Conservazione

Per aumentare l'efficienza e la velocità di trattamento, le informazioni che si riferiscono alle transazioni di Posta Elettronica Certificata sono mantenute dal sistema su un Data Base dedicato. Con cadenza giornaliera, alle ore 01:00, una procedura automatica estrae dal Data Base tutti i dati relativi alle transazioni di Posta Elettronica Certificata che si sono verificate tra le 00:00:00 e le

23:59:59 del giorno precedente. Le informazioni così raccolte costituiscono i log della Posta Elettronica Certificata.

La normativa vigente relativa ai log della Posta Elettronica Certificata stabilisce che:

- successivamente alla relativa estrazione, i log vengano marcati temporalmente allo scopo di garantirne l'integrità e l'inalterabilità;
- i log vengano mantenuti almeno per trenta (30) mesi a cura di ReeVo S.p.A.;
- i log e le buste di trasporto di messaggi PEC contenenti virus informatici vengano sottoposti a un processo di conservazione.

Per svolgere l'attività di marcatura temporale (Time Stamping Authority – TSA) ReeVo S.p.A. si è dotata di software specifico, certificato (SMART_TSP_LOG distribuito da Aruba PEC S.p.A.) e affidabile.

Per garantire la disponibilità dei log per il periodo richiesto, il processo di archiviazione si articola come segue:

- log marcati temporalmente sono sottoposti al processo di Conservazione Digitale, presso un ente qualificato da AgID tramite iscrizione al Marketplace dei Conservatori (Linee guida AgID 2022), nella fattispecie ad Archiva Group S.r.l.;
- log marcati temporalmente sono conservati su un sistema dedicato, secondo modalità idonee a garantirne l'integrità, la disponibilità e la riservatezza, anche ai fini della loro eventuale acquisizione da parte dell'Autorità giudiziaria, in conformità alla normativa applicabile e, ove pertinente, al Provvedimento del Garante per la protezione dei dati personali del 17 gennaio 2008;
- log marcati temporalmente sono inviati su un server di back up presso una sede diversa da quella da cui viene erogato il servizio.

Maggiori dettagli sul processo di Conservazione sono indicati nel "Manuale di Conservazione" di ReeVo S.p.A.

6.4.4 Reperimento e presentazione log

Su richiesta dei soggetti aventi diritto, sono rese disponibili le informazioni contenute nei log, così come individuate dall'allegato tecnico al DM 2/11/2005 [5] (il codice identificativo univoco assegnato al messaggio originale, la data e l'ora dell'evento, il mittente del messaggio originale, i destinatari del messaggio originale, l'oggetto del messaggio originale, il tipo di evento oggetto del log, il codice identificativo dei messaggi correlati generati, il gestore mittente).

Il processo di richiesta, reperimento e presentazione dei log prevede le seguenti attività.

Estrazione dei log richiesti dai soggetti autorizzati dalla Legge o Titolari tramite l'invio di un documento cartaceo o informatico con il quale richiede il recupero e la presentazione dei log. In base alla tipologia adottata la richiesta può essere inviata:

- tramite raccomandata A/R all'indirizzo:

  ReeVo S.p.A. - Servizio Clienti– Via Energy Park, 22 (Ed 4) 20871 Vimercate (MB) Italia.

  In questo caso la richiesta da parte dei Titolari deve essere effettuata su carta intestata e corredata da una copia di un documento di riconoscimento.

- Posta Elettronica Certificata all'indirizzo richiestalog.pec@pec.reevo.it utilizzando la propria casella di Posta Elettronica Certificata

La richiesta dev'essere corredata dai dati identificativi della e-mail per la quale si richiede l'estrazione dei log:

- data della trasmissione (invio/ricezione);
- indicazione del mittente (From/da) e del destinatario (TO/a);
- codice identificativo della trasmissione (facoltativo);
- parte dell'oggetto (facoltativo).

Di seguito i punti riguardanti il processo:

- l'estrazione dei log è eseguita mediante accesso ai server o agli archivi ottici da parte del personale tecnico ReeVo S.p.A. autorizzato;
- la presentazione dei log avviene tramite invio degli stessi all'indirizzo di Posta Elettronica Certificata del richiedente o, in alternativa, ad altro indirizzo specificato dal Titolare nella richiesta. Le informazioni rilasciate potranno essere utilizzate per gli usi consentiti dalla legge.

In ogni caso l'accesso ai log può avvenire anche su richiesta dell'Autorità Giudiziaria.

In tale accezione il processo di estrazione dei file di log potrà essere eseguito a partire dall'Archivio di Conservazione, come descritto nel "Manuale di Conservazione".

Ulteriori modalità di richiesta potranno essere comunicate anche attraverso il sito del Gestore.

7 Interoperabilità tra gestori

Al fine di garantire l'attività di monitoraggio continuo del servizio, è implementata una procedura automatizzata per la verifica periodica per il controllo dell'invio e della ricezione dei messaggi di Posta Elettronica Certificata verso gli altri Gestori qualificati.

In considerazione dell'evoluzione del quadro normativo e regolamentare applicabile ai servizi di recapito elettronico certificato, ReeVo mantiene la propria infrastruttura tecnologica costantemente adeguata ai requisiti applicabili e pianifica gli interventi evolutivi necessari, anche con riferimento all'adozione di sistemi di autenticazione a più fattori e all'integrazione con sistemi di identità digitale, ove previsti dalla normativa e dalle specifiche tecniche applicabili.

8 Misure di sicurezza, monitoraggio, continuità del servizio

8.1 Organizzazione del personale

Nell'ambito dell'organizzazione del servizio PEC è individuato un Responsabile del Servizio PEC, cui compete il coordinamento complessivo delle attività connesse all'erogazione del servizio. Sono inoltre individuate, in conformità all'art. 21 del Decreto del Ministro per l'Innovazione e le Tecnologie 2 novembre 2005, le seguenti figure responsabili:

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

Le figure sopra elencate possono avvalersi, nello svolgimento delle funzioni di propria competenza, di personale addetto e di operatori. Per il personale coinvolto nell'erogazione del servizio sono previste specifiche attività di formazione e addestramento, finalizzate ad assicurare il possesso delle conoscenze, delle competenze e dell'esperienza necessarie allo svolgimento dei compiti assegnati.

Contestualmente agli aggiornamenti apportati al sistema di Posta Elettronica Certificata, il Gestore provvede inoltre all'erogazione di specifiche attività di addestramento alle figure professionali interessate, in conformità a quanto previsto dall'art. 22 del Decreto 2 novembre 2005.

8.2 Approccio organizzativo

La continuità dell'erogazione del servizio di Posta Elettronica Certificata è garantita mediante misure tecnologiche e organizzative finalizzate ad assicurare l'affidabilità, la disponibilità e la sicurezza dell'infrastruttura, nonché mediante attività di supervisione e monitoraggio del sistema e procedure di escalation per la gestione delle anomalie e degli eventi che potrebbero comprometterne il corretto funzionamento.

Per procedure di escalation si intende l'esecuzione delle attività correlate alla risoluzione dei malfunzionamenti sugli elementi che compongono i moduli del sistema, per i quali sia necessario un passaggio al livello di competenza/responsabilità superiore.

Il processo di escalation è attivato all'accertata impossibilità di risolvere la problematica a un determinato livello di competenza/responsabilità (se il problema risulta chiaramente identificato ed esistono le condizioni per procedere alla sua risoluzione, il caso non viene scalato).

Attività da effettuare entro 60 minuti dal malfunzionamento:

Il personale preposto al servizio di Posta Elettronica Certificata, coordinato dal Responsabile dei Servizi Tecnici, rilevato il guasto/anomalia, identifica le azioni per il ripristino della situazione di esercizio.

Nella fattispecie il Responsabile dei Servizi Tecnici:

- informa il Responsabile del Servizio PEC;
- informa l'Help Desk di primo livello (HD) mediante apertura di Warning Trouble Ticket a cui dovranno essere correlati tutti i Customer Trouble Ticket generati dalle eventuali chiamate dei clienti;

- richiede l'intervento di ulteriori risorse specialistiche (altri sistemisti o reperibile di secondo livello se fuori orario base), se non è possibile procedere autonomamente;
- coinvolge l'eventuale fornitore interessato dal malfunzionamento in relazione alla tipologia del problema emerso;
- provvede, qualora le contromisure adottate fossero efficaci, a chiudere il Warning Trouble Ticket affinché Help Desk possa contattare tutti i clienti che hanno riscontrato problemi per comunicare l'avvenuta risoluzione.

Attività da effettuare entro 120 minuti dal malfunzionamento:

Il Responsabile dei Servizi Tecnici coadiuvato dal Responsabile del Servizio PEC si attiva per individuare le azioni più opportune da mettere in atto al fine di effettuare una stima dei tempi necessari al superamento del problema;

- avvio processo con comunicazione verso i clienti coinvolgendo gli enti preposti;
- chiusura processo con la risoluzione del problema registrandone la chiusura tramite i sistemi predisposti (chiusura ticket) al monitoring e alla gestione dei guasti.

Qualora il malfunzionamento risultasse imputabile a un incidente di sicurezza, è prevista la registrazione dell'evento nel "database degli Incidenti", tale registrazione è sottoposta ad analisi fino alla completa risoluzione dell'evento e al ripristino del servizio. L'evento viene, inoltre, segnalato ad AgID mediante gli appositi canali e strumenti messi a disposizione dall'Agenzia, nel rispetto delle modalità e delle tempistiche previste dalla disciplina vigente applicabile ai Gestori PEC.

8.3 Approccio tecnologico

Come già enunciato la piattaforma tecnologica utilizzata per il servizio di Posta Elettronica Certificata si basa su un'architettura completamente ridondata atta a garantire:

- affidabilità;
- disponibilità;
- sicurezza;
- scalabilità.

Di seguito sono riportati ulteriori aspetti tecnologici atti a garantire un'adeguata sicurezza del sistema di Posta Elettronica Certificata.

8.3.1 Firma

Le chiavi utilizzate da ReeVo S.p.A. per le operazioni di firma nel proprio servizio di Posta Elettronica Certificata sono generate all'interno di un apparato HW crittografico sicuro (HSM – Hardware Security Module), utilizzando l'algoritmo asimmetrico RSA con chiavi di lunghezza non inferiore a 2048 bit. Gli HSM sono totalmente dedicati al servizio e ridondati, in modo da garantire la sicurezza e l'affidabilità necessaria in caso di guasti.

8.3.2 Autenticazione

Il sistema di Posta Elettronica Certificata ReeVo S.p.A. prevede che tutti gli utenti siano autenticati con "username" e "password" personali sia per l'invio di e-mail sia per la ricezione delle stesse o con Autenticazione a due fattori (MFA).

Tale processo garantisce che il messaggio sia inviato da un Utente del servizio di Posta Elettronica Certificata i cui dati di identificazione siano congruenti con il mittente specificato al fine di evitare la falsificazione di questo ultimo.

8.3.3 Colloquio sicuro

Al fine di garantire l'inalterabilità del messaggio originale spedito dal mittente si realizza l'imbustamento e la firma dei messaggi in uscita dal punto di accesso e la successiva verifica in ingresso al punto di ricezione.

Il messaggio originale (completo di header, testo ed eventuali allegati) è inserito come allegato all'interno di una busta di trasporto.

La busta di trasporto firmata dal gestore mittente permette di verificare che il messaggio originale non sia stato modificato durante il suo percorso dal dominio mittente al dominio destinatario.

La sicurezza del colloquio tra mittente e destinatario prevede un meccanismo di protezione per tutte le connessioni previste dall'architettura di Posta Elettronica Certificata (tra Utente e punto di accesso ReeVo S.p.A., tra ReeVo S.p.A. e gli altri gestori, tra punto di consegna ReeVo S.p.A. ed Utente) attuato tramite l'impiego di canali sicuri.

L'integrità e la confidenzialità delle connessioni tra ReeVo S.p.A. e l'Utente sono garantite mediante l'uso di protocolli sicuri.

Il colloquio con gli altri gestori avviene con l'impiego del protocollo SMTP su trasporto TLS.

8.3.4 Sistema Antivirus e Antispam

Ulteriore elemento rilevante ai fini della garanzia della sicurezza dell'infrastruttura, è relativo all'architettura tecnico/funzionale del sistema di antivirus.

ReeVo S.p.A. utilizza un sistema Antispam e un sistema Antivirus ridondato su più Server che impedisce quanto più possibile il trasporto di virus all'interno di messaggi di Posta Elettronica.

Le configurazioni adottate sono tali per cui tutti i messaggi in cui viene rilevato un virus vengono gestiti per analizzare se sia opportuno consegnare un messaggio di non "accettazione/rilevazione/mancata consegna per virus informatico" o respingere/cancellare il messaggio nel rispetto della normativa vigente.

Il sistema effettua automaticamente controlli per verificare la presenza di aggiornamenti del prodotto di antivirus con cadenza oraria e, se disponibili, li rende immediatamente operativi.

8.3.5 Data Center - Standard di Sicurezza

Il Data Center utilizzato da ReeVo S.p.A., nel quale risiedono i server per l'erogazione del servizio di Posta Elettronica Certificata, è oggetto della certificazione UNI ISO/IEC 27001:2022 - UNI CEI EN ISO/IEC 27001:2024.

Il campo di applicazione di detta norma, riportato sul certificato è:

"Gestione delle infrastrutture fisiche e di connettività di Data Center e dei processi a supporto con particolare riferimento a continuità elettrica, temperatura, controllo degli accessi e sicurezza fisica. Erogazione dei servizi Cloud e posta elettronica certificata (PEC)". Ulteriore misura di sicurezza: i server dedicati all'erogazione del servizio sono installati in un'area segregata ricavata all'interno del Data Center. L'accesso a tale area è consentito al solo personale incaricato ed è controllato da un lettore di badge.

8.3.6 Back up dei dati

I sistemi di erogazione del servizio di Posta Elettronica Certificata sono soggetti a regolare backup. Le politiche di back up prevedono un salvataggio in forma incrementale con cadenza giornaliera; con cadenza settimanale è eseguito il back up di tipo Full. Il tempo di ritenzione dei salvataggi effettuati è di 1 (un) mese.

8.3.7 Monitoraggio

La disponibilità del servizio di Posta Elettronica Certificata è garantita da sonde e strumenti specifici per il controllo dei singoli elementi dei differenti moduli e per l'esecuzione dei test case afferenti ai diversi Servizi disponibili.

Le sonde/controlli agiscono a livello di singolo sistema/servizio in modo da rilevare i malfunzionamenti prima che questi causino l'indisponibilità dell'intero servizio.

Al rilevamento di un malfunzionamento il sistema invia una e-mail e un SMS ai sistemisti interessati affinché siano attivate le procedure di emergenza previste.

Il servizio PEC è garantito in modalità continuativa, 24 ore su 24 e 7 giorni su 7, per l'intero arco dell'anno.

8.3.8 Gestione delle emergenze

In qualità di Gestore di Posta Elettronica Certificata, e al fine di garantire i livelli di servizio previsti dal Decreto del Ministro per l'Innovazione e le Tecnologie 2 novembre 2005 [5], ReeVo ha predisposto un'infrastruttura tecnologica dedicata all'erogazione del servizio, secondo le modalità di seguito descritte.

- infrastruttura di virtualizzazione e Storage Area Network progettata e realizzata secondo criteri di alta affidabilità e ridondanza (vedi dettagli al paragrafo 6.1);
- gruppi di continuità distinti a supporto dei 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;
- le sedi di erogazione del servizio sono certificate UNI ISO/IEC 27001:2022 - UNI CEI EN ISO/IEC 27001:2024 (vedi dettagli al paragrafo 8.3.5);

È prevista, altresì, una procedura di "urgenza" a fronte di un evento disastroso.

Tale procedura prevede il coinvolgimento del gruppo di gestione delle emergenze, composto dai responsabili dell'organizzazione PEC, preposto all'analisi e determinazione della gravità dell'evento stesso; il gruppo di gestione delle emergenze ha la responsabilità e l'onere di predisporre le azioni necessarie per minimizzarne i danni e per fornire indicazioni sulle modalità e politiche da adottare per il ripristino del servizio. Per tali eventi straordinari sono individuate le funzionalità indispensabili a garanzia della minima interruzione del servizio e del rispetto dei requisiti di legge anche in relazione alla reperibilità delle informazioni registrate sui log dei messaggi.

Per gli eventi non catastrofici, la continuità del servizio è garantita mediante la ridondanza dei sistemi che consente di assicurare l'erogazione del servizio anche in caso di guasti hardware e durante gli interventi di aggiornamento e manutenzione hardware e software.

Nella misura in cui occorressero uno o più eventi, come sopra riportato, ReeVo S.p.A., in qualità di gestore qualificato, invierà le opportune comunicazioni ai Titolari, ai Reseller nonché informerà l'Agenzia per l'Italia Digitale, tramite i consueti canali di comunicazione in uso.

La gestione degli incidenti di sicurezza, dei malfunzionamenti e delle indisponibilità del servizio è effettuata nel rispetto della normativa vigente e delle disposizioni applicabili emanate da AgID e, ove applicabili, dall'Agenzia per la Cybersicurezza Nazionale (ACN).

Ove ricorrano i presupposti previsti dalla normativa applicabile, gli eventi sono notificati alle competenti Autorità mediante gli strumenti e i canali previsti, nel rispetto delle relative modalità e tempistiche.

Legenda Codici Identificativi delle difformità	
Codice	**Significato**
1	Comportamento anomalo non circoscritto
2	Comportamento anomalo circoscritto
3	Malfunzionamento bloccante
4A/4B	Malfunzionamento grave
5A/5B	Malfunzionamento
A	Evento rilevato direttamente dal Gestore
B	Evento rilevato da soggetti terzi

Note: il codice identificativo si compone di una parte numerica, identificativa della tipologia di disservizio e di una componente alfabetica, identificativa del soggetto rilevatore dell'evento.

Classificazione degli incidenti PEC

Le tipologie di disservizio sono classificate secondo quanto previsto dalla Tabella A della Circolare CNIPA n. 51 del 7 dicembre 2006, nell'ambito delle disposizioni applicabili alla vigilanza sui Gestori di Posta Elettronica Certificata.

La classificazione costituisce il riferimento per l'identificazione e la gestione degli eventi che possono compromettere, in misura diversa, il regolare funzionamento del servizio PEC.

Codice	Tipologia disservizio	Descrizione
1A/1B	Comportamento anomalo non circoscritto	Comportamento difforme dalle regole tecniche relative alle funzionalità di base del servizio PEC (trattamento del messaggio originario, ricevute e avvisi), il cui potenziale impatto non risulta circoscritto.
2A/2B	Comportamento anomalo circoscritto	Comportamento difforme dalle regole tecniche relative alle funzionalità di base del servizio PEC, il cui potenziale impatto risulta circoscritto.
3A/3B	Malfunzionamento bloccante	Malfunzionamento che impedisce, totalmente o parzialmente, l'utilizzo delle funzionalità essenziali del sistema PEC da parte degli utenti.
4A/4B	Malfunzionamento	Malfunzionamento, che in particolari circostanze, compromette totalmente o parzialmente l'utilizzo delle funzionalità del sistema PEC, determinando un impatto significativo sull'erogazione del servizio.
5	Malfunzionamento grave	Situazione che determina un degrado delle funzionalità del sistema PEC o un comportamento anomalo relativo a funzionalità secondarie, con esclusione delle funzioni essenziali del servizio (identificazione, trattamento del messaggio originario, ricevute, avvisi e buste).

9 Piano di cessazione

Qualora venga assunta la decisione di cessare l'attività di Gestore di Posta Elettronica Certificata, ReeVo S.p.A. provvede ad attuare le procedure previste dalla normativa vigente e dalle disposizioni emanate da AgID, assicurando la continuità delle attività necessarie alla gestione della cessazione e, ove previsto, al trasferimento del servizio a un Gestore sostitutivo.

In particolare, sono previste le seguenti attività:

- comunicazione all'Agenzia per l'Italia Digitale dell'intenzione di cessare l'attività, secondo le modalità e le tempistiche previste dalla disciplina vigente (cfr. nota dedicata alla "Modalità per la cessazione di un gestore iscritto nell'elenco pubblico dei gestori PEC");
- comunicazione ai Titolari delle caselle PEC della cessazione dell'attività e, ove individuato, del Gestore sostitutivo, nonché delle modalità operative per l'eventuale trasferimento del servizio;
- comunicazione agli altri Gestori PEC interessati, secondo le modalità previste dalla disciplina applicabile;
- pubblicazione sul sito istituzionale delle informazioni relative alla cessazione e alle modalità di gestione del servizio;
- informazione alle strutture di supporto tecnico e di assistenza alla clientela, affinché possano fornire ai Titolari le necessarie indicazioni;
- gestione e conservazione dei log e delle altre informazioni previste dalla normativa applicabile per il periodo stabilito dalla medesima;
- attuazione, alla data di cessazione, delle procedure previste per la dismissione delle chiavi di firma e dei relativi dispositivi, nonché delle ulteriori misure tecniche e organizzative necessarie alla cessazione del servizio.

Riferimento Normativo: *Agenzia per l'Italia Digitale (AgID), Istruzioni per la cessazione di un gestore PEC, pubblicato l'**8 novembre 2018***

10 Protezione dati personali

10.1 Informativa

Il trattamento dei dati personali effettuato da ReeVo S.p.A. nell'ambito dell'erogazione del servizio PEC è effettuato nel rispetto della normativa vigente in materia di protezione dei dati personali e, in particolare, delle disposizioni applicabili al servizio di posta elettronica certificata e ai servizi elettronici di recapito certificato.

La normativa di riferimento per il trattamento dei dati personali nell'ambito del servizio è rappresentata, per quanto applicabile, da:

- Regolamento (UE) 2016/679 (GDPR) 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;
- Decreto Legislativo 30 giugno 2003, n. 196, recante il Codice in materia di protezione dei dati personali, come successivamente modificato e integrato, in particolare dal D.Lgs. 10 agosto 2018, n. 101;
- D.Lgs. 10 agosto 2018, n. 101, recante disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento (UE) 2016/679;
- Regolamento (UE) n. 910/2014 (eIDAS) del Parlamento europeo e del Consiglio del 23 luglio 2014, relativo all'identificazione elettronica e ai servizi fiduciari per le transazioni elettroniche nel mercato interno, come modificato dal Regolamento (UE) 2024/1183;
- normativa nazionale e disposizioni tecniche applicabili al servizio di posta elettronica certificata e ai servizi di recapito certificato, nonché le pertinenti disposizioni e linee guida emanate dalle Autorità competenti.

Nell'ambito dei trattamenti connessi all'erogazione del servizio PEC sono individuate le seguenti figure:

- Titolare del trattamento: ReeVo S.p.A., con sede legale in Foro Buonaparte, 57 20121 Milano, per i trattamenti per i quali determina autonomamente le finalità e i mezzi del trattamento.
- Responsabile del trattamento: il soggetto, persona fisica o giuridica, autorità pubblica, servizio o altro organismo che tratta dati personali per conto del Titolare del trattamento, sulla base delle istruzioni impartite dal Titolare e nell'ambito di uno specifico contratto o altro atto giuridico previsto dalla normativa applicabile.
- Interessato: la persona fisica cui si riferiscono i dati personali oggetto di trattamento.
- Persone autorizzate al trattamento: i soggetti che, operando sotto l'autorità del Titolare del trattamento o del Responsabile del trattamento, sono autorizzati a trattare dati personali e hanno ricevuto adeguate istruzioni in merito alle modalità di trattamento, agli obblighi di riservatezza e alle misure di sicurezza da adottare.
- Amministratori di sistema: i soggetti incaricati di attività di gestione e manutenzione dei sistemi informatici e delle infrastrutture tecnologiche utilizzate nell'ambito del servizio, le cui funzioni possono comportare la possibilità tecnica di accesso ai dati personali trattati mediante tali sistemi. Gli amministratori di sistema sono individuati sulla base delle competenze e dell'esperienza possedute e operano nell'ambito di specifici profili di autorizzazione e secondo le procedure aziendali applicabili. Per tali figure sono adottate le misure previste dalla normativa e dai provvedimenti applicabili del Garante per la protezione dei dati personali.

ReeVo S.p.A. provvede alla formalizzazione delle autorizzazioni e all'attribuzione dei relativi profili di accesso, assicurando che ciascun soggetto possa accedere esclusivamente alle informazioni e alle risorse necessarie per lo svolgimento delle proprie funzioni.

Gli accessi ai sistemi e alle informazioni sono gestiti secondo il principio del minimo privilegio e sono soggetti alle misure di sicurezza e ai controlli previsti dalle procedure aziendali.

Il personale coinvolto nelle attività connesse all'erogazione del servizio è adeguatamente sensibilizzato sull'importanza di un corretto e responsabile trattamento dei dati personali ai quali può avere accesso nello svolgimento delle proprie mansioni, nel rispetto degli obblighi di riservatezza e delle disposizioni normative e aziendali applicabili.

Eventuali problematiche, richieste o segnalazioni relative alla protezione dei dati personali possono essere indirizzate a:

ReeVo S.p.A.

Servizio Clienti ReeVo

Via Energy Park, 22 (ed. 4) – 20871 - Vimercate (MB) – Italia

10.2 Procedura di riferimento

Trattamento dei dati personali

ReeVo S.p.A. fornisce al Titolare, unitamente alla documentazione contrattuale e secondo quanto previsto dalla normativa vigente, l'informativa relativa al trattamento dei dati personali, nella quale sono indicate le finalità e le modalità del trattamento, le relative basi giuridiche, i tempi di conservazione, i soggetti o le categorie di soggetti ai quali i dati possono essere comunicati, nonché i diritti riconosciuti agli interessati ai sensi del Regolamento (UE) 2016/679 (GDPR) e della normativa nazionale applicabile.

Il trattamento dei dati personali effettuato nell'ambito del servizio PEC è svolto nel rispetto dei principi di liceità, correttezza e trasparenza, limitazione delle finalità, minimizzazione dei dati, esattezza, limitazione della conservazione, integrità e riservatezza, nonché secondo quanto previsto dalla normativa vigente in materia di protezione dei dati personali.

In particolare, nell'ambito delle attività connesse all'erogazione del servizio:

- i dati personali sono raccolti presso l'interessato o presso soggetti legittimati a fornirli e sono trattati per finalità determinate, esplicite e legittime;
- sono trattati esclusivamente i dati personali adeguati, pertinenti e necessari rispetto alle finalità perseguite;
- le operazioni di trattamento sono effettuate esclusivamente per le finalità connesse all'erogazione, alla gestione e alla sicurezza del servizio PEC, nonché per l'adempimento degli obblighi previsti dalla normativa vigente;
- sono adottate adeguate misure tecniche e organizzative volte a garantire la sicurezza dei dati personali e a prevenire accessi, utilizzi, modifiche, divulgazioni o trattamenti non autorizzati;
- l'accesso ai dati personali è consentito esclusivamente ai soggetti autorizzati al trattamento e nei limiti delle funzioni e delle attività loro attribuite;
- ai soggetti autorizzati al trattamento sono impartite specifiche istruzioni in merito alle modalità di trattamento dei dati personali, agli obblighi di riservatezza e alle misure di sicurezza da adottare.

Finalità e base giuridica del trattamento

I dati personali forniti dall'interessato sono trattati da ReeVo S.p.A. per le finalità connesse all'instaurazione, gestione ed esecuzione del rapporto contrattuale e all'erogazione del servizio PEC, nonché per l'adempimento degli obblighi previsti dalla normativa applicabile.

I trattamenti sono effettuati sulla base degli specifici presupposti di liceità previsti dall'art. 6 del GDPR, in relazione alla natura e alle finalità del singolo trattamento. Tali presupposti possono comprendere, ove applicabili, la necessità di eseguire il contratto o di adottare misure precontrattuali, l'adempimento di obblighi di legge e il perseguimento di un legittimo interesse del Titolare, nel rispetto delle condizioni previste dalla normativa vigente.

Diritti degli interessati

Gli interessati possono esercitare i diritti previsti dagli articoli 15 e seguenti del GDPR, nei limiti e alle condizioni stabiliti dalla normativa vigente. In particolare, l'interessato ha diritto a ottenere la conferma che sia o meno in corso un trattamento di dati personali che lo riguarda e, in tal caso, di ottenere l'accesso ai propri dati personali e alle informazioni previste dall'art. 15 del GDPR; di ottenere la rettifica dei dati personali inesatti e l'integrazione di quelli incompleti; di ottenere, nei casi previsti dalla normativa, la cancellazione dei dati personali; di ottenere, nei casi previsti dalla normativa, la limitazione del trattamento; di ricevere i dati personali in un formato strutturato, di uso comune e leggibile da dispositivo automatico e di trasmetterli ad altro titolare, nei casi previsti dall'art. 20 del GDPR;

- di opporsi, nei casi previsti dalla normativa, al trattamento dei dati personali che lo riguarda;
- di opporsi in qualsiasi momento al trattamento dei dati personali effettuato per finalità di marketing diretto; di revocare il consenso eventualmente prestato, qualora il trattamento sia basato sul consenso.

I dati personali possono essere comunicati a soggetti terzi esclusivamente nei casi e nei limiti previsti dalla normativa applicabile, dal rapporto contrattuale o da specifici obblighi di legge, ovvero qualora la comunicazione risulti necessaria per l'erogazione del servizio e sia effettuata nel rispetto della normativa in materia di protezione dei dati personali.

Per esercitare tali diritti l'interessato dovrà inviare richiesta scritta a:

ReeVo S.p.A.

Servizio Clienti ReeVo

Via Energy Park, 22 (Ed 4) 20871 Vimercate (MB) – Italia.

10.3 Misure di sicurezza per la protezione dei dati personali

Come previsto dalle norme vigenti in materia, ReeVo S.p.A., in qualità di Titolare del trattamento, adotta almeno tutte le necessarie misure adeguate (GDPR art. 32) al fine di garantire sempre i seguenti principi relativi ai dati forniti dal cliente.

- Disponibilità: i dati sono sempre fruibili, quando è necessario, e sono ridotti al minimo i rischi di perdita o distruzione anche accidentali grazie ad un sistema di back up e di disaster recovery.
- Integrità: i dati sono difesi da manomissioni o da modifiche improprie da soggetti non autorizzati.
- Riservatezza: i dati sono accessibili solo da persone che hanno le credenziali per accedervi e sono protetti, quindi, da sistemi di identificazione con più punti di controllo.

10.3.1 Trasmissione e accesso ai dati da parte dell'utente

Si evidenzia che i messaggi di Posta Elettronica Certificata e il colloquio attraverso l'interfaccia Web o il Client utilizzato tra l'Utente e l'applicazione preposta avvengono attraverso protocolli e connessioni sicure come SMTP/S, IMAP/S, POP3/S e HTTPS (cfr. 8.3.3).

10.3.2 Misure di sicurezza per la protezione dei dati

Dal punto di vista tecnico ReeVo S.p.A., ha identificato le seguenti misure di sicurezza al fine di prevenire il rischio di distruzione, perdita, accessi non autorizzati ed errata trasmissione dei dati.

Misure di sicurezza fisiche individuate:

- antincendio – l'integrità fisica del personale e dei Data Center è garantita da meccanismi in grado di rilevare principi d'incendio, tramite rilevatori, allarmi automatici e un sistema centralizzato di controllo;
- continuità nell'alimentazione elettrica - per soddisfare tale esigenza si ricorre all'utilizzazione di diverse sorgenti di energia elettrica quali:
  - fornitura di energia elettrica da parte dell'ente erogatore;
  - fornitura di sorgenti autonome di energia in grado di sopperire in diverso modo ma comunque efficacemente alla eventuale mancanza di energia da parte dell'ente erogatore. (ad esempio, sorgenti di continuità assoluta, come UPS, e sorgenti di alimentazione di emergenza, come gruppi elettrogeni G.E.);
- perimetrazione/Antintrusione.

Principali misure adottate:

- Data Center fisicamente isolati;
- presidio con agenti di vigilanza 24 ore su 24, per sette giorni su sette;
- telecamere a circuito chiuso e archiviazione digitale delle riprese;
- controllo degli accessi: la limitazione dell'accesso con mezzi fisici è rappresentata da sorveglianza elettronica, serrature da sbloccare con schede magnetiche, carte intelligenti, chiavi classiche e barriere comandate a distanza.

Tutti coloro che intendono accedere e circolare all'interno delle sedi aziendali di ReeVo S.p.A. devono essere muniti di un tesserino di riconoscimento aziendale.

Misure di sicurezza di tipo informatico individuate.

Antivirus - Per minimizzare i danni che possono essere causati dai virus informatici ReeVo S.p.A. agisce con:

- politiche di prevenzione per impedire l'introduzione dei virus all'interno dell'azienda;
- politiche per la rilevazione della presenza dei virus all'interno di applicazioni, dati o boot record;
- politiche di rimozione di eventuali virus presenti;

Per il back up dei dati e restore - ReeVo S.p.A. adotta una serie di procedure mirate attraverso le quali viene periodicamente effettuata una copia di tutti i dati presenti nei sistemi su dispositivi opportuni.

In caso di guasto hardware dei dischi è quindi possibile "ripristinare" il sistema nello stesso stato in cui si trovava nel momento dell'ultimo back up. Le politiche di back up sono organizzate in maniera tale da poter disporre di uno storico e poter così recuperare lo stesso dato in più stadi.

I sistemi di back up sono posizionati in locali diversi da quelli che ospitano i sistemi con i dati. L'accesso fisico e logico ai sistemi di back up e al recupero dei dati è consentito esclusivamente a personale autorizzato;

- password - al fine di evitare che le informazioni vengano trattate e consultate da chi non ne sia preventivamente autorizzato e al fine di evitare possibili danni dovuti all'uso improprio (volontario o involontario) delle informazioni, sono previste formali procedure per l'allocazione dei diritti di accesso degli utenti, che potranno quindi accedere solamente ai dati per i quali sono abilitati.

  Identificazione e autenticazione è la tecnica che permette di riconoscere e verificare utenti o processi;

- formazione: al fine di adempiere quanto richiesto sia dal Decreto Legislativo 196/2003 [2], da tutta la normativa in materia e dalla norma ISO 27001, sono erogate a tutti gli autorizzati individuati e, comunque, a tutti i dipendenti della Società, sessioni di formazione volte a descrivere le parti principali del decreto e della normativa. Durante la formazione ad ogni struttura organizzativa sono impartite istruzioni differenziate a seconda dei trattamenti dei dati (comuni particolari e relativi a condanne penali) svolti nel corso delle attività lavorative. L'obiettivo è quello di annullare o, comunque, ridurre al minimo il rischio di trattamento non consentito o improprio dei dati.

Principali temi trattati nelle sessioni formative:

- interpretazione del Regolamento (UE) 2016/679 (GDPR) 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) [7];
- interpretazione del Decreto Legislativo 101/18 "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento (UE) 2016/679 (GDPR) 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";
- interpretazione della norma ISO 27001;
- descrizione del corretto utilizzo dei dati e dei trattamenti effettuati dalla struttura di cui il dipendente fa parte;
- livelli di classificazione dei documenti e loro corretta gestione;
- corretto utilizzo delle dotazioni microinformatiche al fine di prevenire usi impropri o non autorizzati dei dati (gestione password, utilizzo corretto dei file di memoria, aree condivise ecc.).