

Posta Elettronica Certificata

Descrizione del servizio

DOCUMENTO DESCRITTIVO

VERSIONI DEL DOCUMENTO

Revisione	Descrizione delle modifiche	Emissione
00	Revisione dei contenuti e aggiornamento Logo e template. Sostituisce analogo documento cod. CERTPECE.TT.SODS10001.04	12/08/2016
01	Par. 2.1 L'offerta PEC di TI Trust Technologies. Variazione canale e-commerce.	03/10/2017
02	Par. 5.3 FAQ specifiche del servizio di PEC di TI Trust Technologies. Modalità di recupero password	12/12/2018

Telecom Italia Trust Technologies è proprietaria delle informazioni contenute nel presente documento, che può essere liberamente divulgato all'esterno del Gruppo Telecom Italia, con riserva di tutti i diritti rispetto all'intero contenuto.

Indice degli argomenti

Scopo del documento	5
1 Il servizio di Posta Elettronica Certificata.....	5
1.1 Descrizione del servizio	5
1.1.1 <i>Punti di forza del servizio</i>	7
1.2 Il mercato di riferimento	7
1.2.1 <i>L'Agenzia per l'Italia Digitale (AgID)</i>	7
1.2.2 <i>I Gestori PEC accreditati</i>	7
2 Il servizio PEC di TI Trust Technologies.....	8
2.1 L'offerta PEC di TI Trust Technologies	8
2.2 Caselle PEC	8
2.2.1 <i>Proprietà delle caselle PEC</i>	8
2.2.2 <i>L'Archivio di backup</i>	9
2.2.3 <i>Conservazione a norma della PEC</i>	10
2.3 Funzionalità accessorie	10
2.3.1 <i>Alert email</i>	11
2.3.2 <i>Alert SMS</i>	11
2.3.3 <i>Inoltro email</i>	11
2.4 Caratterizzazione del servizio.....	11
2.4.1 <i>Domini di Posta Elettronica Certificata</i>	11
2.4.2 <i>Tipologia di casella</i>	12
2.4.2.1 <i>Casella individuale</i>	12
2.4.2.2 <i>Casella multiutente</i>	12
2.4.2.3 <i>Casella applicativa</i>	13
2.5 Elementi distintivi del servizio erogato da TI Trust Technologies	14
2.5.1 <i>Supporto tecnico</i>	14
2.5.2 <i>Antivirus e Antispam</i>	14
2.5.2.1 <i>Antivirus</i>	14
2.5.2.2 <i>Antispam</i>	15
2.5.3 <i>Integrazione con gli altri servizi di Certificazione digitale di TI Trust Technologies</i>	15
2.5.4 <i>Creazione massiva delle caselle PEC e migrazione da altro Gestore</i>	16
3 Procedure di gestione.....	16
3.1 Attivazione standard	16
3.1.1 <i>Macro-processo di delivery delle caselle PEC</i>	16
3.2 Attivazione con acquisto e-commerce da Trust Store.....	18
3.2.1 <i>Macro-processo di delivery delle caselle PEC</i>	18
3.3 Rinnovo.....	19
3.3.1 <i>Macro-processo di gestione dei rinnovi delle caselle PEC</i>	19
3.3.2 <i>Rinnovo di una casella acquistata su Trust Store</i>	19

3.4	Cessazione	20
3.4.1	<i>Macro-processo di gestione delle cessazioni delle caselle PEC</i>	20
3.4.2	<i>Cessazione di una casella acquistata su Trust Store</i>	20
3.4.2.1	<i>Cessazione per causa imputabile all'utente</i>	21
3.4.2.2	<i>Cessazione per volontà dell'utente</i>	21
4	Quadro normativo di riferimento	22
4.1	Le norme.....	22
5	FAQ	25
5.1	FAQ tecniche	25
5.2	FAQ normative.....	26
5.3	FAQ specifiche del servizio di PEC di TI Trust Technologies	27
6	Informazioni sul documento, definizioni, abbreviazioni e termini tecnici	30
6.1	Standard	30
6.2	Definizioni	30
6.3	Abbreviazioni e termini tecnici	33
Appendice	34
	La dematerializzazione dei documenti cartacei	34
Riferimenti	36

Scopo del documento

Questo documento descrive il servizio di Posta Elettronica Certificata (PEC) erogato da TI Trust Technologies S.r.l. (in breve TI Trust Technologies o Gestore) e le procedure per la gestione del servizio. È liberamente disponibile per la consultazione ed il download sul sito di TI Trust Technologies: <https://www.trusttechnologies.it>.

1 Il servizio di Posta Elettronica Certificata

La Posta Elettronica Certificata (PEC) è un servizio che, grazie ad un insieme di strumenti tecnologici e informatici configurati e gestiti sulla base di una precisa normativa, **conferisce pieno valore legale alla trasmissione di un messaggio e-mail da un mittente ad un destinatario**. Al mittente è fornita la documentazione elettronica, con valenza legale, attestante l'invio e la consegna di documenti informatici.

Utilizzando un parallelo con il mondo cartaceo, potremmo dire che la posta elettronica certificata può essere assimilata ad una raccomandata A/R, pur mantenendo delle caratteristiche specifiche, che forniscono ulteriori vantaggi¹.

Tutto questo, ovviamente, se la comunicazione avviene tra due caselle PEC. In caso contrario (es. si invia una PEC ad una casella email di posta elettronica ordinaria) vengono sensibilmente ridotte le caratteristiche di garanzia legale del tracciamento delle operazioni di trasmissione, mancando le necessarie verifiche e conferme dai sistemi del il ricevente.

Dal punto di vista dell'utente finale, l'esperienza d'uso di una casella di posta elettronica certificata non si discosta da quella di casella di posta elettronica ordinaria; ciò che cambia sono i "meccanismi tecnologici" di comunicazione tra sistemi e l'introduzione del concetto di "certificazione tramite ricevute" scambiate dai Gestori PEC mittente e destinatario.

La posta elettronica certificata, per essere tale, deve rispettare le specifiche tecnico-normative di riferimento (per le quali si rimanda al Capitolo 4) emanate dagli organismi competenti che ne stabiliscono le caratteristiche, la validità legale e le modalità di utilizzo.

Il servizio di PEC è sottoposto alla vigilanza da parte di Agenzia per l'Italia Digitale - AgID.

1.1 Descrizione del servizio

La PEC si basa su meccanismi di validazione e certificazione che **garantiscono al mittente**:

- l'inalterabilità del messaggio;
- la notifica, mediante ricevute o avvisi, dell'esito di ciascuna tratta percorsa dal messaggio per raggiungere la casella di destinazione. Tali notifiche costituiscono la prova certa con valore legale dell'avvenuta (o mancata) trasmissione del messaggio.

In particolare, l'**inalterabilità del messaggio** è garantita dall'operazione di imbustamento, dall'inserimento, cioè, del messaggio originale in una "busta", una sorta di sigillo elettronico. I messaggi possono essere "imbustati" dal Gestore in due differenti tipologie di buste:

- **di trasporto**, se il messaggio proviene da una casella di PEC e supera tutti i controlli di esistenza, provenienza e validità della firma;
- **di anomalia**, se il messaggio proviene da una casella e-mail non PEC oppure ha un formato non corretto.

Le **notifiche** si distinguono in due categorie: le ricevute e gli avvisi.

Le ricevute hanno carattere positivo, comunicano e attestano che determinate azioni sono andate a buon fine. Si distinguono in:

- **ricevuta di accettazione**: generata dal Gestore PEC del mittente, certifica al mittente che il messaggio è stato correttamente preso in carico e imbustato per l'invio al destinatario;
- **ricevuta di consegna**: generata dal Gestore PEC del destinatario, certifica al mittente che il messaggio è stato recapitato nella casella di posta del destinatario.

¹ Ad esempio, il contenuto di un messaggio trasmesso via PEC non può essere alterato, mentre questo può accadere con una lettera inviata con il tradizionale mezzo cartaceo, anche usando la posta raccomandata.

Gli **avvisi** hanno carattere negativo e notificano problematiche intercorse nel processo di consegna della PEC. Si contano tre tipi di avviso:

- **avviso di non accettazione:** generato dal Gestore PEC del mittente, indica che il messaggio non è stato accettato dal server incaricato della spedizione. Le cause di mancata accettazione possono essere molteplici (es. presenza di virus, destinatario inesistente, ecc.) e sono contenute nel corpo dell'avviso. In questo caso il messaggio non viene spedito;
- **avviso di mancata consegna:** generato dal Gestore PEC del mittente, indica che il messaggio non ha raggiunto l'infrastruttura PEC del destinatario e pertanto non è stato possibile portare a conclusione il recapito. Le cause di mancata consegna sono, anche in questo caso, molteplici e contenute nel corpo dell'avviso;
- **avviso di rilevazione virus:** generato dal Gestore PEC del mittente o del destinatario, indica che il messaggio originale è stato soggetto a contagio di virus informatico e pertanto non si è potuta portare a termine la consegna al destinatario.

La figura riportata di seguito mostra il funzionamento della PEC. "User A" è il mittente della PEC, "User B" è il destinatario.

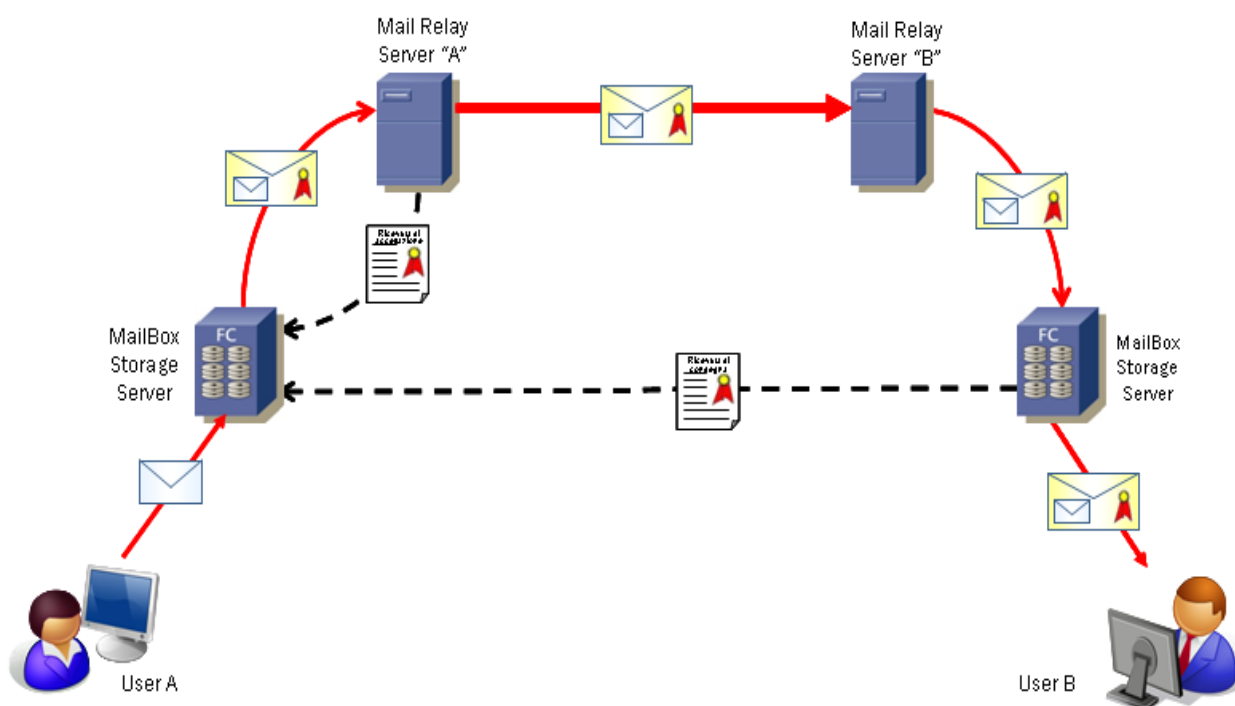


Figura 1

- Il mittente "User A" predispone il messaggio PEC e lo sottopone (lo invia) al Gestore PEC mittente. Il Gestore PEC mittente, dopo le opportune verifiche (es. autenticazione mediante Username e Password), riconosce il mittente come autorizzato alla spedizione di PEC.
- Riconosciuto l'utente, il Gestore PEC mittente verifica la correttezza formale (per esempio assenza di destinatari in Ccn, correttezza formale degli indirizzi dei destinatari, coincidenza fra l'utente autenticato al client ed il mittente della PEC, rispetto dei limiti sul numero massimo di destinatari contemporanei del messaggio PEC e, in caso positivo, restituisce al mittente la ricevuta di accettazione che notifica l'avvenuta presa in carico del messaggio per l'invio.
- Il Gestore PEC mittente invia il messaggio al Gestore destinatario inserendolo in una busta di trasporto firmata per permettere al Gestore destinatario di verificarne l'inalterabilità durante il trasporto.
- Il Gestore PEC destinatario, una volta ricevuto il messaggio PEC, consegna al Gestore PEC mittente una ricevuta di presa in carico che attesta il passaggio di consegne tra i due Gestori. Il Gestore PEC destinatario verifica in fase di ricezione la correttezza del messaggio e si accerta che non siano presenti virus informatici.
- Se il messaggio ha superato tutti i controlli di cui sopra viene consegnato alla casella di posta del destinatario che può quindi leggerne il contenuto.

Va specificato che la Posta Elettronica Certificata offre ai suoi utilizzatori la garanzia della **certificazione dell'esito dell'invio del messaggio** (recapito del messaggio nella casella PEC del destinatario, ovvero avviso in caso di impossibilità di consegna entro le 24 ore), ma **non offre la garanzia della lettura** da parte del destinatario. In altre

parole nulla è detto sul fatto che il destinatario abbia letto o meno il messaggio PEC, ma, al pari della ricevuta di ritorno della raccomandata tradizionale, si hanno garanzie sull'avvenuto recapito, in caso di perfetto funzionamento dell'intero processo.

Su tutti gli eventi che costituiscono la transazione di elaborazione dei messaggi (generazione notifiche, generazione buste, etc.) il Gestore appone un riferimento temporale ed una firma elettronica che consente di rendere manifesta la provenienza ed assicurarne l'autenticità e l'integrità. Una marca temporale è apposta quotidianamente anche sul log dei messaggi, cioè sul registro informatico che traccia tutte le operazioni relative alle trasmissioni effettuate mediante PEC.

Qualora il mittente smarrisca una o più notifiche, può richiedere, al Gestore del servizio, il log file delle fasi di trasmissione che, dal punto di vista legale, ha lo stesso valore delle notifiche. I Gestori PEC sono obbligati, secondo la normativa vigente, a conservare i log delle transazioni della PEC per un periodo di 30 (trenta) mesi.

1.1.1 Punti di forza del servizio

Il servizio PEC, se comparato con la tradizionale raccomandata A/R e con un servizio di posta elettronica ordinaria, mostra una serie di vantaggi:

- notifica del recapito o della mancata consegna della mail;
- **validità legale** del recapito nella casella di posta certificata destinataria;
- **integrità** del messaggio e dei suoi allegati;
- piena **tracciabilità** della casella mittente di un dato messaggio e di conseguenza del suo titolare evitando per esempio contraffazioni ed i falsi tipici (es. phishing);
- **costi inferiori** rispetto a quello delle raccomandate. Il costo di invio di una tradizionale raccomandata A/R spesso è già di base superiore al costo annuale di una casella PEC. Tale costo cresce in funzione del numero di pagine e del peso del plico;
- **disponibilità 24x7** di un servizio di elevata qualità, garantito dai Gestori di PEC e dalla vigilanza degli organismi preposti (ogni Gestore deve garantire, su base quadrimestrale, una disponibilità pari al 99.8%, che equivale di fatto ad un servizio perennemente attivo);
- disponibilità, presso il Gestore, del **tracciamento delle operazioni** svolte durante le fasi di trasmissione (Log File) per 30 mesi;
- garanzia della **riservatezza dei dati personali**;
- garanzia della **sicurezza della comunicazione**, protetta anche da servizi antivirus e antispyware.

1.2 Il mercato di riferimento

Come meglio precisato nel Capitolo 4, il servizio di PEC è regolato da una normativa molto stringente che sottopone i Gestori che lo erogano ad una disciplina dettagliata e alla vigilanza da parte di un ente di emanazione governativa (Agenzia per l'Italia Digitale – AgID).

1.2.1 L'Agenzia per l'Italia Digitale (AgID)

L'**Agenzia per l'Italia Digitale – AgID** è l'ente che ha sostituito DigitPA (già **CNIPA – Centro Nazionale per l'Informatica nella Pubblica Amministrazione**) nell'ambito dell'attuazione delle politiche governative in tema di Innovazione e tecnologie.

Nell'ambito del servizio di Posta Elettronica Certificata, secondo quanto stabilito nella Normativa in vigore, AgID svolge le funzioni seguenti:

- verificare il rispetto dei requisiti richiesti per l'esercizio dell'attività di Gestore di PEC;
- tenere l'elenco pubblico dei Gestori di PEC;
- effettuare le attività di vigilanza e controllo sul servizio erogato dai Gestori di PEC;
- supportare le Pubbliche Amministrazioni ai fini dell'introduzione della PEC nei procedimenti Amministrativi.

1.2.2 I Gestori PEC accreditati

I Gestori di PEC (diversi dalle Pubbliche Amministrazioni) devono avere natura giuridica di società di capitali e capitale sociale interamente versato non inferiore a un milione di euro. Inoltre, devono possedere i requisiti di onorabilità richiesti ai soggetti che svolgono funzioni di amministrazioni, direzione e controllo presso le banche (*di cui all'art. 26 del testo unico delle leggi in materia bancaria e creditizia, di cui al decreto legislativo 1° settembre 1993, n.385, e successive modificazioni*).

AgID sottopone i Gestori ad un'attività di verifica ispettiva per accertare:

- adeguatezza del personale;
- processi di sicurezza;
- esperienza nell'erogazione di servizi analoghi;
- ridondanza e servizi di emergenza.

I singoli Gestori hanno l'obbligo di:

- rispettare i requisiti, le prescrizioni tecniche e i livelli di servizio minimi;
- dotarsi della certificazione ISO per il processo PEC;
- dotarsi di una polizza assicurativa di copertura dei rischi dell'attività e dei danni causati a terzi;
- consentire l'attività di vigilanza da parte di incaricati dell'ente.

L'elenco pubblico dei Gestori è reso disponibile sul sito dell'Agenzia per l'Italia Digitale e contiene, per ogni Gestore, le seguenti indicazioni:

- Denominazione sociale;
- Sede legale;
- Rappresentante Legale;
- indirizzo Internet;
- data di iscrizione all'elenco;
- data di cessazione ed eventuale Gestore sostitutivo.

2 Il servizio PEC di TI Trust Technologies

2.1 L'offerta PEC di TI Trust Technologies

L'offerta di Trust Technologies prevede tagli standard predefiniti che sono configurati come segue:

- solo **mailbox**
- **mailbox + Archivio di backup**
- **mailbox + Archivio di backup + Conservazione a norma** dei messaggi e delle ricevute.

Per il dettaglio dell'offerta è disponibile la sezione dedicata sul sito istituzionale del Gestore di PEC, raggiungibile all'indirizzo:

<https://www.trusttechnologies.it/trusted-services/pec-posta-certificata-privati-professionisti-imprese/> .



Da oggi **Aziende, Professionisti e Privati possono acquistare online la propria casella PEC:**

- collegandosi direttamente al sito e-commerce di Trust Technologies ("**Trust Shop**"), disponibile al link <https://www.trusttechnologies.it/trusted-services/pec-posta-certificata-privati-professionisti-imprese/>.

2.2 Caselle PEC

2.2.1 Proprietà delle caselle PEC

Il servizio standard di Posta Elettronica Certificata di TI Trust Technologies presenta le seguenti caratteristiche:

- **3 tipologie** di casella (Individuale, Multiutente, Applicativa);
- **fino a 5 Gb di spazio** mailbox;
- invio di messaggi di dimensione fino a 100 Mb;
- invio dello stesso messaggio fino a 1.000 destinatari contemporaneamente;
- generazione della ricevuta di accettazione nell'arco di pochi secondi;
- recupero della password, in caso di smarrimento, in maniera completamente autonoma con ricezione della stessa via SMS o email di posta elettronica ordinaria (impostazione configurabile dall'utente);
- gestione **Contatti e Gruppi**;
- **ricerca** messaggi e ricevute.

La casella PEC può essere configurata in abbinamento a:

- **Archivio di backup**, dei messaggi e delle ricevute transitati nella propria casella PEC;
- **Conservazione a norma** dei messaggi e delle ricevute di PEC secondo quanto previsto dalla normativa specifica del servizio (DPCM 03/12/2013).

2.2.2 L'Archivio di backup

L'Archivio di backup è il servizio che consente di avere una copia dei messaggi e delle ricevute transitati nella propria casella PEC, proteggendoli da eventuali cancellazioni accidentali.

Per garantire il recupero di tutti i messaggi e delle ricevute, **l'Archivio di backup deve essere abbinato alla casella dal momento dell'attivazione della stessa.**

Il servizio presenta le seguenti caratteristiche:

- ✓ tagli dimensionali da **1 Gb, 5 Gb e 10 Gb**;
- ✓ gestione dei messaggi archiviati: **Ricerca, Visualizzazione e Download** in locale dei messaggi archiviati;
- ✓ **alert al raggiungimento dell'80%** dello spazio occupato.

L'Archivio di backup è abilitato con la funzionalità di **cancellazione dei messaggi** (l'opzione è attivabile dall'amministratore della PEC del Cliente). Ciascun titolare della casella potrà quindi procedere alla liberazione dello spazio occupato attraverso due modalità, a scelta:

- a) selezione manuale di uno o più messaggi tra quelli presenti (vedi figura 2);
- b) liberazione automatica del 75% dello spazio occupato, partendo dai contenuti più datati.

Per ulteriori dettagli sulle caratteristiche e le funzionalità dell'Archivio di backup è possibile fare riferimento ai Manuali presenti nel portale Webmail PEC, all'indirizzo: <https://www.telecompost.it/manuali/>.

Archivio mese corrente

Selezionare: Tutti, Nessuno Azioni ▼

|< << Precedente | Pagina 1 di 3 | Successiva >> >|

<input type="checkbox"/>	Da	Acronimo	Oggetto	Data	Download	Cancella
<input type="checkbox"/>	team.babel@newsvippec.babel.it	RIC_COM_A_CON	Prova Virus	09/01/2015 18:13		
<input type="checkbox"/>	team.babel@newsvippec.babel.it	AVV_M_CON_VIR	Prova Virus	09/01/2015 18:12		
<input type="checkbox"/>	team.babel@newsvippec.babel.it	AVV_M_CON_VIR	Prova Virus	09/01/2015 18:12		
<input type="checkbox"/>	team.babel@newsvippec.babel.it	RIC_ACC	Prova Virus	09/01/2015 18:07		
<input type="checkbox"/>	team.babel@newsvippec.babel.it	BUS_TRA	Prova Virus	09/01/2015 18:07		
<input type="checkbox"/>	posta-certificata@newsvippec.babel.it	BUS_TRA	Avviso di creazione archivio	09/01/2015 18:06		
<input type="checkbox"/>	posta-certificata@newsvippec.babel.it	BUS_TRA	Avviso di creazione archivio	09/01/2015 18:06		
<input type="checkbox"/>	posta-certificata@newsvippec.babel.it	BUS_TRA	Avviso di creazione archivio	09/01/2015 18:06		
<input type="checkbox"/>	posta-certificata@newsvippec.babel.it	BUS_TRA	Avviso di creazione archivio	09/01/2015 18:06		
<input type="checkbox"/>	posta-certificata@newsvippec.babel.it	BUS_TRA	Avviso di creazione archivio	09/01/2015 18:06		
<input type="checkbox"/>	posta-certificata@newsvippec.babel.it	BUS_TRA	Avviso di creazione archivio	09/01/2015 18:06		
<input type="checkbox"/>	Stefano <smangia@babel.it>	BUS_ANO	BUSTA DI ANOMALIA PER TE. D	09/01/2015 18:06		
<input type="checkbox"/>	posta-certificata@newsvippec.babel.it	BUS_TRA	Avviso di creazione archivio	09/01/2015 18:06		
<input type="checkbox"/>	posta-certificata@newsvippec.babel.it	BUS_TRA	Avviso di creazione archivio	09/01/2015 18:06		
<input type="checkbox"/>	posta-certificata@newsvippec.babel.it	BUS_TRA	Avviso di creazione archivio	09/01/2015 18:06		

Selezionare: Tutti, Nessuno Azioni ▲

|< << Precedente | Pagina 1 di 3 | Successiva >> >|

Figura 2

2.2.3 Conservazione a norma della PEC

Alle caselle configurate con il servizio di Archivio di backup è possibile associare anche il servizio di **Conservazione a norma dei messaggi e delle ricevute di PEC**.

Il servizio **garantisce nel tempo l'autenticità, integrità, affidabilità, leggibilità e reperibilità dei dati**.

La Conservazione a norma consente al Responsabile dei contenuti, e al massimo 2 suoi delegati, di ricercare, consultare ed esibire, quando occorre, i messaggi, secondo quanto previsto dalla normativa del servizio (DPCM 3 dicembre 2013 in tema di "Regole tecniche per il protocollo informatico ai sensi degli articoli 40 –bis, 41, 47, 57 –bis e 71, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005").

Il servizio di Conservazione a norma è **disponibile nei tagli da 1 Gb, 5 Gb e 10 Gb**.

Al raggiungimento della soglia di 10 Gb è possibile richiedere l'**ampliamento** dello spazio disponibile per **multipli dimensionali di 5 Gb**.

[Il servizio di Conservazione a norma NON equivale al servizio di Archivio di backup.](#)

È regolato dalle rigide normative emesse dall'Agenzia per l'Italia Digitale, che prevedono un processo di accreditamento all'Albo pubblico dei Conservatori e un'attività di vigilanza del rispetto della normativa – DPCM 03/12/2013 – sempre a cura di AgID.



- I Clienti che hanno attivato il servizio di Conservazione a norma possono effettuare la ricerca dei messaggi nell'Archivio di backup solo per l'ultimo periodo;
- Il contenuto dell'Archivio di backup più vecchio di 45 giorni, se non diversamente contrattualizzato, viene quotidianamente spostato in Conservazione a norma in maniera automatica. Di conseguenza i messaggi precedentemente presenti nell'Archivio di backup saranno consultabili esclusivamente nell'ambiente di Conservazione a norma o, se ancora presenti, nella casella.
- Per motivi di sicurezza legati all'incidentale smarrimento/cancellazione dei messaggi in Archivio di backup, i Clienti che hanno attivato il servizio di Conservazione a norma non hanno a disposizione la funzione di cancellazione dei messaggi in Archivio di backup.

2.3 Funzionalità accessorie

Incluse nel servizio base sono attivabili, a discrezione del Cliente, una serie di funzionalità accessorie, utili per la gestione della propria casella:

- servizio di **alert via email**;
- servizio di **alert via SMS**;
- servizio di **inoltrato a posta elettronica ordinaria**.

Le funzionalità di notifica sono particolarmente utili qualora il traffico di Posta Elettronica Certificata non sia tale da giustificare una consultazione quotidiana della casella. Si ricorda che, dal punto di vista legale, un messaggio di posta certificata si intende consegnato nel momento in cui è reso disponibile nella mailbox del destinatario.



Le funzionalità di notifica non esonerano in alcun modo il titolare dall'obbligo di controllo diretto del contenuto della propria casella di PEC.

Tutte le funzionalità sopra elencate sono abilitate dall'amministratore della PEC del Cliente e personalizzate da ciascun utente attraverso una semplice interfaccia.

2.3.1 Alert email

Il servizio prevede l'invio, ad uno o più indirizzi di posta ordinaria, di una **email di notifica della ricezione di nuovi messaggi** sulla casella PEC. L'utente può impostare la frequenza con la quale ricevere tali notifiche.

Il numero massimo di indirizzi di posta ordinaria che possono essere impostati è pari a 3.

La frequenza temporale di notifica può essere di 1, 12, 24, 36, 48 ore.

2.3.2 Alert SMS

Il servizio prevede l'invio, ad uno o più recapiti telefonici, di un **SMS di notifica della ricezione** di nuovi messaggi sulla casella PEC. L'utente può impostare la frequenza con la quale ricevere le notifiche.

Il numero massimo di recapiti telefonici selezionabili è pari a 3.

Le frequenze selezionabili per la ricezione delle notifiche sono di 2, 4, 6, 12 e 24 ore.

2.3.3 Inoltro email

Il servizio provvede **all'inoltro automatico di tutto il traffico ricevuto sulla casella di Posta Certificata** su un indirizzo di Posta elettronica ordinaria indicato dal Titolare. Tale funzionalità è utile per la gestione remota della casella di PEC.



I messaggi PEC inoltrati sulla casella di Posta elettronica ordinaria non hanno valore legale.

Possono essere configurate per l'inoltro al massimo 2 caselle di posta elettronica ordinaria.

2.4 Caratterizzazione del servizio

Il servizio di PEC offerto da TI Trust Technologies si caratterizza sulla base delle diverse possibili combinazioni dei seguenti elementi:

- **Dominio** sul quale sono configurate le caselle di posta elettronica:
 - **standard**, dominio preimpostato di TI Trust Technologies;
 - **personalizzato**, dominio scelto dal cliente (l'acquisto del dominio è a cura del cliente);

- **Tipologia di Casella** (casella individuale, casella multiutente, casella applicativa).

2.4.1 Domini di Posta Elettronica Certificata

Il sistema dei nomi di dominio internet è un sistema convenzionale e standardizzato che consente e semplifica l'identificazione precisa di un server sulla rete e dei relativi servizi da esso offerti traducendo un indirizzo numerico, quale è, ad esempio, l'indirizzo IP in un nome "alfabetico" e facilmente memorizzabile. Esempi di domini internet sono "telecomitalia.it"; "sole24ore.com".

Un dominio internet è composto tipicamente da 3 componenti: **XXX.NOMEDOMINIO.TLD**, dove:

- **XXX** rappresenta il **servizio specifico offerto**, ad esempio "www" per il world wide web (le pagine internet), "ftp" per il protocollo di trasferimento file, ecc;
- **NOMEDOMINIO**, detto anche **prefisso**, è il nome "alfabetico" che facilita la memorizzazione e il riconoscimento del soggetto che lo ha "registrato" (ovvero che ne è proprietario, es. "telecomitalia");
- **TLD** (top-level domain), detto anche **suffisso**, può assumere diversi significati. In particolare, la Internet Assigned Numbers Authority (IANA), l'organismo che regola la gestione dei domini internet, classifica attualmente i domini in tre tipi differenti:
 - domini di primo livello **nazionali** (country code top-level domain o ccTLD): usati da uno stato o una dipendenza territoriale. È costituito da due lettere, per esempio jp per il Giappone e it per l'Italia, o eu per l'Unione Europea;
 - domini di primo livello **generici** (generic top-level domain o gTLD): usati (almeno in teoria) da particolari classi di organizzazioni (per esempio, com per organizzazioni commerciali). Tale suffisso è di tre o più lettere. La maggior parte dei gTLDs sono disponibili in tutto il mondo, ma per ragioni storiche gov, mil e edu sono riservati rispettivamente al governo, all'esercito e agli enti educativi statunitensi;
 - domini di primo livello **infrastrutturali** (infrastructure top-level domain): il dominio di primo livello arpa è l'unico esistente.



Le caselle di Posta Elettronica Certificata devono essere configurate e gestite su un dominio internet definito e dedicato.

Non è quindi possibile effettuare la gestione mista sullo stesso dominio di caselle email ordinarie e caselle di PEC.

Il dominio utilizzato per la PEC deve essere gestito dai server mail del Gestore di PEC. Tale dominio può essere:

- **quello del Gestore di PEC** accreditato presso l'ente di vigilanza che fornisce il servizio. In tal caso le caselle avranno una connotazione del tipo xxxxx@DOMINIO_GESTORE_PEC.YY che, nel caso del servizio di PEC erogato da TI Trust Technologies diventa [xxxxx@NOME_AZIENDA.telecompost.it](#);
- **un dominio ad hoc** registrato dal cliente finale appositamente per il servizio PEC la cui gestione in esercizio, per quanto concerne gli aspetti mail (record MX – Mail Exchanger), è demandata al Gestore di PEC. In questo caso le caselle di PEC saranno del tipo [xxxxx@NOME_AZIENDA.YY](#);
- **un dominio di terzo livello**, ossia un livello secondario di un dominio già esistente che ha forma AAAA.NOME_AZIENDA.YY (es. "PEC.NOME_AZIENDA.YY") la cui gestione in esercizio, per quanto concerne gli aspetti mail (record MX – Mail Exchanger), è demandata al Gestore di PEC. In questo caso le caselle di PEC saranno del tipo [xxxxx@TERZO LIVELLO.NOME_AZIENDA.YY](#).

2.4.2 Tipologia di casella

2.4.2.1 Casella individuale

La Casella Individuale è di **esclusiva pertinenza del singolo utente** che vi accede mediante userid e password personali.

Per consentire al Cliente di mantenere il controllo sulla gestione delle utenze, è prevista l'individuazione di incaricati alla registrazione degli utenti (c.d. "amministratori della PEC") che effettuano, secondo le procedure indicate da TI Trust Technologies, la registrazione e l'attivazione delle utenze e delle caselle di PEC, nonché la gestione dell'utenza.

La casella di posta elettronica certificata individuale può essere utilizzata:

- ✓ Attraverso un portale web, c.d. Webmail PEC, raggiungibile da qualunque browser collegandosi all'indirizzo <https://www.telecompost.it/pec>;
- ✓ attraverso il nuovo portale Webmail Light, con funzionalità ridotte rispetto al portale Webmail tradizionale, ma dotato di interfaccia moderna, veloce ed ancora più intuitiva.
- ✓ attraverso un comune client di posta (Outlook, Outlook Express, Mozilla Thunderbird, etc.).

2.4.2.2 Casella multiutente

La casella multiutente (o "istituzionale") è una casella a cui è **consentito l'accesso da parte di un gruppo di utenti autorizzati** (fino ad un massimo di 10).

Questo servizio nasce per soddisfare le esigenze di organizzazioni di grandi dimensioni e di enti della Pubblica Amministrazione in cui, normalmente, la corrispondenza in ingresso o in uscita è gestita centralmente da operatori addetti alla classificazione e all'inoltro dei messaggi verso le funzioni preposte alla lavorazione piuttosto che all'invio verso destinatari esterni.

Anche in questo caso, allo scopo di consentire al Cliente di mantenere il controllo sulla gestione delle utenze, è prevista l'individuazione di incaricati alla registrazione degli utenti (c.d. "amministratori della PEC") che effettuano, secondo le procedure indicate da TI Trust Technologies, la registrazione e l'attivazione delle utenze e delle caselle di PEC, nonché la gestione dell'utenza.

La casella di posta certificata multi-utente può essere utilizzata:

- ✓ Attraverso un portale web, c.d. Webmail PEC, raggiungibile da qualunque browser collegandosi all'indirizzo <https://www.telecompost.it/pec>;
- ✓ attraverso il nuovo portale Webmail Light, con funzionalità ridotte rispetto al portale Webmail tradizionale, ma dotato di interfaccia moderna, veloce ed ancora più intuitiva.
- ✓ attraverso un comune client di posta (Outlook, Outlook Express, Mozilla Thunderbird, etc.).

L'interfaccia Webmail tradizionale, in particolare, soddisfa le esigenze di:

- sicurezza nell'accesso e protezione dei contenuti: Tutte le operazioni effettuate dagli operatori (risposta, accesso alla corrispondenza elettronica, lavorazione etc.) sono registrate;
- praticità di utilizzo: il sistema attribuisce a ciascun messaggio un codice identificativo progressivo che consente di gestire flussi consistenti di corrispondenza elettronica in entrata ed in uscita, garantendo le funzionalità di visualizzazione, ordinamento e lavorazione della corrispondenza elettronica. 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. Il servizio offre, inoltre, numerose funzioni d'uso che permettono di snellire e velocizzare le operazioni di trattamento della corrispondenza elettronica. È infine previsto un meccanismo di controllo delle possibili sovrapposizioni tra i vari utenti appartenenti al gruppo. Ciò consente la presa in carico di un messaggio, da parte di un utente, per la sua lavorazione e rende impossibile una contestuale modifica da parte di altro utente, fino a che il messaggio non viene rilasciato.

2.4.2.3 Casella applicativa

Il servizio di PEC di TI Trust Technologies, oltre che nelle modalità individuale e multiutente viste in precedenza, può essere fornito anche in modalità "applicativa" per soddisfare **specifiche esigenze di integrazione in strumenti di**

gestione del workflow e/o altri strumenti software. Tale tipologia di servizio non prevede l'archiviazione dei contenuti (messaggi e ricevute) che è interamente demandata al software applicativo in cui verrà integrata.



La casella applicativa è rivolta ai clienti che, attraverso l'integrazione con i propri sistemi informatici, hanno esigenza di automatizzare la gestione della PEC.

La casella applicativa è integrabile mediante i normali strumenti di sviluppo e le normali interfacce di comunicazione. A differenza delle normali caselle PEC, la casella applicativa è in grado di **gestire l'invio di un gran numero di messaggi con notevole velocità ed in modalità completamente automatica**, senza quindi l'intervento umano. I dati in ingresso ed uscita dovranno essere archiviati sui sistemi di archiviazione propri del sistema all'interno del quale la casella applicativa viene integrata.



La casella applicativa non è una casella PEC tradizionale bensì una interfaccia di comunicazione verso l'infrastruttura PEC di TI Trust Technologies da utilizzarsi da parte di sviluppatori che integreranno le funzioni di creazione messaggi, archiviazioni messaggi e ricevute all'interno dei loro sistemi.

L'interfaccia di comunicazione con la casella applicativa, pur essendo la classica interfaccia POP/SMTP dei clienti di posta elettronica, si presenta come uno strumento per sviluppatori software che hanno esigenza di gestire una grande mole di dati in maniera totalmente automatizzata.

2.5 Elementi distintivi del servizio erogato da TI Trust Technologies

2.5.1 Supporto tecnico

Il servizio di PEC di TI Trust Technologies beneficia di un'assistenza in grado di risolvere sia problematiche di natura commerciale che tecnica.

L'Help Desk è raggiungibile tramite **Numero Verde nazionale (800.28.75.24)** e fornisce:

1. informazioni base su tematiche di natura commerciale e tecnica: dal lunedì al venerdì dalle 9.00 alle 17.00, festivi esclusi;
2. risoluzione 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, risolveranno 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".

2.5.2 Antivirus e Antispam

Il servizio di PEC TI Trust Technologies è erogato unitamente ai servizi di controllo Antivirus e Antispam per la protezione e il filtraggio delle mail in transito da e per le caselle PEC.

I due assicurano il controllo dei messaggi in transito sulle caselle PEC affinché:

- i messaggi in arrivo ed in uscita dalle caselle mail PEC non siano “infettati” da virus informatici in grado di compiere azioni potenzialmente nocive;
- i messaggi in ingresso ed in uscita dalle caselle non siano messaggi di spam, indesiderati e/o *phishing* con l'intento di sottrarre dati all'utente della casella PEC.

I servizi Antivirus e Antispam vengono forniti mediante l'impiego di appositi strumenti (hardware e software) che, filtrando tutto il traffico in transito, ne garantiscono il controllo.

Le funzionalità offerte lavorano in modo totalmente trasparente per il cliente, senza necessità di alcuna configurazione, in quanto sono gestiti centralmente. All'utilizzatore finale è lasciato solo il compito di verificare, nel caso dello spam, che i messaggi contrassegnati come tali (vengono considerati spam solo i messaggi di posta elettronica ordinaria) siano realmente messaggi validi (c.d. gestione dei falsi positivi) mentre, in caso di rilevazione di virus, come anticipato nel paragrafo di descrizione tecnica del servizio, viene generato un avviso di “mancato invio/ricezione del messaggio contenente virus”.

2.5.2.1 Antivirus

Un Antivirus è tipicamente un software che può essere installato direttamente sul sistema da proteggere o essere integrato in uno specifico hardware, chiamato comunemente *security appliance*, da installare a monte del sistema da proteggere.

L'antivirus basa il suo funzionamento principalmente sulla ricerca nella memoria RAM o all'interno dei file (siano essi e-mail, o altri tipologie di file) di uno schema tipico di ogni virus. In sostanza ogni virus è composto da un numero ben preciso di istruzioni (righe di codice che contengono le istruzioni da eseguire) che possono essere viste come una stringa di byte ben definita. Il programma antivirus non fa altro che cercare se questa stringa di byte è presente all'interno dei file o in memoria e, quando presente, rimuoverla o rimuovere il file che la contiene.

Il successo di questa tecnica di ricerca si basa, come intuibile, sul costante aggiornamento degli schemi tipici che l'antivirus è in grado di riconoscere. Tale aggiornamento è curato dai produttori dei software ed è una vera e propria banca dati a livello globale di tutti i virus (noti) esistenti. La scoperta di nuovi virus avviene, in genere, a seguito delle segnalazioni degli utenti e/o da gruppi specializzati nell'individuazione di nuovi virus.

Oltre alla tecnica di riconoscimento dei virus per confronto delle stringhe di byte, esiste anche un'altra tecnica di riconoscimento detta “ricerca euristica”. La ricerca euristica consiste nell'analisi comportamentale dei diversi software presenti sul sistema alla ricerca di istruzioni, anche non note, ma sospette perché tipiche del comportamento dei virus (come, ad esempio, la ricerca di file di un certo tipo o le routine di inserimento di codice all'interno di altri file). Le tecniche di ricerca euristica prevedono, oltre alla mera analisi comportamentale, anche le ricerche sulle eventuali varianti di virus già conosciuti; un virus, infatti, variando una o più istruzioni nel suo codice originario, può ottenere lo stesso risultato finale (azioni malevole) pur presentandosi con una forma differente. Questa variazione di forma data dal cambio parziale delle righe di codice che lo compongono, infatti, comporta l'impossibilità di riconoscimento del virus mediante il solo database delle firme (almeno fino al suo successivo aggiornamento). La ricerca euristica, analizzando il risultato finale del codice sospetto è in grado di valutare e discriminare se si tratta di codice virale o meno, agendo di conseguenza (rimozione o autorizzazione).

Uno strumento (software) antivirus, stante la premessa appena fatta, si compone di diverse parti (o “moduli”), alcune indipendenti tra loro, che svolgono compiti differenti:

- il file (o database) delle firme: sono file che contengono tutte le firme (le stringhe note) dei virus conosciuti. Questa parte è fondamentale ed essenziale per il funzionamento corretto di qualsiasi altro componente ed il suo costante aggiornamento è alla base del successo dell'antivirus;
- l'eseguibile che è in grado di ricercare (utilizzando i file delle firme) e riconoscere il virus all'interno dei singoli file. Questo componente è il cuore di tutto il sistema; in sostanza è l'antivirus vero e proprio ed è comunemente “chiamato scanner”;
- l'eseguibile che rimane residente in memoria e richiama l'antivirus (lo scanner) ogni qual volta viene creato/modificato un nuovo file o viene modificata una zona di memoria per controllare che il computer non sia stato infettato con questa operazione. Comunemente viene chiamato “monitor” ed è la parte in genere “visibile” all'utilizzatore di un Antivirus;
- altri componenti, strettamente appartenenti al sistema antivirus, che variano da prodotto a prodotto, come ad esempio l'eseguibile che effettua gli update del file delle firme e di tutti gli altri eseguibili dell'antivirus (software update);
- eventuali moduli aggiuntivi, quali il modulo anti-spam che, pur non essendo propriamente legati alle funzionalità dell'antivirus, spesso ne completano le funzionalità. Questi moduli possono funzionare in maniera indipendente o essere integrati nelle funzionalità dell'antivirus per fornire protezione completa da virus e spam.

2.5.2.2 Antispam

Unitamente al servizio di antivirus le caselle PEC di TI Trust Technologies sono dotate di sistema antispam. Uno strumento antispam è tipicamente un software che può essere installato:

- direttamente sul sistema ed integrato con il server mail che deve proteggere, oppure
- integrato in uno specifico hardware da installare a monte del sistema da proteggere.

Il servizio PEC di TI Trust Technologies, come richiesto dalla normativa specifica, garantisce in ogni caso la ricezione delle email di Posta Elettronica Ordinaria (PEO) e di Posta Elettronica Certificata (PEC).

Tuttavia, ove venga rilevata attività sospetta, il sistema antispam contrassegnerà come "Spam" i soli messaggi di PEO e, laddove il traffico anomalo persista, verrà contattato l'utente (per i messaggi in uscita) o il Gestore della PEC (per i messaggi in entrata), per comunicare e verificare quanto accaduto.

È prevista la sospensione del/degli account compromessi a discrezione del Gestore ed in particolare nel caso in cui non si riesca a contattare gli utenti e circoscrivere in tempi brevi il traffico anomalo.

2.5.3 Integrazione con gli altri servizi di Certificazione digitale di TI Trust Technologies

Il servizio di PEC, abbinato ai servizi di Firma digitale e Conservazione a norma, permette la gestione elettronica di tutte le fasi del ciclo di vita di un documento, dalla creazione alla consultazione e trasmissione, fino alla conservazione per tutto il tempo necessario, consentendo in tal modo la "dematerializzazione" del documento cartaceo.

2.5.4 Creazione massiva delle caselle PEC e migrazione da altro Gestore

TI Trust Technologies mette a disposizione, previa contrattualizzazione specifica, un servizio di **prima creazione massiva delle caselle**.

È inoltre disponibile, previa contrattualizzazione specifica, un servizio di caricamento dei messaggi preesistenti nelle caselle PEC, verso le nuove caselle PEC create, come nel caso di **migrazione del servizio da un altro gestore di PEC**.

Ciò è possibile solo ed esclusivamente se vengono rispettate le seguenti condizioni:

1. Le nuove caselle PEC mantengono lo stesso nome di quelle dismesse;
2. i dati vengono consegnati a TI Trust Technologies su supporto elettronico messo a disposizione dal Cliente e in formato Maildir++.

3 Procedure di gestione

Le procedure di gestione del servizio coinvolgono, oltre a TI Trust Technologies, le seguenti figure lato Cliente:

- **Riferimento tecnico del Cliente:** colui che richiede l'attivazione del servizio di PEC a beneficio degli utilizzatori;
- **Incaricati alla gestione e amministrazione delle caselle PEC** (c.d. amministratori della PEC): sono i soggetti che effettuano la registrazione degli utilizzatori e l'attivazione delle relative caselle. Se viene acquistata una sola casella le attività di gestione ed amministrazione delle utenze sono a carico di TI Trust Technologies;
- **Utilizzatori:** sono i soggetti per cui viene attivata l'utenza di PEC (utenti finali del servizio).

3.1 Attivazione standard

3.1.1 Macro-processo di delivery delle caselle PEC

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

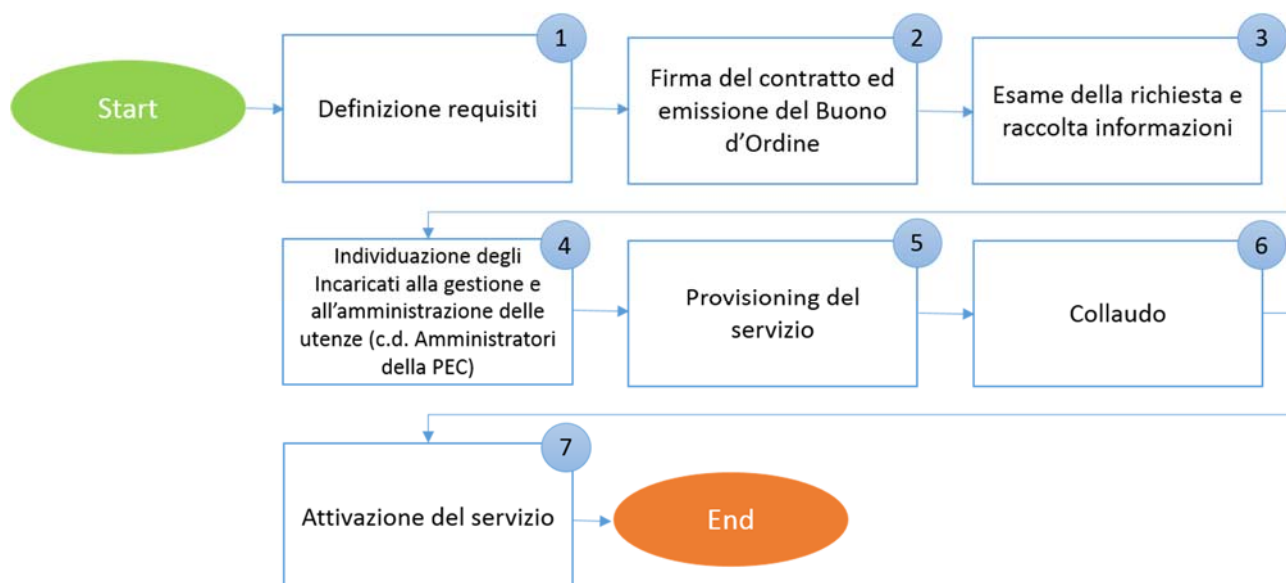


Figura 3

Di seguito sono descritte sinteticamente le singole fasi del processo:

Id	Macro Fase	Descrizione
1	Definizione dei requisiti	Il processo di attivazione inizia con la raccolta delle esigenze lato Cliente in merito alle caratteristiche del servizio di cui si richiede l'erogazione (dominio, tipologia e numero caselle, dimensioni, servizi aggiuntivi, etc.).
2	Firma del contratto ed emissione del buono d'ordine	Una volta consolidati i requisiti, sono necessarie: <ul style="list-style-type: none"> • la sottoscrizione del contratto da parte del Cliente; • l'accettazione delle Condizioni di fornitura del servizio di Posta Elettronica Certificata erogato da TI Trust Technologies; • l'emissione di un buono d'ordine. Tale BO deve contenere il Riferimento tecnico del cliente, che sarà responsabile della compilazione della documentazione necessaria per l'attivazione del servizio.
3	Esame della richiesta e raccolta informazioni	Ricevuto il buono d'ordine, TI Trust Technologies provvede ad effettuare le verifiche necessarie. In caso di esito positivo, TI Trust Technologies contatta il titolare per raccogliere le informazioni necessarie per l'attivazione delle caselle richieste.
4	Individuazione degli Incaricati alla gestione e all'amministrazione delle utenze (c.d. amministratori della PEC)	Nel caso in cui il Cliente acquisti più di una casella è richiesto che il Riferimento tecnico del cliente individui, a sua volta, gli Incaricati alla gestione e all'amministrazione delle utenze e ne comunichi le generalità a TI Trust Technologies mediante invio (via fax) della Scheda di attivazione . Se viene acquistata una sola casella le attività di gestione ed amministrazione delle utenze sono a carico di TI Trust Technologies.
5	Provisioning del servizio	Ricevuta la Scheda di Attivazione, TI Trust Technologies esamina la richiesta e, in caso di accettazione, provvede alle seguenti operazioni: <ul style="list-style-type: none"> • attivare il Cliente; • se l'attivazione riguarda più di una casella, TI Trust Technologies genera e comunica (via mail) le credenziali per l'accesso al

		<p>servizio da parte dell'Amministratore della PEC, per le attività di gestione ed amministrazione delle utenze;</p> <ul style="list-style-type: none"> • se l'attivazione riguarda una casella, TI Trust Technologies genera e comunica (via mail) le credenziali per l'accesso al servizio all'utilizzatore finale; • se l'attivazione prevede il servizio <u>aggiuntivo</u> di prima creazione massiva delle caselle, TI Trust Technologies genera e comunica (via mail) le credenziali per l'accesso ai singoli utenti oppure all'Amministratore della PEC; • se l'attivazione prevede il servizio <u>aggiuntivo</u> di caricamento dei dati nelle caselle, TI Trust Technologies provvede a scaricare i messaggi dal supporto fornito dal Cliente e ad inserirli nelle caselle di PEC attivata (i tempi di tale attività dipendono dalla mole dei dati da caricare nelle caselle); • inviare il c.d. Manuale dell'Incaricato PEC che contiene le istruzioni per l'Amministratore della PEC (attivazione utenti, creazione caselle, etc.). L'Amministratore della PEC, mediante apposita interfaccia, attivano gli utenti del servizio, associano all'utente la casella PEC creata e gli comunicano le proprie credenziali di accesso.
6	Collaudo	<p>Ricevute le credenziali, gli utenti accedono al servizio per verificare la correttezza delle credenziali e il funzionamento del servizio.</p> <p>Nel caso l'utente riscontri problematiche di accesso è disponibile l'help-desk di TI Trust Technologies.</p>
7	Attivazione del servizio	<p>Completate le verifiche, constatata la validità delle credenziali di accesso e il corretto funzionamento delle caselle, il servizio è considerato attivo.</p>

3.2 Attivazione con acquisto e-commerce da Trust Store

3.2.1 Macro-processo di delivery delle caselle PEC

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



Figura 4

Di seguito sono descritte sinteticamente le singole fasi del processo:

Id	Macro Fase	Descrizione
----	------------	-------------

1	Acquisto e pagamento da sito e-commerce: https://store.cloud.trusttechnologies.it	Il processo di attivazione inizia con il collegamento dell'utente al sito e-commerce Trust Store, dove sarà completato il processo di acquisto e pagamento (tramite Paypal). 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 i dati necessari all'attivazione del servizio PEC e prevede 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 genera la documentazione elettronica di attivazione e la trasmette, via email, al Gruppo di provisioning, per consentire l'avvio delle attività necessarie all'attivazione della casella.
4	Provisioning del servizio	Il Gruppo di provisioning esamina la documentazione e provvede alla configurazione della casella richiesta. 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.
5	Collaudo	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 Trust Technologies.

3.3 Rinnovo

3.3.1 Macro-processo di gestione dei rinnovi delle caselle PEC

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

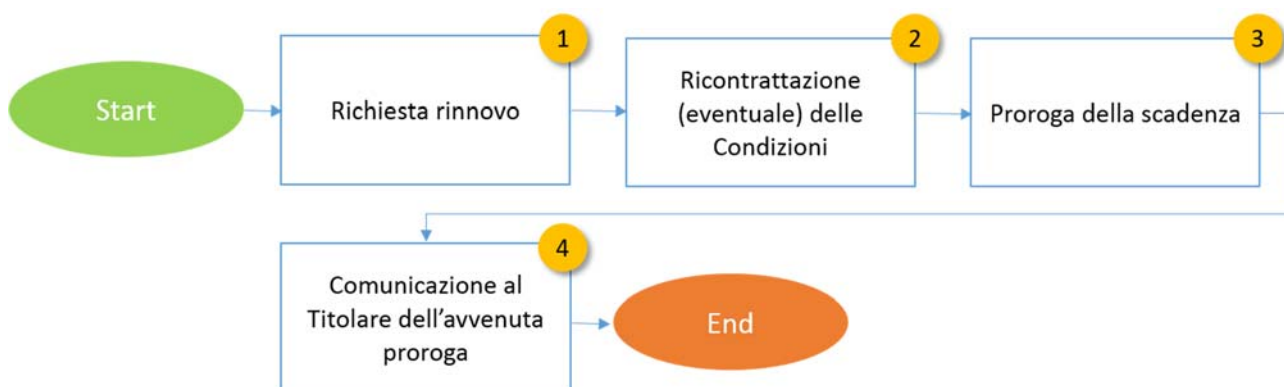


Figura 5

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 Trust Technologies 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.

3.3.2 Rinnovo di una casella acquistata su Trust Store

Il processo di rinnovo del servizio PEC su Trust Store è automatico, con periodicità annuale e pagamento ricorrente con il sistema di pagamento utilizzato nella fase di acquisto (Paypal).

Fino a quando l'utente non cessa la propria casella dal pannello personale di Trust Store (area MyAccount) la casella sarà automaticamente rinnovata di anno in anno.

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

3.4 Cessazione

3.4.1 Macro-processo di gestione delle cessazioni delle caselle PEC

La figura sottostante rappresenta, schematicamente, il macroprocesso di cessazione del servizio PEC.

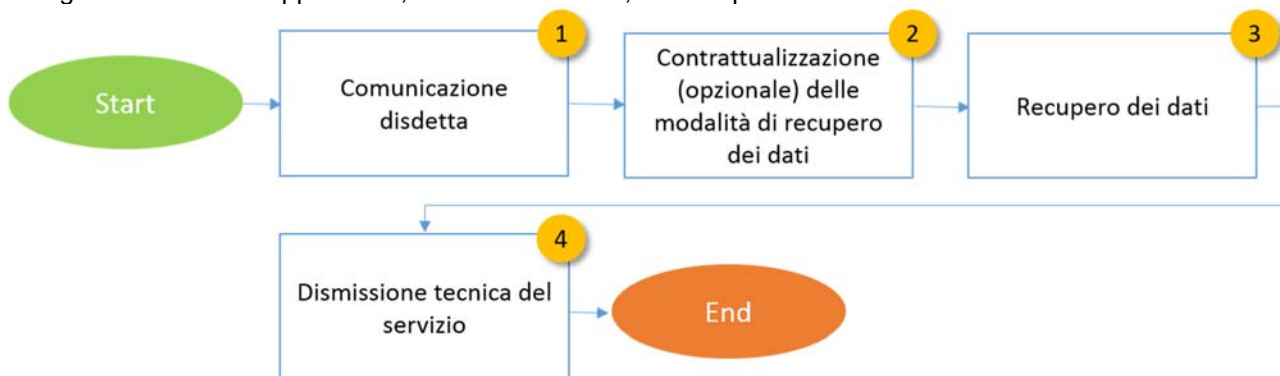


Figura 6

Di seguito sono descritte sinteticamente le singole fasi del processo:

Id	Macro Fase	Descrizione
1	Comunicazione disdetta	Il Titolare comunica la disdetta.
2	Contrattualizzazione (opzionale) delle modalità di recupero dei dati con il Cliente	Vengono contrattualizzate con il Cliente le attività di recupero dei dati. Se richiesto, saranno resi disponibili solo i messaggi presenti nelle caselle di PEC nel momento della cessazione delle caselle. I dati verranno forniti in formato Maildir++ su supporto elettronico fornito dal Cliente stesso. Non è prevista la fornitura del contenuto degli archivi di backup che verranno cancellati contestualmente alla chiusura del servizio.
3	Eventuale recupero dati	Il cliente recupera i propri dati.

4	Dismissione tecnica del servizio	TI Trust Technologies provvede alla dismissione tecnica del servizio. Si ricorda che l'eliminazione di una casella determina la cancellazione definitiva di tutti i messaggi in essa contenuti, che non potranno essere recuperati in alcun modo.
---	----------------------------------	--

3.4.2 Cessazione di una casella acquistata su Trust Store

Nel caso di acquisto della casella PEC dal sito e-commerce di TI Trust Technologies, il processo di cessazione può essere ricondotto a casistiche specifiche, distinte per:

- 1) **Causa imputabile all'utente**, come da art. 21 "Risoluzione del Contratto" delle Condizioni generali di vendita dei servizi TITT, pubblicate nello Store online.
- 2) **Volontà dell'utente**, come da art. 17 "*Durata e recesso dai Servizi a canone anticipato e rinnovo automatico annuale*" e art. 22 "*Diritto di Ripensamento*" presenti nelle Condizioni generali di vendita dei servizi TITT, pubblicate nello Store online.

3.4.2.1 Cessazione per causa imputabile all'utente

TI Trust Technologies 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 Trust Technologies procederà alla cancellazione delle caselle di PEC e del loro contenuto a partire dal trentesimo giorno successivo alla data di scadenza o di scioglimento del contratto, salvi gli adempimenti di Legge.

3.4.2.2 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, al seguente indirizzo: recesso-ttstore@tpec.telecomitalia.it. Nella comunicazione di recesso, il Cliente dovrà evidenziare la data a decorrere dalla quale si richiede la cessazione del Servizio.

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

4 Quadro normativo di riferimento

Il servizio di Posta Elettronica Certificata costituisce un tassello del percorso di digitalizzazione della Pubblica Amministrazione il cui obiettivo finale è la **“dematerializzazione” della documentazione**. Tale obiettivo sarà raggiunto mediante il progressivo incremento della gestione documentale informatizzata e la sostituzione dei supporti tradizionali in favore del documento informatico, a cui la normativa ha conferito pieno valore giuridico già dal 1997 (Legge 15 marzo 1997 n. 59, articolo 15 comma 2).

La PEC è un servizio prettamente italiano, non legato in alcun modo ad una normativa comunitaria e/o internazionale, ed è regolamentato da una serie di norme che, da un lato ne stabilisce valore legale, modalità di utilizzo, caratteristiche e standard tecnici di riferimento, dall'altro ne regola l'erogazione da parte dei Gestori del servizio.

4.1 Le norme

Le norme ad oggi in vigore, su cui si fonda la regolamentazione normativa del servizio PEC, sono elencate nella tabella sottostante che riporta anche una breve descrizione dei contenuti e dei punti rilevanti della norma stessa.

Norma	Descrizione
DPR 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" (G.U. del 28 aprile 2005, n. 97)	"Stabilisce le caratteristiche e le modalità per l'erogazione e la fruizione dei servizi di trasmissione di documenti informatici mediante Posta Elettronica Certificata". In particolare il decreto: <ul style="list-style-type: none"> • sancisce il valore legale della trasmissione di messaggi mediante PEC; • disciplina le modalità di utilizzo della PEC nei rapporti con la Pubblica Amministrazione e tra privati cittadini; • definisce i requisiti richiesti a privati che intendano esercitare l'attività di Gestore di PEC; • attribuisce all'ente di vigilanza le funzioni di controllo delle attività esercitate dai soggetti iscritti nell'elenco dei Gestori di PEC.
D. Lgs. del 7 marzo 2005, n. 82 (G.U. del 16 maggio 2005, n. 93), "Codice dell'Amministrazione Digitale" e successive modifiche	Costituisce il principale strumento giuridico per le applicazioni delle nuove tecnologie alla Pubblica Amministrazione, nonché alle società interamente partecipate da enti pubblici o con prevalente capitale pubblico inserito nel conto economico consolidato dalla pubblica amministrazione. <p>In particolare, in merito alla PEC, il decreto:</p> <ul style="list-style-type: none"> • sancisce l'obbligo, per le Pubbliche Amministrazioni centrali all'utilizzo della posta elettronica certificata per le comunicazioni che necessitano di una ricevuta di invio e di una ricevuta di consegna con i soggetti interessati che ne fanno richiesta e che hanno preventivamente dichiarato il proprio indirizzo di posta elettronica certificata; • sancisce la validità della verifica della provenienza delle comunicazioni trasmesse attraverso sistemi di posta elettronica certificata; • obbliga le Pubbliche Amministrazioni, e gli altri soggetti ai quali devono essere applicate le disposizioni del presente codice, ad istituire e pubblicare nell'Indice PA almeno una casella di posta elettronica certificata per ciascun registro di protocollo; • specifica che il cittadino può rivolgersi all'indirizzo istituzionale di posta elettronica certificata pubblicato dalle Pubbliche Amministrazioni sui propri siti, per qualsiasi richiesta, obbligando le amministrazioni ad assicurare un servizio che renda noti al pubblico i tempi di risposta;

	<ul style="list-style-type: none"> • sancisce che la trasmissione del documento informatico per via telematica, effettuata mediante la posta elettronica certificata, equivale, nei casi consentiti dalla legge, alla notificazione per mezzo della posta; • stabilisce che la data e l'ora di trasmissione e di ricezione di un documento informatico trasmesso mediante posta elettronica certificata sono opponibili ai terzi se conformi alle disposizioni di cui al decreto del Presidente della Repubblica 11 febbraio 2005, n. 68, ed alle relative regole tecniche.
<p>DM 2 novembre 2005, “Regole tecniche per la formazione, la trasmissione e la validazione, anche temporale, della posta elettronica certificata” (G.U. del 15 novembre 2005, n. 266) e successive “Regole tecniche del servizio di trasmissione dei documenti informatici mediante posta elettronica certificata”.</p>	<p>“Definisce le regole tecniche relative alle modalità di realizzazione e funzionamento della Posta Elettronica Certificata”. In particolare il decreto:</p> <ul style="list-style-type: none"> • formalizza gli standard tecnici di riferimento; • definisce le caratteristiche dei messaggi gestiti e delle tipologie di ricevute; • definisce i livelli minimi di disponibilità del servizio e di limiti di utilizzo; • introduce, per i Gestori di PEC, l'obbligo della certificazione ISO 9001:2000; • definisce i requisiti richiesti ai Gestori sia in termini organizzativi che di competenza, esperienza ed aggiornamento professionale del personale.
<p>Provvedimento del Direttore dell'Agenzia delle Entrate n. 188870 del 22 dicembre 2005 “Disposizioni attuative dell'articolo 32, terzo comma, del decreto del Presidente della Repubblica 29 settembre 1973, n. 600, e dell'articolo 51, quarto comma, del decreto del Presidente della Repubblica 26 ottobre 1972, n. 633, relative alle modalità di trasmissione telematica delle richieste e delle risposte, nonché dei dati, notizie e documenti in esse contenuti”, (G.U. del 10 gennaio 2006, n. 7).</p>	<p>Stabilisce che ciascun operatore finanziario è tenuto a dotarsi di un indirizzo di posta elettronica certificata (PEC), tramite il quale ricevere le richieste di indagine da parte degli Organi preposti ai controlli, ai sensi degli articoli 32, primo comma, numero 7), del DPR n. 600/1973 e dell'articolo 51, secondo comma, numero 7), del DPR n. 633/72, nonché, entro il termine previsto dalle stesse norme, trasmettere in risposta i dati oggetto della richiesta.</p>
<p>Provvedimento del Direttore dell'Agenzia delle Entrate n. 32951 del 24 febbraio 2006 “Disposizioni attuative dell'articolo 32, terzo comma, del decreto del Presidente della Repubblica 29 settembre 1973, n. 600, e dell'articolo 51, quarto comma, del decreto del Presidente della Repubblica 26 ottobre 1972, n. 633, relative alle modalità di trasmissione telematica delle richieste e delle</p>	<p>Introduce modifiche ed integrazioni al provvedimento del Direttore dell'Agenzia delle Entrate del 22 dicembre 2005, in particolare:</p> <ul style="list-style-type: none"> • proroga i termini previsti dallo stesso; • stabilisce un intervallo temporale fra il termine per la comunicazione dell'indirizzo di posta elettronica certificata da parte degli intermediari finanziari e quello iniziale per l'inoltro delle richieste e delle risposte in materia di accertamenti bancari e finanziari; • specifica termini e modalità della comunicazione degli indirizzi di posta elettronica certificata per gli intermediari finanziari di nuova costituzione; • introduce precisazioni che tengono conto delle specificità tecnico-operative rappresentate da alcune categorie di intermediari finanziari.

risposte, nonché dei dati, notizie e documenti in esse contenuti” (G. U. del 10 Marzo 2006 n. 58).	
Provvedimento del Direttore dell’Agenzia Entrate, 12 novembre 2007 , “Disposizioni integrative e correttive del provvedimento del 22 dicembre 2005 pubblicato nella Gazzetta Ufficiale n. 7 del 10 gennaio 2008”.	Introduce modifiche ed integrazioni al provvedimento del Direttore dell’Agenzia delle Entrate del 22 dicembre 2005, in particolare: <ul style="list-style-type: none"> • semplifica il formato delle richieste e delle risposte per agevolare gli adempimenti da parte degli operatori finanziari; • introduce la possibilità di cumulare e trasmettere simultaneamente con un’unica transazione le risposte negative al fine di snellire i flussi telematici innescati dalle richieste degli organi di controllo fiscale e di ridurre i costi amministrativi sostenuti dagli operatori finanziari; • regola, attraverso il canale telematico, la cancellazione dall’elenco dei destinatari delle indagini finanziarie degli operatori che cessano la propria attività.
Legge 28 Gennaio 2009, n. 2 (G.U. del 28 Gennaio 2009, n. 22, supplemento ordinario 14)	Sancisce l'obbligatorietà: <ul style="list-style-type: none"> • dell'adozione di una casella PEC o di "un analogo indirizzo di posta elettronica basato su tecnologie che certifichino data e ora dell'invio e della ricezione delle comunicazioni e l'integrità del contenuto delle stesse, garantendo l'interoperabilità con analoghi sistemi internazionali” per iscritti ad Albi, professionisti ed imprese. La legge precisa inoltre che le comunicazioni tra professionisti iscritti ad albi, imprese e Pubblica Amministrazione, che abbiano provveduto a tali adempimenti possono essere inviate attraverso la posta elettronica certificata <i>o analogo indirizzo di posta elettronica</i>, senza che il destinatario debba dichiarare la propria disponibilità ad accettarne l'utilizzo; • dell'utilizzo esclusivo della posta elettronica certificata da parte della Pubblica Amministrazione per le comunicazioni e le notificazioni aventi come destinatari dipendenti della stessa o di altra Amministrazione Pubblica.

Tale quadro normativo è completato dalla documentazione prodotta dall'ente di vigilanza (Circolari, Raccomandazioni e Norme Integrative emesse da AgID, già CNIPA e AIPA), che dispone in materia di regolamentazione e standardizzazione tecnico operativa, che, in sintesi:

- definisce le procedure di iscrizione nell’elenco pubblico dei Gestori di posta elettronica certificata (Circolare CNIPA 21 maggio 2009, n. 56);
- descrive le modalità di esercizio, da parte del CNIPA, dei compiti di vigilanza e controllo sull'attività esercitata dai Gestori di PEC (Circolare CNIPA 7 dicembre 2006, n. 51);
- migliora la comprensione di alcuni temi che potenzialmente possono presentare ambiguità interpretative (Note integrative alle norme tecniche contenute nel DM 2 novembre 2005, G.U. del 15 novembre 2005, n. 266).

5 FAQ

5.1 FAQ tecniche

Quali caratteristiche ha in più la PEC rispetto all'email tradizionale?

La PEC, per quanto in apparenza simile alla posta elettronica "tradizionale", offre un servizio più completo e sicuro, prevedendo:

- certificazione dell'invio e della consegna del messaggio (ovvero dell'impossibilità della sua consegna entro 24 ore dal suo invio);
- opponibilità a terzi delle evidenze relative alle operazioni di invio e ricezione di un messaggio;
- livelli minimi di qualità del servizio e di sicurezza stabiliti dalla legge.

Che differenza c'è tra la raccomandata con ricevuta di ritorno ed il servizio di PEC (dal punto di vista legale, economico, di tempo e praticità del servizio)?

Il servizio di PEC consente di effettuare l'invio di documenti informatici con la "certificazione" dell'invio e dell'avvenuta (o mancata) consegna. Il servizio ha, pertanto, lo stesso valore legale di una raccomandata A/R cui si aggiungono notevoli vantaggi sia in termini di tempo che di costi. In particolare, nella PEC si riscontra:

- semplicità ed economicità di trasmissione, inoltro e riproduzione;
- semplicità ed economicità di archiviazione e ricerca;
- facilità di invio multiplo, cioè a più destinatari contemporaneamente, con costi estremamente più bassi rispetto a quelli dei mezzi tradizionali;
- velocità della comunicazione e consegna indipendente dalla presenza del destinatario;
- possibilità di consultazione ed uso anche da postazioni diverse da quella del proprio ufficio o abitazione (basta un qualsiasi dispositivo connesso ad Internet e un normale browser web), ed in qualunque momento grazie alla persistenza del messaggio nella casella di posta elettronica;
- la presenza dei contenuti del messaggio originale nella ricevuta di avvenuta consegna;
- integrità ed inalterabilità del messaggio trasmesso e ricevuto.

In quali casi è preferibile inviare messaggi di PEC?

La casella di PEC è indicata soprattutto per effettuare comunicazioni "ufficiali" per le quali il mittente vuole avere l'evidenza, con valore legale, dell'invio e della consegna del messaggio. La casella può comunque essere utilizzata per qualsiasi comunicazione anche nel caso in cui non sia indispensabile la certificazione dell'invio e della consegna. Bisogna solo ricordare che per ogni messaggio inviato si otterranno una **ricevuta di accettazione** e, in caso di trasmissione tra due indirizzi PEC, una **ricevuta di consegna**.

In che modo si ha la certezza della consegna di un messaggio di PEC?

Nel momento in cui l'utente invia il messaggio, riceve, da parte del proprio Gestore di PEC, una ricevuta di accettazione con relativa attestazione temporale. Tale ricevuta costituisce prova legale dell'avvenuta spedizione del messaggio.

Quando il messaggio perviene nella casella del destinatario, il suo Gestore di PEC invia al mittente la ricevuta di avvenuta (o mancata) consegna, con l'indicazione di data e orario, a prescindere dalla visualizzazione del messaggio da parte del destinatario.

La PEC certifica la lettura del messaggio da parte del destinatario?

No, la certificazione è relativa ai soli eventi di invio del messaggio e di consegna dello stesso nella casella di PEC del destinatario.

Il destinatario di un messaggio di Posta Elettronica Certificata può negare di averlo ricevuto?

Nel caso in cui il messaggio sia stato effettivamente consegnato, il destinatario non può negare l'avvenuta ricezione, dal momento che la ricevuta di avvenuta consegna del messaggio, firmata ed inviata al mittente dal Gestore di PEC

scelto dal destinatario, riporta la data e l'ora in cui il messaggio è stato consegnato nella casella di PEC del destinatario, certificandone l'avvenuta consegna.

La PEC è in grado di garantire l'identità della casella mittente?

Sì, in quanto è assicurata l'inalterabilità dell'indirizzo associato alla casella dalla quale si effettua l'invio del messaggio.

Da una casella di PEC è possibile inviare un messaggio certificato a chiunque abbia una casella di posta elettronica?

Sì, a meno che il Gestore non abbia inserito dei filtri per impedire lo spam. In ogni caso, se il messaggio viene preso in carico, non sarà prodotta la ricevuta che attesta la consegna al destinatario.

E' possibile inviare messaggi di Posta Elettronica Certificata tra utenti che utilizzano Gestori di PEC differenti?

Sì, la normativa impone ai differenti Gestori di PEC di garantire la piena interoperabilità dei servizi offerti.

E' possibile certificare e registrare il dominio principale di un cliente (Ente Pubblico, Comune, ASL, etc.) come dominio di posta elettronica certificata?

Tecnicamente è possibile, ma, poiché per legge (DPR 11 Febbraio 2005, n 68, articolo 1, lettera d) un "DOMINIO DI POSTA ELETTRONICA CERTIFICATA" è "l'insieme di tutte e sole le caselle di posta elettronica certificata il cui indirizzo fa riferimento, nell'estensione, ad uno stesso dominio della rete Internet, definito secondo gli standard propri di tale rete" ciò comporta necessariamente la perdita delle mailbox associate attestata sui server di posta che gestiscono il dominio e la creazione ex novo delle caselle sul dominio certificato gestito in server farm del certificatore. Per evitare ciò, è prassi dei clienti (Enti, Comuni, ASL) certificare un sottodominio del dominio di proprietà e non il dominio principale (del tipo @pec.comunex).

Quali sono gli aspetti concernenti la sicurezza e la privacy dei dati personali dei titolari di caselle PEC?

La Norma impone ai Gestori di PEC di applicare tutte le procedure atte a garantire la sicurezza e la privacy dei dati personali. Analogo livello di sicurezza è garantito anche per le informazioni archiviate nel Log delle trasmissioni.

Quali sono i livelli di sicurezza garantiti per il servizio?

La normativa di riferimento fissa i livelli minimi di sicurezza che devono essere garantiti dal Gestore ai propri utenti. In particolare, il Gestore è tenuto ad informare il mittente, bloccandone la trasmissione, della eventuale presenza di virus nelle e-mail inviate/ricevute.

Esistono dei livelli minimi di qualità del servizio garantiti dai Gestori del servizio di PEC?

La normativa di riferimento impone ai Gestori il rispetto di requisiti minimi di qualità e continuità del servizio.

Esistono registri o elenchi, pubblicamente consultabili, delle caselle di PEC?

Esiste solo per le PA e fa riferimento all'"Indice delle Pubbliche Amministrazioni" (IPA) consultabile on-line all'indirizzo <http://www.indicepa.gov.it/>.

5.2 FAQ normative

Dove è possibile trovare la normativa di riferimento della PEC?

La normativa è interamente presente e scaricabile dall'apposita sezione del sito dell'Ente di Vigilanza, l'Agenzia per l'Italia Digitale - AgID (già DigitPA).

Quali sono le condizioni per considerare spedito un documento informatico trasmesso via PEC? E quali quelle per cui il documento si considera ricevuto?

"Il documento informatico trasmesso per via telematica si intende spedito dal mittente se inviato al proprio Gestore, e si intende consegnato al destinatario se reso disponibile all'indirizzo elettronico da questi dichiarato, nella casella

di posta elettronica del destinatario messa a disposizione dal Gestore” (DPR 11 febbraio 2005, n.68), ovvero quanto il messaggio è consegnato nella casella del destinatario.

Chi è obbligato ad avere una casella PEC?

Le **Pubbliche Amministrazioni** (D.Lgs. del 7 marzo 2005, n. 82) e gli **operatori finanziari** per le comunicazioni con la Pubblica Amministrazione in merito ad indagini finanziarie (Provvedimento del Direttore dell'Agenzia delle Entrate n. 188870 del 22 dicembre 2005). Inoltre **iscritti ad albi, professionisti ed imprese** sono obbligati all'adozione di una casella PEC o di "un analogo indirizzo di posta elettronica basato su tecnologie che certifichino data e ora dell'invio e della ricezione delle comunicazioni e l'integrità del contenuto delle stesse, garantendo l'interoperabilità con analoghi sistemi internazionali” (Legge 28 Gennaio 2009, n. 2).

Tutte le Pubbliche Amministrazioni sono dotate di PEC?

Il D.Lgs. del 7 marzo 2005, n. 82 ha obbligato tutte le Pubbliche Amministrazioni ad istituire almeno una casella di posta elettronica istituzionale ed una casella di posta elettronica certificata ai sensi del decreto del Presidente della Repubblica 11 febbraio 2005, n. 68, per ciascun registro di protocollo entro ventiquattro mesi dalla data di entrata in vigore del codice e a pubblicarne gli indirizzi sui siti specificando se si tratta di una casella di posta elettronica certificata.

Le Pubbliche Amministrazioni sono obbligate all'utilizzo della PEC per lo scambio di documenti e informazioni con i soggetti interessati che ne fanno richiesta?

Le Pubbliche Amministrazioni centrali e, salvo diverse indicazioni, quelle regionali, sono obbligate “all'utilizzo della posta elettronica certificata per ogni scambio di documenti e informazioni con i soggetti interessati che ne fanno richiesta e che hanno preventivamente dichiarato il proprio indirizzo di posta elettronica certificata” (D.Lgs. del 7 marzo 2005, n. 82).

La data e l'ora di trasmissione e di ricezione di un documento informatico trasmesso mediante posta elettronica certificata sono opponibili ai terzi?

Sì, se conformi alle disposizioni di cui al decreto del Presidente della Repubblica 11 febbraio 2005, n. 68, ed alle relative regole tecniche.

Qual è l'ente preposto al controllo delle attività esercitate dagli iscritti nell'elenco dei Gestori di PEC?

L'**Agenzia per l'Italia Digitale** (AgID) - istituita con decreto legge n. 83, convertito nella legge n. 134/2012 - coordina le azioni in materia di innovazione per promuovere le tecnologie ICT a supporto della pubblica amministrazione, garantendo la realizzazione degli obiettivi dell'Agenda digitale italiana in coerenza con l'Agenda digitale europea. Il nuovo ente eredita le competenze del Dipartimento per la Digitalizzazione e l'Innovazione della Presidenza del Consiglio, dell'Agenzia per la diffusione delle tecnologie per l'innovazione, di DigitPA e dell'Istituto superiore delle comunicazioni e delle tecnologie dell'informazione per le competenze sulla sicurezza delle reti.

Quali sono i riferimenti normativi che disciplinano l'attività di vigilanza e di controllo svolta nei confronti dei Gestori di Posta Elettronica Certificata (PEC)?

5.3 FAQ specifiche del servizio di PEC di TI Trust Technologies

Le modalità di utilizzo della PEC sono diverse da quelle di una normale posta elettronica?

Le modalità di accesso sono sostanzialmente le stesse. Si può accedere alla propria casella di PEC sia attraverso un client di posta elettronica che attraverso un browser Internet. Nel primo caso, prima di poter utilizzare la propria casella è necessario configurare il proprio client con gli appositi parametri.

Sulla casella PEC, è possibile gestire una rubrica dei contatti?

Sì, il client consente la creazione e la gestione di una rubrica.

Quali sono i parametri di configurazione dei client di posta?

I client di posta elettronica più comuni (Outlook, Outlook Express, Thunderbird, ...) possono essere configurati utilizzando, nelle impostazioni dell'account di posta elettronica, i seguenti parametri:

- Server POP3: MAIL.TELECOMPOST.IT
- Impostazioni di sicurezza: utilizzo del protocollo SSL
- Nome Utente: il nome utente fornito all'atto dell'attivazione della casella PEC
- Password: la password fornita all'atto dell'attivazione della casella PEC
- Server SMTP: SMTP.TELECOMPOST.IT
- Impostazioni di sicurezza: utilizzo del protocollo SSL
- Sicurezza e autenticazione del server SMTP: selezionare le voci “*utilizza nome utente e password*” e “*utilizza il protocolloSSL*”

Ho configurato il mio client di posta, riesco a ricevere i messaggi di PEC ma non ad inviarli

L'invio dei messaggi viene gestito dal protocollo SMTP e dai relativi server. È necessario controllare la configurazione e le relative impostazioni del client per quanto concerne il nome del server SMTP che deve essere SMTP.TELECOMPOST.IT. Inoltre deve essere impostato l'utilizzo del protocollo SSL e l'autenticazione mediante nome utente e password per l'invio dei messaggi. Il nome utente e la password da utilizzare per l'invio dei messaggi sono gli stessi che vengono utilizzati per la ricezione dei messaggi.

Ho configurato il mio client di posta, riesco a inviare i messaggi di PEC ma non a riceverli

La ricezione dei messaggi viene gestita dal protocollo POP3 e dai relativi server. È necessario controllare la configurazione e le relative impostazioni del client per quanto concerne il nome del server POP che deve essere MAIL.TELECOMPOST.IT. Inoltre deve essere impostato l'utilizzo del protocollo SSL e l'autenticazione mediante nome utente e password per la ricezione dei messaggi. Il nome utente e la password da utilizzare sono quelli forniti in fase di attivazione della casella PEC.

Posso accedere alla mia casella PEC in modalità WEB?

Sì, l'accesso via WEB è consentito tramite il portale Webmail della PEC di TI Trust Technologies, raggiungibile, mediante connessione sicura HTTPS, all'indirizzo: <https://www.telecompost.it/pec> e <https://webmail.telecompost.it>.

Ho smarrito/dimenticato la password di accesso alla mia casella PEC, cosa devo fare?

È possibile recuperare la password, in completa autonomia, cliccando su “*Vuoi cambiare la password o l'hai dimenticata?*” dal portale WEB. Seguendo le istruzioni a video riceverai un SMS (o una EMAIL) contenenti una OTP (One time Password) attraverso la quale sarà possibile impostare la nuova password.

TI Trust Technologies offre un servizio di assistenza? Come posso contattarlo?

Sì, TI Trust Technologies mette a disposizione dei propri clienti un numero verde (800.28.75.24) per le informazioni commerciali e l'aiuto in linea per l'impiego del software e dei dispositivi hardware forniti con i propri servizi. Per gli interventi urgenti, come la soluzione di inconvenienti, è disponibile un servizio 24 ore su 24.

Ho cancellato dei messaggi/ricevute per errore, posso recuperarli?

I messaggi cancellati possono essere recuperati solo se si è sottoscritto, unitamente alla casella PEC, il **servizio di archiviazione**. In caso contrario non è possibile recuperare il messaggio. È però possibile richiedere il log che attesta l'invio/ricezione del messaggio. Tale log viene conservato da TI Trust Technologies, come previsto dalla legge vigente, per 30 mesi.

Ho inviato un messaggio dalla mia casella PEC ad un destinatario che ha una casella email ordinaria (NON PEC). Come mai non ricevo le ricevute?

La PEC, per sfruttare le sue potenzialità al massimo, deve essere utilizzata per comunicare con altre caselle PEC. Nel caso di un messaggio di PEC inviato ad una casella mail tradizionale non sarà possibile avere le ricevute e relative certificazioni perché il sistema remoto non è in grado di riconoscere il messaggio PEC e trattarlo di conseguenza.

Sono passate 4 ore (oppure 6, 8, 10, 12, 20 ore) dall'invio di un messaggio di PEC ma non ho ancora avuto la ricevuta di consegna. Come mai? Non è stata recapitata?

Un messaggio di PEC, in genere, viene recapitato in tempi brevi però, a volte, per anomalie del sistema remoto o eccessivo traffico sulla rete, ci può volere più tempo. Il massimo tempo di attesa per il recapito di una PEC è 24 ore. Scaduto questo termine verrà generato un avviso di impossibilità di recapito della PEC. Pertanto è necessario attendere la scadenza delle 24 ore.

Sto ricevendo dei messaggi indesiderati sulla mia casella PEC, cosa posso fare?

In caso di ricezione di messaggi indesiderati (spam) sulla propria casella è opportuno contattare il servizio di assistenza tecnica TI Trust Technologies che provvederà ad analizzare i messaggi e adottare le opportune misure correttive sui sistemi antivirus e antispam centralizzati.

La mia casella si è riempita e non riesco più a ricevere messaggi

Le caselle PEC, al pari delle normali caselle email hanno una capienza predefinita. In caso di riempimento è possibile scaricare i messaggi localmente sul proprio PC liberando spazio nella casella PEC. Si suggerisce di archiviare su supporto ottico i dati scaricati in locale sul Personal Computer. In alternativa è possibile ampliare la capacità della propria casella, facendone richiesta al Gestore.

Vorrei acquistare una casella PEC con più spazio, come faccio?

È necessario rivolgersi alle strutture di vendita Telecom Italia o, se l'acquisto è avvenuto tramite lo Store online, scrivere ai recapiti indicati nella sezione "Termini e Condizioni".

Una mail PEC può essere spedita a più destinatari?

Sì, è possibile inviare lo stesso messaggio a più destinatari. Esistono però dei limiti di invio che devono essere rispettati: una mail può avere al massimo 1.000 destinatari contemporanei ed il prodotto tra il numero di destinatari e le dimensioni dell'allegato non devono superare i 100 MB (ad esempio un file da 100 KB inviato a 1.000 destinatari produce un traffico pari a 100 MB).

6 Informazioni sul documento, definizioni, abbreviazioni e termini tecnici

La società TI Trust Technologies S.r.l. esercita l'attività di certificazione della firma qualificata in qualità di Certificatore Accreditato ai sensi del DPR 28 dicembre 2000, n. 445 e quella di gestione del servizio di Posta Elettronica Certificata, quale iscritto nell'elenco pubblico dei Gestori ai sensi dell'Art. 14 del DPR 11 febbraio 2005, n. 68.

6.1 Standard

Il servizio di PEC erogato da TI Trust Technologies è conforme agli standard di riferimento internazionalmente riconosciuti (e qui sotto riportati) secondo l'Art. 3 del DM 2 novembre 2005.

Standard Tecnologici di riferimento

Codice	Descrizione
RFC 1847	Security Multiparts for MIME: Multipart/Signed and Multipart/Encrypted
RFC 1891	SMTP Service Extension for Delivery Status Notifications
RFC 1912	Common DNS Operational and Configuration Errors
RFC 2252	Lightweight Directory Access Protocol (v3): Attribute Syntax Definitions
RFC 2315	PKCS #7: Cryptographic Message Syntax Version 1.5
RFC 2633	S/MIME Version 3 Message Specification
RFC 2660	The Secure HyperText Transfer Protocol
RFC 2821	Simple Mail Transfer Protocol
RFC 2822	Internet Message Format
RFC 2849	The LDAP Data Interchange Format (LDIF) - Technical Specification
RFC 3174	US Secure Hash Algorithm 1 (SHA1)
RFC 3207	SMTP Service Extension for Secure SMTP over Transport Layer Security
RFC 3280	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

TI Trust Technologies S.r.l. è certificata **ISO 9001:2008** e **ISO 27001:2013**, a garanzia dei processi e della sicurezza delle informazioni. La supervisione periodica da parte di un Ente terzo accreditato, verifica la corretta applicazione degli standard internazionali richiamati dalle normative.

6.2 Definizioni

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

Le definizioni adottate dalla normativa di riferimento non sono riportate e si rimanda ai testi in vigore per la loro consultazione.

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

Si definisce:

AgID – Agenzia per l'Italia Digitale. Il nuovo Ente (istituito con decreto legge n. 83, convertito nella legge n. 134/2012) che eredita le competenze del Dipartimento per la Digitalizzazione e l'Innovazione della Presidenza del Consiglio, dell'Agenzia per la diffusione delle tecnologie per l'innovazione, di DigitPA e dell'Istituto superiore delle comunicazioni e delle tecnologie dell'informazione per le competenze sulla sicurezza delle reti. L'AgID coordina le

azioni in materia di innovazione per promuovere le tecnologie ICT a supporto della pubblica amministrazione, garantendo la realizzazione degli obiettivi dell'Agenda digitale italiana in coerenza con l'Agenda digitale europea.

Avviso di mancata consegna. Nel caso in cui il Gestore di PEC sia impossibilitato a consegnare il messaggio nella casella di PEC del destinatario, il sistema emette un avviso di mancata consegna per indicare 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.

Certificatore (Certification Authority, CA, Autorità di Certificazione). È il soggetto che presta servizi di certificazione delle firme elettroniche o che fornisce altri servizi connessi con queste ultime.

Certificazione. È 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 Carta Nazionale dei Servizi (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.

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. È l'organismo di cui all'articolo 4, comma 1 del decreto legislativo 12 febbraio 1993, n. 39, come modificato dall'articolo 176, comma 3 del decreto legislativo 30 giugno 2003, n. 196. Il CNIPA ha incorporato le strutture e le funzioni dell'AIPA e del Centro Tecnico della RUPA e, con D.Lgs. 1 dicembre 2009, n. 177, ha assunto la denominazione "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 (ex-CNIPA). Ente pubblico non economico che svolge funzioni di natura progettuale, tecnica e operativa, con la missione di contribuire alla creazione di valore per cittadini e imprese da parte della pubblica amministrazione, attraverso la realizzazione dell'amministrazione digitale. Opera secondo le direttive, per l'attuazione delle politiche e sotto la vigilanza del Presidente del Consiglio dei Ministri o del Ministro delegato, con autonomia tecnica e funzionale, amministrativa, contabile, finanziaria e patrimoniale.

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. È 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.

Firma digitale. Un particolare tipo di firma elettronica qualificata, basata su un sistema di chiavi asimmetriche a coppia, una pubblica e una privata, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici.

Firma elettronica. Insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di autenticazione informatica.

Firma elettronica avanzata. Firma elettronica ottenuta attraverso una procedura informatica che garantisce la connessione univoca al firmatario e la sua univoca identificazione, creata con mezzi sui quali il firmatario può conservare un controllo esclusivo e collegata ai dati ai quali si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati.

Firma elettronica qualificata. Firma elettronica avanzata basata su un certificato qualificato e creata mediante un dispositivo sicuro per la creazione della firma.

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 (art. 23 del DM 2/11/05). Esso è depositato presso l'ente di vigilanza 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, come previsto dall'art. 20, comma 2 del DM 2/11/05.

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.

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 della busta di trasporto.

Ricevuta di accettazione. È la 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. È il soggetto a cui è assegnata una casella di posta elettronica certificata. Nell'ambito del servizio di PEC erogato dal Gestore TI Trust Technologies, il Titolare è il soggetto che acquista il servizio di PEC per il tramite di Telecom Italia, per consentire agli utilizzatori di fruirne.

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.

6.3 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 un'estensione del protocollo Internet standard HTTP (Hypertext Transfer Protocol), attraverso il protocollo SSL.

INTERNET: Un sistema globale di reti informatiche nel quale gli utenti di singoli computer possono ottenere informazioni da luoghi diversi. La sua grande diffusione è stata determinata principalmente dall'introduzione dei protocolli di trasmissione di documenti con riferimenti ipertestuali (HTTP) e dallo sviluppo del World Wide Web (WWW).

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.

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.

RFC – Request For Comments: Definizioni scritte di protocolli o standard in uso su Internet emessi dalla Internet Engineering Task Force (IETF).

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.

Appendice

La dematerializzazione dei documenti cartacei

Oggi, nell'era dello sviluppo digitale, è sempre più pressante, soprattutto in materia di circolazione dei documenti, l'esigenza di disporre di soluzioni che puntano alla circolazione delle "informazioni" piuttosto che alla circolazione delle "cose".

Il ciclo di vita di un documento, in genere, si compone principalmente di quattro fasi ben definite che vanno dalla sua creazione alla sua conservazione:

- **la creazione** comprende la generazione del documento, a partire da una esigenza specifica, e la sua validazione, con lo scopo di attribuirgli valore;
- **l'uso** è il momento in cui il documento produce gli effetti per i quali è stato creato. In questa fase si colloca anche lo scambio delle informazioni in esso contenute, cioè il suo invio;
- **l'archiviazione** è la catalogazione del documento secondo criteri ben precisi (la c.d. cartellinatura) e la relativa indicizzazione; questa fase comprende anche la verifica di congruità degli archivi;
- **la conservazione** comprende tutte le operazioni di preparazione del documento per la sua conservazione nel tempo, compresa la sua conservazione materiale.

Nel caso di **documenti cartacei** la realizzazione delle varie fasi è garantita dalle seguenti attività:

- la stampa e la firma autografa;
- l'invio mediante gli abituali canali di trasferimento e comunicazione (quali ad es. la posta tradizionale);
- la protocollazione;
- l'archiviazione.

Ognuna di queste fasi comporta dei costi (acquisto della carta, stampa, spedizione, spazio di archiviazione, fruibilità delle informazioni, ecc.) che incidono significativamente, in modo diretto o indiretto, sul bilancio delle aziende.

La figura sottostante mostra come, oggi, la tecnologia possa migliorare significativamente il processo di gestione dei documenti, mediante strumenti che soddisfano i requisiti di sicurezza necessari per la **gestione digitale di tutto il ciclo di vita di un documento** (figura 1):



Figura 1

Infatti, analizzando nel dettaglio un singolo documento si può, con ragionevole certezza, verificare che:

- le informazioni spesso nascono già in formato digitale, in quanto prodotte da strumenti informatici, e sono sempre e comunque riconducibili a tale formato; inoltre le attuali tecniche di **firma digitale**, consentono di sottoscrivere i documenti elettronici conferendo loro pieno valore ai fini giuridici e fiscali;
- i sistemi di **Posta Elettronica Certificata (PEC)**, riconosciuti e certificati a livello normativo, consentono la trasmissione dei documenti elettronici attestandone con certezza inconfutabile:
 - data e ora di invio;

- buon fine o meno dell'invio;
- data e ora di recapito nella cassetta postale del destinatario;
- l'**archiviazione elettronica**, come quella cartacea, consente lo smistamento ordinato e sistematico dei documenti secondo determinati criteri e procedure;
- la **conservazione a norma** consente di conservare documenti in formato elettronico, dotati di firma digitale e marcatura temporale, senza l'obbligo della stampa cartacea.

Dal punto di vista strettamente legale, tali strumenti sono pienamente riconosciuti e totalmente equivalenti a quelli con cui tradizionalmente vengono gestiti i documenti cartacei: la firma digitale ha la stessa valenza di una firma autografa, la posta elettronica certificata dà valore giuridico all'invio e alla consegna del documento, la conservazione a norma di un documento consente di eliminarne le copie cartacee. Questo significa che **un documento "smaterializzato" e conservato digitalmente è ESATTAMENTE IDENTICO, per efficacia, valore legale e tributario, all'omologo cartaceo.**

L'utilizzo combinato di tali tecniche consente di realizzare la **dematerializzazione** dei documenti, cioè la progressiva perdita di consistenza fisica da parte degli archivi, tradizionalmente costituiti da documentazione cartacea e la loro sostituzione con documenti informatici, con notevole riduzione dei costi e delle inefficienze.

A livello organizzativo, la "dematerializzazione" comprende due distinte azioni:

1. la digitalizzazione dei processi nella gestione delle informazioni e dei documenti (processi *paperless*);
2. l'archiviazione e la conservazione dei documenti di qualsiasi natura in formato digitale, soprattutto se questi hanno rilevanza per le organizzazioni pubbliche o valore legale, e quindi devono essere conservati per un certo numero di anni, come prescritto dalle vigenti normative.

Volendo descrivere questo procedimento in termini prettamente filosofici, si potrebbe affermare che una tale rivoluzione ci fa passare, per quanto riguarda i documenti, dal mondo degli atomi, popolato di documenti stampati su carta mediante l'uso di inchiostro, un liquido delebile nel tempo, al mondo dei bit in cui ogni documento altro non è che una sequenza ordinata di bit appunto che rimangono inalterati nel tempo e che, nel tempo, sono in grado di affermare la loro validità e autenticità.

Riferimenti

TI Trust Technologies Srl con unico socio

Direzione e Coordinamento Telecom Italia S.p.A.

Sede legale: S.S. 148 Pontina, km 29,100 - 00071 Pomezia (Roma)

C.F. P. IVA e Iscriz. Reg. Imp. Roma n. 04599340967 REA n. 1085826

TI Trust Technologies è accreditata presso l'Agenzia per l'Italia Digitale (AGID), in qualità di:

- **Gestore dell'identità digitale** nell'ambito del Sistema Pubblico di Identità Digitale (**SPID**);
- **Conservatore per la conservazione di documenti informatici**, ai sensi del DPCM 3 dicembre 2013;
- **Gestore del servizio di Posta Elettronica Certificata**;
- **Certificatore per l'emissione di certificati qualificati** per la firma digitale e certificati di autenticazione per le carte nazionali dei servizi.

TI Trust Technologies S.r.l. è certificata **ISO 9001:2008** e **ISO 27001:2013**, a garanzia della qualità dei processi e della sicurezza delle informazioni. La supervisione periodica da parte di un Ente terzo accreditato, verifica la corretta applicazione degli standard internazionali richiamati dalle normative.