Manuale Operativo
Posta Elettronica Certificata (PEC)
ai sensi del DPR 68/05

MANUALE OPERATIVO

VERSIONI DEL DOCUMENTO		
Revisione	Descrizione delle modifiche	Emissione
00	Cap. 3	19/09/2013
	Par. 3.1 nuovo paragrafo “Tabella di corrispondenza”	
	Par. 3.2 aggiornati “Riferimenti interni”	
	Par. 3.3 aggiornati “Riferimenti normativi”	
	Par. 3.7 aggiornato “Sistema di Gestione per la Qualità (rif. norma ISO9001:2008)”	
	Par. 3.8 nuovo paragrafo “Sistema di Gestione per la Sicurezza delle Informazioni (rif. norma ISO27001:2005)”	
	Par. 5.2 aggiornato “Organizzazione del personale”	
	Par. 5.3 revisione completa “Tipologie del servizio PEC”	
	Par. 5.6 nuovo paragrafo “Procedura di attivazione”	
	Cap. 6 aggiornato “Cenni sulle infrastrutture del Gestore e sulle misure di sicurezza”	
	Cap. 7 aggiornato “Modalità di generazione, conservazione, reperimento e presentazione dei log dei messaggi”	
	Cap. 8 aggiornato “Obblighi, Responsabilità e Indennizzi”	
	Cap. 9 aggiornato “Protezione dei dati”	
01	Cap. 2 aggiornato “Identificazione del Gestore e del Responsabile del Manuale Operativo” e tutti i riferimenti alla precedente Denominazione sociale	14/04/2014
	Inserito nuovo capitolo “Procedura di cessazione delle caselle PEC”	
	Inserito nuovo capitolo “Cessazione del Gestore”	
	Inserito nuovo capitolo “Assistenza al Cliente”	
	Nuovo modulo per richiesta Log PEC	
02	Par. 5.3.2.1.1 aggiornati parametri di accesso alle caselle PEC tramite Client	14/10/2014
	Integrato, in appendice, il documento Posta Elettronica Certificata – Descrizione del servizio	
03	Par. 3.2 aggiornati “Riferimenti interni”	24/10/2016
	Par. 3.7 aggiornato con i riferimenti al “Sistema di Gestione per la Qualità e per la Sicurezza delle Informazioni integrato”	
	Par. 3.8 eliminato “Sistema di Gestione per la Sicurezza delle Informazioni (rif. norma ISO27001:2005)” ed incluso nel paragrafo 3.7	
	Par. 5.3.2.1 aggiornato “Caselle individuali”	
	Par. 5.4 aggiornate “Condizioni di fornitura dei servizi erogati da TI Trust Technologies”	
	Par. 5.5 aggiornati “Livelli di servizio e indicatori di qualità”	
	Par. 5.6 revisione completa “Attivazione del servizio”	
	Inserito nuovo Par. 5.7 “Rinnovo del servizio”	
	Par. 5.8 revisione completa “Cessazione del servizio”	
	Par 7.3 aggiornato “Reperimento e presentazione dei Log”	
	Par. 8.1 aggiornata “Polizza assicurativa”	
	Cap. 10 aggiornato “Assistenza al cliente”	
04	Aggiornamento dei riferimenti normativi in occasione dell’entrata in vigore del Regolamento Generale sulla Protezione dei Dati n. 2016/679/UE	25/05/2018
05	Cap. 2 – Aggiornamento responsabile del MO Par. 5.3 – Precisazioni ed integrazioni relative alla gestione delle caselle di PEC Cap. 7 – Aggiornamento delle modalità di raccolta e gestione dei LOG del servizio	25/01/2019
06	Par. 3.2 – Aggiornamento del riferimento documentale delle condizioni di utilizzo del servizio Par. 5.8 - Precisazioni ed integrazioni relativi alle richieste di cessazione delle caselle di PEC Par. 8.1 – Aggiornamento della polizza assicurativa	25/02/2020

07	Par 5.3.1.1 e Par 5.3.2.2- Integrate le modalità di accesso Par. 5.3.2.4 e 5.3.2.5 – Integrate le tipologie di caselle PEC Par. 5.6.2 – Integrata procedura di attivazione del servizio con acquisto e-commerce Par. 5.8 – Integrate le modalità di cessazione Par. 6.3.1 – Inserita la gestione degli allegati ammessi Par. 7.2.1 – Precisati dettagli inerenti la modalità di conservazione log	21/05/2021

Indice degli argomenti

1 Scopo del documento

Questo documento illustra le regole generali e le procedure seguite dal Gestore del servizio di Posta Elettronica Certificata (PEC) TI Trust Technologies S.r.l. (nel seguito TI.TT) nell'erogazione del servizio stesso.

Il presente documento:

- è pubblicato dal Gestore a garanzia dell'affidabilità del proprio servizio di PEC nei confronti degli utilizzatori finali e contiene le modalità operative del servizio indicato;
- costituisce documento pubblico secondo le disposizioni vigenti;
- è liberamente disponibile per la consultazione ed il download in formato PDF sul sito predisposto dal Gestore TI.TT: http://www.trusttechnologies.it.

2 Identificazione del Gestore e del Responsabile del Manuale Operativo

La società Telecom Italia Trust Technologies S.r.l., con unico socio, Gruppo TIM – Direzione e coordinamento di TIM S.p.A., con sede in Pomezia (RM) – S.R.148 Pontina Km. 29,100, 00040, esercita l'attività di gestione di Posta Elettronica Certificata (PEC) ed è iscritto nell'elenco pubblico dei Gestori ai sensi dell'art. 14 del Decreto del Presidente della Repubblica n.68 dell'11 febbraio 2005.

Il responsabile del Manuale Operativo è Salvatore Nappi, AD e Responsabile Operations della struttura organizzativa del Gestore.

3 Riferimenti, standard e definizioni

3.1 Tabella di corrispondenza

Manuale Operativo	Circolare CNIPA
Cap. 2	Circolare 21 Maggio 2009 n. 56, 2.1 Manuale Operativo **Punto a**: Dati identificativi del gestore
Cap. 2	Circolare 21 Maggio 2009 n. 56, 2.1 Manuale Operativo **Punto b**: Il nominativo del responsabile del manuale stesso
Cap. 3; Par. 3.3	Circolare 21 Maggio 2009 n. 56, 2.1 Manuale Operativo **Punto c**: i riferimenti normativi necessari per la verifica dei contenuti
Cap. 1	Circolare 21 Maggio 2009 n. 56, 2.1 Manuale Operativo **Punto d**: l'indirizzo del sito web del gestore ove è pubblicato e scaricabile
Cap. 3; Par. 3.4	Circolare 21 Maggio 2009 n. 56, 2.1 Manuale Operativo **Punto e**: le procedure nonché gli standard tecnologici e di sicurezza utilizzati dal gestore nell'erogazione del servizio
Cap. 3; Par. 3.5	Circolare 21 Maggio 2009 n. 56, 2.1 Manuale Operativo **Punto f**: le definizioni relative alle abbreviazioni e ai termini tecnici che in esso figurano
Cap. 5	Circolare 21 Maggio 2009 n. 56, 2.1 Manuale Operativo **Punto g**:

	la descrizione e le modalità del servizio offerto
Cap. 7; Par. 7.3	Circolare 21 Maggio 2009 n. 56, 2.1 Manuale Operativo **Punto h**: la descrizione delle modalità di reperimento e di presentazione delle informazioni presenti nei log dei messaggi
Cap. 5; Cap. 5.4	Circolare 21 Maggio 2009 n. 56, 2.1 Manuale Operativo **Punto i**: le modalità di accesso e di fornitura del servizio
Cap. 5; Par. 5.5	Circolare 21 Maggio 2009 n. 56, 2.1 Manuale Operativo **Punto j**: i livelli di servizio e i relativi indicatori di qualità di cui all'articolo 12 del decreto del Ministro per l'innovazione e le tecnologie 2 novembre 2005
Cap. 9	Circolare 21 Maggio 2009 n. 56, 2.1 Manuale Operativo **Punto k**: le modalità di protezione dei dati dei titolari delle caselle, gli obblighi e le responsabilità che ne discendono, le esclusioni e le eventuali limitazioni in caso di indennizzo, relativamente ai soggetti previsti all'articolo 2 del decreto del Presidente della Repubblica n. 68/2005
Cap. 5; Par. 5.7	Circolare 21 Maggio 2009 n. 56, 2.1 Manuale Operativo **Punto l**: le procedure operative da attuare nel caso di cessazione dell'attività di gestore di posta elettronica certificata
Copertina pag. 1	Circolare 21 Maggio 2009 n. 56, 2.1 Manuale Operativo **Punto m**: la versione del medesimo manuale

3.2 Riferimenti Interni

La tabella di seguito riporta i riferimenti alla documentazione interna al gruppo TIM.

Rif.	Codice Documento	Descrizione
[1]	CAITPRIN.TT.SOCF16000 TITT	Condizioni generali di Utilizzo dei Servizi
[2]	CERTPECE.TT.SODS16000	Posta Elettronica Certificata – Descrizione del servizio
[3]	n.a.	Sito internet del Gestore di PEC TI.TT: https://www.trusttechnologies.it

3.3 Riferimenti Normativi

La tabella di seguito riporta le norme che definiscono le modalità attraverso le quali avviene lo scambio di messaggi di posta certificata e le regole per l'interoperabilità tra i gestori del servizio. Il servizio offerto dal Gestore è conforme a tale quadro normativo, che è sintetizzato nella tabella di seguito indicata, nella quale si riportano le abbreviazioni utilizzate nel testo del presente Manuale Operativo per riferimento alle singole norme:

Rif.	Descrizione
[RT]	**Allegato al Decreto Ministeriale 2 novembre 2005** - Regole tecniche del servizio di trasmissione di documenti informatici mediante posta elettronica certificata.
[DL 185/08]	**Decreto Legge 185/2008** - Decreto convertito in legge, con modificazioni, dall'art. 1, legge 28 gennaio 2009 n. 2, art. 16 e 16-bis.

[NI]	**Note Integrative ai documenti di riferimento della PEC -** Forniscono chiarimenti in riferimento al Decreto del Presidente della Repubblica 11 febbraio 2005 n.68 e al Decreto Ministeriale del 2 novembre 2005 e relativo allegato.
[Normativa Privacy]	Regolamento Generale sulla Protezione dei Dati n. 2016/679/UE e s.m.i. **Decreto Legislativo n. 196 del 30 giugno 2003** - Codice in materia di protezione dei dati personali, pubblicato sul Supplemento ordinario n. 123 della Gazzetta Ufficiale n. 174 del 29 luglio 2003 e s.m.i.
[DPCM 2009]	**Decreto del Presidente del Consiglio dei Ministri 30 marzo 2009 - Regole tecniche in materia di firme digitali** - Regole tecniche in materia di generazione, apposizione, e verifica delle firme digitali e validazione temporale dei documenti informatici (Gazzetta Ufficiale n. 129 del 6 giugno 2009).
[DPR 68/05]	**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.
[CAD]	**Decreto Legislativo 7 marzo 2005, n. 82** - Codice dell'amministrazione digitale, recante le disposizioni in base alle quali lo Stato, le Regioni e le autonomie locali assicurano la disponibilità, la gestione, l'accesso, la trasmissione, la conservazione e la fruibilità dell'informazione in modalità digitale mediante le tecnologie dell'informazione e della comunicazione.
[DM 2/11/05]	**Decreto 2 novembre 2005 del Ministro per l'Innovazione e le Tecnologie**, recante ***Regole tecniche*** per la formazione, la trasmissione e la validazione, anche temporale, della posta elettronica certificata (GU n. 266 del 15-11-2005).
[VIGIL]	**Circolare CNIPA n. 51 del 7 dicembre 2006** – Espletamento della vigilanza e del controllo sulle attività esercitate dagli iscritti nell'elenco dei gestori di PEC di cui all'articolo 14 del decreto del Presidente della Repubblica 11 febbraio 2005, n. 68 (Gazzetta Ufficiale n. 296 del 21 dicembre 2006.
[ACCR]	**Circolare CNIPA n. 56 del 21 maggio 2009** - Modalità per la presentazione della domanda di iscrizione nell'elenco pubblico dei gestori di posta elettronica certificata (PEC) di cui all'articolo 14 del decreto del Presidente della Repubblica 11 febbraio 2005, n. 68.

3.4 Procedure e standard tecnologici e di sicurezza

Il servizio di PEC erogato da TI.TT, in base a quanto dettagliato nel presente documento, è conforme agli standard di riferimento internazionalmente riconosciuti (e qui sotto riportati), secondo l'art. 3 del **DPR 68/05** e ai loro eventuali aggiornamenti.

Codice	Titolo
RFC 1847	Security Multiparts for MIME: Multipart/Signed and Multipart/Encrypted
RFC 1891	SMTP Service Extension for Delivery Status Notifications
RFC 1912	Common DNS Operational and Configuration Errors
RFC 2045	Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies
RFC 2049	Multipurpose Internet Mail Extensions (MIME) Part Five: Conformance Criteria and Examples
RFC 2252	Lightweight Directory Access Protocol (v3): Attribute Syntax Definitions
RFC 2315	PKCS #7: Cryptographic Message Syntax Version 1.5

RFC 2633	S/MIME Version 3 Message Specification
RFC 2660	The Secure HyperText Transfer Protocol
RFC 2821	Simple Mail Transfer Protocol
RFC 2822	Internet Message Format
RFC 2849	The LDAP Data Interchange Format (LDIF) - Technical Specification
RFC 3174	US Secure Hash Algorithm 1 (SHA1)
RFC 3207	SMTP Service Extension for Secure SMTP over Transport Layer Security
RFC 3280	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

3.5 Definizioni

Secondo la normativa vigente e ai fini dell'interpretazione del presente Manuale Operativo, i termini e le espressioni sotto elencate avranno il significato descritto nella definizione riportata.

I termini e le espressioni non definiti avranno il significato loro attribuito all'interno del paragrafo o sezione che li contiene.

Agenzia per l'Italia Digitale (AgID, ex DigitPA). L'articolo 20, comma 2, della legge 134/2012 attribuisce all'Agenzia lo svolgimento delle funzioni di coordinamento, di indirizzo e regolazione precedentemente affidate a DigitPA, nonché l'emanazione di pareri obbligatori sugli schemi di contratto concernenti l'acquisizione di beni e servizi informatici e telematici, secondo quanto previsto dall'articolo 3 del D.lgs. n. 177/2009. In forza del quadro normativo citato, in particolare vengono attribuite all'Agenzia anche le funzioni di consulenza e proposta, (già previste nell'articolo 3, comma 2, lettera a) del citato del D.lgs. 177/2009) nonché l'emissione di valutazioni e pareri facoltativi (secondo quanto previsto dal citato articolo 3, comma 2 lettera c) del D.lgs177/2009 e dall'articolo 20, comma 3 lettera l) della legge 134/2012).

Avviso di mancata consegna. È l'avviso che viene emesso quando il gestore mittente è impossibilitato a consegnare il messaggio nella casella di PEC del destinatario. Tale avviso, generato dal sistema, segnala l'anomalia al mittente del messaggio originale.

Avviso di non accettazione. È l'avviso che viene emesso quando il gestore mittente è impossibilitato ad accettare il messaggio in ingresso. La motivazione per cui non è possibile accettare il messaggio è inserita all'interno del testo della ricevuta che esplicita inoltre che il messaggio non potrà essere consegnato al destinatario. L'avviso di non accettazione è firmato con la chiave del gestore di PEC del mittente.

Busta di anomalia. È la busta, sottoscritta con la firma del gestore di PEC del destinatario, nella quale è inserito un messaggio errato ovvero non di PEC e consegnata ad un titolare, per evidenziare al destinatario detta anomalia.

Busta di trasporto. È la busta creata dal punto di accesso e sottoscritta con la firma del gestore di PEC mittente, all'interno della quale sono inseriti il messaggio originale inviato dall'utente di PEC ed i relativi dati di certificazione.

Casella di PEC. È una casella di posta elettronica alla quale è associata una funzione che rilascia delle ricevute di avvenuta consegna al ricevimento di messaggi di PEC. Una casella di PEC può essere definita esclusivamente all'interno di un dominio di PEC.

Centro Servizi del Gestore: La struttura logistica del Gestore in cui vengono eseguite le operazioni relative all'erogazione del servizio di PEC.

Certificatore (Certification Authority, CA, Autorità di Certificazione): prestatore di servizi di certificazione, la società TI Trust Technologies S.r.l. Per certificatore, si intende il soggetto che presta servizi di certificazione delle firme elettroniche o che fornisce altri servizi connessi con queste ultime.

Certificatore Accreditato: È tale***,*** ai sensi dell'art. 2, comma 1, lettera c) del Dl. 10/02, il certificatore accreditato in Italia ovvero in altri Stati membri dell'Unione Europea ai sensi dell'art. 3, paragrafo 2, della direttiva 1999/93/CE; TI Trust Technologies S.r.l. è un certificatore accreditato in Italia, che emette, pubblica nel registro e revoca Certificati Qualificati operando in conformità alla normativa vigente.

Certificato Qualificato*:* Un certificato emesso da un certificatore accreditato che risponde ai requisiti di cui all'allegato II della direttiva 1999/93/CE e conforme ai requisiti di cui all'allegato I della medesima direttiva.

Certificazione: Il risultato della procedura informatica applicata alla chiave pubblica e rilevabile dai sistemi di validazione, mediante la quale si garantisce la corrispondenza biunivoca tra chiave pubblica e soggetto titolare cui essa appartiene, si attesta il periodo di validità della predetta chiave e il termine di scadenza del relativo certificato.

Chiavi asimmetriche: La coppia di chiavi crittografiche una privata e una pubblica, correlate tra loro, e utilizzate nell'ambito dei sistemi di validazione di documenti informatici.

Chiavi di certificazione: Chiavi asimmetriche utilizzate esclusivamente per apporre la firma su certificati relativi a chiavi di sottoscrizione, di marcatura temporale e di autenticazione per CNS emessi dal Certificatore, sulle liste dei certificati sospesi e revocati e su nuovi certificati relativi a chiavi di certificazione generate in sostituzione di chiavi scadute.

Chiavi di marcatura temporale: Chiavi asimmetriche utilizzate dal Certificatore per apporre la firma alle marche temporali.

Chiavi di sottoscrizione: Chiavi asimmetriche associate a persone fisiche, da utilizzare per l'apposizione di firme digitali a documenti e ad evidenze informatiche.

Chiave Privata: L'elemento della coppia di chiavi asimmetriche, destinato ad essere conosciuto soltanto dal soggetto titolare, mediante il quale si appone la firma digitale sul documento informatico.

Chiave Pubblica: L'elemento della coppia di chiavi asimmetriche, destinato ad essere reso pubblico, con il quale si verifica la firma digitale apposta sul documento informatico dal titolare delle chiavi asimmetriche.

Cifratura: La trascrizione di una evidenza informatica secondo un codice riservato che la renda inintelligibile ai terzi. Le operazioni di cifratura e decifrazione si effettuano applicando algoritmi standard che prevedono l'utilizzo di chiavi segrete.

CNIPA - Centro nazionale per l'informatica nella pubblica amministrazione. Organismo che, in attuazione di quanto disposto dal decreto legislativo 177 del 1 dicembre 2009, è stato trasformato in DigitPA.

Dati di certificazione. È un insieme di dati che descrivono il messaggio originale e sono certificati dal gestore di PEC del mittente. I dati di certificazione sono inseriti nelle varie ricevute e sono trasferiti al titolare/utente di PEC di destinazione insieme al messaggio originale per mezzo di una busta di trasporto.

Destinatario. Utente di PEC che si avvale del Servizio di PEC del Gestore o di altro gestore di posta elettronica certificata per la ricezione di documenti prodotti mediante strumenti informatici.

***DigitPA - Ente nazionale per la digitalizzazione della Pubblica Amministrazione*:** Organismo fuso con l'Agenzia per la diffusione delle tecnologie per l'innovazione e il Dipartimento per la Digitalizzazione e Innovazione tecnologica della presidenza del Consiglio dal Decreto Sviluppo del Governo Monti nel 2012 per formare l'Agenzia per l'Italia digitale;

Documento informatico. È la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti.

Dominio di posta elettronica certificata. Corrisponde ad un dominio DNS dedicato alle caselle di posta elettronica degli utenti di PEC. All'interno di un dominio di PEC tutte le caselle di posta elettronica devono appartenere ad utenti di PEC.

Evidenza informatica. È una sequenza di simboli binari che può essere elaborata da una procedura informatica.

Firma del Gestore di PEC. la firma elettronica avanzata, basata su un sistema di chiavi asimmetriche, che consente di rendere manifesta la provenienza e di assicurare l'integrità e l'autenticità dei messaggi del sistema di posta elettronica certificata. La Firma del Gestore di PEC è generata attraverso una procedura informatica che garantisce la connessione univoca al gestore e la sua univoca identificazione, creata automaticamente con mezzi che garantiscano il controllo esclusivo da parte del Gestore.

Gestore di PEC. È il soggetto che gestisce uno o più domini di PEC con i relativi punti di accesso, ricezione e consegna. È titolare della chiave usata per la firma delle ricevute e delle buste. Si interfaccia con altri gestori di PEC per l'interoperabilità con altri utenti di PEC.

Indice dei gestori di PEC. È il sistema che contiene l'elenco dei domini e dei gestori di PEC, con i relativi certificati corrispondenti alle chiavi usate per la firma delle ricevute, degli avvisi e delle buste, realizzato per mezzo di un server LDAP, posizionato in un'area raggiungibile dai vari gestori di PEC e che costituisce, inoltre, la struttura tecnica relativa all'elenco pubblico dei gestori di PEC.

Log dei messaggi. È il registro informatico delle operazioni relative alle trasmissioni effettuate mediante PEC, tenuto dal gestore.

Manuale Operativo. Il documento pubblico che definisce e descrive le procedure applicate dal Gestore del servizio di PEC nello svolgimento della sua attività. Esso è depositato presso l'*Agenzia per l'Italia digitale* ed è reso disponibile presso il Gestore stesso.

Manuale della Qualità. Il manuale predisposto dal Gestore, finalizzato alla documentazione del proprio sistema di qualità certificato UNI EN ISO 9001:2000.

Marca temporale (Riferimento temporale). È un'evidenza informatica con cui si attribuisce, ad uno o più documenti informatici, un riferimento temporale opponibile ai terzi.

Messaggio di posta elettronica certificata. È un documento informatico composto dal testo del messaggio, dai dati di certificazione e dagli eventuali documenti informatici allegati.

Messaggio originale. È il messaggio originale inviato da un utente di PEC prima del suo arrivo al punto di accesso. Il messaggio originale è consegnato all'utente di PEC di destinazione per mezzo di una busta di trasporto che lo contiene.

Mittente. Utente di PEC che si avvale del Servizio di PEC del Gestore o di altro gestore di PEC per l'invio di documenti prodotti mediante strumenti informatici.

Piano per la Sicurezza: Il documento, previsto dall'art. 16, comma 1, lettera e del DM 2/11/05, che definisce le modalità di gestione delle attività connesse alla protezione e conservazione di dati, programmi ed apparati del Gestore.

Posta elettronica certificata (PEC). Sistema di posta elettronica nel quale è fornita al mittente la documentazione elettronica attestante l'invio e la consegna di documenti informatici.

Posta elettronica, un sistema elettronico di trasmissione di documenti informatici.

Punto di accesso. È il punto che fornisce i servizi di accesso per l'invio e la lettura di messaggi di PEC. Il punto di accesso fornisce i servizi di identificazione ed accesso dell'utente, di verifica della presenza di virus informatici all'interno del messaggio, di emissione della ricevuta di accettazione, di imbustamento del messaggio originale nella busta di trasporto.

Punto di consegna. È il punto che compie la consegna del messaggio nella casella di posta elettronica dell'utente di PEC destinatario. Verifica la provenienza/correttezza del messaggio, emette, a seconda dei casi, la ricevuta di avvenuta consegna o l'avviso di mancata consegna.

Punto di ricezione. È il punto che riceve il messaggio all'interno di un dominio di PEC. Compie i controlli sulla provenienza/correttezza del messaggio ed emette la ricevuta di presa in carico, imbusta i messaggi errati in una busta di anomalia e verifica la presenza di virus informatici all'interno dei messaggi di posta ordinaria e delle busta di trasporto.

Ricevuta di accettazione. È a ricevuta, sottoscritta con la firma del gestore di PEC del mittente, contenente i dati di certificazione, rilasciata al mittente dal punto di accesso a fronte dell'invio di un messaggio di PEC;

Ricevuta di avvenuta consegna. È la ricevuta, sottoscritta con la firma del gestore di PEC del destinatario, emessa dal punto di consegna al mittente nel momento in cui il messaggio è inserito nella casella di PEC del destinatario. Le diverse tipologie di Ricevute di avvenuta consegna, distinte in base al grado di sintesi del contenuto, sono descritte nel corpo del presente Manuale Operativo.

Ricevuta di presa in carico. È la ricevuta, sottoscritta con la firma del gestore di posta elettronica certificata del destinatario, emessa dal punto di ricezione nei confronti del gestore di posta elettronica certificata mittente per attestare l'avvenuta presa in carico del messaggio da parte del sistema di posta elettronica certificata di destinazione, recante i dati di certificazione per consentirne l'associazione con il messaggio a cui si riferisce.

Titolare. Il soggetto che richiede l'attivazione del servizio di PEC a beneficio dei propri utilizzatori.

Utente di PEC. La persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi ente, associazione o organismo, nonché eventuali unità organizzative interne ove presenti, che sia mittente o destinatario di PEC.

Virus informatico. È un programma informatico avente per scopo o per effetto il danneggiamento di un sistema informatico o telematico, dei dati o dei programmi in esso contenuti o ad esso pertinenti, ovvero l'interruzione, totale o parziale, o l'alterazione del suo funzionamento.

3.6 Abbreviazioni e termini tecnici

DNS - Domain Name System. Sistema di gestione dei nomi simbolici associati ad indirizzi di siti e domini Internet. Quando un messaggio di posta elettronica (e-mail), o un applicativo di consultazione di siti Internet (browser) punta ad un dominio, il DNS traduce il nome inserito sotto forma di URL (es. http://www.telecomitalia.it)/ in un indirizzo costituito da una sequenza numerica convenzionale (es. 123.123.23.3). Con il termine DNS si intendono, per estensione, anche le sequenze numeriche convenzionali che identificano i domini.

HTTP (Hypertext Transfer Protocol) . Protocollo di trasmissione, che permette lo scambio di file (testi, immagini grafiche, suoni, video e altri documenti multimediali) su World Wide Web.

HTTPS (Secure Hypertext Transfer Protocol) . Protocollo di trasmissione, sviluppato da Netscape Communications Corporation, per la cifratura e decifrazione dei dati trasmessi durante la consultazione di siti e pagine Internet. Corrisponde ad una estensione del protocollo Internet standard HTTP (Hypertext Transfer Protocol), attraverso il protocollo SSL.

ISO - International Standards Organization. Organizzazione internazionale per la standardizzazione, costituita da organismi nazionali provenienti da più di 75 paesi. Ha stabilito numerosi standard nell'area dei sistemi informativi. L'ANSI (American National Standards Institute) è uno dei principali organismi appartenenti all'ISO.

ITSEC - Information Technology Security Evaluation Criteria. Criteri europei per la valutazione della sicurezza nei sistemi informatici.

ITU - International Telecommunication Union. Organizzazione internazionale che funge da ente regolatore per gli standard nelle telecomunicazioni.

ITU–T. Sigla identificativa del Settore Telecomunicazioni ("Telecommunication Sector") dell'ITU.

LDAP – Lightweight Directory Access Protocol. Protocollo utilizzato per la gestione degli accessi al registro dei certificati e l'effettuazione di operazioni di prelievo di certificati e liste di revoca e sospensione.

MIME – Multipurpose Internet Mail Extensions. Estensione del protocollo di posta elettronica standard che consente la trasmissione di contenuti binari con applicazioni specifiche.

S-MIME – Secure/MIME. Versione "securizzata" del protocollo di posta elettronica MIME.

OID - Object identifier. Sequenza numerica che identifica un oggetto (struttura, algoritmo, parametro, sistema) nell'ambito di una gerarchia generale definita dall'ISO.

PIN - Personal Identification Number. Codice di sicurezza riservato che permette l'attivazione delle funzioni del dispositivo di firma.

POP – Point of Presence. Punto di accesso alla rete Internet.

PKCS - Public Key Cryptography Standard. Standard tecnici per applicazioni crittografiche, realizzati dalla RSA Data Security Inc.

PKI – Public Key Infrastructure. Infrastruttura informatica costituita da applicazioni che utilizzano tecniche crittografiche a chiavi asimmetriche (pubblica e privata). Una infrastruttura di questo tipo include servizi di generazione e distribuzione di chiavi, di emissione e pubblicazione di certificati, di gestione dei registri dei certificati emessi e delle liste di sospensione e revoca, oltre ad altri servizi come la marcatura temporale. Esempi di utilizzazioni basate sull'infrastruttura sono: la generazione di transazioni informatiche riservate (crittografia), la gestione di sistemi di autorizzazione, autenticazione e identificazione (firma digitale), riferibilità soggettiva ed integrità dei dati (firma digitale e marcatura temporale).

RFC – Request for Comments. Definizioni scritte di protocolli o standard in uso su Internet.

SL - Secure Socket Layer. Protocollo standard per la gestione di transazioni sicure su Internet, basato sull'utilizzo di algoritmi crittografici a chiave pubblica.

URL - Uniform Resource Locator. Sistema standard di nomenclatura specificante un sito, dominio o altro oggetto (file, gruppo di discussione, ecc.) su Internet. La prima parte dell'URL (http:, ftp:, file:, telnet:, news:) specifica le modalità di accesso all'oggetto.

WWW – World Wide Web. L'insieme delle risorse e degli utenti su Internet che utilizzano il protocollo HTTP.

3.7 Sistema di Gestione per la Qualità (ISO9001) e per la Sicurezza delle Informazioni (ISO27001)

Il Gestore adotta un sistema integrato di **Gestione per la Qualità** e per la **Sicurezza delle Informazioni** (SGQSI) conforme alle norme di riferimento **ISO 9001** e **ISO27001** per le attività svolte all'interno dell'azienda sui servizi e soluzioni basati sulle tecnologie di crittografia a chiave pubblica (comprese le attività di progettazione, erogazione ed assistenza del servizio di PEC).

Il Certificato del Sistema di Gestione per la Qualità è stato rilasciato in data 18 novembre 2010, mentre il Certificato del Sistema di Gestione per la Sicurezza delle Informazioni è stato rilasciato in data 30 ottobre 2012.

Entrambi i certificati sono stati rilasciati dall'Ente di Certificazione CISQ/IMQ-CSQ, partner italiano di IQNet, il quale provvede, con cadenza annuale, a confermare la validità dei certificati rilasciati.

4 Natura del Servizio di PEC

Il servizio di PEC è un servizio finalizzato all'invio e alla ricezione di messaggi in formato elettronico e degli eventuali documenti informatici allegati, analogamente alla tradizionale posta elettronica, con le seguenti caratteristiche aggiuntive:

- fornisce al mittente la documentazione elettronica attestante l'invio e la consegna dei messaggi informatici, assicurandone il tracciamento mediante una serie di ricevute appositamente generate dai sistemi di posta certificata dei gestori del servizio. Per aumentare il livello di garanzia dell'avvenuta trasmissione dei messaggi, tali ricevute sono firmate e marcate elettronicamente dai sistemi di gestione, con l'ausilio di specifici certificati digitali, così da assegnare anche un riferimento temporale certo all'avvenuta trasmissione

dei dati. La posta inoltrata tra domini di posta certificati, infatti, viene elaborata applicando criteri di inserimento e controllo della firma elettronica, fornendo così un meccanismo di certificazione dei messaggi scambiati tra mittenti e destinatari;

- la trasmissione dei dati avviene attraverso dei canali cifrati e quindi non intercettabile da terzi.
- dà al processo di trasmissione valore equivalente a quello della notifica a mezzo posta nei casi consentiti dalla legge.

4.1 I soggetti del servizio secondo la normativa

Secondo l'art. 2 del DPR 68/05, il servizio di PEC prevede tre distinti soggetti:

1. **mittente**: è l'utente iniziale che si avvale del servizio di posta elettronica certificata per la trasmissione di documenti prodotti mediante strumenti informatici;
2. **destinatario**: è l'utente finale che si avvale del servizio di posta elettronica certificata per la ricezione di documenti prodotti mediante strumenti informatici;
3. **gestore del servizio:** è il soggetto, pubblico o privato che eroga il servizio di posta elettronica certificata e che gestisce uno o più domini di posta certificata con i relativi punti di accesso, ricezione e consegna. I gestori del servizio di posta elettronica certificata devono garantire l'utilizzo di metodi per la verifica che il messaggio sia trasportato dal mittente al destinatario.

Oltre al mittente, al destinatario e al gestore, ulteriori elementi che intervengono nel funzionamento di un sistema di PEC sono:

- il **punto di accesso**, ovvero il Server di Posta Certificata mittente;
- il **punto di ricezione**, ovvero l'infrastruttura che permette lo scambio di messaggi di posta certificata tra diversi gestori di posta certificata e che consente l'inserimento di messaggi di posta elettronica ordinaria nel circuito della posta certificata;
- il **punto di consegna**, ovvero il Server di Posta Certificata destinatario.

4.2 Funzionamento del servizio

Nella figura sottostante è rappresentato il funzionamento generale del servizio di PEC e nei paragrafi seguenti sono descritte le fasi di cui si compone.

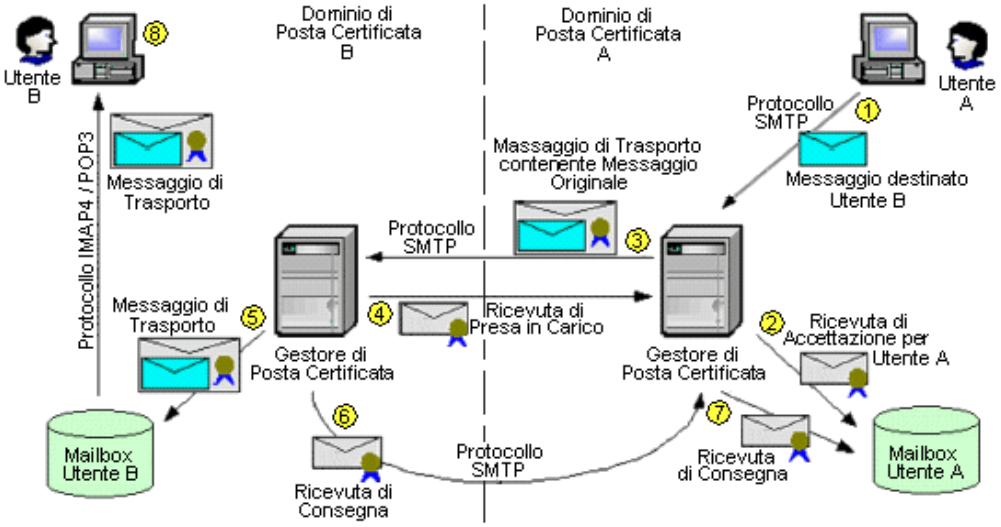


Figura 1: Schema di funzionamento del servizio di posta elettronica certificata

4.2.1 Invio del messaggio da parte del mittente

Il **mittente** invia un messaggio attraverso il servizio di posta certificata. Il server di posta certificata del mittente (**punto di accesso**) esegue una serie di controlli formali sul messaggio pervenuto e provvede a generare una

ricevuta di accettazione. I controlli formali accertano se i destinatari del messaggio appartengono all'infrastruttura di posta certificata o se sono utenti esterni (es. posta Internet). Nel caso in cui i controlli formali diano esito negativo, viene emessa un avviso di mancata accettazione.

Prosegue poi "imbustando" il messaggio originale in un messaggio di trasporto (busta di trasporto) di tipo *"S/MIME"* ed inviando al mittente una ricevuta di accettazione, con la quale conferma al mittente che il suo messaggio è stato accettato dal sistema, ad una data e ora specifiche.

La **ricevuta di accettazione** è un messaggio di posta elettronica firmato dal gestore del mittente, nel quale sono riportati la data ed ora di accettazione, l'oggetto ed i dati del mittente e del destinatario. Nella ricevuta di accettazione è riportata la tipologia dei vari destinatari per informare il mittente del differente flusso seguito dai due gruppi di messaggi.

La busta di trasporto firmata dal gestore del mittente, è un messaggio che contiene, come allegato, il messaggio originale e tutti i dati che ne certificano il trasporto. La busta di trasporto viene quindi inviato al dominio destinatario attraverso il punto di ricezione. Questo accade sia nel caso che il destinatario ed il mittente appartengano ad uno stesso dominio di PEC, sia che appartengano a domini di PEC differenti[1].

4.2.2 Invio del messaggio al punto di ricezione

All'arrivo di un messaggio, il **punto di ricezione** ne verifica la natura e la corretta composizione. In particolare, il punto di ricezione verifica l'esistenza e la validità della firma del gestore che ha consegnato il messaggio del mittente. Se le verifiche sono positive, emette una **ricevuta di presa in carico** verso il gestore mittente e provvede ad inoltrare il messaggio ricevuto verso il punto di consegna.

4.2.3 Invio del messaggio al punto di consegna

Quando la busta di trasporto è stata consegnata al server di posta certificata del destinatario (**punto di consegna**), questo emette ed invia al mittente una **ricevuta di avvenuta consegna**, che conferma al mittente che il suo messaggio è stato effettivamente consegnato al destinatario specificato, certificando la data e l'ora dell'evento. L'emissione della ricevuta di avvenuta consegna avviene contestualmente alla disponibilità del messaggio nella casella di posta elettronica del destinatario, indipendentemente dalla lettura da parte del destinatario stesso.

4.2.4 Problemi di consegna

La situazione appena descritta costituisce la normalità dei casi, ma si possono verificare delle situazioni nelle quali il messaggio di posta elettronica certificata non risulta consegnabile. Qualora il gestore del mittente non abbia ricevuto dal gestore del destinatario, nelle dodici ore successive all'inoltro del messaggio, la ricevuta di presa in carico o di avvenuta consegna del messaggio inviato, il gestore del mittente stesso comunica al mittente che il gestore del destinatario potrebbe non essere in grado di realizzare la consegna del messaggio. Qualora, entro ulteriori dodici ore, il gestore del mittente non abbia ricevuto la ricevuta di avvenuta consegna del messaggio inviato, inoltra al mittente un ulteriore avviso relativo alla mancata consegna del messaggio entro le 24 ore successive all'invio, così come previsto dall'art. 8 del DPR 68/05.

Qualora il gestore del mittente riceva messaggi con virus informatici è tenuto a non accettarli informando tempestivamente il mittente dell'impossibilità di dar corso alla trasmissione. In tal caso il gestore conserva i messaggi ricevuti per trenta mesi secondo le modalità definite dall'art. 12, comma 1 del DPR 68/05. Qualora il gestore del destinatario riceva messaggi con virus informatici è tenuto a non inoltrarli al destinatario informando tempestivamente il gestore del mittente, affinché comunichi al mittente medesimo l'impossibilità di dar corso alla trasmissione. In tal caso il gestore del destinatario conserva i messaggi ricevuti per trenta mesi secondo le modalità definite dall'art. 12, comma 2 del DPR 68/05. In tutti questi casi vengono generati e inviati al mittente specifici avvisi con i motivi della mancata consegna.

4.2.5 Firma elettronica delle ricevute e delle buste di trasporto

Le ricevute e le buste di trasporto rilasciate dal Gestore sono sottoscritte dal medesimo mediante una firma elettronica conforme alla normativa PEC, generata automaticamente dal sistema di posta elettronica e basata su

[1] Con riferimento alla figura 1, si precisa che lo schema di funzionamento è analogo sia nel caso di utilizzatori attestati su domini di PEC differenti, sia nel caso di utilizzatori attestati su uno stesso dominio di PEC.

chiavi asimmetriche a coppia, una pubblica e una privata, che consente di renderne manifesta la provenienza e assicurarne l'integrità e l'autenticità, secondo le modalità previste dalle regole tecniche [RT].

4.2.6 Tipologia delle Ricevute di Avvenuta Consegna

Coerentemente con quanto indicato dalle Regole Tecniche, il Gestore può emettere tre differenti tipologie di Ricevute di Avvenuta Consegna, che possono soddisfare differenti esigenze dell'utenza:

- la **Ricevuta Completa** è costituita da un messaggio di posta elettronica inviato al mittente che riporta in formato leggibile i dati di certificazione (mittente, destinatario, oggetto, riferimenti temporali, codice identificativo del messaggio). Gli stessi dati sono inseriti all'interno di un file XML allegato alla ricevuta. Per le consegne relative ai destinatari primari del messaggio, la ricevuta di avvenuta consegna **contiene anche il messaggio originale, completo di header, testo ed eventuali allegati**;
- la **Ricevuta Breve** ha lo scopo di ridurre i flussi di trasmissione della PEC, soprattutto in quei casi in cui la mole di documenti e di messaggi scambiati è molto consistente. Per questo, la Ricevuta Breve contiene il messaggio originale e gli hash crittografici degli eventuali allegati. Per permettere la verifica dei contenuti trasmessi, il mittente deve conservare gli originali non modificati degli allegati inseriti nel messaggio originale, a cui gli hash fanno riferimento;
- la **Ricevuta Sintetica** segue le regole di emissione della ricevuta completa, solo che nell'allegato contiene esclusivamente il file XML con i dati di certificazione descritti. La ricevuta sintetica è particolarmente utile in tutte quelle fattispecie di servizio che includono la PEC come strumento di trasporto a supporto di una forte automazione dei flussi di comunicazione.

4.2.7 Riferimento temporale

Su tutti gli eventi che costituiscono la transazione di elaborazione dei messaggi (generazione di ricevute, buste di trasporto, log, ecc.) il Gestore appone un riferimento temporale in conformità con il DPR 68/05 e secondo le modalità che il Gestore utilizza nella sua attività di Certificazione Digitale (cfr. 6.2).

Una marca temporale è apposta quotidianamente anche sui log dei messaggi.

5 Il Servizio di PEC erogato da TI Trust Technologies

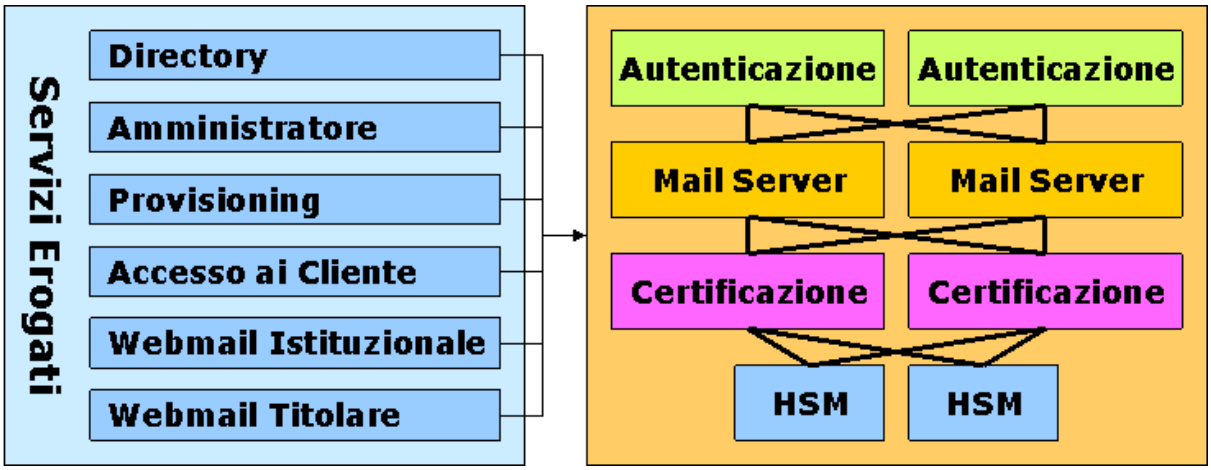
La soluzione di PEC di TI.TT si avvale di un'architettura modulare e scalabile, che consente di impiegare un client di posta elettronica sfruttando un canale sicuro di trasmissione come l'IMAP-S/POP3S e SMTPS[2].

In sintesi, il servizio di Posta Elettronica Certificata di TI.TT, conformemente a quanto disposto dalla normativa vigente in materia, presenta le seguenti caratteristiche:

- è indipendente dal client di posta utilizzato;
- garantisce il tracciamento dell'intero processo di trasferimento;
- rende opponibile a terzi la provenienza, l'avvenuto invio e l'avvenuto recapito del messaggio;
- assicura trasparenza rispetto alla natura del messaggio.

[2] Le Regole Tecniche allegate al DM 2/11/05 stabiliscono che l'integrità e la confidenzialità delle connessioni tra il gestore di posta certificata e l'utente devono essere garantite mediante l'uso di protocolli sicuri. A titolo esemplificativo, e non esaustivo, dei protocolli accettabili per l'accesso figurano quelli basati su TLS (es. IMAPS, POP3S, HTTPS), quelli che prevedono l'attivazione di un colloquio sicuro durante la comunicazione (es. SMTP STARTTLS, POP3 STLS), quelli che realizzano un canale di trasporto sicuro sul quale veicolare protocolli non sicuri (es. IPSec).

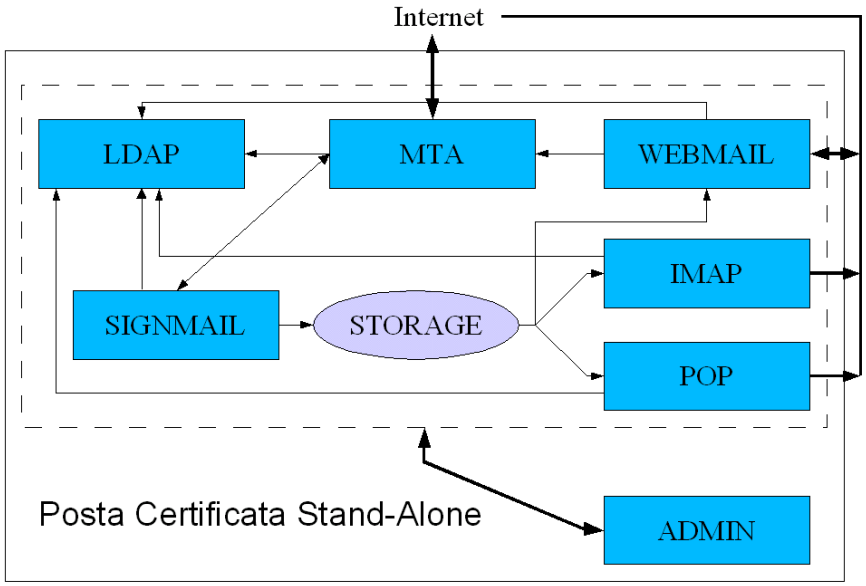
5.1 Architettura del Servizio



L'architettura della piattaforma di PEC TI.TT prevede tre differenti gruppi tecnologici:

- **punti di accesso per l'utente finale** per i vari livelli di amministrazione ai differenti servizi erogati. I primi livelli possono fruire della posta elettronica accedendo a due distinte interfacce Webmail online, differenziata in base al tipo di casella (titolare o multiutente), oppure utilizzando un comune Client di posta (Outlook Express, Microsoft Outlook, Mozilla Thunderbird, ecc.). Il Provisioning invece consente un facile ed intuitivo livello di amministrazione dei servizi stessi da parte del Gestore dei ruoli e dell'Incaricato, laddove invece l'Amministratore della piattaforma tecnologica è dotato di un'interfaccia di gestione personale.
- **sistema di gestione**, smistamento e transazione delle mail (Mailserver), il sistema di autorizzazione ed Autenticazione delle utenze e la parte dedicata alla Certificazione dei messaggi di posta.
- **moduli HSM**, macchine dedicate allo storage protetto delle chiavi private di firma.

La rappresentazione grafica che segue mette in evidenza le interrelazioni fra le diverse componenti presenti nell'architettura generale della PEC stand-alone:



1. MTA - Server di posta che supporta il protocollo SMTP;
2. LDAP - Server Ligthweigth Directory per memorizzazione utenze e preferenze globali;
3. WEBMAIL - Client per accesso remoto tramite Web;

4. IMAP - Server per accesso remoto tramite MUA;
5. POP3 - Server per accesso remoto tramite MUA;
6. ADMIN - Client ad accesso riservato per l'amministrazione/gestione del sistema tramite Web;
7. SIGNMAIL - Plugin per la posta certificata.

5.2 Organizzazione del personale

L'organizzazione del personale addetto all'erogazione del servizio di PEC di TI.TT prevede, tra le altre, le seguenti figure professionali:

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

Tali figure professionali sono costantemente addestrate per garantire le loro competenze in funzione degli aggiornamenti ai quali è soggetto il sistema di PEC e posseggono una esperienza non inferiore a cinque anni nella analisi, progettazione, commercializzazione e conduzione di sistemi informatici (così come definito in [[DM 2/11/**05]**]).

5.3 Tipologie di Servizio

Il servizio di PEC offerto al cliente si differenzia sulla base delle diverse possibili combinazioni dei seguenti elementi:

- **Dominio sul quale sono configurate le caselle di posta elettronica**: di TI.TT o del Cliente;
- **Tipologia di servizio**: casella individuale, casella multiutente, casella applicativa;
- **Modalità di utilizzo**: webmail o client di posta.

5.3.1 Trattamento dei Domini

Il cliente, per la gestione della propria corrispondenza certificata, può avvalersi del dominio di posta certificata di TI.TT oppure può utilizzare un dominio proprio (o sottodominio) richiedendo la configurazione dello stesso come dominio (o sottodominio) di posta certificata.

5.3.1.1 Domini certificati

In questo caso il cliente si appoggia ad un dominio di Posta Certificata del Servizio TI.TT, ottenendo un dominio di terzo livello ad esempio: (@dominiocliente.telecompost.it).

Tutti gli scambi in entrata ed in uscita effettuati dalle caselle di posta del cliente configurate in questo dominio sono trattati come scambi di messaggi di PEC.

5.3.1.2 Dominio del cliente

Nel caso in cui il cliente sia già in possesso di un suo dominio o di un sottodominio internet, deve richiedere al maintainer del suo dominio di configurare il record MX dello stesso in modo che punti a **mail.telecompost.it**. Successivamente, tale dominio sarà configurato da TI.TT come dominio o sottodominio di posta elettronica certificata.

Tutti gli scambi in entrata ed in uscita effettuati dalle caselle di posta del cliente configurate nel dominio certificato sono trattati come scambi di messaggi di posta certificata.

Rispetto al caso precedente, in questo caso il maintainer del DNS del cliente è tenuto a curare la relativa configurazione per assicurare la visibilità in rete dei server coinvolti nel processo di certificazione. TI.TT, da parte sua, verificherà che il cliente che richiede la certificazione del dominio ne sia effettivamente titolare e che il dominio sia regolarmente registrato.

È importante tenere presente che, anche nel caso di dominio o sottodominio del cliente, i servizi relativi al dominio certificato verranno comunque erogati dalla piattaforma TI.TT.

5.3.2 Tipologie di Caselle

In considerazione del fatto che alcuni elementi caratterizzanti i servizi di PEC possono variare nel tempo in funzione delle modifiche delle offerte proposte alla clientela, i dettagli aggiornati su:

- tipologie di caselle
- modalità di accesso
- tagli disponibili
- servizi accessori

sono illustrati nel documento [2] Posta Elettronica Certificata – Descrizione del servizio, disponibile online sul sito del Gestore [3].

5.3.2.1 Caselle individuali

La casella individuale è di esclusiva pertinenza di un singolo utente e non prevede la possibilità che altri possano visualizzarne il contenuto.

L'utilizzo della casella è del tutto simile all'utilizzo di caselle di posta tradizionali, con le garanzie proprie del sistema di PEC.

Allo scopo di consentire al Cliente di mantenere il controllo sulla gestione delle utenze, è prevista l'attivazione di Incaricati della Registrazione per effettuare la registrazione degli utenti secondo le procedure indicate da TI.TT. Inoltre, gli Incaricati provvedono all'attivazione e alla gestione delle utenze e delle caselle di PEC, mediante l'utilizzo dell'utenza di amministrazione.

5.3.2.1.1 Modalità di accesso

- Sistema webmail raggiungibile all'indirizzo di TI.TT https://www.telecompost.it/pec;
- Sistema webmail light raggiungibile all'indirizzo di TI.TT https://webmail.telecompost.it/;
- App TIM PEC;
- Principali client di posta elettronica diffusi sul mercato[3]:
  - Microsoft Outlook
  - Mozilla Thunderbird;
  - Dispositivi Windows Mobile
  - Netscape Messenger
  - Lotus Note Client 6.5.1

5.3.2.1.2 Dimensioni e traffico delle caselle

Il cliente può scegliere tra le diverse opzioni elencate nel documento di descrizione del servizio [2].

5.3.2.2 Caselle multiutente

La casella multiutente prevede la possibilità che un gruppo di utenti (operatori) possa accedere alla medesima casella per la gestione della corrispondenza scambiata attraverso di essa.

Ad una casella multiutente è associato sempre un solo titolare che è l'unico in grado di effettuare tutte le operazioni di gestione dei messaggi tramite la webmail standard del servizio (https://www.telecompost.it/pec), mentre gli operatori della casella hanno a disposizione un numero limitato di funzioni.

Con questo tipo di servizio TI.TT intende soddisfare le esigenze delle maggiori organizzazioni e degli enti della Pubblica Amministrazione nei quali, generalmente, gli indirizzi di posta ricevono i messaggi in entrata che devono essere acquisiti da più operatori, che provvedono a classificarli e smistarli verso le funzioni organizzative competenti. Gli stessi riferimenti centralizzati si occupano anche di trattare la corrispondenza in uscita prodotta dalle varie funzioni interne.

Per soddisfare le esigenze legate a questo tipo di utilizzo, questo servizio, oltre a supportare chi opera nella gestione della corrispondenza, garantisce anche la possibilità di curare l'amministrazione delle utenze e di assicurare i necessari livelli di sicurezza nell'accesso e nella gestione dei contenuti. In modo particolare, la soluzione realizzata

[3] Per i dettagli sulla configurazione è possibile fare riferimento al *Manuale di configurazione del client di posta elettronica per il servizio PEC*, raggiungibile all'indirizzo di accesso alla Webmail: https://www.telecompost.it/webmail/login.jsp (link "Manuali").

da TI.TT prevede l'utilizzo di un'interfaccia Web dedicata alla gestione della corrispondenza scambiata, in grado di soddisfare le seguenti esigenze:

- ***Sicurezza nell'accesso e protezione dei contenuti***: l'accesso al servizio di PEC avviene attraverso autenticazione tramite username e password. Anche se il servizio prevede che più utenti abilitati possano accedere ad una stessa casella di posta multiutente, tutti sono identificati singolarmente
- ***Praticità di utilizzo****:* attraverso un codice identificativo progressivo attribuito a ciascun messaggio, il sistema permette di gestire un consistente flusso di corrispondenza elettronica in entrata ed in uscita, garantendo le funzionalità di visualizzazione, ordinamento e lavorazione della corrispondenza elettronica in entrata ed in uscita. Gli automatismi nell'assegnazione del codice identificativo e delle informazioni correlate (operatore che ha inviato il messaggio, casella di provenienza ecc.) sollevano l'utente da un complesso di attività ripetitive spesso fonte di errori. Le numerose funzioni d'uso permettono, infine, di snellire e velocizzare le operazioni di trattamento della corrispondenza elettronica.

Allo scopo di consentire al Cliente di mantenere il controllo sulla gestione delle utenze, è prevista l'attivazione di Incaricati della Registrazione per effettuare la registrazione degli utenti secondo le procedure indicate da TI.TT. Inoltre, gli Incaricati provvedono all'attivazione e alla gestione delle utenze e delle caselle di PEC, mediante l'utilizzo dell'utenza di amministrazione.

5.3.2.2.1 Principali funzioni del servizio webmail

La soluzione TI.TT prevede un meccanismo di verifica dell'appartenenza dell'utente al gruppo di titolari che possono accedere alla casella multiutente: solo le persone preventivamente autorizzate potranno accedervi. È inoltre previsto un meccanismo di controllo delle possibili sovrapposizioni tra i vari utenti appartenenti al gruppo: questo meccanismo rende impossibile modificare lo stato di un messaggio di posta preso in carico da un altro utente fino al suo rilascio. L'utente che ha in carico il messaggio può decidere di rilasciarlo (consentendo ad altri utenti di prenderlo in carico) oppure può decidere di completarlo.

Ogni singola operazione effettuata sul messaggio viene tracciata e lo storico delle operazioni può essere visualizzato dal titolare della casella.

La presa in carico di un messaggio consente di rispondere, inoltrare ed inserire eventuali allegati al messaggio originale:

- Si può prendere in carico un messaggio solo se nessun altro utente ha preso in carico il messaggio stesso;
- Il titolare e l'amministratore della casella possono vedere se il messaggio è completato.

5.3.2.2.2 Modalità di accesso alle caselle

- Sistema webmail raggiungibile all'indirizzo di TI.TT https://www.telecompost.it/pec;
- Sistema webmail light raggiungibile all'indirizzo di TI.TT https://webmail.telecompost.it/;
- App TIMPEC;
- Principali client di posta elettronica diffusi sul mercato[4]:
  - Microsoft Outlook
  - Mozilla Thunderbird;
  - Dispositivi Windows Mobile
  - Netscape Messenger
  - Lotus Note Client 6.5.1

5.3.2.2.3 Dimensioni e traffico delle caselle

Il cliente può scegliere tra le diverse opzioni elencate nel documento di descrizione del servizio [2].

5.3.2.3 Caselle applicative

La casella applicativa è riservata a clienti che hanno l'esigenza di gestire un numero elevato di invii giornalieri di PEC, come tipicamente avviene nei casi in cui la casella è gestita attraverso un'applicazione specifica.

La casella applicativa è integrabile mediante i normali strumenti di sviluppo e le normali interfacce di comunicazione ai flussi di lavoro del cliente.

[4] Per i dettagli sulla configurazione è possibile fare riferimento al *Manuale di configurazione del client di posta elettronica per il servizio PEC*, raggiungibile all'indirizzo di accesso alla Webmail: https://www.telecompost.it/pec (link "Manuali").

A differenza delle normali caselle PEC, la casella applicativa è in grado di gestire l'invio e la ricezione di un gran numero di messaggi (e relative ricevute) con notevole velocità ed in modalità completamente automatica, senza l'intervento umano. I dati in ingresso ed uscita dovranno essere archiviati sui sistemi di archiviazione del cliente, all'interno del quale la casella applicativa viene integrata.

5.3.2.3.1 Modalità di accesso

L'interfaccia di comunicazione con la casella applicativa, pur presentandosi come uno strumento per sviluppatori software che hanno l'esigenza di gestire una grande mole di dati in maniera totalmente automatizzata, è la classica interfaccia di posta elettronica dei client di posta, ovvero POP3s/IMAPs/SMTPs. È comunque raggiungibile utilizzando le webmail del servizio o i più comuni client di posta.

5.3.2.3.2 Dimensioni e traffico delle caselle

La casella applicativa standard è disponibile in differenti tagli dimensionali, con determinati volume di traffico dati, espressi sulla base del numero di invii giornalieri di e-mail giornaliere (per i dettagli fare riferimento alla descrizione del servizio [2]).

5.3.2.4 Caselle One-Shot

La PEC One-Shot è attivabile solo attraverso un processo di attivazione specifico del Partner, ma verificato da TI.TT su un dominio predefinito.

La casella accetta in ingresso solamente un messaggio di posta elettronica certificata, inviato da una casella di posta certificata predefinita. L'invio dei messaggi è inibito, inoltre, l'indirizzo PEC non è noto all'utente e non può essere revocato.

5.3.2.4.1 Modalità di accesso

L'accesso alla casella è consentito solo attraverso webapp, a seguito di autenticazione, definita in accordo al contratto di riferimento. L'accesso è limitato nel tempo, per un periodo variabile in accordo al contratto di riferimento.

Per la richiesta del log certificato, a differenza di quanto previsto nel paragrafo 7.2 "Conservazione dei Log", la richiesta per questa tipologia di casella deve contenere: indicazione che si tratta di una PEC OneShot, data di ricezione della stessa e il codice fiscale dell'interessato.

5.3.2.5 Caselle Limited

La casella PEC Limited è attivabile solo attraverso un processo di attivazione specifico del Partner, ma verificato da TI.TT, su un dominio predefinito. Il servizio, gratuito per l'utente, permette di aprire un canale di comunicazione formale tra TIM e il cliente, nel pieno rispetto della normativa Fazzolari e delle policy green di gruppo.

La casella accetta in ingresso solamente messaggi di posta elettronica certificata, inviati da una casella di posta certificata predefinita di TIM. L'indirizzo PEC è noto all'utente per accedere alla lettura dei messaggi. La casella non può essere revocata.

5.3.2.5.1 Modalità di accesso

L'accesso alla casella è consentito a seguito di autenticazione, ed è limitato alla durata del rapporto contrattuale tra TIM e l'utente, per un periodo variabile in accordo al contratto di riferimento.

5.3.2.6 Servizi Aggiuntivi

Al servizio di PEC erogato da TI.TT è possibile aggiungere i servizi opzionali di:

- Archiviazione di Backup: consente di mantenere una copia di tutto quanto transita in casella, su uno spazio disco aggiuntivo.
- Conservazione a Norma: consente di inviare su un sistema di Conservazione a Norma, esterno al sistema di PEC, di tutto quanto presente nell'Archivio di Backup

Tali servizi aggiuntivi sono applicabili a qualsiasi tipologia di casella (per i dettagli fare riferimento alla descrizione del servizio).

5.4 Condizioni di fornitura dei servizi erogati da TI Trust Technologies

In considerazione del fatto che le Condizioni di Utilizzo per i servizi di TI.TT possono variare nel tempo in funzione delle modifiche alle offerte proposte alla clientela, si consiglia di prendere visione della versione pubblicata sul sito internet del Gestore al seguente indirizzo: https://www.trusttechnologies.it/download/modulistica.

5.5 Livelli di servizio e indicatori di qualità

Di seguito sono individuati i livelli di servizio e gli indicatori di qualità del servizio di PEC TI.TT, in conformità a quanto previsto dall'*art. 12 – Livelli di servizio* del **[DM 2/11/05][DM 2/11/05]**[DM 2/11/05].

Livelli di Servizio	**TI TRUST TECHNOLOGIES**
Numero massimo di destinatari contemporanei accettati	1.000
Dimensione massima di ogni singolo messaggio (intesa come prodotto tra il numero dei destinatari e la dimensione del messaggio)	Minore o uguale a 100 MB
Disponibilità del servizio nel periodo di riferimento previsto (quadrimestre)	Maggiore o uguale al 99,8%
Indisponibilità del servizio per il singolo fermo nel periodo di riferimento previsto (quadrimestre)	Minore o uguale al 50%
Tempo massimo per il rilascio della ricevuta di accettazione nel periodo di disponibilità del servizio (calcolato escludendo i tempi di trasmissione)	pochi minuti

Indicatori di qualità	**TI TRUST TECHNOLOGIES**
Disponibilità del servizio (invio e ricezione email)	7 giorni su 7 - h24
Disponibilità del servizio di richiesta di attivazione	7 giorni su 7 - h24
Tempo per l'attivazione di un nuovo account di PEC (dalla ricezione di tutta la documentazione necessaria)	15gg (con record MX corretto)
Tempo massimo per l'esecuzione di interventi di manutenzione che causino il fermo servizio	La durata massima di ogni evento di indisponibilità del servizio è ≤ 50% del totale previsto (il totale previsto è ≤ dello 0,2% del periodo temporale di riferimento che è pari ad un quadrimestre)
Disponibilità del servizio di richiesta da parte del titolare della traccia delle comunicazioni effettuate (log)	dal lunedì al venerdì 7 – 20: Sottoscrizione di un documento cartaceo o informatico (mediante firma qualificata) con il quale si richiede il recupero e la presentazione dei log. Il documento può essere inviato sia per raccomandata A/R sia con posta elettronica certificata.
Accesso ai file di log da parte del personale di TI Trust Technologies S.r.l.	5 giorni la settimana (lunedì - venerdì) dalle ore 7.00 alle 20.00
Tempo massimo per l'invio delle informazioni relative ai file di log dietro richiesta del titolare	Entro 15 giorni. La presentazione dei log avviene esclusivamente mediante l'invio PEC to PEC al recapito indicato dal richiedente di un messaggio contenente i log informativi nei quali sono rappresentati in formato testuale i dati minimi di riferimento previsti dalla normativa ed eventualmente ulteriori informazioni.

Sistema di monitoring con invio di messaggi di alert via email ed sms al presentarsi di malfunzionamenti e situazioni critiche	7 giorni su 7, 24 ore su 24 (solo email)
Assistenza standard tramite call center (trouble ticketing)	5 giorni la settimana (lunedì - venerdì) dalle ore 8.30 alle 18.00
Assistenza di emergenza per i gestori tramite il Network Operations Center (NOC)	7 giorni su 7, 24 ore su 24

5.6 Attivazione del servizio

5.6.1 Procedura di attivazione del servizio standard

Per poter attivare il servizio di Posta Elettronica Certificata agli utenti richiedenti, è necessario siano completate le seguenti fasi:

Id	Macro Fase	Descrizione
1	Definizione Requisiti	Vengono definite le esigenze del Cliente in merito alla configurazione del servizio (dominio, tipologia e numero caselle, dimensione, servizi aggiuntivi, etc.)
2	Sottoscrizione documentazione	Sottoscrizione del Contratto e compilazione della Modulistica (a cura del Cliente).
3	Emissione buono d'ordine (BO) e verifica documentazione	Emissione di un Buono d'Ordine (a cura TIM), che contiene un riferimento del Cliente. Successivamente, il personale TI.TT acquisisce e verifica la documentazione di attivazione compilata di cui al punto precedente (compresa l'effettiva emissione del BO).
4	Individuazione Incaricati	Individuazione (a cura di TI.TT) di uno o più referenti interni del Cliente, c.d. "Amministratori del sistema", a cui demandare le attività di gestione ed amministrazione delle utenze e delle caselle PEC.
5	Attivazione servizio	Approvata la documentazione di attivazione, TI.TT provvede ad attivare la casella di Amministrazione. Comunica, via email, le credenziali di accesso al Cliente e fornisce il Manuale dell'Amministratore PEC, necessario per la gestione del servizio. Le credenziali di accesso hanno validità per 3 giorni. Scaduto tale termine, l'utente deve richiedere un nuovo codice.
6	Verifica del servizio	Gli utenti abilitati accedono al servizio per verificare la correttezza delle credenziali e la corretta funzionalità della casella. In caso di malfunzionamenti è disponibile il servizio Help-desk di TI.TT.

Più in dettaglio, la procedura prevede le figure e le attività seguenti:

Titolare	Il soggetto che richiede l'attivazione del servizio di PEC a beneficio dei propri utilizzatori
Utilizzatore	Il soggetto per il quale viene attivata l'utenza di PEC.
Amministratore del sistema	La persona della struttura del Titolare che effettua: • la **registrazione** degli utilizzatori, collegandosi ad un Portale applicativo raggiungibile su Internet; • **l'attivazione**, la **modifica** e la **cancellazione** delle Caselle di PEC per gli utilizzatori.

Una volta sottoscritto il contratto, il Titolare (generalmente il Legale Rappresentante) individua i propri referenti interni, che agiranno in qualità di Amministratori di sistema per la gestione del servizio PEC.

Il Titolare comunica a TI.TT i nominativi degli Amministratori di sistema, inviando la modulistica prevista.

Ricevuta la modulistica, TI.TT verifica i dati e, successivamente, attiva il cliente sulla piattaforma PEC inviando agli Amministratori del sistema i **codici di accesso al servizio**, unitamente al link del Portale di Provisioning dove reperire la manualistica del servizio. È previsto un cambio della password utente al primo accesso[5].

5.6.1.1 Registrazione degli utenti e attivazione delle caselle

L'Amministratore del sistema accede all'interfaccia di provisioning e crea le caselle degli utenti, comunicandogli le credenziali di accesso. È previsto un cambio della password utente al primo accesso[6].

5.6.2 Procedura di attivazione del servizio con acquisto e-commerce

La figura sottostante rappresenta, schematicamente, il macro-processo di attivazione del servizio PEC con acquisto e-commerce.

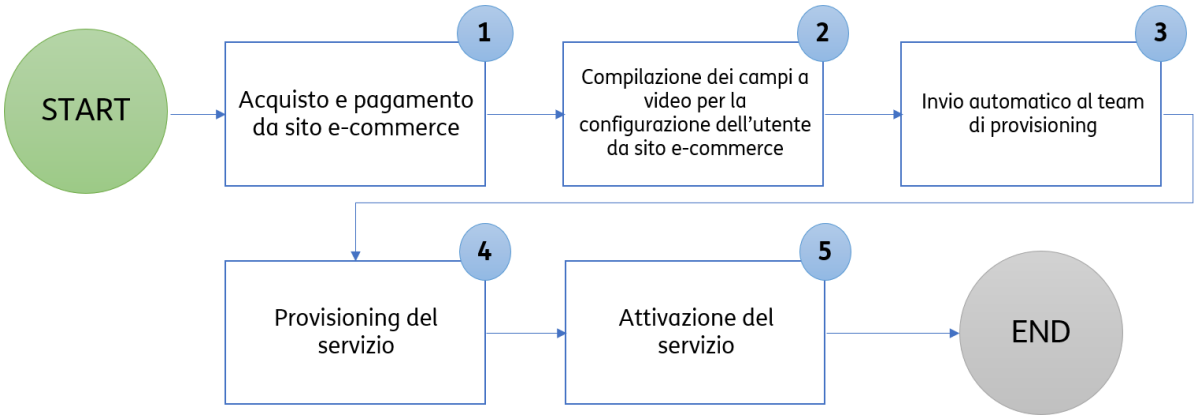


Figura 4

Di seguito sono descritte sinteticamente le singole fasi del processo:

[5] Per maggiori dettagli consultare il *Manuale di amministrazione del servizio PEC*, raggiungibile all'indirizzo di accesso alla Webmail https://www.telecompost.it/webmail/login.jsp ("Manuali").

[6] Per maggiori dettagli consultare il *Manuale di utilizzo del servizio Webmail*, raggiungibile all'indirizzo di accesso alla Webmail https://www.telecompost.it/webmail/login.jsp ("Manuali").

Id	Macro Fase	Descrizione
1	Acquisto e pagamento da sito e-commerce	Il processo di attivazione inizia con il collegamento dell'utente al sito e-commerce, dove sarà completato il processo di acquisto e pagamento. Nel corso della procedura l'utente dovrà accettare le Condizioni di vendita e le clausole vessatorie del servizio.
2	Compilazione dei campi a video per la configurazione dell'utente	Una Welcome Letter, inviata all'utente, conferma l'avvenuto acquisto e invita l'utente a completare l'ordine, attraverso la compilazione di una form a video. La form contiene le informazioni necessarie per l'attivazione del servizio PEC (compresa il numero di P.IVA) e può richiedere l'upload del documento di identità del richiedente.
3	Invio automatico al Gruppo di provisioning di Trust Technologies della documentazione richiesta per l'attivazione	La piattaforma di e-commerce automaticamente invia i dati necessari all'attivazione e li trasmette, via email, al Gruppo di provisioning, per consentire l'avvio delle attività di attivazione della casella.
4	Provisioning del servizio	Il Gruppo di provisioning esamina i dati e, ove richiesta, la documentazione, e provvede alla configurazione della casella. È previsto il contatto con il richiedente qualora i dati inviati non consentissero di procedere con l'attivazione (es. errori ortografici, informazioni parziali, etc.). Se la verifica della documentazione si conclude in modo positivo il Gruppo di provisioning attiva la casella e invia all'utente le credenziali per il primo accesso. Le credenziali di accesso hanno validità per 3 giorni. Scaduto tale termine, l'utente deve richiedere un nuovo codice.
5	Verifica del servizio	Ricevute le credenziali, gli utenti accedono al servizio per verificarne il funzionamento. Nel caso l'utente riscontri problematiche di accesso può contattare l'help-desk di TI.TT.

5.7 Rinnovo del servizio

5.7.1 Gestione dei rinnovi delle caselle PEC

La figura sottostante rappresenta, schematicamente, il macro-processo di rinnovo del servizio PEC.

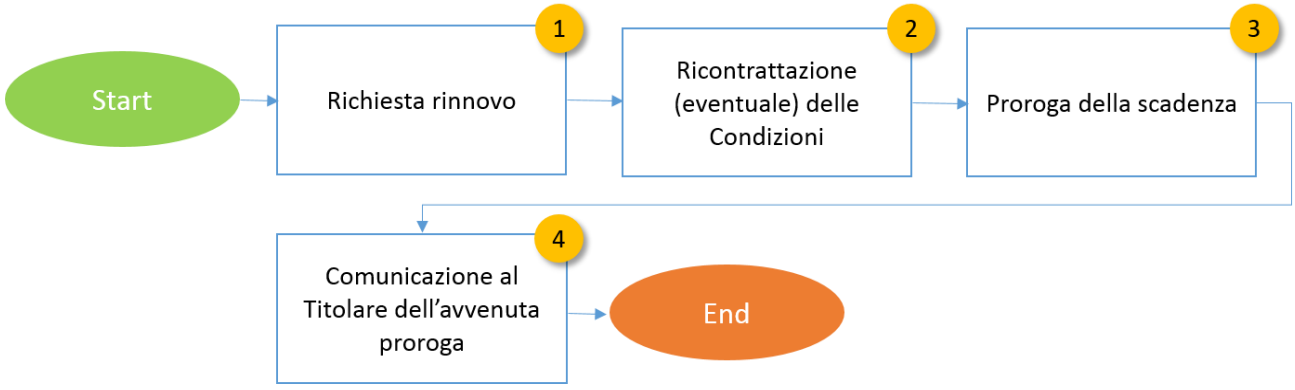


Figura 5

Di seguito sono descritte sinteticamente le singole fasi del processo:

Id	Macro Fase	Descrizione
1	Richiesta rinnovo	Il Titolare inoltra la richiesta di rinnovo del servizio.
2	Eventuale ricontrattazione delle condizioni	In questa fase è possibile una rinegoziazione delle condizioni di fornitura.
3	Proroga della scadenza	TI.TT provvede alle configurazioni necessarie per prorogare la scadenza del servizio.
4	Comunicazione al Titolare dell'avvenuta proroga	Il titolare riceve una comunicazione che attesta il buon esito della procedura e comunica la nuova scadenza.

5.7.2 Gestione dei rinnovi delle caselle PEC acquistate su e-commerce

Il processo di rinnovo del servizio PEC è automatico, con periodicità variabile secondo quanto previsto dal contratto e pagamento ricorrente con il sistema di pagamento elettronico utilizzato nella fase di acquisto.

Nel caso il sistema di pagamento associato non garantisca la copertura economica dell'importo dovuto, TI.TT avvierà i contatti con l'utente invitandolo alla normalizzazione dell'ordine.

5.8 Cessazione del servizio

Le fasi previste per la cessazione del servizio si articolano come segue:

Id	Macro Fase	Descrizione
1	Richiesta cessazione PEC	A seconda della configurazione del servizio, la richiesta di cessazione del servizio può essere inoltrata da: - Rappresentante Legale del Cliente (persona giuridica); - Amministratore del sistema; - Settore TIM contraente di riferimento; - Titolare (persona fisica); - Gestore del servizio. La comunicazione della volontà di cessare il servizio potrà essere inoltrata attraverso i canali riportati nell'area Contatti del sito internet www.trusttechnologies.it .
2	Sottoscrizione documentazione	Il personale di TI.TT provvede ad inviare al Cliente la modulistica per procedere con la cessazione del servizio. Il cliente compila la modulistica e la inoltra ad TI.TT.

3	Cessazione del servizio	Pervenuta la modulistica, si procede con l'attività di cessazione del servizio che prevede: - la cancellazione di tutte le caselle e dati presenti; - la disattivazione di tutte le utenze associate al Cliente; - la cancellazione del Cliente e la *de-certificazione* del dominio. *NOTE*: Qualora il cliente abbia attivo anche il servizio di Archiviazione, dovrà seguire le indicazioni presenti nella modulistica di cessazione, che dovrà in ogni caso essere restituita, debitamente compilata, e inviata via PEC. Se il cliente ha attivo il servizio di Conservazione Sostitutiva della PEC la procedura di cessazione del servizio seguirà due fasi: 1. Procedura di cessazione del servizio PEC, come indicato nel presente paragrafo; 2. Cessazione del servizio di Conservazione a norma della PEC, attraverso una procedura documentata e previamente condivisa con il Cliente (*).
4	Comunicazione avvenuta cessazione	Terminate tutte le attività sopra descritte, il personale di TI.TT provvede a comunicare la cessazione del servizio al Cliente e/o ai Commerciali TIM di riferimento.

(*) il cliente avrà in ogni caso il supporto del Commerciale TIM di riferimento e potrà contattare l'Help desk di TI.TT.

5.8.1 Cessazione di una casella acquistata con e-commerce

Nel caso di acquisto della casella PEC dal sito e-commerce, il processo di cessazione, oltre che dal Gestore del servizio, può essere ricondotto a casistiche specifiche indicate nelle Condizioni generali di vendita dei servizi TI.TT e nella Condizioni specifiche del servizio, pubblicate sui canali di vendita.

5.8.1.1 Cessazione per morosità

TI.TT si riserva la facoltà di dichiarare il Contratto risolto di diritto ai sensi e per gli effetti di cui all'articolo 1456 del codice civile con semplice comunicazione scritta da inviarsi a mezzo raccomandata A/R o tramite comunicazione all'indirizzo di Posta Elettronica Certificata dell'utente.

TI.TT procederà alla cancellazione delle caselle di PEC e del loro contenuto a partire dal trentesimo giorno o dal sessantesimo successivo alla data di scadenza o di scioglimento del contratto, a seconda di quanto definito nelle specifiche condizioni del servizio, salvi gli adempimenti di Legge.

5.8.1.2 Cessazione per volontà dell'utente

L'utente può recedere in qualsiasi momento dal Contratto, con preavviso di almeno 30 giorni.

La volontà di esercitare il diritto di recesso dovrà essere comunicata, a mezzo PEC, o tramite altro strumento elettronico indicato nelle Condizioni specifiche del servizio pubblicate sui canali di vendita.

Il cliente dovrà evidenziare la data a decorrere dalla quale si richiede la cessazione del Servizio.

TI.TT procederà alla cancellazione delle caselle di PEC e del loro contenuto a partire dal giorno indicato dal Cliente per il recesso.

5.8.2 Cessazione del Gestore di PEC

Nel caso di **cessazione dell'attività di provider di Posta Elettronica Certificata**, il Gestore ne darà comunicazione all'Agenzia per l'Italia Digitale almeno sessanta giorni prima della data di cessazione, indicando, qualora conosciuto, il Gestore Sostitutivo che prenderà in carico le caselle di PEC attive.

Contestualmente, con medesimo preavviso, il Gestore comunicherà ai titolari la cessazione dell'attività di Gestore tramite una comunicazione diretta per mezzo PEC e tramite una comunicazione ufficiale pubblicata sul sito internet **[3]**.

Qualora non sia indicato il riferimento del Gestore Sostitutivo che prenderà in carico le caselle PEC, nella suddetta comunicazione sarà specificato che tutte le caselle non saranno più accessibili dal momento della cessazione dell'attività.

6 Cenni sulle infrastrutture e sulle misure di sicurezza del Gestore

Il sistema di PEC di TI.TT presenta tutte le garanzie di sicurezza fisiche ed informatiche compatibili con il servizio erogato. Le caratteristiche di dettaglio della gestione della sicurezza da parte del Gestore di PEC sono contenute nel **Piano della Sicurezza** (documento riservato) depositato presso l'*Agenzia per l'Italia Digitale*.

6.1 Infrastrutture

La piattaforma tecnologica utilizzata da TI.TT per l'erogazione del servizio PEC si basa su **un'architettura modulare e scalabile**, che consente l'adeguamento nel tempo delle *performance* e delle capacità produttive, il dimensionamento del carico, l'interoperabilità con altri soggetti che erogano servizi di PEC e l'integrazione con i servizi di Protocollo informatico.

TI.TT dispone di un pool di risorse con uno specifico know-how sulle tecnologie utilizzate, continuamente aggiornato attraverso attività di scouting e di contatto con i principali vendor del settore. Il Competence Center TI.TT può vantare una collaborazione pluriennale con l'*Agenzia per l'Italia Digitale* e con altri enti italiani e stranieri (Assocertificatori, ecc.) ed è a disposizione dei clienti che necessitano di un supporto tecnico e consulenziale.

L'infrastruttura per l'erogazione del servizio comprende inoltre i seguenti componenti:

- La **Componente di Front-End** realizza tutte le funzionalità necessarie alla gestione e viene inserita nell'ambiente esposto su Internet/Intranet; la Componente di Front-End è l'unica componente autorizzata a colloquiare con la Componente di Back-End posta in ambiente protetto.
- La **Componente di Back-End** è inserita nell'ambiente più protetto della rete del Gestore e non viene esposta all'esterno (ossia non è per nessuna ragione raggiungibile direttamente da Internet/Intranet), essa fornisce le funzionalità fondamentali della PKI e degli altri servizi (Time Stamping Service, Authentication Server, ecc..).
- La **Rete di Gestione** permette agli operatori della Certification Authority di raggiungere i sistemi posti sulle reti di Front End e Back End per le attività di gestione. Gli operatori accedono alla rete di gestione tramite una rete operatori posta all'interno della Certification Authority non raggiungibile dall'esterno. I collegamenti sono effettuati in modalità SSH con accesso controllato da FIREWALL e autenticazione centralizzata LDAP.
- La **Rete di Backup** garantisce il servizio di salvataggio ed archiviazione dei dati.

Le reti di Front-End e di Back-End sono protette da sistemi FIREWALL in configurazione High Availability.

6.2 Riferimento Temporale

A tutti gli eventi previsti dalla normativa, TI.TT nell'ambito dell'erogazione del servizio di *Posta Elettronica Certificata* associa un riferimento temporale garantito da un apposito servizio interno di sincronizzazione temporale.

6.2.1 Sistema di sincronizzazione temporale

La sincronizzazione temporale dei sistemi e degli apparati utilizzati da TI.TT, rispetto alla scala di Tempo Universale Coordinato (UTC), è garantita dall'utilizzo di un sistema composto di due orologi di precisione in associazione con server NTP (Network Time Protocol) incorporato.

Gli orologi di precisione sono sincronizzati con continuità rispetto a due differenti sorgenti di tempo esterne di riferimento accedute con differenti tecnologie: il NIST americano, via telefono e il Sistema GPS internazionale, via radio. Gli orologi utilizzati sono in grado di mantenere un'elevata precisione anche in caso di assenza prolungata delle proprie sorgenti di riferimento.

Gli orologi presenti sui server e sugli apparati di TI.TT sono sincronizzati in modalità automatica rispetto al sistema di sincronizzazione centrale e vengono sottoposti a continuo monitoraggio. Mediante tale monitoraggio, si verifica il corretto allineamento dell'orologio del server rispetto a un ulteriore e differente riferimento temporale esterno italiano erogato dall'ex *Istituto Elettrotecnico Nazionale* "Galileo Ferraris" (IEN) oggi Istituto Nazionale di Ricerca Metrologica o INRIM.

Il buon funzionamento del sistema è garantito da personale di TI.TT espressamente autorizzato. In caso di rilevazione di un disallineamento temporale rilevato dal monitoraggio viene attivato immediatamente il supporto tecnico per la verifica del problema e la sua rapida risoluzione.

6.2.2 Servizio di marcatura temporale

Per *marca temporale* si intende una struttura di dati riferita a un documento informatico e firmata da un *Certificatore Accreditato* in conformità alla normativa vigente. Essa consente di attribuire al documento informatico in oggetto un riferimento temporale (data ed ora) sicuro, verificabile ed opponibile a terzi.

Ciascuna marca generata ed apposta su un documento informatico è indissolubilmente legata al documento stesso grazie a riferimenti certi, quali:

- l'**impronta del documento** (con l'indicazione dell'algoritmo impiegato) che rende univoca l'associazione dello stesso con la marca temporale;
- il **numero progressivo** seriale della marca che ne consente l'identificazione certa nell'ambito dei servizi del Certificatore;
- la **data** e **l'ora** relative alla richiesta pervenuta al Certificatore.

Il servizio di marcatura temporale erogato da TI.TT è conforme ai requisiti previsti dalla normativa in vigore.

6.3 Misure di sicurezza

Fra le principali **misure di sicurezza** che vengono adottate per garantire che le attività del Gestore si svolgano secondo i requisiti di sicurezza richiesti dalla normativa vigente, si ricordano:

- I meccanismi per il controllo dell'accesso logico e fisico alle risorse informatiche e ai sistemi del Gestore, che forniscono le seguenti funzionalità:
  - identificano ed autenticano le persone autorizzate ad accedere alle risorse informatiche;
  - impediscono ad una persona non autorizzata di poter accedere alle risorse informatiche;
  - registrano i dati significativi di tutti gli eventi di accesso in modo che si possa in ogni caso risalire alla persona che ha dato origine ad un determinato evento.
- Il controllo dell'accesso ai locali protetti adotta una politica di autorizzazioni e di procedure di registrazione e auditing.
- L'accesso alla Sala Sistemi del Centro Servizi del Gestore è basata sul principio secondo il quale è consentito l'accesso solo a chi è esplicitamente autorizzato: ogni persona che intende accedere alle risorse della Sala Sistemi è identificata in modo certo, mediante l'utilizzo di una smartcard o un token personale.
- Ogni operazione di firma di messaggi, avvisi e ricevute svolta dal sistema di posta certificata viene tracciata in un registro di controllo al quale viene associata con periodicità almeno giornaliera una marca temporale

6.3.1 Allegati Consentiti

Come da prescrizione dell'ente normativo, tutti i gestori di PEC sono tenuti ad applicare un filtro rispetto alle tipologie (estensioni) di file che possono essere allegati ai messaggi; il filtro su tali estensioni è esteso anche all'interno di archivi compressi e l'individuazione dell'estensione è definita tramite l'identificazione del Media type (o MIME type).

La limitazione è tesa a bloccare le estensioni considerate pericolose, in quanto utilizzate nelle campagne di diffusione malware o che consentano l'esecuzione di codice che può causare la modifica di parametri o dell'ambiente di sistema con ripercussioni negative sulla sua integrità.

6.4 Servizi di emergenza

La sede del Centro Servizi del Gestore è stata costruita con l'intento di proteggere i sistemi dagli eventi di natura disastrosa.

I sistemi critici del Gestore sono stati implementati in ridondanza in modo da sopravvivere all'occorrenza del cosiddetto "primo guasto". In questo modo il Servizio risulta protetto anche da un evento disastroso di lieve intensità o tale da provocare l'intervento dell'impianto di spegnimento incendio, da un eventuale malfunzionamento di un impianto di servizio (es. condizionamento).

In questo caso viene consentito al personale del Centro Servizi di intervenire (con l'ausilio dei fornitori dei contratti di manutenzione) e ripristinare il componente nei tempi tecnici necessari, garantendo i livelli di servizio previsti.

Un disastro di una certa entità che dovesse coinvolgere il sito dell'outsourcer di Pomezia potrebbe però rendere non operativo del tutto o in parte il Gestore.

Per garantire la disponibilità dei servizi essenziali fra quelli offerti dal Gestore a fronte di un disastro di tale natura, è previsto un sito di Disaster Recovery (geograficamente distante) che permette di garantire i servizi minimi previsti dalla normativa.

6.5 Disponibilità e Tempi di ripristino

La tabella seguente riporta la **disponibilità dei siti del Gestore** tenendo in considerazione gli SLA regolati dai contratti di manutenzione con i fornitori esterni:

Disponibilità su base annua	Note
99.8%	La disponibilità è garantita da una infrastruttura in alta affidabilità, con componenti interamente ridondate.

La tabella seguente riporta i **tempi di disponibilità e di ripristino previsti per il servizio di PEC:**

Disponibilità su base quadrimestrale	Durata massima di ogni evento di indisponibilità
99,8%	≤ 50% del totale previsto per il quadrimestre di riferimento

Si precisa che l'architettura del servizio di PEC è completamente ridondata, in modo da evitare disservizio in caso di *single fault* di sistema.

7 Modalità di generazione, conservazione, reperimento e presentazione dei log dei messaggi

In questo capitolo sono descritte le modalità che il Gestore TI.TT adotta per le attività di generazione, conservazione, reperimento e presentazione dei log dei sistemi.

Ulteriori specificazioni relative alla sicurezza dei trattamenti, sono riportate nel Piano della Sicurezza del Gestore, depositato presso l'*Agenzia per l'Italia Digitale*.

7.1 Generazione

Durante le fasi di trattamento dei messaggi il sistema mantiene traccia delle operazioni svolte memorizzando tutte le attività in un registro contenente i seguenti dati:

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

Gli effettivi dati registrati sui singoli log dipendono dalla tipologia dell'operazione tracciata (ricezione di un messaggio, generazione ricevute, ecc.) ed è garantita la possibilità di reperire, su richiesta, le informazioni contenute nei log.

I log generati sono memorizzati con le due seguenti modalità:

- Flat files che vengono ruotati a seconda del:
  - tempo: con periodicità almeno giornaliera;
  - dimensione: secondo una dimensione massima prestabilita (in genere 10 MByte) per consentire un veloce recupero e facile fruibilità delle informazioni in esso contenute.
- Informazioni contenute in tabelle di database Oracle strutturate ed indicizzate in modo da potere recuperare i dati in maniera veloce ed efficace.

I sistemi di front-end generano esclusivamente log di tipo flat-file ed in essi sono memorizzate tutte le informazioni riguardanti:

- Instaurazione del colloquio sicuro (startup TLS – HTTPS etcc.);
- Autenticazione ed identificazione degli utenti che accedono alla piattaforma;
- Ricezione di messaggi da altri server di posta;
- Intercettazione di virus: in questo caso il sistema 'marca' il messaggio come infetto e lo trasmette per la memorizzazione ai sistemi di back-end senza alterarlo;
- Intercettazione dello spam: I messaggi considerati spam vengono "marcati" con una stringa che identifica la % di spam (bassa, media, alta). All'interno della webmail i messaggi saranno visibili nell'apposita sezione dedicata alla posta indesiderata;
- Il tentativo di inoltro di messaggi senza la necessaria autenticazione (RELAY);
- Attività di sincronizzazione degli indici LDIF.

Questi log possono essere generati con diversi livelli di dettaglio di informazioni (debug) ma contengono per ciascun evento almeno:

- il tipo di evento;
- l'identificativo del messaggio trattato (se presente);
- l'indirizzo elettronico del mittente e del destinatario (se presenti);
- il sistema server della piattaforma che lo ha generato;
- il sistema server esterno alla piattaforma coinvolto nel trattamento;
- la data e l'ora dell'evento;
- la componente software di piattaforma che ha gestito l'evento;
- il risultato del trattamento.

I sistemi di Back-end generano entrambi le tipologie di log sopracitati: flat-file e dati su tabelle di database.

Nei flat-file sono contenute informazioni riguardanti il dettaglio di ciascuna fase del trattamento dei messaggi:

- Identificazione del tipo messaggio: busta di trasporto, anomalia ecc.;
- Verifica della firma e della CRL;
- Identificazione del dominio mittente e dei domini destinatari del messaggio;
- Identificazione del mittente e dei destinatari del messaggio;
- Verifiche delle strutture formali: XML, header, etc.;

- Modalità di trattamento da effettuare: generazione ricevute ed anomalie, consegna messaggio, avvisi.

Per la memorizzazione dei log sono presenti tabelle dedicate del database, in queste sono contenuti i dati del trattamento e gli esiti dei trattamenti effettuati; in particolare:

- Tipo di messaggio: trasporto, consegna, avviso, virus ecc.;
- Message-ID del messaggio originale;
- Message-ID dei messaggi generati correlati al messaggio originale;
- Mittente del messaggio originale;
- Destinatario del messaggio originale;
- Gestore mittente;
- Contenuto completo del messaggio (postacert.eml): **solamente in caso di sospetta presenza di virus**, come previsto dalla normativa;
- Data ed ora dell'evento;
- Oggetto del messaggio originale;
- Estratto della firma di ciascun messaggio firmato identificato dai boundary del protocollo S/MIME (smime.p7s);
- Dati XML associati al messaggio.

7.2 Conservazione dei Log

7.2.1 Conservazione dei log su Flat-files e database

I log su flat-file generati sia sui sistemi di front-end che sui sistemi di back-end vengono ruotati con cadenza almeno giornaliera.

Su ciascun server della piattaforma, il processo di rotazione prevede la generazione di una copia del file corrente avente un nome che identifica:

- il server dove è stato generato il log;
- la data e l'ora a cui si riferiscono i log;
- un identificativo della componente software che ha generato il log;
- un identificativo della istanza della componente software che ha generato il log;
- una estensione che identifica la modalità di rappresentazione del log;

Sul server della piattaforma, il processo di estrazione prevede la generazione di un file avente un nome che identifica:

- la data e l'ora a cui si riferiscono i log;
- un identificativo della tipologia di messaggi (inviati/ricevuti);
- un'estensione che identifica la modalità di rappresentazione del log.

La disponibilità dei log su database viene garantita mediante distinti processi di conservazione:

- backup giornaliero incrementale del database;
- backup full settimanale del database con retention pari a due settimane;

copia di tutti i dati contenuti nel database mediante le funzionalità di replica *on-change* del database Oracle sul server di replica presente nel sito di Disaster Recovery.

Ai sensi dell'art. 10, comma 1, lettera a) e b) del DM 2 novembre 2005, tutti gli eventi registrati entro le 24 ore vengono inviati al servizio di conservazione a norma di TI Trust Technologies con i seguenti metadati:

- identificativo univoco del file di log;
- data di chiusura del documento intesa come data della creazione dell'impronta del file di log;
- impronta del file di log;

- gestore dei messaggi di PEC che ha inviato il file in conservazione;
- oggetto, ossia la tipologia del log;
- formato del file di log;
- destinatario del file di log, rappresentato dal responsabile della sicurezza dei log dei messaggi (DM 2 novembre 2005) del gestore di PEC;
- data di inizio del periodo di riferimento per la registrazione dei log;
- data di fine del periodo di riferimento per la registrazione dei log.

Prima di essere inviati al sistema di conservazione viene applica una marca temporale che ne garantisce l'inalterabilità del contenuto alla data.

Come prescritto dalla normativa è garantita la conservazione dei file di log e la possibilità di reperire, a richiesta, le informazioni contenute negli stessi, per un periodo di almeno 30 mesi.

7.3 Reperimento e presentazione dei Log

Il processo di recupero dei log prevede le fasi nel seguito indicate:

- **Fase 1** - La richiesta di accesso ai Log può essere effettuata dai seguenti soggetti:

  I. Il **Titolare** sottoscrive un modulo cartaceo, o informatico mediante firma qualificata, presente sul sito internet del Gestore [3] nell'area Download (CAITMODU.TT.MDRE14001.00 - Modulo Richiesta Log PEC). Il modulo deve essere inviato tramite Posta Elettronica Certificata.
  II. I **soggetti autorizzati per Legge**, con le stesse modalità previste per il Titolare;
  III. Il **Gestore**, che è autorizzato in quanto Incaricato del trattamento dei dati.

- **Fase 2** Il reperimento dei dati di riferimento può avvenire in due modalità, da Database o dal sistema di conservazione.
  I. Database - L'estrazione dei dati di riferimento è effettuata mediante ricerca sul database dei riferimenti necessari al recupero dei log o dei dati relativi allo specifico messaggio di cui si richiede il log del trattamento. Poiché l'interfaccia web si avvale di dati indicizzati presenti su tabelle del database, le fasi di identificazione dei log sono molto veloci ed efficaci anche nel caso si conoscano solamente pochi dati relativi alla trasmissione (ad es. il solo Message-ID, l'indirizzo elettronico del mittente o del destinatario, il gestore ecc.).
  II. Conservazione a Norma - L'estrazione dei dati di riferimento è effettuata tramite ricerca sul sistema di conservazione mediante l'interfaccia di esibizione, attraverso i metadati di riferimento valorizzati con le informazioni fornite dal richiedente.

- **Fase 3** - L'estrazione dei log viene effettuata mediante accesso al server dei log.

- **Fase 4 -** La presentazione dei log avviene esclusivamente mediante l'invio al recapito indicato nel modulo di richiesta Log di PEC.
  In particolare, il processo prevede le seguenti fasi:
  I. copia ed assemblaggio, in un unico archivio, dei log dei messaggi;
  II. invio dell'archivio al richiedente tramite PEC.

8 Obblighi, Responsabilità e Indennizzi

Il Gestore, il Richiedente ed il Titolare assumono gli obblighi previsti dalla normativa vigente (in particolare [[DM 2/11/05]], [VIGIL], [DPR 68/05]), che, essendo soggetti a variazione, sono riportati in versione aggiornata nel documento [1], contenente le condizioni di utilizzo del servizio e pubblicato dal Gestore TI.TT sul proprio sito [3].

8.1 Polizza assicurativa

TI.TT ha stipulato un'apposita assicurazione a copertura dei rischi derivanti da tutte le sue attività, che prevede le seguenti coperture:

TIPO DI RISARCIMENTO	MASSIMALE ANNUO	MASSIMALE PER SINGOLO SINISTRO E SINISTRI IN SERIE
Risarcimento di danni patrimoniali cagionati a Terzi in conseguenza di fatto accidentale verificatosi in relazione allo svolgimento della propria attività, e conseguenti a: • errori, negligenze, ritardi ed omissioni a seguito di obbligazioni assunte contrattualmente e relative alle attività assicurate; • divulgazione di notizie e informazioni avvenute involontariamente o per infedeltà dei dipendenti che abbiano causato richieste di risarcimento da parte di terzi o di Clienti; • azioni ed omissioni compiute nello svolgimento delle attività; • qualsiasi inadempimento delle obbligazioni principali ed accessorie connesse alle prestazioni che contrattualmente deve eseguire nei modi e nei termini tutti previsti dai contratti di fornitura; • fatti o comportamenti di terzi della cui opera TITT si avvalga nell'espletamento delle attività dichiarate, siano essi persone fisiche in rapporto anche occasionale, eventuali subappaltatori, coappaltatori e loro dipendenti, e di cui o con cui TITT sia tenuto a rispondere anche in via solidale; fatti o comportamenti posti in essere da società controllanti o da prestatori d'opera che effettuino prestazioni di carattere professionale o dì servizio e di cui o con cui TITT sia tenuto a rispondere anche in via solidale; • azioni dolose e fraudolente in genere.	€ 2.000.000,00 (due milioni)	€ 2.000.000,00 (due milioni)

9 Protezione dei dati

In considerazione della grande importanza attribuita alla tematica del trattamento dei dati personali nell'ambito dell'organizzazione del Gestore e del Gruppo di appartenenza (TIM), è operativo un sistema organizzativo e normativo interno per garantire che tutti i trattamenti di dati personali si svolgano nel rispetto delle disposizioni di legge vigenti e dei principi di correttezza e liceità dichiarati nel codice etico del Gruppo. Il complesso delle misure previste e messe in atto dal sistema implementato nel Gruppo TIM incorpora anche le misure minime previste dalla [Normativa Privacy].

Tale sistema si caratterizza per alcune importanti elementi di base, fra i quali si ricordano i seguenti:

- i dipendenti che hanno ricevuto la nomina di incaricati ai sensi della [Normativa Privacy], hanno ricevuto dettagliate istruzioni circa le modalità e le misure di sicurezza da adottare per il trattamento dei dati personali.
- Il trattamento dei dati personali avviene sotto la supervisione di Responsabili del trattamento, anch'essi formalmente nominati, i quali hanno a loro volta ricevuto le necessarie istruzioni ed indicazioni operative.
- Apposite funzioni aziendali hanno il compito di definire le Policy per la sicurezza delle informazioni e di verificare, con l'ausilio di funzioni di auditing interno, che esse siano effettivamente applicate.
- il sistema di Policy si basa sulla corretta classificazione degli asset. Con l'ausilio di strumenti di risk assessment, sono individuate le misure di sicurezza più idonee alla tutela dei singoli asset, alla definizione dei controlli e all'applicazione dei sistemi di monitoraggio e verifica più appropriati.
- la tutela dei dati personali non si configura come un processo indipendente, ma risulta del tutto integrato nella gestione corrente della sicurezza degli asset aziendali.

- le politiche di sicurezza fisica e di tutela del patrimonio materiale dell'azienda e le politiche di gestione degli incidenti di sicurezza e delle crisi sono definite tenendo presenti i principi di tutela dei dati personali e le necessità di protezione di questi dati fissate dalla legge.

Nell'ambito delle Policy di sicurezza aziendale sono state sviluppate soluzioni tecniche ed organizzative per la protezione dei dati trasmessi e conservati sulla rete e sui sistemi aziendali, fra cui rientrano:

- protezione dai virus con aggiornamento continuo;
- hardening dei sistemi utilizzati;
- software distribution per l'aggiornamento automatico delle patch di sicurezza sui sistemi aziendali;
- tool e metodologie di vulnerability assessment e risk analisys;
- protezione informatica dei punti di accesso alla rete aziendale;
- partizionamento e protezione delle reti interne;
- monitoraggio della rete e dei sistemi per la prevenzione ed il contrasto degli incidenti di sicurezza.

I dati personali sono trattati, conservati e protetti dal Gestore conformemente a quanto previsto dalla [Normativa Privacy] e secondo quanto riportato nell'Informativa pubblicata nel sito internet del Gestore, all'indirizzo https://www.trusttechnologies.it/download/legale-e-privacy/, in base alla quale l'utente della servizio presta il proprio consenso al trattamento dei propri dati personali, per le finalità dichiarate dal Gestore

10 Assistenza al cliente

TI.TT prevede un servizio di assistenza al cliente, per informazioni di carattere commerciale e per problematiche di natura tecnica.

L'Help Desk è raggiungibile tramite:

- **Numero Verde** nazionale (**800.28.75.24**);
- **Email :** CRPresidio_CA@telecomitalia.it

e fornisce:

a) servizio di informazioni su tematiche di natura commerciale: dal lunedì al venerdì dalle 9.00 alle 17.00, festivi esclusi;
b) servizio di assistenza ai clienti: dal lunedì al venerdì dalle 9:00 alle 17.00, festivi esclusi;
c) servizio di risoluzioni di inconvenienti: 24 ore su 24, 7 giorni su 7.

Un team di tecnici specializzati è in grado di supportare il cliente in tutto il ciclo di vita del servizio.
Le procedure di accesso ai servizi di assistenza tecnica prevedono l'identificazione del cliente mediante codici di riconoscimento e/o password. Questa prima fase di identificazione ha il duplice scopo di impedire un utilizzo fraudolento e di fornire ai tecnici la specifica esatta del servizio sottoscritto dal cliente per il quale si richiede supporto.
Terminata la fase di identificazione i tecnici provvedono ad una prima analisi dell'anomalia segnalata (analisi di 1° livello), assegnando un grado di severità e un codice di priorità. Questa fase prevede anche l'apertura di uno specifico "cartellino di guasto" (trouble ticket) per il tracciamento storico ed una successiva analisi comparativa dei guasti e delle loro cause al fine di adottare azioni correttive.
Nel corso dell'analisi di 1° livello è possibile, qualora non siano necessari interventi ulteriori da parte di specialisti, la immediata risoluzione del problema. In caso contrario l'anomalia verrà fatta scalare ai tecnici specialistici di 2° livello che, nel 100% dei casi, sono in grado di risolvere il problema.
Alla soluzione dell'anomalia il cliente viene avvisato del ripristino completo del servizio e guidato nella verifica della funzionalità al fine di chiudere il "cartellino di guasto".

Nei casi in cui il Cliente abbia concordato con TI.TT un servizio di assistenza dedicato, le modalità personalizzate sono dettagliate nella specifica contrattualistica.