Servizio di Posta Elettronica Certificata
Manuale Operativo
Codice documento: ICERT-PEC-MO

Versione 2.13

InfoCert
GRUPPO TECNOINVESTIMENTI

SOMMARIO

1. Introduzione al documento

1.1 Novità introdotte rispetto alla precedente emissione

Versione/Release n°:	2.13	**Data Versione/Release**:	29/11/2019
Descrizione modifiche:	1. §4.1.3: aggiornati i dettagli relativi certificato digitale utilizzato nella firma dei log dei messaggi. 2. §4.7.3: specificata la modalità di impostazione delle credenziali di accesso in caso di intermediari 3. §4.5.4: aggiunto il paragrafo 4. §7.2: specificata la necessità di utilizzo TLS 1.2 5. Correzioni errori di formattazione minori		
Motivazioni:	Revisione periodica dei contenuti del presente Manuale Operativo.		

Versione/Release n°:	2.12	**Data Versione/Release**:	20/09/2018
Descrizione modifiche:	6. §7.1: aggiornato il rifermento normativo e il link all'informativa sulla privacy. 7. §2.2: aggiornata la sede operativa di Milano 8. §6.2.1 Aggiornati i massimali dell'assicurazione 9. Rimossa la menzione della possibilità di firma messaggi da webmail 10. Correzioni errori di formattazione minori		
Motivazioni:	Revisione periodica dei contenuti del presente Manuale Operativo.		

Versione/Release n°:	2.11	**Data Versione/Release**:	26/10/2016
Descrizione modifiche:	Correzioni varie di errori di battitura e di link con puntamenti sbagliati.		
Motivazioni:	Revisione periodica dei contenuti del presente Manuale Operativo.		

Versione/Release n°:	2.10	**Data Versione/Release**:	22/06/2016

Descrizione modifiche:	1. §2.2: aggiornata la sede operativa di Padova. 2. §4.5.3: tolto il concetto di spam sospetto e relativa gestione. 3. §4.1, §5.1: aggiornate dimensioni massime dei messaggi. 4. §5.1: tolto il vincolo relativo alla moltiplicazione tra dimensione del messaggio e numero di destinatari. 5. §5.1: tolto il vincolo di numero massimo destinatari in To 6. §7.1: aggiornato il link all'informativa sulla privacy.
Motivazioni:	§2.2: cambio indirizzo sede operativa di Padova. §4.5.3: dismissione della gestione dello spam sospetto. §4.1, §5.1: aumento limite minimo richiesto da AgID. §5.1: dismissione del vincolo di moltiplicazione. §5.1: dismissione del vincolo di destinatari in To. §7.1: nuovo link all'informativa sulla privacy.

Versione/Release n°:	2.9	**Data Versione/Release**:	18/09/2015
Descrizione modifiche:	7. §1.4: corrette le definizioni di Cliente, Richiedente; aggiunta la definizione di User-id; 8. §4.1: corretto il destinatario delle funzionalità Legalmail; 9. §4.1.1: modificati i livelli di servizio minimi; 10. §4.9: specificato che le richieste di revoca vengono conservate; 11. §4.10.1: corretto il proprietario delle informazioni aggiuntive di sicurezza e della password; 12. §7.1: sostituito il capitolo con il link all'informativa ai sensi e per gli effetti del D.L.vo n. 196/2003, "Codice in materia di protezione dei dati personali".		
Motivazioni:	§1.4, §4.1 e §4.10.1: revisione dei ruoli e responsabilità tra Richiedente, Titolare e Utilizzatore; §4.1.1: coerenza con l'evoluzione del servizio; §4.9: allineamento procedure; §7.1: evitare duplicazione di informazioni.		

Versione/Release n°:	2.8	**Data Versione/Release**:	26/08/2015

Descrizione modifiche:	1. §2.2: aggiornati i dati identificativi del gestore; 2. §2.2.2: aggiornati i riferimenti del responsabile del Manuale Operativo; 3. §4: rimossa la funzionalità di cifratura da webmail; 4. §4: precisazioni sulle modalità di utilizzo dei servizi aggiuntivi 5. §11.4: rimossa la posizione del sito di Disaster Recovery.
Motivazioni:	§2.2: aggiornamento dei dati; §4: funzionalità dismessa; §4: coerenza con lo stato di evoluzione dei sistemi operativi e dei browser §11.4: mantenersi generici sulla posizione della DR.

Versione/Release n°:	2.7	**Data Versione/Release**:	13/05/2015
Descrizione modifiche:	1. §4.9: aggiornato il link al modulo di revoca; 2. §4.10.2: aggiornata la procedura per la richiesta; 3. §4.11: aggiunti l'URL e gli host per gli accessi al provider unit "Zucchetti".		
Motivazioni:	§4.9 e §4.10.2: allineamento delle informazioni; §4.11: attivazione del provider unit "Zucchetti".		

Versione/Release n°:	2.6	**Data Versione/Release**:	13/02/2015
Descrizione modifiche:	1. §1.4: aggiunta la definizione di spam 2. §4.1: modificati i livelli di servizio minimi 3. §4.1.3: modificate le modalità di richiesta delle informazioni contenute nel log dei messaggi 4. §4.2: modificata la descrizione di casella chiusa 5. §4.5.3: corrette le modalità di contrasto allo spam 6. §4.9: aggiunti l'URL al modulo di disdetta e la specifica sull'avviso di revoca delle caselle 7. §4.11.2: specificati gli host e le porte per le connessioni sicure		
Motivazioni:	Prescrizione AgID del 08/10/2014. §4.1.3: aggiornamento delle procedure.		

Versione/Release n°:	2.5	**Data Versione/Release**:	01/09/2014

Descrizione modifiche:	1. §4.1: aggiunto limite numero cartelle IMAP 2. §4.2: modificato da "casella esclusiva" a "casella chiusa" 3. §4.3.1: tempo di accesso al log statistico portato da 2 a 3 mesi 4. §4.5.3: descritto trattamento per la limitazione dello spam in uscita 5. §4.7.1: specificato SLA di attivazione di una casella 6. §4.8: aggiornamento dei dati modificabili in autonomia dall'utente 7. §4.9: specificato SLA di disattivazione di una casella
Motivazioni:	Punti: • 1: refuso della versione precedente • 2: cambio denominazione • 3: modifica SLA • 4: nuove procedure per la limitazione dello spam in uscita • 5: informazione omessa nella versione precedente • 6: aggiornamento procedura • 7: informazione omessa nella versione precedente

Versione/Release n°:	2.4	**Data Versione/Release**:	23/04/2014
Descrizione modifiche:	1. Aggiornati § vari: variazione denominazione e sito DigitPA in AgID 2. aggiornato §4.1: limiti funzionali per casella standard, procedure per la richiesta di informazioni contenute nel log dei messaggi 3. rimosso §4.1.4: estrazione log del gestore InfoCamere 4. aggiornato §4.5: politiche di sicurezza del sistema 5. aggiornato §4.7.2: invio contratto tramite firma digitale on-line, pagamento tramite bonifico 6. inserito §4.8: definizione modalità di modifica dei dati della casella direttamente da parte del titolare 7. aggiornato §4.9: revoca delle caselle 8. aggiornato §4.10: forzatura della password		
Motivazioni:	Punti: • 1: variazione denominazione DigitPA in AgID • 2, 4, 5, 6, 7, 8: revisione periodica documento • 3: dismissione dei log del gestore InfoCamere		

Versione/Release	2.3	**Data**	01/10/2010

n°:		**Versione/Release**:	
Descrizione modifiche:	1. Tab. 2 § 2.2: modifica legale rappresentante 2. § 4.1 definizione limiti funzionali per casella standard 3. Modifica § 1.2 4. §1.3: aggiunto riferimento [9] 5. §1.5: variazione denominazione CNIPA in DigitPA 6. §2.2: modifica tabella 2 7. Aggiornamento §2.5.3 8. aggiornamento cap.4: utilizzo del sistema di PEC in luogo del corrispettivo cartaceo 9. §4.1 modifica funzionalità standard 10. § 4.3.1 e 4.3.2: modifica descrizione log statistico e di sistema 11. modifica § 4.3.3 e aggiunto § 4.3.4 12. § 4.9: modifica procedure di forzatura password 13. modifiche §4.10 sulla modalità di accesso al servizio 14. variazione § 4.10.1 15. modifica requisiti tecnici cap. 5 16. modifica § 5.2 17. variazioni § 7.1 18. eliminazione § 9.4 sulla conservazione dei log 19. § 4.2: modifica descrizione modalità pec esclusiva		
Motivazioni:	Punti: • 1: Variazione consiglio di amministrazione • 2,3,4,7,8,10,13,14,16,17,18: Revisione periodica documento • 4,10: variazione normativa su traffico telefonico e telematico • 5: variazione denominazione CNIPA in DigitPA • 6,17: variazione sede legale • 9,11,12,13,15,19: aggiornamento caratteristiche del servizio		

Versione/Release n°:	2.2	**Data Versione/Release**:	20/10/2009
Descrizione modifiche:	1. §1.4, §4.1.3, §4.7.2, §4.9 Aggiunta definizione documento di identità e specificato l'utilizzo di documenti ad essa equipollenti 2. §2.3.2 Modificato il riferimento al manuale operativo 3. Cap. 3 Aggiornamento dello schema e della descrizione 4. §4.5.1 Revisione delle informazioni contenute nella descrizione del servizio di monitoring		

	5. §4.5.2 Aggiornamento del paragrafo 6. §4.1 e §5.1 Aggiornata la dimensione massima del messaggio a 50 MByte
Motivazioni:	Punti: • 1: specificata la possibilità di utilizzare come documento di riconoscimento i documenti equipollenti alla carta di identità come da normativa • 2, 3: revisione e controllo del Manuale Operativo • 4, 5: spostamento dei sistemi di PEC in una nuova area dedicata ai sistemi InfoCert con aggiornamento dei sistemi di monitoring e storage/backup • 6: adeguamento per esigenze dei clienti

Versione/Release n°:	2.1	**Data Versione/Release**:	16/10/2008
Descrizione modifiche:	Modifica riferimento al call center al paragrafo		
Motivazioni:	utilizzato riferimento al sito www.legalmail.it		

Versione/Release n°:	2.0	**Data Versione/Release**:	24/06/2008
Descrizione modifiche:	1. Modifica a par. 2.3.1. Inserito riferimento alle condizioni generali del contratto in relazione alla validità delle versioni del Manuale Operativo. 2. Modifica par. 4.1.3. Aggiunta della possibilità per il titolare di invio delle richieste di accesso alle informazioni del log dei messaggi tramite fax oltre che tramite PEC (in caso il titolare non disponga più della casella). 3. Inserimento nel paragrafo 4.3.1 della durata del mantenimento del log statistico e dei log di sistema. 4. Modifica al 4.3.3 per rendere maggiormente chiari gli aspetti operativi e le responsabilità nella gestione di domini personalizzati. 5. Modifica a par. 4.7 degli indirizzi e-mail dell'assistenza. 6. Eliminati paragrafi "I sistemi utilizzati" e "Gli strumenti utilizzati" 7. Inseriti par. 4.8 e 4.9. Fornire informazioni agli utenti sugli aspetti relativi alla scadenza/revoca della casella e della forzatura della password. 8. Modifica paragrafo 5.1 (dimensione massima del messaggio). Il sistema permette un invio/ricezione di un messaggio con un allegato di dimensione massima di 30 Mbyte (quindi dimensione effettiva del messaggio di 45 Mbyte, tenendo conto delle		

	conversioni di formato)
Motivazioni:	Punti 1, 2, 3, 4, 6,7. Revisione e controllo del Manuale Operativo. Punto 5. Variazione delle caselle e-mail per l'assistenza. Punto 8. Adeguamento alle indicazioni del CNIPA sulle dimensioni minime dei messaggi.

Versione/Release n°:	1.1	**Data Versione/Release**:	18/02/2008
Descrizione modifiche:	Aggiunto paragrafo 4.1.4 Modificati riferimenti al call center al par. 2.2.2		
Motivazioni:	Aggiunta della procedura per l'accesso alle informazioni del log dei messaggi del Gestore cessato InfoCamere S.c.p.A. Variazione del numero del call center.		

Versione/Release n°:	1.0	**Data Versione/Release**:	18/07/2007
Descrizione modifiche:	Nessuna		
Motivazioni:	Prima emissione		

1.2 Scopo e campo di applicazione del documento

Il documento ha lo scopo di descrivere le regole e le procedure operative adottate da InfoCert nella conduzione del servizio di Posta Elettronica Certificata.
Il contenuto si basa sulle regole tecniche allegate al Decreto Ministeriale del 2 novembre 2005 recante "Regole tecniche per la formazione, la trasmissione, la validazione, anche temporale, della posta elettronica certificata" e della Circolare CNIPA sulle modalità per la presentazione delle domande di iscrizione nell'elenco pubblico dei gestori di Posta Elettronica Certificata.

Il presente manuale costituisce una integrazione di dettaglio alla informativa fornita ai titolari del servizio ai sensi dell'articolo 13 del D.Lgs. 196/03 e l'art. 13 del Regolamento (UE) 679/2016.

1.3 Riferimenti normativi e tecnici

Riferimenti normativi

[1] Decreto del Presidente della Repubblica 7 aprile 2003, n.137 (G.U. n.138 del 17 giugno 2003) e art. 13 del Regolamento (UE) 679/2016

[2] Decreto legislativo 7 marzo 2005, n. 82 (in G.U. n. 112 del 16 maggio 2005 - S.O. n. 93) - Codice dell'amministrazione digitale e successive modificazioni (nel seguito referenziato come CAD)

[3] Decreto del Presidente della Repubblica 28 Dicembre 2000, n. 445 (G.U. n. 42 del 20/2/2001) e sue modificazioni secondo DPR 137/2003 (nel seguito referenziato come TU)

[4] Decreto del Presidente del Consiglio dei Ministri 13 gennaio 2004 (G. U. n. 98 del 27/04/2004)

[5] Decreto Ministeriale del 2 novembre 2005 recante "Regole tecniche per la formazione, la trasmissione, la validazione, anche temporale, della posta elettronica certificata" (GU n.266 del 15/11/2005)

[6] Decreto Legislativo 30 giugno 2003, n. 196 (G.U. n. 174 del 29 luglio 2003) recante "Codice in materia di protezione dei dati personali"

[7] Circolare CNIPA 24 novembre 2005, n. CNIPA/CR/49, "Modalità per la presentazione delle domande di iscrizione nell'elenco pubblico dei gestori di posta elettronica certificata (PEC) di cui all'articolo 14 del decreto del Presidente della Repubblica 11 febbraio 2005, n. 68"

[8] 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.

[9] Recepimento normativo in tema di dati di traffico telefonico e telematico - 24 luglio 2008 - G.U. n. 189 del 13 agosto 2008" emesso dal Garante per la protezione dei dati personali.

Riferimenti tecnici

[10] RFC 1847 (Security Multiparts for MIME: Multipart/Signed and Multipart/Encrypted)

[11] RFC 1891 (SMTP Service Extension for Delivery Status Notifications)

[12] RFC 1912 (Common DNS Operational and Configuration Errors)

[13] RFC 2252 (Lightweight Directory Access Protocol (v3): Attribute Syntax Definitions)

[14] RFC 2315 (PKCS #7: Cryptographic Message Syntax Version 1.5)

[15] RFC 2633 (S/MIME Version 3 Message Specification)

[16] RFC 2660 (The Secure HyperText Transfer Protocol)

[17] RFC 2821 (Simple Mail Transfer Protocol)

[18] RFC 2822 (Internet Message Format)

[19] RFC 2849 (The LDAP Data Interchange Format (LDIF) - Technical Specification)

[20] RFC 3174 (US Secure Hash Algorithm 1 – SHA1)

[21] RFC 3207 (SMTP Service Extension for Secure SMTP over Transport Layer Security)

[22] RFC 3280 (Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List - CRL Profile)

[23] Information Technology – Open Systems Interconnection – The Directory: Authentication Framework; ITU-T Recommendation X.509 (1997) | ISO/IEC 9594-8

1.4 Definizioni

Vengono di seguito elencate le definizioni utilizzate nella stesura del presente documento. Per i termini definiti nelle norme sopra referenziate si rimanda alle definizioni in essi stabilite. Dove appropriato viene indicato tra parentesi graffe il termine inglese corrispondente, generalmente usato nella pubblicistica, negli standard e nei documenti tecnici.

Allegato/i:
i documenti tecnici che descrivono in maniera analitica il Servizio di posta elettronica certificata Legalmail e le condizioni per la prestazione degli stessi che costituiscono parte integrante e sostanziale del Contratto;

Autorità per la marcatura temporale {*Time-stamping authority*}
È il sistema software/hardware, gestito da un Certificatore accreditato, che eroga il servizio di marcatura temporale.

Avviso di mancata consegna – [5]

Avviso di non accettazione – [5]

Busta di anomalia – [5]

Busta di trasporto – [5]

Casella di posta elettronica certificata – [5]

Cliente
si identifica con la definizione di **Titolare:** il soggetto, ivi compresa l'impresa, per il quale viene attivato il Servizio di posta elettronica certificata Legalmail, identificato in base a quanto riportato nella Richiesta di attivazione;

Contratto
denominato anche "Contratto per l'attivazione del servizio di posta elettronica certificata Legalmail" indica le presenti Condizioni Generali di Contratto e i documenti ad esso allegati e gli atti richiamati che costituiscono complessivamente la disciplina dei rapporti tra le parti;

Dati di certificazione – [5]

Destinatario – [8]

Dominio di posta elettronica certificata – [5]

Firma elettronica – [TU]

Firma elettronica qualificata – [TU]

Firma digitale {*digital signature*} – [TU]

CAD – Codice dell'amministrazione digitale
Ci si riferisce al Decreto legislativo 7 marzo 2005, n. 82 (in G.U. n. 112 del 16 maggio 2005 - S.O. n. 93)

Gestore/Provider di posta elettronica certificata – [5]

Indice dei gestori di posta elettronica certificata – [5]

Log dei messaggi – [8]

Marca temporale – [4]

Messaggio di posta elettronica certificata – [8]

Messaggio originale – [5]

Posta elettronica – [8]

Posta elettronica certificata – [8]

Punto di accesso – [5]

Punto di consegna – [5]

Punto di ricezione – [5]

Regole tecniche
Allegato al DM 2 novembre 2005 [5], recante le norme tecniche per il trattamento dei messaggi di Posta Elettronica Certificata.

Ricevuta breve di avvenuta consegna – [5]

Ricevuta completa di avvenuta consegna – [5]

Ricevuta di accettazione – [5]

Ricevuta di avvenuta consegna – [5]

Ricevuta di presa in carico – [5]

Ricevuta sintetica di avvenuta consegna – [5]

Richiedente
È il soggetto che richiede al Gestore una casella di Posta Elettronica Certificata

Richiesta di attivazione
è la proposta del Cliente in cui viene richiesta l'attivazione del Servizio di posta elettronica certificata Legalmail;

Riferimento temporale – [8]

Servizio Legalmail
è il servizio in base al quale InfoCert assegna al Cliente delle caselle di posta elettronica certificata a valore legale Legalmail conformi alle caratteristiche specificate nell'Allegato tecnico al DM [5].

Spam
comunicazioni per l'invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale (v. artt. 7, comma 4, lett. b), 130, comma 1 e 140 del Codice in materia di protezione dei dati personali - D.Lgs. 30 giugno 2003, n. 196)

Titolare – [5]

User-id

identificativo dell'Utilizzatore che può essere usato, insieme alla password, come credenziale di autenticazione; si distingue tra:

- "user-id master": identificativo rilasciato al momento dell'attivazione e che ha il pieno controllo della casella;
- "user-id slave": identificativo secondario che può inviare e accedere alla casella ma non ne può modificare la configurazione.

Utente di posta elettronica certificata – [8]

Virus informatico – [8]

Tempo Universale Coordinato {*Coordinated Universal Time*}
Scala dei tempi con precisione del secondo come definito in ITU-R Recommendation TF.460-5

Ufficio di Registrazione
Ente incaricato dal Gestore a svolgere le attività necessarie al rilascio, da parte di quest'ultimo, delle caselle di Posta Elettronica Certificata.

Utilizzatore
soggetto a cui è assegnato dal Cliente l'utilizzo della casella di posta elettronica certificata Legalmail;

Documento di identità
Carta d'identità o documento ad essa equipollente (cfr. art. 35 comma 2 del TU) in corso di validità.

1.5 Acronimi e abbreviazioni

AgID - Agenzia per l'Italia Digitale: istituita con decreto legge n. 83, convertito nella legge n. 134/2012. Eredita le competenze del Dipartimento per la Digitalizzazione e l'Innovazione della Presidenza del Consiglio, dell'Agenzia per la diffusione delle tecnologie per l'innovazione, di DigitPA e dell'Istituto superiore delle comunicazioni e delle tecnologie dell'informazione per le competenze sulla sicurezza delle reti.

CNIPA – Centro Nazionale per l'informatica nella Pubblica Amministrazione – dal 29 dicembre 2009, ai sensi e per gli effetti dell'art. 2, comma 1 del D.Lgs. 177/2009, il Centro nazionale per l'informatica nella pubblica amministrazione (CNIPA) assume la denominazione: "DigitPA"

DPCM - Decreto del Presidente del Consiglio dei Ministri
Ci si riferisce al DPCM 13 gennaio 2004 recante "Regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti".

IETF - Internet Engineering Task Force
IETF è una comunità aperta ed internazionale di progettisti di rete, operatori, venditori e ricercatori coinvolti nell'evoluzione dell'architettura Internet e delle normali operazioni su Internet.

ISO - International Organization for Standardization
Fondata nel 1946, l'ISO è un'organizzazione internazionale costituita da organismi nazionali per la standardizzazione.

ITU - International Telecommunication Union

Organismo intergovernativo mediante il quale le organizzazioni pubbliche e private sviluppano le telecomunicazioni. L'ITU fu fondato nel 1865 e diventò l'ente regolatore per gli standard nelle telecomunicazioni.

LDAP – Lightweight Directory Access Protocol
Protocollo utilizzato per accedere al registro dei Gestori.

MX - Mail eXchange record
Entry in un "database di nomi di dominio che identifica il mail server responsabile per gestire le e-mail per quel dominio.

DNS - Domain Name System
È il servizio di ricerca del dominio. È un programma in grado di tradurre i nomi mnemonici utilizzati dagli utenti per identificare un sito, nei relativi indirizzi IP

Indirizzo IP
Indirizzo numerico che identifica gli elaboratori connessi alla rete.

PEC – Posta Elettronica Certificata

PIN – Personal Identification Number
Codice associato ad una smart card, utilizzato dal Titolare per accedere alle funzioni della carta.

TSA – Time Stamping Authority

TU – Testo Unico
Ci si riferisce al DPR n. 445/2000 e sue successive modificazioni, , *"Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa"*.

2. Generalità

L'uso sempre più frequente della posta elettronica in sostituzione dei tradizionali mezzi (posta, fax, corriere) pone la necessità di disporre di sistemi affidabili, sicuri ed adeguati a fornire le garanzie richieste dalle norme sulla documentazione amministrativa. Un complesso di norme e regolamenti ha, nel corso degli ultimi anni, definito le caratteristiche tecniche ed organizzative per dare ai messaggi di posta elettronica una valenza uguale alle tradizionali forme di comunicazione.

Il presente Manuale Operativo fornisce agli utenti le informazioni necessarie a valutare l'offerta di InfoCert come Gestore di un sistema di posta elettronica certificata, nonché a descrivere le modalità di accesso al servizio.

2.1 Identificazione del documento

Questo documento è denominato "Manuale Operativo" ed è caratterizzato dal codice documento: ICERT-PEC-MO
La versione e il livello di rilascio sono identificabili in calce ad ogni pagina.

2.2 Dati identificativi del gestore

InfoCert S.p.A. è il **Gestore di Posta Elettronica Certificata** (ai sensi del DM 2 novembre 2005 [5]) che gestisce uno o più domini di posta elettronica certificata, operando in conformità alle Regole Tecniche e secondo quanto prescritto dal Testo Unico dal CAD e dal DPR 68/2005 [8]. In questo documento si usa il termine Gestore per indicare InfoCert.

I dati completi dell'organizzazione che svolge la funzione di Gestore sono i seguenti:

Tabella 2

Denominazione Sociale	**InfoCert S.p.A. - Società soggetta alla direzione e coordinamento di Tecnoinvestimenti S.p.A.**
Sede legale	**Piazza Sallustio n. 9 - 00187 Roma**
Rappresentante legale	**Daniele Vaccarino** In qualità di Presidente del Consiglio di Amministrazione
Direzione Amministrativa	**Via Marco e Marcelliano 45, 00147 Roma**

N° Iscrizione Registro Imprese	**Codice fiscale e numero d'iscrizione: 07945211006** del registro delle imprese di ROMA Data di iscrizione: 09/04/2004
N° partita IVA	**07945211006**
Sito web	http://www.infocert.it http://www.legalmail.it/
Sede Operativa	Via Marco e Marcelliano 45, 00147 Roma **Piazza Luigi da Porto 3, 35131 Padova** **Via Carlo Bo 11, 20143 Milano**

2.2.1 Uffici di Registrazione

Le caselle PEC vengono commercializzate da InfoCert sia attraverso rete di vendita diretta, sia tramite partner.

2.2.2 Responsabilità del Manuale Operativo, contatto per utenti finali e comunicazioni

InfoCert è responsabile della definizione, pubblicazione ed aggiornamento di questo documento.

Domande, osservazioni e richieste di chiarimento in ordine al presente Manuale Operativo dovranno essere rivolte all'indirizzo e alla persona di seguito indicate:

InfoCert S.p.A.
Responsabile del Servizio di Posta Elettronica Certificata
Piazza Luigi da Porto 3
35131 Padova

Call Center: i riferimenti al Call Center Legalmail sono disponibili alla pagina http://help.infocert.it/
Web: http://www.legalmail.it
e-mail: infocert@legalmail.it

2.2.3 Sito WEB del gestore

Le informazioni relative ai servizi di Posta Elettronica Certificata offerti da InfoCert sono consultabili online al sito **http://www.legalmail.it**

2.3 Amministrazione del Manuale Operativo

2.3.1 Procedure per l'aggiornamento

Il Gestore si riserva di apportare variazioni al presente documento per esigenze tecniche o per modifiche alle procedure intervenute sia a causa di norme di

legge o regolamenti, sia per ottimizzazioni del ciclo lavorativo.
Ogni nuova versione del Manuale Operativo annulla e sostituisce le precedenti versioni, secondo quanto previsto nelle condizioni generali di contratto.

Variazioni che non hanno un impatto significativo sugli utenti comportano l'incremento del numero di release del documento, mentre variazioni con un impatto significativo sugli utenti (come ad esempio modifiche rilevanti alle procedure operative) comportano l'incremento del numero di versione del documento. In ogni caso il manuale sarà prontamente pubblicato e reso disponibile secondo le modalità previste.

Con frequenza non superiore all'anno, il Gestore esegue un controllo di conformità di questo Manuale Operativo al proprio processo di erogazione del servizio di Posta Elettronica Certificata.

Ogni variazione al manuale operativo sarà preventivamente sottoposta ad AgID prima della sua pubblicazione sul sito da parte del gestore.

2.3.2 Regole per la pubblicazione e la notifica

Questo documento è pubblicato in formato elettronico presso il sito Web del Gestore all'indirizzo: http://www.legalmail.it/manualeoperativo.pdf

2.3.3 Responsabile dell'approvazione

Questo Manuale Operativo viene verificato dal Responsabile del Servizio.

2.3.4 Conformità

I contenuti del presente Manuale Operativo sono pienamente rispondenti alla normativa relativa alla Posta Elettronica Certificata, con particolare riferimento alle regole tecniche descritte nel DPR [8], nel DM [5] e alle specifiche della Circolare CNIPA [7].

2.4 Rapporti con AgID

Il presente Manuale Operativo, compilato dal Gestore nel rispetto delle indicazioni legislative, è stato consegnato, in copia, ad AgID.

2.5 Standard di riferimento

2.5.1 Tecnologici

Per gli standard tecnologici si è fatto riferimento alla lista delle specifiche emesse dall'IETF (RFC) citate nei riferimenti.

2.5.2 Procedurali

Tutti i processi operativi del Gestore descritti in questo Manuale Operativo, come ogni altra attività del Gestore, sono svolti in modalità conforme al Piano

di qualità aziendale, conformemente allo standard ISO9001.

2.5.3 Sicurezza

Per assicurare la sicurezza del servizio di PEC, InfoCert utilizza tecniche e procedure basate su standard (*de jure* o *de facto*) internazionali e sulle norme specifiche esistenti in Italia.

Nella redazione e nella messa a punto delle procedure ci si è basati sugli standard:

- Information Technology Security Evaluation Criteria (ITSEC) v. 1.2
- Common Criteria for Information Technology Security Evaluation v 2.2
- ISO/IEC 17799 - Information technology -- Security techniques -- Code of practice for information security management
- UNI CEI ISO/IEC 27001:06 – Tecnologia delle Informazioni – Tecniche di Sicurezza – Sistemi di gestione della sicurezza delle informazioni – Requisiti.
- ISO IEC 27002:05 – Information Technology – Security Techniques – Code of practice for Information Security Management

I dispositivi crittografici utilizzati sono certificati FIPS 140-2 level 3.

3. Introduzione al servizio di posta elettronica certificata

La seguente rappresentazione grafica illustra schematicamente il servizio di posta elettronica certificata. Questa breve descrizione non vuole essere una descrizione tecnica esaustiva del servizio, ma vuole introdurre l'utente in modo semplice e intuitivo alle specificità del servizio di posta elettronica certificata. Di seguito, in questo stesso documento, sono approfonditi tutti i punti del servizio come richiesto dalla normativa sancita dal DM [5].

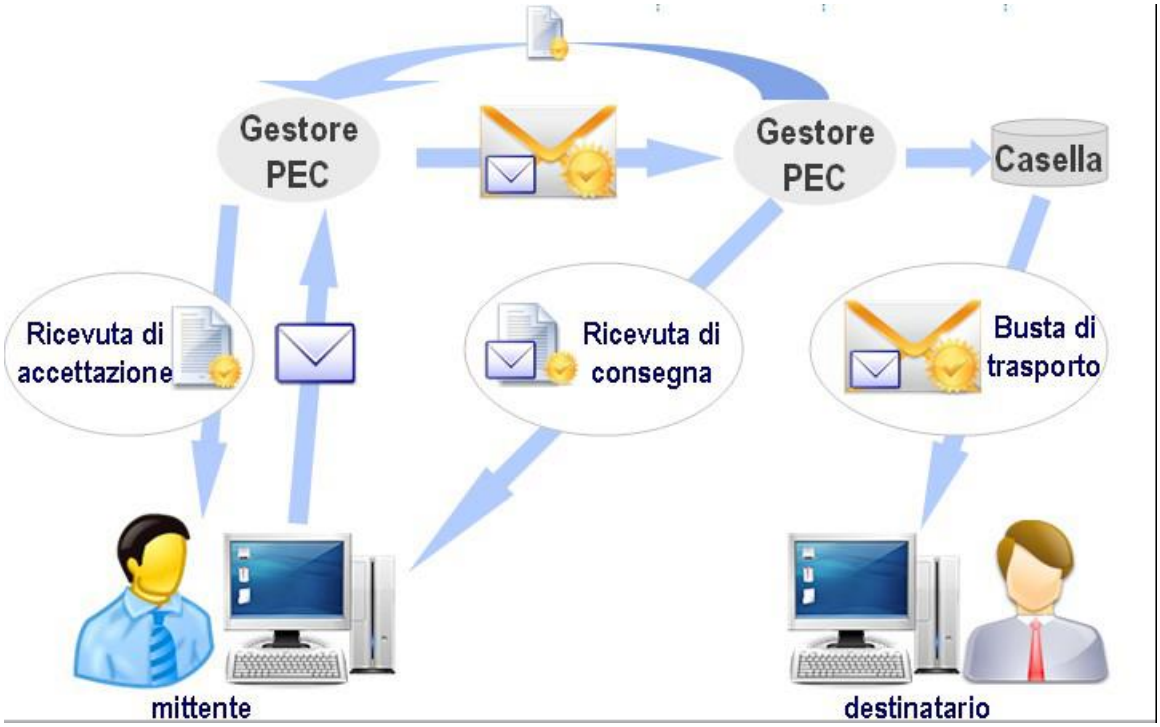

Figura 1

L'utente, 'mittente' dopo aver superato la fase di identificazione ed autenticazione al sistema che ne convalida le credenziali, è in grado di inoltrare un messaggio.

Il messaggio (la busta bianca in figura 1) raggiunge il sistema del proprio provider dove viene analizzato per verificare la sua conformità alle regole di posta elettronica certificata e, in caso positivo, è imbustato in un altro messaggio, a sua volta firmato dal gestore di posta, ed inoltrato verso la sua destinazione.

Il mittente riceve in questo caso la '*ricevuta di accettazione*' firmata dal proprio gestore ed ha così la prova che il suo messaggio è stato correttamente acquisito dal sistema.

Nel caso in cui il gestore non possa accettare il messaggio, il mittente riceverà un avviso ('*avviso di non accettazione*') con il motivo della mancata accettazione da parte del sistema.

La figura illustra il caso in cui mittente e destinatario appartengono a domini gestiti da provider diversi, pertanto il messaggio deve transitare dal dominio A al dominio B.

Il gestore del destinatario (dominio B) notifica con la '*ricevuta di presa in carico*' al gestore del mittente (dominio A) che ha preso in carico con successo il messaggio.

Il transito del messaggio è così tracciato, in modo da poter rispondere comunque al mittente riguardo all'iter percorso dal suo messaggio.

Il provider di posta del dominio B deposita il messaggio nella casella del destinatario e notifica il successo dell'operazione al mittente tramite la *'ricevuta di consegna*' che contiene anche in allegato il messaggio originale, a meno che il mittente non richieda diversamente.

Il messaggio è ora disponibile al destinatario che lo può leggere a sua discrezione.

In totale il mittente riceverà almeno 2 ricevute per ogni invio: una '*ricevuta di accettazione*' e una '*ricevuta di consegna*'.

Se il mittente invia un messaggio a più destinatari con un unico invio riceverà una *ricevuta di consegna* per ogni destinatario di pec, per cui normalmente le ricevute saranno in totale in numero pari al numero dei destinatari +1 (*ricevuta di accettazione*).

Nel caso in cui si verifichino eventi particolari (rilevazione virus, destinatari errati, ...) si possono ricevere altre segnalazioni.

L'emissione della ricevuta di consegna non è legata al fatto che il destinatario apra il messaggio o meno ed è rilasciata comunque quando il messaggio è depositato in casella; questa è una delle peculiarità del sistema di posta elettronica certificata.

Le notifiche dei sistemi di posta ordinari sono di fatto legate all'apertura del messaggio e alla volontà del mittente di far pervenire la notifica di avvenuta ricezione al mittente: una notifica di questo tipo non ha però il valore legale di opponibilità a terzi delle ricevute rilasciate e firmate da gestori accreditati.

4. Legalmail - il servizio di posta elettronica certificata di InfoCert

Il servizio di posta elettronica certificata che garantisce un elevato grado di affidabilità e sicurezza, è erogato da InfoCert sotto il nome Legalmail. Esso consente al Cliente di disporre di caselle di posta elettronica certificata, che permettono di comunicare con altre caselle di stessa tipologia sulla rete mondiale Internet.
Il servizio permette inoltre di inviare, ricevere e consultare i messaggi di posta elettronica ordinaria.
L'utilizzo di caselle di Posta Elettronica Certificata garantisce al cliente l'accesso sicuro alla propria casella di posta elettronica, sia attraverso un client di posta (Thunderbird, Outlook Express, ...), sia direttamente da Internet utilizzando i più comuni browser (il servizio viene definito Webmail).
Il servizio include l'invio nella casella del cliente delle diverse tipologie di ricevute descritte nel capitolo precedente.

Le caselle di posta elettronica certificata, diversamente dalle usuali caselle di posta elettronica, consentono l'invio di posta elettronica con valore legale in conformità di quanto previsto dalla normativa relativa alla Posta Elettronica Certificata.

Legalmail è pienamente conforme alle regole tecniche richiamate dal DM [5] e pubblicate da AgID sul sito http://www.agid.gov.it/ ; le caratteristiche di queste caselle sono pertanto tali da renderle interoperabili con le caselle di posta elettronica certificata distribuite da altri gestori di posta certificata accreditati.

Nei casi consentiti dalla legge, la posta certificata può essere utilizzata in sostituzione della posta cartacea. I messaggi ricevuti nella casella di posta certificata si intendono **pervenuti** al titolare della casella.

Si ricorda che la possibilità di utilizzare il sistema PEC in luogo dei corrispettivi cartacei è subordinata alla specifica normativa e, tra privati è al momento necessaria una preventiva dichiarazione da parte del destinatario di disponibilità all'utilizzo della posta elettronica certificata.

4.1 Funzionalità standard

Le funzionalità più rilevanti del servizio, in conformità alla normativa ufficiale, sono:

- invio al mittente di una ricevuta di accettazione per ogni messaggio in uscita che sia conforme ai requisiti normativi.
- inserimento dei messaggi in uscita dalla casella del mittente in una busta cosiddetta "di trasporto" firmata dal Gestore. La busta di trasporto è consegnata senza modifiche nella casella di posta di destinazione.
- emissione di una ricevuta di consegna per ogni destinatario al quale il messaggio risulta consegnato, se il messaggio è inviato ad una casella di posta elettronica certificata con valore legale (previsto da AgID)
- inserimento dei messaggi in ingresso, non provenienti da caselle di posta elettronica certificata, in una busta "di anomalia"
- la firma elettronica del Gestore del servizio di posta elettronica certificata sulle ricevute e sulla busta di trasporto che contengono sempre informazioni relative al messaggio time (ora), from (da), to (a), ecc.) sia in formato testo leggibile sia in

formato XML
- allineamento al tempo ufficiale coordinato (UTC) dell'ora delle ricevute e del messaggio di trasporto, a meno di un secondo
- invio, in allegato alla ricevuta di consegna al mittente, di tutto il messaggio originario (come prova di quanto ha spedito ed è stato consegnato) per ogni destinatario in "TO (A)", a meno di richiesta diversa da parte del mittente
- conservazione di un log degli eventi principali; il sistema mantiene traccia delle operazioni svolte, memorizzando su un registro i dati significativi dell'operazione: il codice identificativo univoco del messaggio (Message-ID), la data e l'ora dell'evento, il mittente del messaggio originale, l'oggetto del messaggio, etc.; il sistema non serba alcuna informazione che permetta di risalire al contenuto del messaggio dopo che l'utente ha scaricato e cancellato il messaggio dal server, a meno di disposizioni normative specifiche o di esplicita richiesta da parte del cliente (tramite adesione a servizi aggiuntivi).
- divieto di utilizzo dei destinatari nascosti (BCC o CCN)
- obbligo di almeno un destinatario in "TO (A)".
- ricevuta di presa in carico tra diversi provider di posta del circuito (non visibile agli utenti, ma fondamentale per tenere traccia dell'iter completo percorso dal messaggio)

Le precedenti funzionalità saranno soggette a tutte le variazioni necessarie in caso di evoluzione della normativa e delle disposizioni da parte del AgID.

InfoCert non assume alcuna responsabilità della corretta gestione dei messaggi da parte degli altri gestori di posta elettronica certificata.

InfoCert mette in grado il titolare di usufruire delle funzionalità elencate attraverso il servizio Legalmail che pertanto comprende:

- *rilascio della casella di posta elettronica certificata e relativa user-id per l'accesso*
- *assegnazione di una password e riassegnazione e cambio su richiesta*
- *accesso alla casella da client di posta*
- *spedizione di messaggi con client di posta*
- *accesso alla casella e spedizione di messaggi con webmail*
- *possibilità di firmare e cifrare i messaggi attraverso i client di posta (utilizzando dispositivi di firma e certificati emessi sia da InfoCert che da altri Enti Certificatori)*
- *possibilità di salvare da webmail i messaggi*
- *utilizzo del sito legalmail (www.legalmail.it) con informazioni di supporto*
- *call center per il supporto informativo*
- *presenza di un antivirus aggiornato che controlla i documenti e i messaggi in entrata e in uscita.*

Il servizio Legalmail garantisce:

- dimensione della casella di posta elettronica certificata non inferiore a 100 MB;
- dimensione massima del messaggio pari a 100 MB;

- la possibilità di definire sottocartelle interne che possono contenere sino a 5.000 messaggi ciascuna;
- fino a 50.000 messaggi in totale presenti nella casella;
- fino ad un totale di 500 cartelle/sottocartelle presenti nella casella.

Il Gestore si riserva la facoltà di inibire l'accesso al servizio in caso di superamento dei limiti sopra indicati o dove si verificassero situazioni che possano compromettere la sicurezza della casella o del servizio, come indicato nel § 4.5.

Eventuali esigenze specifiche troveranno soluzione in un accordo contrattuale che, partendo dalle caratteristiche elencate garantite a tutti gli utenti, potrà offrire maggiori servizi e/o volumi.

Il servizio di posta elettronica certificata InfoCert è conforme alle regole tecniche e organizzative indicate dalla normativa in riferimento, ed esattamente:

- DPR 11 febbraio 2005, n. 68, "Regolamento recante disposizioni per l'utilizzo della posta elettronica certificata";
- DM 2/11/2005 recante "Regole tecniche per la formazione, la trasmissione e la validazione, anche temporale, della posta elettronica certificata"
- Allegato tecnico al DM indicato al punto precedente "Regole tecniche del servizio di trasmissione di documenti informatici mediante posta elettronica certificata"

InfoCert si impegna inoltre ad adeguare tempestivamente il servizio alle eventuali variazioni normative.

4.1.1 Elaborazione dei messaggi

Il sistema garantisce il rispetto di tutte le regole previste per la posta elettronica certificata dai documenti in riferimento [8] e [5], in particolare delle norme riguardanti l'elaborazione e lo scambio di messaggi tra caselle di posta elettronica certificata elencate di seguito:

1. **la ricevuta di accettazione e la busta di trasporto, per l'invio**
   Il sistema di posta elettronica certificata notifica all'utente attraverso la ricevuta di accettazione il successo dell'invio di un messaggio, dato dal superamento di tutti i controlli formali e di contenuto (ad esempio viene controllata la presenza nel messaggio di virus informatici) e lo rende conforme al sistema 'imbustandolo' nella busta di trasporto.

2. **gli avvisi di non accettazione per eccezioni formali e per virus informatico**;
   Il sistema di posta elettronica certificata notifica all'utente la non accettazione del messaggio e la motivazione per cui è stato respinto (errore formale, presenza di virus nel messaggio sottomesso dall'utente).
   Un motivo di non accettazione di un messaggio per errore formale è, per esempio, la violazione della regola di posta elettronica certificata che non

permette l'utilizzo nel campo "From (Da)" di un indirizzo di e-mail diverso da quello proprio della casella dell'utente mittente cioè quella che corrisponde alle credenziali utilizzate per accedere al servizio. È inoltre necessario che vi sia congruenza tra il from (da) utilizzato a livello di protocollo SMTP ed il from (da) indicato all'interno del messaggio di posta.

3. **le ricevute di preso in carico;**
   i sistemi di posta elettronica certificata del circuito notificano l'uno all'altro la presa in carico del messaggio che transita tra domini diversi, per tracciare completamente l'iter del messaggio; queste ricevute non pervengono all'utente, ma solo ai gestori del servizio.

4. **La ricevuta completa di avvenuta consegna**
   L'utente riceve dal sistema di posta elettronica certificata un messaggio di notifica dell'avvenuto inserimento, del messaggio inviato, nella casella di posta elettronica certificata del destinatario. Nel caso usuale il sistema invia una ricevuta completa con, in allegato, i dati di certificazione e il messaggio originale per i destinatari diretti in 'to (a)'.

5. **La ricevuta breve di avvenuta consegna:**
   A richiesta dell'utente, in sostituzione della ricevuta completa, il sistema invia una ricevuta breve con, in allegato, i dati di certificazione ed un estratto del messaggio originale.
   È indispensabile che, in questo caso, l'utente conservi il messaggio originale se reputa che sia necessario dimostrare, oltre all'invio e alla avvenuta consegna del messaggio nella casella del destinatario, anche il contenuto del messaggio stesso.
   L'estratto del messaggio non è infatti leggibile di per sé, ma può essere associato tramite strumenti informatici (funzioni di hash), soltanto al messaggio che lo ha generato, rendendolo così opponibile a terzi.
   Nel caso il messaggio originale non sia disponibile o sia stato alterato anche in minima parte, viene meno l'opponibilità dello stesso.

6. **La ricevuta sintetica di avvenuta consegna:**
   Per destinatari di posta elettronica certificata in copia 'Cc' la notifica avviene tramite una ricevuta sintetica con in allegato solo i dati di certificazione.
   La ricevuta sintetica può essere richiesta anche per i destinatari in TO; in questo caso, tuttavia, si perde la certificazione sul contenuto dell'invio e rimane solo la certificazione sull'oggetto / data e ora / mittente / destinatario.
   Il motivo di non allegare ad ogni tipo ricevuta il messaggio originale completo risiede nell'obbiettivo di salvare spazio nella casella dell'utente, evitando di riempirla con messaggi potenzialmente molto onerosi e, nel caso di invii multipli, ridondanti.

7. **La busta di anomalia per i messaggi provenienti da caselle di posta non certificata:**
   Quando un messaggio non di posta elettronica certificata è recapitato ad una casella di posta elettronica certificata, viene inserito in una busta di anomalia per evidenziare l'evento, in modo che il destinatario possa distinguere agevolmente i messaggi certificati dagli altri. Normalmente l'anomalia è dovuta

al fatto che il messaggio di posta proviene da un mittente estraneo al circuito di posta elettronica certificata

8. L'avviso di rilevazione virus informatico:

Il servizio di posta elettronica certificata si pone come obbiettivo anche quello di garantire, in modo più efficace rispetto ai sistemi di posta ordinari, la sicurezza dei propri utenti anche dalla ricezione e propagazione di virus informatici.
Il Gestore controlla i messaggi di posta elettronica certificata in ingresso provenienti da altri gestori per verificare l'assenza di virus. I messaggi che contengono virus informatici non vengono inoltrati al destinatario e il Gestore genera un avviso di rilevazione virus da restituire al gestore mittente indicando come indirizzo quello specificato per le ricevute nell'Indice dei gestori di posta elettronica certificata, con l'indicazione dell'errore riscontrato. Questo messaggio non è inoltrato all'utente, ma è utilizzato dal gestore del mittente per notificare al proprio utente l'impossibilità di consegnare il messaggio.

9. Gli avvisi di mancata consegna, nei casi previsti:

Il mittente riceve sempre notifica dell'esito della spedizione di un messaggio. Nel caso il messaggio non possa essere recapitato, il mittente riceverà, da parte del gestore del destinatario, un **avviso di mancata consegna** con il motivo per cui il sistema non ha potuto depositare il messaggio nella casella di destinazione. Alcuni casi di errore, come un indirizzo errato e l'avviso che la casella di destinazione non ha lo spazio necessario per depositare il messaggio, forniscono all'utente delle indicazioni utili sulle azioni da intraprendere per poter inviare correttamente il messaggio.
Nel caso in cui il gestore destinatario non notifichi la "presa in carico" del messaggio entro 12 ore dalla sua spedizione, il mittente riceve, da parte del proprio gestore, un "avviso di mancata consegna per superamento dei tempi massimi previsti", ovvero una notifica che allerta sul possibile fallimento della consegna. Se il gestore destinatario non notifica la "consegna" entro le 24 ore successive alla spedizione, il mittente riceve, dal proprio gestore, un "avviso di mancata consegna".

10. La generazione di tutti i file xml previsti dalla normativa:

Questi file contengono dati che descrivono il messaggio (data e ora di invio, mittente, destinatario, oggetto, identificativo del messaggio etc.) e sono utilizzati dai sistemi di posta elettronica certificata per elaborazioni automatiche.

11. L'inserimento del riferimento temporale in tutti i messaggi/log previsti:

In tutti i messaggi / log previsti viene inserito un riferimento temporale. Il riferimento temporale utilizzato ha un errore inferiore al secondo rispetto al Tempo Universale Coordinato (UTC).

12. La conservazione per 30 mesi dei log con gli eventi principali riguardanti i messaggi in transito:

La normativa prevede che nel registro di log certificato siano registrate le seguenti informazioni:

- 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 (accettazione, ricezione, consegna, ricevute, errore, ecc.)
- il codice identificativo dei messaggi correlati generati (ricevute, errori, ecc.)
- il gestore mittente

La possibilità di reperire queste informazioni presso tutti i gestori di posta elettronica certificata garantisce all'utente la possibilità di avere, entro un periodo di 30 mesi dall'invio, gli elementi, opponibili a terzi, relativi all'invio effettuato, all'iter del messaggio e all'esito dell'invio stesso.

4.1.2 Conservazione delle informazioni presenti nel log certificato dei messaggi

Il registro di *log certificato* è un file in cui vengono registrate le operazioni svolte dal sistema di posta elettronica certificata.
Sono definiti nelle regole tecniche della posta elettronica certificata il formato e le informazioni da mantenere tramite il log certificato (log dei messaggi indicato nel DM [5], art. 10 e par. 6.2 del relativo allegato tecnico).

InfoCert garantisce il contenuto del file di log con:

- firma elettronica e marcatura temporale (giornaliera) del file di log certificato da parte del sistema di posta elettronica certificata;
- invio giornaliero dei file di log marcati e firmati al sistema di conservazione InfoCert per la conservazione dei documenti informatici, in conformità alle regole tecniche contenute nella Deliberazione CNIPA n. 11/2004. Il sistema di conservazione a norma prevede:
  - la conservazione sostitutiva, tramite invio telematico, di un documento analogico opportunamente digitalizzato o di un documento informatico;
  - l'esibizione per via telematica di un documento già conservato in modalità sostitutiva;
  - la responsabilità del procedimento, che comporta anche l'apposizione della marca temporale, della firma di controllo del procedimento effettuata tramite tecnologie di firma digitale e marcatura temporale digitale;
  - la conservazione su supporto ottico presso InfoCert di una copia di tutti i documenti inviati per la conservazione;

È possibile richiedere la visione delle informazioni contenute nel log certificato.

Con le dovute restrizioni derivanti dall'esigenza di garantire la protezione dei dati personali degli utenti, potranno essere forniti dei report estratti dal log certificato contenenti informazioni sul transito dei messaggi all'interno del sistema di posta elettronica certificata.

Per accedere alle informazioni contenute nel log certificato l'utente deve seguire la procedura descritta nella sezione successiva.

4.1.3 Procedura per la richiesta di informazioni contenute nel log dei messaggi

Il titolare della casella deve inviare all'indirizzo servizio_legalmail@legalmail.it, tramite la propria casella di posta elettronica certificata, una richiesta di informazioni contenute nel log dei messaggi, indicando le informazioni di cui necessita.

La richiesta deve essere così formulata:

Si fa richiesta al supporto del servizio di posta elettronica certificata "Legalmail" di InfoCert delle informazioni relative all'invio/ricezione dei messaggi identificati tramite le seguenti indicazioni:

- *periodo temporale* (obbligatorio, non antecedenti ai 30 mesi);
- *mittente* (facoltativo, se specificato si intende tutti i messaggi inviati da tale mittente verso la casella del richiedente);
- *destinatario* (facoltativo, se specificato si intende tutti i messaggi inviati dalla casella del richiedente verso tale destinatario)
- *solo i messaggi inviati dal richiedente / solo i messaggi ricevuti dal richiedente / sia i messaggi inviati sia i messaggi ricevuti dal richiedente*.

Il supporto Legalmail provvede all'invio delle informazioni richieste dall'utente presso la medesima casella utilizzata per l'invio delle richieste. Le informazioni estratte dai log verranno inviate in formato CSV (comma separated values), firmato in formato P7M con un certificato di firma automatica intestato al Responsabile del Servizio Legalmail. Le informazioni rilasciate potranno essere utilizzate dall'utente per gli usi consentiti dalla legge.
Il servizio di rilascio informazioni sui log è a titolo oneroso tranne quando diversamente concordato con il cliente.

4.2 Funzionalità in modalità PEC "chiusa"

Per particolari tipologie di caselle sarà possibile attivare il funzionamento della casella in modalità "PEC chiusa".
In questa modalità la casella accetta in ingresso solamente messaggi di posta elettronica certificata (inviati da altre caselle di posta certificata). I messaggi di posta elettronica tradizionale verranno quindi rifiutati dal sistema.

L'attivazione di questa modalità sarà riservata:

- ad alcune tipologie contrattuali di caselle come modalità standard ed unica;
- ad altri tipi di casella su richiesta degli utenti (configurazione tramite webmail).

4.3 Funzionalità aggiuntive

Nel servizio sono state inserite inoltre delle ulteriori funzionalità, per rendere più agevole e comprensibile all'utente l'utilizzo della posta elettronica certificata.

Le principali sono:

- nelle buste di trasporto, di anomalia e nelle ricevute viene inserito del testo aggiuntivo, rispetto al minimo previsto dalle regole tecniche, con l'obiettivo di aiutare gli utenti ad interpretare il significato di quanto stanno ricevendo;

- nel testo aggiuntivo delle ricevute di accettazione viene inserito l'identificativo originario del messaggio inviato dal mittente. Questo identificativo, per le regole di posta elettronica certificata, deve essere sovrascritto da un nuovo identificativo, apposto dal server di posta elettronica certificata per garantire l'univocità dell'identificativo dei messaggi originali accettati nel complesso dell'infrastruttura di posta certificata e per consentire una corretta tracciatura dei messaggi e delle relative ricevute.
  Qualora il client di posta elettronica che colloquia con il punto di accesso avesse già inserito un Message ID all'interno del messaggio originale da inviare, questo dovrà essere sostituito con l'identificativo sopra descritto. Al fine di consentire al mittente l'associazione tra il messaggio inviato e le corrispondenti ricevute, l'eventuale Message ID originale, se presente, sarà disponibile all'interno delle ricevute e della busta di trasporto e riportato nei Dati di certificazione [**5**].

- in webmail (se si richiede l'attivazione del servizio) sono state inserite delle particolari funzionalità per agevolare la lettura dei messaggi di posta elettronica certificata (che arrivano "imbustati"), per impedire l'invio di messaggi che poi sarebbero rifiutati per le regole di posta elettronica certificata (privi di "TO (A)", con "CCN"/"BCC") e per verificare la validità le firme dei gestori di posta elettronica certificata.

4.3.1 Log di sistema

I servizi e i prodotti che fanno parte dell'architettura del sistema d PEC, coinvolti nella erogazione del servizio, registrano informazioni relative al traffico dei messaggi in transito per permettere verifiche sullo stato del servizio o su eventuali malfunzioni.

Le informazioni dei registri dei log di sistema vengono mantenute dal gestore per un periodo massimo di sei mesi in ossequio a quanto previsto dal "Recepimento normativo in tema di dati di traffico telefonico e telematico - 24 luglio 2008 - G.U. n. 189 del 13 agosto 2008" emesso da Garante per la protezione dei dati personali.

4.3.2 Gestione domini certificati

InfoCert offre la possibilità di definire/personalizzare altri domini o sottodomini per le caselle di posta elettronica certificata. È anche possibile utilizzare dei sottodomini nell'ambito di domini già utilizzati per caselle di posta non certificata (il nuovo sottodominio certificato verrà gestito dai sistemi InfoCert).

Il cliente ha la possibilità di richiedere l'utilizzo di domini di posta diversi da quelli standard legalmail.it.

L'utilizzo di domini diversi può essere realizzato in modi diversi:

1. personalizzazione di un sottodominio interno a quelli nella disponibilità di InfoCert
2. personalizzazione di un sottodominio proprio

Il sottodominio interno ad InfoCert sarà configurato come un dominio di secondo livello del tipo <NOME_IMPRESA>.legalmail.it; gli indirizzi saranno quindi del tipo <CASELLA>@<NOME_IMPRESA>.legalmail.it (ad esempio, mario.rossi@acme.legalmail.it). <NOME_IMPRESA> è un nome che verrà proposto dal Cliente, ma deciso a discrezione di InfoCert, che si riserva la facoltà di rifiutare le proposte avanzate secondo quanto previsto al successivo paragrafo 4.7.1. del presente Manuale Operativo.

La personalizzazione di un sottodominio proprio, invece, consisterà nella configurazione di un dominio del tipo <SOTTO_DOMINIO>.<DOMINIO>.it (dove <DOMINIO>.it è un dominio esistente e gestito dal cliente); gli indirizzi saranno quindi del tipo <CASELLA>@<SOTTO_DOMINIO>.<DOMINIO>.it (ad esempio, mario.rossi@cert.acme.it). <SOTTO_DOMINIO> è un nome definito dall'utente e utilizzato come sottodominio del dominio principale.
In questo caso sarà a carico del Cliente fare in modo che siano configurati opportunamente i server DNS del gestore del dominio NOME_IMPRESA.it, in modo che la posta elettronica del sottodominio sia indirizzata verso i server di Legalmail.

È responsabilità del cliente il mantenimento della corretta configurazione dei domini a livello DNS. InfoCert provvederà ad eliminare dall'indice dei domini certificati i domini che non risulteranno, a fronte di verifica, configurati correttamente.
A fronte di ogni variazione, anomalia o ripristino dei record MX il cliente è tenuto a comunicare l'evento al gestore (utilizzare la casella servizio_legalmail@legalmail.it).
In mancanza di una comunicazione non può essere garantito il corretto espletamento del servizio.

Si fa presente che i domini/sottodomini utilizzati, in base alle regole di posta elettronica certificata, non possono essere utilizzati anche per caselle di posta non certificata.

InfoCert provvederà all'inserimento dei domini utilizzati nell'indice dei gestori di posta elettronica certificata. Questo indice, infatti, deve contenere, tra le altre cose, la lista di tutti i domini di posta elettronica certificata gestiti da ciascun operatore.

4.3.3 Personalizzazioni

Legalmail prevede alcune ulteriori funzionalità, offerte separatamente, che consentono la personalizzazione della modalità di accesso alle caselle Legalmail.

Gli elementi modificabili sono relativi a:

1. url di accesso all'interfaccia webmail. Il cliente o intermediario può richiedere l'attivazione di un accesso web personalizzato, quale ad esempio "https://webmail.nomeimpresa.it" o "https://pec.sitoordine.it", con il quale far accedere i propri utenti all'interfaccia webmail.

2. Indirizzo dei servizi SMTP, IMAP e POP3 per personalizzare la configurazione tramite client. Il cliente o intermediario può richiedere l'attivazione di servizi SMTP/IMAP/POP3 personalizzati, quali ad esempio "smtp.pec.nomeimpresa.it", oppure "imap.pec.sitoordine.it", per permettere di personalizzare la configurazione dell'accesso tramite client alle proprie caselle.

3. personalizzazione grafica della interfaccia webmail. La personalizzazione grafica di Webmail consiste nella possibilità di modificare alcuni elementi grafici, per gli utenti di un dominio diverso da quelli standard (vedi par. 4.3.3), oppure per l'accesso tramite url personalizzato (vedi punto 1). Gli elementi modificabili sono: le immagini (banner) nella parte superiore delle pagine; i colori di molti degli elementi delle pagine

È responsabilità del cliente il mantenimento della corretta configurazione DNS delle url personalizzate richieste (punti 1 e 2), ove il dominio utilizzato non sia sotto la diretta responsabilità di InfoCert.

L'accesso tramite servizi personalizzati garantisce comunque l'utilizzo di protocolli protetti (HTTPS per l'accesso Webmail, SMTPS o SMTP STARTTLS per l'invio da client, IMAPS o POP3S per accesso e consultazione della casella).

InfoCert si riserva la facoltà di rifiutare l'attivazione di servizi o l'inserimento di materiali che possano creare problemi alla fruizione del servizio (ad esempio abbinamenti di colori senza contrasto che rendano difficilmente leggibili alcune diciture o immagini di dimensioni non compatibili con la struttura della pagine di webmail), nonché l'attivazione di servizi o inserimento di materiali che possano recare offesa o configurare violazioni di legge, fermo rimanendo che InfoCert non assume, salvo il caso di dolo o colpa grave, responsabilità in merito al controllo sugli elementi forniti dal Cliente e sulla legittimazione al loro uso da parte di quest'ultimo.

Questi servizi opzionali di Legalmail non prevedono lo sviluppo di nuovi elementi grafici o nuove soluzioni, ma si limitano ad applicare quanto ricevuto dal cliente.

4.4 Autogestione delle caselle

L'autogestione delle caselle consiste nella possibilità, data al Cliente, di gestire e aggiornare in autonomia le proprie caselle Legalmail, in un dominio diverso da quello standard.
L'autogestione delle caselle viene valutata da InfoCert in funzione della specifica situazione del cliente che la richiede.

InfoCert si riserva la facoltà di non fornire questo servizio opzionale. Alcuni esempi, non esaustivi, di motivi per cui l'autogestione può essere rifiutata sono:

1. il Cliente richiede la definizione di un numero esiguo di caselle;
2. il Cliente non fornisce le garanzie di affidabilità e sicurezza necessarie per gestire in proprio funzioni come la definizione di utenze e caselle di posta.

4.5 La sicurezza del sistema di posta elettronica certificata InfoCert

InfoCert aggiorna ed integra con continuità i propri sistemi di sicurezza.

I sistemi di posta elettronica certificata si propongono di garantire:

- la sicurezza del sistema attraverso sistemi duplicati e firewall
- la sicurezza degli accessi basati su invio della password protetta e/o accesso via certificati digitali su dispositivi di firma
- la sicurezza del messaggio con colloquio protetto (con il cliente e con gli altri gestori), supporto di firma e crittografia da dispositivi di firma e controllo antivirus per tutta la posta in transito
- l'invio di messaggi di posta elettronica certificata nel rispetto della normativa, che prevede l'invio di specifiche ricevute di accettazione e di consegna.

Per realizzare il sistema di posta elettronica certificata sono stati integrati strumenti di mailing e componenti applicative per il controllo del messaggio e l'invio delle specifiche ricevute.

Il Gestore si riserva la facoltà di mettere in atto azioni sulle caselle e sull'accesso al servizio, dove si verificassero situazioni che possano compromettere la sicurezza delle caselle o del servizio stesso.

4.5.1 Servizio di monitoring

Per verificare la disponibilità del prodotto sono state attivate sonde web e strumenti di Event Management che, a fronte di componenti non disponibili, provvedono ad allertare sistemisti ed operatori.

Vengono utilizzate due sonde automatiche realizzate allo scopo:

- una sonda che simula il comportamento di un utilizzo dell'utente da client di posta: invia un messaggio e attende le opportune risposte, controllandone la coerenza con quanto inviato;
- una sonda che simula il comportamento di un utente che accede al WebMail: la sonda accede infatti all'applicazione web, si autentica, esegue una serie di operazioni sulla casella ed esegue il log-out.

Ognuno di questi strumenti, qualora rilevi un malfunzionamento, invia un messaggio di alert gestiti per assicurare la migliore risposta all'utente.

Le segnalazioni delle sonde vengono analizzate dal processo di Problem

Management aziendale (procedura inclusa nelle procedure aziendali certificate Vision 2000); il processo prevede la produzione di specifici output.

4.5.2 Backup dei dati

In analogia con quanto previsto per le Certification Authority, anche per i sistemi di posta sono eseguiti regolarmente i backup dei file system, utilizzati dalle diverse piattaforme presenti all'interno del CED.

InfoCert fa uso delle più moderne infrastrutture per l'esecuzione di salvataggi dei contenuti dei dischi. I prodotti utilizzati per la gestione dei backup controllano e gestiscono l'esecuzione dei salvataggi e la loro archiviazione.
Le politiche di backup prevedono salvataggio delle caselle di posta con frequenza settimanale; è inoltre previsto un salvataggio incrementale giornaliero.

Il tempo di ritenzione di un salvataggio è mensile salvo casi specificatamente individuati.

4.5.3 Antivirus e contrasto allo spam

Tutti i sistemi di posta sono dotati di antivirus, sia per la posta in ingresso sia per la posta in uscita.
Gli antivirus adottati sono installati sui sistemi di front end, le configurazioni adottate sono tali per cui tutti i messaggi con virus rilevati vengono comunque consegnati al motore di PEC 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 e, se disponibili, li rende immediatamente operativi.

Il servizio offre un sistema di antispam che opera su tutti i messaggi. L'antispam è installato sui sistemi di front-end e la configurazione adottata è tale per cui tutti i messaggi rilevati come spam vengono comunque consegnati al motore di PEC. Vengono poi attivati controlli e azioni dipendentemente se il messaggio è in ingresso o in uscita.

Per i messaggi in ingresso, l'utente destinatario può scegliere l'opzione più opportuna alle sue esigenze tramite l'interfaccia web. L'utente può scegliere se spostare i messaggi marcati come spam nella sottocartella "Posta Indesiderata" oppure eliminarli. Non è data facoltà all'utente di disabilitare completamente il controllo dello spam.

Per i messaggi in uscita, viene tenuta traccia in un apposito log su database della loro individuazione. Tale log viene scansionato periodicamente: se risultasse che una casella ha inviato più di 180 messaggi di spam in un'ora, tale casella verrà bloccata modificando la sua password. La nuova password verrà comunicata all'utente tramite e-mail o un SMS ad uno dei suoi riferimenti di contatto.

Con questa operatività si vuole contrastare gli invii di spam eseguiti grazie al furto di credenziali operato tramite phishing o malware.
Le caselle possono essere bloccate tramite modifica della password anche nel caso di rilevazione di attività sospetta di furto d'identità quali, per esempio, l'invio ad intervalli regolari di messaggi vuoti o dal contenuto irrilevante per il monitoraggio della validità delle credenziali acquisite.

4.5.4 Monitoraggio e gestione accessi sospetti

InfoCert effettua un monitoraggio continuo degli accessi alle caselle PEC tramite tutti i protocolli consentiti (webmail, IMAP4s e POP3s) al fine di identificare possibili accessi non autorizzati da parte di malintenzionati o malware/bot.
Alcuni dei criteri utilizzati per questa attività sono:

- Reputazione dell'IP di connessione
- Geo localizzazione dell'IP di connessione
- Verifica dei tentativi errati in correlazione con le credenziali utilizzate
- Sequenze di operazioni sospette

In caso ci sia il ragionevole sospetto che una casella sia stata oggetto di accesso non autorizzato, la stessa viene:

- bloccata tramite modifica della password
- inviata sull'email secondaria comunicazione più link di reimpostazione credenziali
- avvertito il customer care InfoCert e l'eventuale intermediario

Il blocco inibisce sia l'invio che l'accesso manon ha effetto sulla ricezione di nuovi messaggi e sul contenuto della casella al momento del blocco stesso.

4.6 Modalità dell'offerta

Il servizio di posta elettronica certificata viene offerto sotto forma di caselle attestate su un dominio inserito nell'apposito indice presso AgID

L'offerta comprende:

- caselle appartenenti a domini già di proprietà di InfoCert (per esempio: legalmail.it)
- caselle appartenenti a sottodomini scelti dall'utente, all'interno di domini già di proprietà di InfoCert (per esempio: *nomecliente*.legalmail.it)
- caselle appartenenti a domini nella disponibilità del cliente.

È consentito pertanto ai clienti di utilizzare anche sottodomini di domini in loro possesso.
In questo caso si richiede al cliente che il gestore del suo dominio inserisca un opportuno record **MX** nei suoi server **DNS** in modo che la gestione della posta elettronica del dominio venga indirizzata verso il sistema di posta elettronica certificata di InfoCert.

La responsabilità della corretta configurazione **DNS** è esclusiva competenza del cliente.

Tutte le caselle, salvo diverso accordo con l'utente, sono accessibili:

- tramite interfaccia web offerta con il prodotto (webmail)
- tramite i più diffusi protocolli sicuri per la posta elettronica; questo permette l'utilizzo della casella sia con i normali strumenti presenti comunemente nelle stazioni di lavoro (per esempio Outlook Express) sia da parte di applicativi del cliente

Il prodotto webmail fornisce, tra le altre, le seguenti funzionalità:

- lista dei messaggi in arrivo, ordinamento lista
- consultazione e download del messaggio e dei suoi allegati
- ricerca messaggi nelle cartelle
- gestione cartelle
- rubrica indirizzi e certificati
- gestioni opzioni principali del servizio
- filtri

Su richiesta dell'utente InfoCert può rilasciare caselle con caratteristiche particolari come, ad esempio, caselle che rifiutino tutti i messaggi in ingresso di posta non certificata.

Il prezzo di riferimento dell'offerta è quello previsto nel sito www.legalmail.it per la singola casella e caratteristiche descritte nel sito stesso.
Su questo prezzo InfoCert può praticare sconti di diversa consistenza in base ad elementi di vario genere. Le caselle hanno tutte le funzionalità e le caratteristiche previste per la posta elettronica certificata.

Tra le altre caratteristiche principali vi sono (a meno di richieste in senso contrario da parte dell'utente):

- un sistema di antispam
- la possibilità di accedere a webmail utilizzando sia user-id e password sia un certificato digitale
- il supporto di un call center disponibile sia tramite telefono sia tramite e-mail (vedi par. 2.2.2 per i dettagli)

L'offerta prevede anche la possibilità di personalizzare alcune caratteristiche delle caselle. Tali personalizzazioni sono soggette a condizioni economiche separate. A titolo di esempio si citano:

- la personalizzazione di alcuni elementi grafici nell'interfaccia webmail, per tutte le caselle di un dominio
- lo spazio disco aggiuntivo rispetto allo standard

Inoltre, InfoCert può fornire altri servizi complementari eventualmente richiesti dal cliente come, ad esempio, l'integrazione della casella in altri servizi offerti da InfoCert.

4.7 Modalità di attivazione e accesso al servizio

InfoCert mette a disposizione di nuovi utenti o utenti esistenti varie modalità per effettuare le seguenti richieste relative al servizio di posta elettronica certificata:

- richieste nuove caselle
- rinnovi caselle
- attivazioni servizi aggiuntivi
- revoca caselle

Legalmail viene commercializzata da InfoCert sia attraverso rete di vendita diretta, sia tramite partner: le modalità possono sono diverse a seconda della quantità di caselle richieste e della tipologia del cliente.

Per ricevere informazioni di dettaglio il Richiedente può scrivere a: legalmail@infocert.it.

È possibile acquistare le caselle anche attraverso il sito www.legalmail.it

4.7.1 Attivazione del servizio

Il servizio di posta elettronica certificata InfoCert è attivato attraverso l'acquisizione di una casella di posta appartenente al dominio certificato di InfoCert.

InfoCert si riserva la facoltà di rifiutare i nominativi proposti dal cliente laddove si verifichino le seguenti ipotesi, che si riportano a mero titolo esemplificativo: omonimie, nomi molto lunghi, nomi molto simili tra loro, nomi molto simili a marchi noti, nomi riservati ad Enti ed Istituzioni pubblici, ecc.

Le modalità per le richieste di attivazioni sono le seguenti:

- richiesta diretta tramite sito www.legalmail.it
- richiesta tramite intermediario autorizzato di InfoCert
- richiesta tramite il personale commerciale InfoCert.

La nuova casella viene attivata entro due giorni lavorativi dal complemento della richiesta.

4.7.2 Richiesta attivazione casella acquistata via sito Legalmail (www.legalmail.it)

Per le caselle acquistate dal sito non sono previste personalizzazioni (utilizzo di

particolari domini ecc..) pertanto saranno definite nel dominio legalmail.it.

Il flusso per la richiesta della casella è il seguente:

1) Formulazione della richiesta.

L'utente compila online le informazioni necessarie per la richiesta (compreso il nome della casella) – la comunicazione avviene con modalità sicura (canale crittato HTTPS)

Nelle pagine del sito è presente la documentazione di cui l'utente deve preventivamente prendere visione:

- Condizioni generali
- Richiesta di Attivazione
- Allegato al contratto
- Informativa sul trattamento dei dati personali

Se la richiesta si conclude positivamente, la procedura rilascia all'utente le informazioni relative alla casella e al codice di attivazione (la casella viene riservata ma NON attivata fino al completamento del flusso).

2) Invio del contratto.

Il titolare deve a questo punto compilare il contratto, firmarlo ed inviarlo ad un centro di raccolta predisposto (presso InfoCert, attraverso un numero fax predisposto oppure ad una casella e-mail); nel caso in cui il contratto non sia sottoscritto con firma digitale deve essere accompagnato da una fotocopia leggibile di un documento di identità valido o documento ad essa equipollente (vedi par. 1.4).

Le modalità per l'invio del contratto sono le seguenti:

- **via Fax con firma autografa:** l'utente deve inviare al numero indicato nel processo di attivazione sul sito azionela richiesta di attivazione compilata e firmata, accompagnata dalla fotocopia (fronte-retro) di un documento di identità valido del richiedente (vedi par. 1.4);
- **via mail con firma autografa:** l'utente deve inviare all'indirizzo mail indicato nel processo di attivazione sul sito la richiesta di attivazione compilata, firmata e scansionata, accompagnata dalla fotocopia (fronte-retro) di un documento di identità valido del richiedente (vedi par. 1.4);
- **con firma digitale on-line**: il sistema richiede di apporre due firme digitali del richiedente nelle specifiche sezioni del contratto compilato on line.

3) Attivazione casella

Se il controllo della documentazione inviata, sia amministrativa sia contrattuale, supera le verifiche necessarie viene predisposta l'attivazione della casella. L'utente viene avvisato della avvenuta attivazione tramite una e-mail alla casella preventivamente indicata nella richiesta.

4.7.3 Richiesta attivazione casella acquistata tramite intermediario

Di seguito sono descritte le attività necessarie per l'attivazione delle caselle di posta elettronica certificata acquistate tramite intermediario o attraverso il commerciale InfoCert di riferimento.

Per le caselle acquistate tramite intermediario sono possibili personalizzazioni (utilizzo di particolari domini, grafica webmail ecc.).

L'utente riceve dall'intermediario la documentazione e la modulistica InfoCert relative ai seguenti punti:

- Condizioni generali
- Richiesta di Attivazione
- Informativa sul trattamento dei dati personali

L'intermediario raccoglie le informazioni relative alla richiesta da parte del titolare della casella. Tutti i contratti sono predisposti da InfoCert e contengono le condizioni del servizio. Il titolare, o un suo delegato, deve procedere alla sottoscrizione della richiesta di attivazione; è compito dell'intermediario la verifica della correttezza e completezza della richiesta.

L'intermediario procede alla attivazione delle richieste tramite strumenti forniti dal gestore.

Al momento della finalizzazione della procedura di inserimento da parte dell'Intermediario, viene inviata dalla piattaforma di autogestione InfoCert una e-mail ad una casella di appoggio indicata dall'utilizzatore finale contenente un link che permette, sempre tramite procedure online erogate da InfoCert, l'impostazione della password della casella PEC appena creata.

In alcuni casi specifici, tipicamente quando il cliente è un ordine professionale, l'impostazione della password è preceduta dall'accettazione dei termini di utilizzo della casella PEC che riporta, tra le altre cose, il riferimento alle Condizioni Generali di Contratto e informativa privacy.

4.7.4 Richiesta attivazione tramite personale commerciale di InfoCert

Il commerciale raccoglie le informazioni relative alla richiesta e alle caselle da attivare; procede all'identificazione del richiedente, alla definizione dell'accordo e alla firma del relativo contratto con il titolare, verificando la correttezza e la completezza del contratto.

Procede quindi direttamente, o tramite altro personale InfoCert preposto, alla attivazione delle caselle richieste.

4.7.5 Modalità alternative per l'attivazione del servizio

InfoCert si riserva la facoltà di fornire nuove modalità e flussi per la richiesta di nuove attivazioni da parte degli utenti. Le modalità utilizzate attualmente e quelle che potranno essere utilizzate in futuro garantiranno il rispetto delle norme relative alla privacy degli utenti, alla sicurezza e segretezza delle transazioni.

4.8 Modifica dati della casella direttamente da parte del titolare

Viene fornito al titolare della casella la possibilità di modificare on line, in totale autonomia, alcuni dati inseriti in fase di registrazione della casella.
Il titolare, una volta autenticato attraverso le credenziali della casella, accede alla sezione "La mia casella" del webmail e può modificare i seguenti dati:

- e-mail per comunicazioni tecniche, commerciali o di servizio;
- telefono
- cellulare

Inoltre, per venire incontro alle esigenze di chi ha commesso un errore nella definizione del nome casella, entro (e soltanto) i primi 10 giorni dall'attivazione della casella, sarà possibile la modifica del nome da autogestione Legalmail (vedi paragrafo 4.4.). Il vecchio nome rimane comunque registrato nei sistemi Legalmail e non più disponibile per altra registrazione.

4.9 Revoca delle caselle

La revoca di una casella PEC può avvenire:

- alla scadenza naturale del contratto in caso il titolare non ne effettui il rinnovo;
- su richiesta diretta da parte del titolare, utilizzando il modulo disponibile all'URL:https://www.legalmail.it/upload/Legalmail-D-1-Modulo_disdetta.pdf; le richieste di revoca vengono conservate per un minimo di dieci anni.

Il cliente viene avvertito dell'avvenuta revoca della casella ed informato dell'iter procedurale per la completa cancellazione del contenuto della casella stessa (vedere punti successivi).

Dalla revoca della casella:

- non è più possibile utilizzare la casella per spedire o ricevere nuovi messaggi
- per i 30 giorni successivi alla revoca l'utente potrà consultare i messaggi presenti in casella, pervenuti prima della revoca; **Oltre il 30esimo giorno successivo alla revoca non sarà più possibile accedere alla casella**
- per 185 giorni successivi alla revoca viene mantenuto dal gestore il contenuto della casella e ne viene riservato il nome, che non potrà essere assegnato a diverso titolare; in questo periodo il titolare può quindi procedere al rinnovo della casella, ripristinandone le funzionalità e il contenuto
- successivamente tutti i contenuti della casella verranno eliminati. Il nome della

casella verrà mantenuto riservato e non più utilizzabile per nuove attivazioni. Il titolare potrà successivamente riattivare la casella, senza il ripristino del contenuto.

4.10 Forzatura della password

In caso il titolare della casella non abbia più a disposizione la password per l'accesso alla casella, è possibile impostarne una nuova in una delle due modalità descritte nei paragrafi che seguono.

Attenzione: nel caso il titolare disponga della password per accedere alla casella, è disponibile la funzione di cambio password tramite le opzioni dell'interfaccia Webmail.
La sostituzione periodica delle password utilizzate è a totale carico del titolare.

4.10.1 Forzatura password tramite informazioni aggiuntive di sicurezza

In fase di accesso al servizio tramite Webmail e nelle opzioni dello stesso è a disposizione un servizio che permette di:

- definire alcune informazioni aggiuntive di sicurezza (mail alternativa, numero di telefono cellulare, domanda segreta e risposta segreta) abbinate alla user-id

- definire una nuova password per la user-id con una delle seguenti alternative:
  - inserendo domanda segreta e risposta segreta
  - ricevere un token al numero di cellulare precedentemente inserito
  - ricevere tramite la mail alternativa un link che permette di inserire la nuova password

Nella fase di inserimento delle informazioni di sicurezza è possibile inserire una o più delle informazioni richieste; nel momento della richiesta di forzatura è possibile scegliere tra le varie opzioni in base alle informazioni precedentemente fornite.

4.10.2 Forzatura password tramite modulo firmato

In caso si abbia la necessità di forzare una nuova password e non si siano definite le informazioni di sicurezza del paragrafo precedente, il titolare deve seguire la seguente procedura:

- scaricare dall'URL https://www.infocert.it/pdf/ForzaturaPassword.pdf il modulo apposito
- compilare il modulo e firmarlo
- inviare il modulo firmato via fax con allegato un documento di identità (vedi

par. 1.4), o in alternativa firmato digitalmente via posta elettronica certificata.

Se il titolare hai smarrito o dimenticato la password di accesso ad un servizio InfoCert acquistato attraverso un rivenditore autorizzato, può recuperarla rivolgendosi all'assistenza clienti del rivenditore.

4.11 Accesso al servizio

Il Cliente usufruirà del servizio tramite collegamento alla rete Internet di cui si dovrà dotare attraverso separato abbonamento con apposito operatore.

La velocità di trasferimento dei dati del collegamento del Cliente ha un'influenza determinante sulle prestazioni del servizio percepite dall'utente. Si ricorda pertanto che un collegamento ad elevata velocità assicura un servizio migliore e deve essere concordato con l'operatore di telecomunicazioni.

L'utilizzatore può accedere al servizio Legalmail tramite user-id e password assegnate da InfoCert con apposito profilo di abilitazione al servizio di posta.

Per accedere alla casella di posta elettronica Legalmail, l'utente può utilizzare il proprio client di posta elettronica. È inoltre disponibile, in aggiunta alla modalità standard, l'accesso con un browser Internet collegandosi all'applicazione Webmail tramite il sito www.legalmail.it (o eventuali personalizzazioni – vedi par. 30) e quindi alla casella di posta.
L'accesso alla casella di posta Legalmail, sia con client sia via Webmail, e lo scambio di messaggi avviene tramite protocolli sicuri (vedi par. 5.2)

Per il client, utilizzabile via POP3 e IMAP, è necessario come versione minima: Outlook Express 6, o prodotti equivalenti/superiori.

Per il browser è necessario come versione minima Internet Explorer 8, o prodotti equivalenti/superiori.

Se l'utente utilizza la posta elettronica certificata Legalmail via client, deve attivare sul proprio client una connessione protetta TLS per il server di posta in arrivo, mentre se l'utente utilizza la posta elettronica certificata Legalmail via browser (Webmail) non è necessaria alcuna configurazione.

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

4.11.1 Accesso via Webmail

A Webmail si accede tramite user-id/indirizzo e-mail e password. Per le caselle attestate sul provider principale l'URL di accesso è https://www.legalmail.it, mentre per le caselle attestate sul provider unit "Zucchetti" l'URL di accesso è https://webmail.zucchettipec.it.

Per motivi di sicurezza si RACCOMANDA di provvedere subito al cambio della password fornita inizialmente.

Il cambio password è accessibile nella sezione "Opzioni" di webmail.

Lo strumento permette di consultare la posta in arrivo, spedire messaggi di posta elettronica e organizzare la posta in arrivo.

Per accedere al servizio è necessario avere un Personal Computer dotato di un browser Internet Explorer 8 (con livello di codifica 1024 bit) o superiore, oppure prodotti equivalenti. In ogni caso saranno supportati solo gli accessi provenienti da stazioni di lavoro operanti con i sistemi operativi supportati dalle case produttrici

La sessione di lavoro con webmail, in caso di inutilizzo, ha una durata di tempo limitata; fatta eccezione per alcune funzionalità, dopo 30 minuti di mancata comunicazione con il sistema che gestisce webmail, il Titolare non sarà più in grado di continuare correttamente il lavoro intrapreso. In tal caso deve provvedere alla apertura di una nuova sessione di lavoro.

4.11.2 Accesso via client

Per accedere alla posta elettronica certificata InfoCert attraverso un client di posta è necessario utilizzare uno dei seguenti client:

- Microsoft Outlook 2003 o successive;
- Microsoft Outlook Express 6 o successive;
- Microsoft Windows Live Mail 12 o successive;
- Mozilla Thunderbird 24 o successive;
- Apple Mail di Mac OS X 10 e successive.

È inoltre necessario configurare il client con gli opportuni parametri per definire, ad esempio, il tipo di server di posta a cui collegarsi ed i parametri utilizzati dal server stesso per eseguire le operazioni di autenticazione della casella utente.

Per tutte le modalità di accesso è necessaria una connessione protetta.

Questi i protocolli, gli host e le porte utilizzabili per il servizio di invio e accesso alla casella:

Provider principale:

Servizio	Protocollo	Host	Porta
Invio	SMTP/S	sendm.cert.legalmail.it	465
	SMTP StartTLS	sendm.cert.legalmail.it	25
Accesso alla casella	POP3/S	mbox.cert.legalmail.it	995

	IMAP/S	mbox.cert.legalmail.it	993

Provider unit "Zucchetti":

Servizio	**Protocollo**	**Host**	**Porta**
Invio	SMTP/S	smtp.zucchettipec.it	465
	SMTP StartTLS	smtp.zucchettipec.it	25
Accesso alla casella	POP3/S	pop3.zucchettipec.it	995
	IMAP/S	imap.zucchettipec.it	993

Per firmare i messaggi di posta elettronica è necessario avere una smart card rilasciata da un Ente Certificatore (es. InfoCert) con il certificato di autenticazione contenente l'indirizzo della casella di posta utilizzata.

4.11.3 Raccomandazioni generali per l'utenza

Si ricorda che lo strumento scelto dal Cliente determina la modalità di utilizzo con esclusione delle particolarità legate al servizio di posta elettronica certificata, come ad esempio spiegato nei paragrafi del capitolo 5.

Per un corretto utilizzo delle caselle di posta si suggerisce al Titolare di consultare frequentemente la casella; infatti ogni messaggio ricevuto nella casella di posta elettronica certificata si intende pervenuto al Titolare della casella stessa (DPR 68/2005 [8]).

E' bene cancellare dal server di posta i messaggi con una frequenza sufficiente per evitare che venga occupato tutto lo spazio assegnato alla casella stessa e quindi i messaggi successivi vengano rifiutati. Il servizio Legalmail tiene traccia dei soli log degli eventi principali, ma non comprende (per le caselle standard) il sistema di conservazione a norma dei documenti scambiati via posta elettronica né delle relative ricevute.

Ai fini di garantire il più alto livello di sicurezza nel controllo degli accessi, come già scritto in precedenza, si invita l'utilizzatore a cambiare al più presto la password di accesso ricevuta da InfoCert.

È opportuno dotare le stazioni di lavoro di un antivirus costantemente aggiornato per garantire maggiore sicurezza per quanto viene spedito e ricevuto. Infatti, se pure la casella Legalmail è dotata di antivirus in grado di proteggere l'utente dai principali pericoli di infezione, non è possibile controllare automaticamente tutti i contenuti potenzialmente dannosi; in particolare si fa presente che i messaggi o file crittografati non possono essere sottoposti a controlli.

Verificare l'identità del mittente e dei destinatari con i mezzi più idonei è una prassi consigliabile. A puro titolo di esempio si cita la possibilità di utilizzare la firma di sottoscrizione apposta su un allegato al messaggio per identificare il mittente. In nessun caso il nome della casella può costituire un indizio valido per identificare con sicurezza il titolare

Portare a conoscenza dei propri corrispondenti che si è in possesso di una casella di posta a valore legale, costituisce una garanzia anche per i destinatari.

4.11.4 Cessazione del servizio

Nel caso di cessazione dell'attività di provider di Posta Elettronica Certificata, il Gestore comunicherà questa intenzione a AgID con un anticipo di almeno 60 giorni, indicando, se già conosciuto, il Gestore che prenderà in carico le caselle.

Con pari anticipo il Gestore informa (a mezzo posta elettronica certificata e/o apposito annuncio sul sito www.legalmail.it) della cessazione delle attività tutti i possessori di caselle PEC da esso gestiti.
Nel caso in cui non sia indicato il gestore che prenderà in carico le caselle, nella comunicazione sarà chiaramente specificato che tutte le caselle non saranno più accessibili dal momento della cessazione delle attività del Gestore. InfoCert comunque prevede che le caselle oggetto di cessazione del servizio restino attive in sola lettura (senza possibilità di invio / ricezione messaggi) per un periodo non inferiore a 30 giorni a decorrere dal giorno definito per la cessazione del servizio.

5. Requisiti Tecnici

5.1 Dimensioni casella e messaggi

La dimensione iniziale minima di una casella è di 1 GB: questa dimensione può essere ampliata.

Si ricorda che la dimensione massima garantita di un messaggio PEC è pari a 100 MB. È garantito l'invio o la ricezione di un messaggio con allegati di peso complessivo fino a 70 MB.
I sistemi di posta elettronica trasformano gli allegati per permetterne la trasmissione e questo fa aumentare la dimensione del messaggio inviato. Questo significa che un messaggio con un allegato di 100 KB potrebbe diventare durante la spedizione di 135 KB (il rapporto non è costante, si tratta di un puro esempio).

È buona norma, prima di spedire un messaggio di dimensioni significative, verificare di avere **spazio** sufficiente per ricevere tutte le ricevute di consegna. Se il messaggio viene inviato (in "TO (A)") a molti destinatari di posta elettronica certificata e la dimensione del messaggio è significativa si deve considerare che ogni ricevuta di consegna ha in allegato tutto il messaggio inviato, a meno di disposizioni contrarie da parte del mittente.

Per acquisire correttamente tutte le ricevute di consegna deve essere disponibile, pertanto, nella propria casella mittente lo spazio sufficiente. In caso contrario, le ricevute eccedenti la dimensione della casella non saranno recapitate.

Per questo motivo sono stati posti dei limiti sul numero dei destinatari per un singolo invio:

- il numero massimo di destinatari totali (To (a) e Cc) è 500

È responsabilità dell'utente la verifica dello stato di riempimento della propria casella PEC, e il suo periodico svuotamento.

5.2 Connettività e configurazione Client / Browser

Per utilizzare il servizio, la postazione dell'utente dovrà essere già dotata di accesso a internet che permetta il colloquio con i server InfoCert attraverso i protocolli elencati con le relative porte standard elencati di seguito:

- **SMTPS 465 per spedire messaggi (via SMTP + TLS) con client di posta**
- **SMTP 25 per spedire messaggi (via SMTP STARTTLS) con client di posta**
- **IMAP-S 993 per ricevere messaggi (via IMAP + TLS) con client di posta**
- **POP3-S 995 per ricevere messaggi (via POP3 + TLS) con client di posta**
- **HTTPS 443 per accedere al sito www.legalmail.it contenente informazioni sul servizio**
- **HTTPS 443 per utilizzare Webmail come strumento di invio e lettura dei messaggi**

Per ogni strumento scelto dal Cliente si dovranno seguire le istruzioni

specifiche di attivazione del client di posta.

Le prestazioni del servizio Legalmail sono condizionate dalle caratteristiche del collegamento alla rete di telecomunicazioni di cui usufruisce il titolare.

Per ulteriori informazioni si rimanda al sito www.legalmail.it

6. Condizioni per la fornitura del servizio di posta elettronica certificata

Il servizio è disciplinato e fornito in conformità con la normativa vigente e con quanto previsto nel Contratto che comprende:

- la richiesta di attivazione;
- le condizioni generali di fornitura del servizio;
- l'allegato contenente il Manuale operativo;
- l'informativa sulla privacy.

Tutta la documentazione è reperibile sul sito www.legalmail.it

6.1 Obblighi e Responsabilità

6.1.1 Obblighi del Gestore

Il Gestore garantisce la fornitura del servizio di posta elettronica certificata in conformità con le previsioni normative vigenti, secondo i livelli di servizio ivi descritti, ed in base alle disposizioni del Contratto.

InfoCert non assume alcun obbligo di conservazione dei messaggi trasmessi e ricevuti dal Cliente e/o dagli Utilizzatori con la casella di posta elettronica certificata oggetto del Servizio.
Tale conservazione è di esclusiva responsabilità del Cliente e/o degli Utilizzatori medesimi.

InfoCert non assume responsabilità in merito ai servizi di posta certificata resi dagli altri gestori

6.2 Obblighi dei Titolari

Il Cliente assume gli obblighi e le responsabilità previste dalla normativa vigente e dal Contratto.

6.2.1 Limitazioni e indennizzi

Il Gestore in nessun caso risponderà di eventi ad esso non imputabili ed in particolare di danni subiti dal Cliente, dall'Utilizzatore e da qualsiasi terzo causati direttamente o indirettamente dal mancato rispetto da parte degli stessi delle regole indicate nel presente Manuale Operativo e nel Contratto ovvero dallo svolgimento di attività illecite.

Fatto salvo il caso di dolo o colpa grave, il Gestore non sarà responsabile in caso di disservizi rientranti nell'ambito dei parametri di livello di servizio indicati al successivo paragrafo 9 e, comunque, nei limiti previsti nel contratto intercorso con il Cliente
Il Gestore, fatto salvo il caso di dolo o colpa grave, non sarà responsabile della mancata esecuzione delle obbligazioni assunte con il contratto di servizio, qualora tale mancata esecuzione sia dovuta a cause non imputabili al Gestore stesso, quali - a scopo puramente esemplificativo - caso fortuito, disfunzioni di ordine tecnico imprevedibili e non controllabili, interventi dell'autorità, cause di forza maggiore, calamità naturali ed altre cause imputabili a terzi.

Il Gestore ha stipulato un contratto assicurativo per la copertura dei rischi dell'attività e dei danni causati a terzi che ha come massimali:

- **10.000.000 euro per singolo sinistro**
- **10.000.000 euro per annualità.**

InfoCert si riserva, nel corso dell'esecuzione del presente contratto, di modificare le modalità di erogazione del Servizio Legalmail per adeguarlo e renderlo conforme alle disposizioni normative che saranno eventualmente emanate a disciplina dei servizi di posta elettronica certificata.

7. Protezione dei dati dei titolari

7.1 Normativa applicata

Si veda l'informativa ai sensi e per gli effetti dell'art. 13 del D. L.vo 196/2003 e all'art. 13 del Regolamento (UE) 679/2016, c.d. Regolamento Generale sulla Protezione dei Dati personali ("RGPD") e ai provvedimenti del Garante per la Protezione dei Dati Personali disposizioni di attuazione.

La documentazione completa è disponibile all'URL:
https://www.infocert.it/pdf/privacy-attivazione.pdf

7.2 Misure di sicurezza per la protezione dei dati personali

Tutti i messaggi di posta elettronica certificata e il colloquio attraverso client di posta o interfaccia WEB tra l'utente ed il sistema avvengono attraverso protocolli e connessioni sicuri, come (SMTP + TLS), (IMAP + TLS), (POP3 + TLS) e HTTPS.

È necessario utilizzare un client/browser che supporti il protocollo TLS1.2. Tutte le versioni precedenti, considerati non più sicuri, sono state disattivate.

Inoltre, solo utenti accreditati che abbiano superato i controlli di sicurezza possono accedere alle proprie caselle di posta elettronica certificata InfoCert.

8. Precisione del riferimento temporale

Il riferimento temporale del sistema del Gestore è basato sulla sincronizzazione con il sistema di marcatura temporale tenuto da InfoCert, in quanto Certificatore Accreditato per la Firma Qualificata.

Il sistema InfoCert prevede che tutte le procedure facciano riferimento alla data/ora del clock del sistema che viene mantenuto allineato con i sistemi della TSA (Time Stamping Authority). Quest'ultima ricava l'ora esatta UTC (Tempo Universale Coordinato) grazie al segnale di sincronismo ottenuto da un ricevitore esterno di qualità: questo ricava il tempo da un ricevitore radio sintonizzato con il segnale emesso dall'Istituto Elettronico Nazionale (IEN) "Galileo Ferraris". Il ricevitore utilizzato è stato preventivamente tarato e certificato dallo IEN stesso; poiché i tempi di attraversamento della rete interna (a 1 Gbs) sono tendenti a zero, il segnale orario così ottenuto rispetta i margini di precisione richiesti dalla normativa vigente (DPCM 13/1/2004) pari a 1 minuto secondo.

8.1.1 Sicurezza del sistema di validazione temporale

Il sistema per il servizio di marcatura temporale può essere attivato solo da operatori autorizzati tramite l'utilizzo di una serie di password e disponendo di un certo numero di smartcard.
Una volta attivato, il sistema non necessita di ulteriori procedure interattive di login, tranne che per arrestarlo e riattivarlo a scopo di manutenzione.

Un eventuale arresto del sistema può essere risolto solamente dagli operatori autorizzati.

Il sistema di TSA dispone di uno specifico componente dedicato al monitoraggio delle seguenti condizioni:

1. tentativi di manomissione della sicurezza del sistema
2. perdita del segnale di sincronismo con la fonte esterna di tempo
3. degrado delle prestazioni in termini di tempo di risposta
4. disponibilità del supporto di archiviazione non riscrivibile

Al verificarsi di una o più delle suddette condizioni, viene valutata la gravità dell'evento, provvedendo all'arresto del servizio di marcatura temporale qualora non sussistano le necessarie misure di sicurezza.

9. Livelli di servizio

Gli orari di erogazione del servizio sono:

Servizio	Orario
Spedizione messaggi da webmail o da client di posta	*Dalle 0:00 alle 24:00* 7 giorni su 7
Accesso a messaggi pervenuti da webmail o da client di posta	*Dalle 0:00 alle 24:00* 7 giorni su 7

Il servizio è pertanto disponibile 24 ore al giorno tutti i giorni della settimana.

La disponibilità del servizio è non inferiore al 99,8% su base quadrimestrale con durata massima del singolo fermo inferiore a 2 h 52 min. e 48 sec.

Il livello di servizio si intende riferito ai sistemi di InfoCert compreso il collegamento tra InfoCert e la rete di telecomunicazioni, ma non riguarda la rete di telecomunicazioni medesima o l'accesso del Cliente alla stessa il cui livello di servizio è imputabile al fornitore della rete di telecomunicazioni.

Per dettagli sulle limitazioni al servizio non imputabili ad InfoCert si rimanda al precedente paragrafo 'Limitazioni e indennizzi' del capitolo 6.

9.1 Controllo del livello di servizio del Gestore

Sono predisposte procedure e sistemi automatici per il controllo dello stato del sistema che eroga il servizio PEC e dell'intera infrastruttura tecnica del Gestore.

Sono installati strumenti di controllo automatico che consentono al Gestore di controllare il sistema valutando gli eventi e gli stati in cui il sistema stesso viene a trovarsi.

Il sistema è configurato in modo da intraprendere, in funzione dell'evoluzione dei suoi stati, delle azioni fra le seguenti tipologie:

- memorizzazione degli eventi;
- riconoscimento di eventi;
- risoluzione dei problemi;
- notificazione agli operatori.

L'architettura del sistema di posta elettronica certificata di InfoCert è stata disegnata per garantire l'alta affidabilità del sistema utilizzando sistemi ridondati come illustrato nel paragrafo 'Gli strumenti adottati' del capitolo 4.

9.2 Manutenzione sistemi.

Per la corretta configurazione dei nuovi sistemi e la corretta ripartenza di un sistema sottoposto a manutenzione è prevista una checklist che elenca le prove da fare volte per garantire che, a conclusione di qualsiasi attività manutentiva il sistema lavori correttamente e nel rispetto delle normative PEC.

9.3 Verifiche di sicurezza e qualità

Le procedure operative e le procedure di sicurezza del Gestore sono soggette a controlli periodici legati a verifiche predisposte dalla funzione di auditing interno. Tali controlli mirano a verificare la corretta applicazione delle procedure previste e la loro effettiva funzionalità in relazione agli obiettivi prefissati.
Oltre alle attività di auditing di processi sono pianificate le analisi e i controlli da effettuare sulle registrazioni prodotte dalle applicazioni e dai sistemi durante il normale funzionamento. Tale attività ha lo scopo di controllare che tutti gli eventi verificatisi rientrino nella normale operatività e che non si verifichino eventi pregiudicanti la sicurezza. La registrazione e la conseguente imputabilità degli eventi verificatisi costituiscono inoltre una ulteriore misura di sicurezza.

Il sistema di posta elettronica certificata Legalmail per consentire la custodia della posta in ambiente protetto è dotato di più livelli di firewall, intrusion detection, antivirus per i messaggi in entrata ed in uscita.

Gli eventi registrati nei log tecnici e applicativi sono sottoposti a controlli automatici e controlli a campione.

9.4 Procedure di salvataggio dei dati

Il salvataggio periodico dei dati relativi ai sistemi collegati in rete è effettuato giornalmente tramite un sistema di archiviazione automatizzato.
Periodicamente copia dei supporti contenenti i dati del salvataggio viene archiviata in un armadio di sicurezza, il cui accesso è consentito unicamente all'operatore addetto che appartiene alla struttura del Gestore.

Periodicamente copia di tali supporti è inoltre trasportata in un luogo sicuro esterno alla sede del Gestore, in modo da averne la disponibilità anche in caso di eventi disastrosi.

A garanzia della possibilità di poter ripristinare il sistema completo a seguito di guasti, sono effettuati salvataggi di tutti gli altri dati e programmi necessari per l'erogazione del servizio. Le modalità e i tempi di archiviazione dei salvataggi sono gli stessi delle procedure di salvataggio dei dati.

9.5 Servizi di emergenza

Al fine di garantire il completamento della trasmissione ed il rilascio delle ricevute sono state predisposte le seguenti soluzioni tecniche ed organizzative:

- Sistemi ridondati: tutti i sistemi sono ridondati in modo da garantire l'alta affidabilità del servizio, mentre le caselle utente, accessibili da più sistemi, sono conservate su sistemi NAS (Network Attachment Storage) – vedi dettagli cap. 4, "Gli strumenti adottati".
- Strumenti di controllo automatico: sono attivi nel sistema di Posta Certificata strumenti automatici di verifica del sistema e delle varie componenti funzionali. In base ai problemi rilevati il sistema prevede azioni per la risoluzione degli stessi o la notifica ad operatori per consentirne l'intervento (vedi cap. 9, "Controllo del livello di servizio del Gestore").
- Gestione dei disastri: il Gestore ha adottato le procedure necessarie a garantire la continuità del servizio anche in situazioni di elevata criticità o di disastro – si veda per i dettagli cap. 11, "Procedure di Gestione dei Disastri".
- Notifiche problemi elaborativi: il sistema (motore di Posta Certificata) prevede un controllo dei messaggi in transito, con il rilevamento di problemi nella propagazione o elaborazione dei messaggi. A fronte di rilevamento di problema il sistema procede:
  - al salvataggio della transazione in corso su apposite code di errore
  - al tentativo di ripristino automatico della transazione a intervalli di tempo predefiniti per il recupero dei messaggi presenti nella coda di errore
  - ad avvisare tempestivamente gli operatori del problema con avvisi automatici. Gli operatori autorizzati intervengono tramite apposita console alla verifica e gestione del problema e procedono al ripristino delle transazioni bloccate dopo la riattivazione dei sistemi o del software necessario.

10. Interoperabilità gestori

InfoCert, in ottemperanza a quanto previsto dal DPR 68/2005 [8], garantisce l'interoperabilità con gli altri gestori in conformità alle regole di Posta Elettronica Certificata (DM 2/11/2005 [5]).

InfoCert ripeterà periodicamente le opportune verifiche con gli altri gestori al fine di mantenere l'interoperabilità tra i relativi sistemi.

11. Misure di Sicurezza

Il Gestore ha realizzato un sistema di sicurezza del sistema informativo relativo al servizio di PEC.
Il sistema di sicurezza implementato è articolato su tre livelli:

- un livello fisico che mira a garantire la sicurezza degli ambienti in cui il Gestore gestisce il servizio
- un livello procedurale, con aspetti prettamente organizzativi
- un livello logico, tramite la predisposizione di misure tecnologiche hardware e software che affrontano i problemi e i rischi connessi con la tipologia del servizio e con l'infrastruttura utilizzata.

Tale sistema di sicurezza è realizzato per evitare rischi derivanti dal malfunzionamento dei sistemi, della rete e delle applicazioni, oltre che dall'intercettazione non autorizzata o dalla modifica dei dati.

Tutti i processi operativi del Gestore nella erogazione del servizio di PEC sono conformi al Piano di qualità aziendale.

11.1 Descrizione delle misure di sicurezza

11.1.1 Sicurezza fisica

Le misure adottate forniscono adeguate garanzie di sicurezza in merito a:

1. Caratteristiche dell'edificio e della costruzione;
2. Sistemi antintrusione attivi e passivi;
3. Controllo degli accessi fisici;
4. Alimentazione elettrica e condizionamento dell'aria;
5. Protezione contro gli incendi;
6. Protezione contro gli allagamenti;
7. Modalità di archiviazione dei supporti magnetici;
8. Siti di archiviazione dei supporti magnetici.

11.1.2 Sicurezza delle procedure

A garanzia che nessun individuo possa singolarmente compromettere o alterare la sicurezza globale del sistema oppure svolgere attività non autorizzate nella gestione del servizio, l'organizzazione del lavoro prevede la separazione dei ruoli con l'incarico a persone diverse con compiti separati e ben definiti per le attività ritenute critiche.
Il personale addetto alla progettazione ed erogazione del servizio di Posta Certificata è dipendente del gestore ed è stato selezionato in base alla esperienza nella progettazione, realizzazione e conduzione di servizi informatici e a caratteristiche di affidabilità e riservatezza.
Interventi di formazione sono pianificati periodicamente per sviluppare la consapevolezza dei compiti assegnati. In particolare, prima dell'inserimento del personale nell'attività operativa, sono realizzati interventi formativi allo scopo

di fornire ogni competenza (tecnica, organizzativa e procedurale) necessaria a svolgere i compiti assegnati

11.1.3 Sicurezza logica

L'accesso ai sistemi è consentito solo al personale autorizzato.

Gli operatori hanno diritto di accesso ai sistemi con le autorizzazioni minime necessarie allo svolgimento delle proprie mansioni.

I sistemi mantengono traccia degli accessi e delle operazioni effettuate.

11.2 Regole comportamentali

Le Politiche di Sicurezza di InfoCert e i documenti collegati illustrano le linee guida e la policy aziendale per tutti i servizi presenti in azienda. Tali documenti hanno l'obiettivo di creare una maggiore coscienza e considerazione in tutto il personale, circa la riservatezza delle informazioni e delle attività effettuate durante l'orario d'ufficio. Il personale viene esplicitamente invitato "alla massima riservatezza" riguardo a tutte le informazioni di cui venga in possesso. Sono indicate le norme per l'accesso fisico dei dipendenti e dei consulenti esterni, le norme per l'utilizzo del badge, e le regole per l'accesso fuori orario. Parte dei documenti sono dedicati alla sicurezza delle apparecchiature, dei sistemi e delle applicazioni informatiche. Sono indicate le norme circa l'uso della password (segretezza e necessità di cambiarla periodicamente) e del PC (utilizzo limitato all'uso professionale, cura e responsabilità della macchina, divieto di utilizzo di software non rilasciato dall'apposito ufficio, norme per la connessione remota, norme per la gestione dei virus, norme per l'accesso ad Internet e per l'utilizzo della posta elettronica, rimozione immediata degli accessi qualora non più necessari). Obiettivo delle politiche in essi espresse è, anche, minimizzare la possibilità che software illegale o non autorizzato possa essere introdotto, anche involontariamente, nella rete interna.
Tutti i documenti non riservati rivolti al personale sono disponibili nella Intranet aziendale.

11.3 Procedure di Gestione dei Disastri

Il Gestore ha adottato le procedure necessarie a garantire la continuità del servizio anche in situazioni di elevata criticità o di disastro.

Gli eventi disastrosi presi in considerazioni sono quelli che determinerebbero l'inagibilità di uno dei locali che ospitano i sistemi di InfoCert. Ai fini del ripristino delle funzionalità critiche del Gestore, si prende quindi in considerazione l'inagibilità della Sala CED.

Per gli eventi non catastrofici la continuità del servizio è garantita in quanto:

- tutti i sistemi sono replicati e forniscono un servizio in alta affidabilità, a fronte di un guasto hardware il servizio è comunque garantito da un sistema gemello;
- il bilanciamento e la ridondanza di rete fra i sistemi è garantito da dispositivi dedicati che sono configurati in modo che, se un sistema non dovesse rispondere, il traffico in transito sia dirottato verso il suo sistema gemello.

La ridondanza dei sistemi, oltre a garantire la continuità di servizio a fronte di guasti hardware, permette di garantire continuità di servizio anche a fronte di upgrade software o hardware ai sistemi.

11.4 Funzionalità da ripristinare e tempi massimo di ripristino

Per il servizio di Gestione PEC InfoCert ha predisposto un'infrastruttura dotata di meccanismi logistici e procedurali, atti a prevenire l'insorgere di eventi, che possano comprometterne le capacità di erogazione del servizio.

InfoCert utilizza un centro remoto di Disaster Recovery, presso il quale esiste una sottorete di sistemi off line, mantenuti aggiornati per poter fornire servizio ai prodotti aziendali più critici nel caso dovesse verificarsi un evento disastroso che rendesse non più operativo il CED di Padova; la sede di Disaster Recovery è collegata alla sede di Padova con linea ad alta velocità per reggere il carico degli aggiornamenti che vengono eseguiti con cadenza giornaliera.
Presso la sede di Disaster Recovery sono presenti sistemi in stand by per ospitare il servizio di posta elettronica certificata.

Nell'eventualità di eventi disastrosi sono state comunque individuate le funzionalità indispensabili al fine di minimizzare l'interruzione del servizio e garantire il rispetto dei requisiti di legge in relazione alla reperibilità delle informazioni registrate sul log dei messaggi.