[Ermanno Goletto](#)
Microsoft Most Valuable Professional
Microsoft Certified

Posta elettronica certificata riferimenti normativi e funzionamento

Introduzione

La posta elettronica certificata (PEC) è un sistema di trasmissione sicuro e regolamentato dalla legge, per inviare documenti e messaggi di posta elettronica con valore legale. Viene istituita come versione digitale della raccomandata con ricevuta di ritorno e punta a rendere più agili, immediati ed economici, tutti gli scambi di informazioni tra i soggetti interessati, sfruttando le potenzialità del digitale.

Per certificare l'invio e la ricezione di un messaggio di PEC, il gestore di posta invia al mittente una ricevuta che costituisce prova legale dell'avvenuta spedizione del messaggio e dell'eventuale documentazione allegata. Allo stesso modo, il gestore invia al mittente la ricevuta di avvenuta (o mancata) consegna del messaggio, con precisa indicazione temporale.

Di seguito analizzeremo l'evoluzione normativa che introdotto l'utilizzo della PEC nell'ambito della comunicazione tra persone, imprese, pubbliche amministrazioni e professionisti. Inoltre approfondiremo il funzionamento della PEC e gli aspetti tecnologici di questo sistema di trasmissione.

Argomenti

Riferimenti normativi

La **posta elettronica certificata (PEC)** è stata introdotta nel nostro ordinamento con il 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" in cui vengono emanate le regole per l'utilizzo della PEC e le specifiche che il sistema deve avere e viene stabilito, tramite l'Art. 4 comma1, che **la PEC consente l'invio di messaggi la cui trasmissione è valida agli effetti di legge**.

Sempre nel 2005 con l'emanazione del **CAD** (Codice dell'Amministrazione Decreto Legislativo 7 marzo 2005, n. 82) con l'**Art. 6** viene introdotta la **possibilità da parte della Pubblica Amministrazione di utilizzare la PEC** per ogni scambio di documenti e informazioni con i soggetti che ne hanno fatto preventivamente richiesta e che hanno preventivamente dichiarato il proprio indirizzo di posta elettronica certificata. Sempre nel CAD l'Art. 47 indica che le comunicazioni di documenti tra le pubbliche amministrazioni avvengono tramite posta elettronica certificata sono valide ai fini del procedimento amministrativo, mentre l'Art 48 del CAD indica che la trasmissione telematica di comunicazioni che necessitano di una ricevuta di invio e di una ricevuta di consegna avviene mediante la posta elettronica certificata.

Le **Regole Tecniche** della PEC sono state definite con il DM 2 novembre 2005 "Regole tecniche per la formazione, la trasmissione e la validazione, anche temporale, della posta elettronica certificata" e il relativo Allegato al DM 2 novembre 2005 "Regole tecniche del servizio di trasmissione di documenti informatici mediante posta elettronica certificata".

Successivamente l'emanazione del Decreto Legge 29 novembre 2008, n.185 (convertito con modificazioni dalla legge 28 gennaio 2009, n.2) introduce con l'Art. 16 l'**obbligo da parte delle imprese e dei professionisti di creare un indirizzo di PEC** e di comunicarlo al **Registro Imprese e agli Ordini o Collegi di appartenenza**.

L'**obbligo di creare un indirizzo di PEC è stato esteso anche alle imprese individuali**, che dovevano comunicarlo al Registro Imprese entro il 30 giugno 2013, con il decreto legge 18 ottobre 2012, n.179 (convertito con modificazioni dalla legge 17 dicembre 2012, n.221) con l'Art. 5, commi 1 e 2.

Sempre con il Decreto Legge 18 ottobre 2012, n. 179 il **CAD viene aggiornato introducendo l'Art 6-bis** che prevede l'**introduzione dell'Indice nazionale degli indirizzi di posta elettronica certificata** (INI-PEC) delle imprese e dei professionisti presso il Ministero per lo sviluppo economico. In base all'Art. 6-bis la creazione dell'Indice nazionale degli indirizzi di posta elettronica certificata è realizzata a partire dagli elenchi di indirizzi PEC già registrati presso il Registro delle Imprese e gli Ordini o Collegi professionali di appartenenza dei singoli professionisti, come previsto dall'Art. 16 del decreto legge 29 novembre 2008, n.185.

Con il Decreto legislativo 26 agosto 2016 n. 179 il **CAD viene aggiornato introducendo l'Art 6-ter** che prevede **l'introduzione dell'Indice dei domicili digitali della pubblica amministrazione e dei gestori di pubblici servizi** (IPA), realizzato e gestito da AgID, in cui è consultare ed estrarre gli indirizzi PEC di qualsiasi ente pubblico.

In base al CAD all'Agenzia per l'Italia digitale sono attribuite le seguenti competenze per quanto riguarda la PEC:

- definizione e aggiornamento delle regole tecniche;
- gestione dell'iscrizione e dell'elenco dei gestori di posta elettronica certificata;
- vigilanza e controllo delle attività esercitate dai gestori iscritti nell'elenco.

Posta elettronica certificata e Regolamento UE n. 910/2014 - eIDAS

Per quanto riguarda la compliance della PEC rispetto al Regolamento Europeo 910/2014 eIDAS, come indicato nella pagina del sito dell'AgID PEC verso eIDAS, ai sensi dell'Art. 32-bis del CAD, **il Gestore di Posta Elettronica Certificata deve soddisfare i requisiti previsti per i prestatori di servizi fiduciari qualificati, in conformità al Regolamento eIDAS**.

Il Regolamento eIDAS ha introdotto anche il Servizio elettronico di recapito certificato (SERC) **e il Servizio elettronico di recapito certificato qualificato** tramite l'Art 3 n. 36 e 37 definiti come segue:

> *«servizio elettronico di recapito certificato», un servizio che consente la trasmissione di dati fra terzi per via elettronica e fornisce prove relative al trattamento dei dati trasmessi, fra cui prove dell'avvenuto invio e dell'avvenuta ricezione dei dati, e protegge i dati trasmessi dal rischio di perdita, furto, danni o di modifiche non autorizzate;*
>
> *«servizio elettronico di recapito qualificato certificato», un servizio elettronico di recapito certificato che soddisfa i requisiti di cui all'articolo 44;*

Nell'Art. 43 del Regolamento eIDAS vengono fornite indicazioni circa gli **effetti giuridici del servizio elettronico di recapito certificato**:

> ***1.*** *Ai dati inviati e ricevuti mediante un servizio elettronico di recapito certificato non sono negati gli effetti giuridici e l'ammissibilità come prova in procedimenti giudiziali per il solo motivo della loro forma elettronica o perché non soddisfano i requisiti del servizio elettronico di recapito certificato qualificato.*
>
> ***2.*** *I dati inviati e ricevuti mediante servizio elettronico di recapito certificato qualificato godono della presunzione di integrità dei dati, dell'invio di tali dati da parte del mittente identificato, della loro ricezione da parte del destinatario identificato e di accuratezza della data e dell'ora dell'invio e della ricezione indicate dal servizio elettronico di recapito certificato qualificato.*

Infine nell'Art.44 del Regolamento eIDAS vengono definiti i requisiti per i servizi elettronici di recapito certificato qualificati:

> ***1.*** *I servizi elettronici di recapito certificato qualificati soddisfano i requisiti seguenti:*
> ***a)*** *sono forniti da uno o più prestatori di servizi fiduciari qualificati;*
> ***b)*** *garantiscono con un elevato livello di sicurezza l'identificazione del mittente;*
> ***c)*** *garantiscono l'identificazione del destinatario prima della trasmissione dei dati;*
> ***d)*** *l'invio e la ricezione dei dati sono garantiti da una firma elettronica avanzata o da un sigillo elettronico avanzato di un prestatore di servizi fiduciari qualificato in modo da escludere la possibilità di modifiche non rilevabili dei dati;*
> ***e)*** *qualsiasi modifica ai dati necessaria al fine di inviarli o riceverli è chiaramente indicata al mittente e al destinatario dei dati stessi;*
> ***f)*** *la data e l'ora di invio e di ricezione e qualsiasi modifica dei dati sono indicate da una validazione temporale elettronica qualificata.*
> *Qualora i dati siano trasferiti fra due o più prestatori di servizi fiduciari qualificati, i requisiti di cui alle lettere da a) a f) si applicano a tutti i prestatori di servizi fiduciari qualificati.*
> ***2.*** *La Commissione può, mediante atti di esecuzione, stabilire i numeri di riferimento delle norme applicabili ai processi di invio e ricezione dei dati. Si presume che i requisiti di cui al paragrafo 1 siano stati rispettati ove il processo di invio e ricezione dei dati risponda a tali norme. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.*

Sempre come riportato nella pagina del sito dell'AgID PEC verso eIDAS la Posta Elettronica Certificata **soddisfa i requisiti per il servizio elettronico di recapito certificato** previsti dal Regolamento eIDAS, **ma non soddisfa appieno i requisiti di recapito certificato qualificato** previsti sempre dal Regolamento. Infatti attualmente **non è prevista la verifica certa dell'identità del richiedente della casella di PEC** e **non è previsto che il gestore debba obbligatoriamente sottoporsi a delle verifiche di conformità** da parte degli organismi designati.

La PEC è stata oggetto di attenzione anche con le modifiche introdotte dal D.lgs. 217 del 13.12.2017 (pubblicato in G.U. 9 del 12.1.2018) al testo del CAD prevedono l'introduzione del **domicilio digitale** che, sulla base di quanto definito nell'Art. 1 comma 1 lettera n-ter e comma 1-ter, può essere **un indirizzo elettronico eletto presso un servizio di posta elettronica certificata o un servizio elettronico di recapito certificato qualificato**:

> ***1. lettera n-ter)*** *domicilio digitale: un indirizzo elettronico eletto presso un servizio di posta elettronica certificata o un servizio elettronico di recapito certificato qualificato, come definito dal regolamento (UE) 23 luglio 2014 n. 910 del Parlamento europeo e del Consiglio in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE, di seguito «Regolamento eIDAS»,valido ai fini delle comunicazioni elettroniche aventi valore legale;*
>
> ***1-ter.*** *Ove la legge consente l'utilizzo della posta elettronica certificata è ammesso anche l'utilizzo di altro servizio elettronico di recapito certificato qualificato ai sensi degli articoli 3, numero 37), e 44 del Regolamento eIDAS.*

Inoltre sempre D.lgs. 217 del 13.12.2017con l'Art.65 abroga l'Art. 48 del CAD a decorrere dal 1 gennaio 2019, quindi **la PEC viene ricondotta allo strumento tecnologico mediante il quale è possibile eleggere il domicilio digitale**.

Il CAD ha quindi ripreso il principio tecnologicamente neutro in ambito comunitario dei servizi elettronici di recapito certificato (SERC) qualificato stabilendo appunto che tale elemento è associabile, come le PEC, al domicilio digitale.

L'**Indice nazionale dei domicili digitali delle persone fisiche** e degli altri enti di diritto privato, non tenuti all'iscrizione in albi professionali o nel registro delle imprese è definito nell'Art. 6-quarter del CAD e realizzato e gestito da AgID che provvederà al trasferimento dei domicili digitali nell'ANPR quando quest'ultima sarà completata.

Nell'ambito della standardizzazione comunitaria (ETSI) **i SERC saranno invece basati sull'evoluzione della Registered Electronic Mail (REM)** già standardizzata nel 2010/2011 con i documenti della serie ETSI TS 102 640.

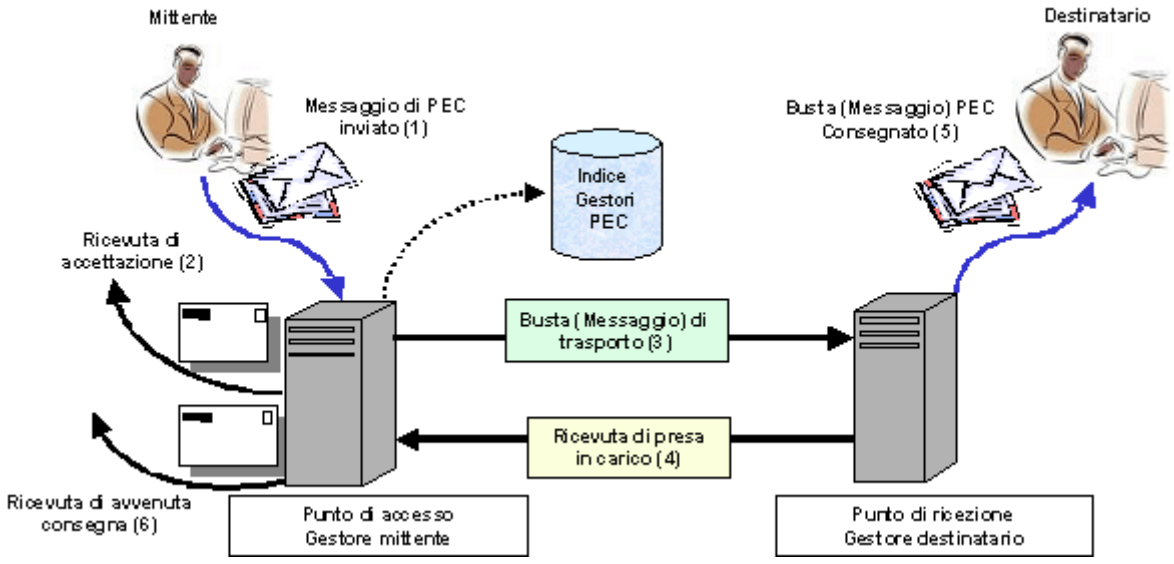
Dal momento che la PEC è un SERC, ma non ha tutti i requisiti per poter essere un SERC qualificato, il Legislatore nazionale dovrà decidere se stabilire un percorso di evoluzione della PEC verso i SERC qualificati o se mantenere separate le due tipologie di servizio postale.

Scambio di messaggi tra due caselle di PEC

La PEC ha lo stesso valore legale di una raccomandata tradizionale con avviso di ricevimento. Per certificare l'invio e la ricezione di un messaggio di PEC, il gestore di posta invia al mittente una ricevuta che costituisce prova legale dell'avvenuta spedizione del messaggio e dell'eventuale documentazione allegata. Allo stesso modo, il gestore invia al mittente la ricevuta di avvenuta (o mancata) consegna del messaggio, con precisa indicazione temporale.

Quando avviene uno **scambio di un messaggio di Posta Elettronica Certificata tra due caselle di posta elettronica certificata** vengono eseguite le seguenti operazioni:

1. il mittente invia un messaggio al destinatario, attraverso il server di PEC del proprio gestore che esegue il **controllo delle credenziali d'accesso**; il gestore PEC del mittente esegue il **controllo delle caratteristiche formali del messaggio** ed esegue l'**invio al mittente di una ricevuta di accettazione** (o eventualmente di non accettazione) con tutti gli estremi: data e ora dell'invio, mittente, destinatario, oggetto;
2. **Il messaggio viene "imbustato" dentro un altro messaggio**, detto "busta di trasporto", e **firmato digitalmente** dal gestore PEC del mittente in modo da certificare ufficialmente l'invio e successivamente la consegna;
3. **la "busta di trasporto" viene ricevuta dal gestore PEC del destinatario** che esegue il **controllo della validità della firma del gestore PEC del mittente** e la validità del messaggio;
4. se tutti i controlli hanno avuto esito positivo **il gestore PEC del destinatario invia all'altro gestore una ricevuta di presa in carico** e **inoltra il messaggio al destinatario**;
5. il messaggio arriva in un "punto di consegna", che può essere descritto come una specie di cassetta postale con la funzione di eseguire l'**invio della ricevuta di presa in carico dal gestore PEC del destinatario** quando riceve il messaggio;
6. **il mittente riceve la ricevuta di avvenuta o mancata consegna** nella propria casella postale e se il messaggio è stato inviato a più destinatari, riceve una ricevuta per ogni destinatario.



Si noti che **la ricevuta di consegna attesta che il messaggio è stato depositato correttamente** nella casella PEC del destinatario, **non garantisce che il messaggio sia stato letto dal destinatario**.

Dettagli tecnici dei messaggi di PEC

Scendendo nel dettaglio implementativo, in base a quanto riportato nel 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", nelle Regole Tecniche PEC (Allegato al DM 2 novembre 2005), nelle Note integrative alle Regole Tecniche e nel documento Regole tecniche del servizio di trasmissione di documenti informatici mediante posta elettronica certificata, **la PEC genera messaggi conformi allo standard internazionale S/MIME** descritto nella RFC 2633 che si dividono i tre categorie **ricevute**, **avvisi** e **buste** e sono **differenziati in base alla struttura dell'header** prevista dallo standard S/MIME.

I messaggi, generati dai sistemi di PEC, **sono sottoscritti dai gestori mediante la firma del gestore di PEC** e l'elaborazione dei messaggi PEC avviene anche nel caso in cui il mittente ed il destinatario appartengano allo stesso dominio di posta elettronica certificata. Si noti che la firma digitale viene applicata dal gestore, per cui non accompagna il messaggio in tutto il suo percorso, in particolare dal mittente al destinatario.

I dettagli tecnici sono riportati nelle Regole tecniche del servizio di trasmissione di documenti informatici mediante posta elettronica certificata:

> *Il messaggio (composto dall'insieme delle parti descritte nelle specifiche sezioni del presente allegato) è quindi inserito in una struttura S/MIME v3 in formato CMS, firmata con la chiave privata del gestore di posta certificata. Il certificato associato alla chiave usata per la firma deve essere incluso in tale struttura. Il formato S/MIME usato per la firma dei messaggi generati dal sistema è il "multipart/signed" (formato .p7s) così come descritto nella RFC 2633 §3.4.3*
>
> *I messaggi sono trasferiti tra gestori usando una codifica a 7 bit sia per gli header sia per il corpo del messaggio e gli eventuali allegati.*

Durante le fasi di trasmissione del messaggio di PEC, **i gestori mantengono traccia delle operazioni svolte su un apposito log dei messaggi**. I dati contenuti nel suddetto registro sono **conservati dal gestore di PEC per trenta mesi**.

A ciascuna trasmissione è apposto un unico riferimento temporale che può essere generato con qualsiasi sistema che garantisca stabilmente uno **scarto non superiore ad un minuto secondo rispetto alla scala di Tempo Universale Coordinato (UTC)**, determinata ai sensi dell'articolo 3, comma 1, della legge 11 agosto 1991, n. 273.

Di seguito una tabella delle tipologie di messaggi PEC:

Ricevute (*)	Avvisi	Buste (**)
Accettazione	Non accettazione per eccezioni formali ovvero per virus informatici	Trasporto
Presa in carico	Rilevazione di virus informatici	Anomalia
Avvenuta consegna completa Avvenuta consegna breve Avvenuta consegna sintetica	Mancata consegna per superamento dei tempi massimi previsti ovvero per rilevazione di virus informatici	

(*) La ricevuta di avvenuta consegna è rilasciata per ogni destinatario al quale il messaggio è consegnato.
(**) La busta di trasporto è consegnata immodificata nella casella di PEC di destinazione per permettere la verifica dei dati di certificazione da parte del ricevente

Per quando riguarda gli aspetti tecnici dell **operazioni di firma** questi vengono approfonditi nel documento Regole tecniche del servizio di trasmissione di documenti informatici mediante posta elettronica certificata:

> *La chiave privata e le operazioni di firma devono essere gestite utilizzando un dispositivo hardware dedicato, in grado di garantirne*

Dettagli tecnici della Busta di trasporto

Per quanto riguarda la **Busta di trasporto**, come riportato nel documento Regole tecniche del servizio di trasmissione di documenti informatici mediante posta elettronica certificata, va precisato che essa **contiene il messaggio originale immodificato in formato conforme alla RFC 2822**:

> *La busta di trasporto consiste in un messaggio generato dal punto di accesso e che contiene il messaggio originale ed i dati di certificazione.*

> *All'interno della busta di trasporto è inserito in allegato l'intero messaggio originale immodificato in formato conforme alla RFC 2822 (tranne per quanto detto a proposito del Message ID) completo di header, corpo ed eventuali allegati. Nella stessa busta di trasporto è inoltre incluso un allegato XML che specifica in formato elaborabile i dati di certificazione già riportati nel testo ed informazioni aggiuntive sul tipo di messaggio e tipo di ricevuta richiesta (cfr. 7.4). Alla busta di trasporto possono inoltre essere allegati ulteriori elementi opzionali per specifiche funzionalità fornite dal gestore di posta certificata.*
>
> *Anche se il campo "From" della busta di trasporto è modificato per consentire la verifica della firma da parte del destinatario, i dati di instradamento della busta di trasporto (forward path e reverse path del messaggio) rimangono immutati rispetto agli stessi dati del messaggio originale.*

Sempre nel documento Regole tecniche del servizio di trasmissione di documenti informatici mediante posta elettronica certificata vengono anche approfonditi gli **aspetti relativi alla sicurezza della PEC** relativi al **colloquio tra gestore PEC e mittente o destinatario** che avviene mediante l'uso di protocolli sicuri (TSL, SMTP STARTTLS, POP3 STLS, IPSec) e al **colloquio tra il gestore PEC del mittente e il gestore PEC del destinatario** che avviene tramite protocollo SMTP su trasporto TLS:

> *Al fine di garantire l'inalterabilità del messaggio originale spedito dal mittente si realizza l'imbustamento e la firma dei messaggi in uscita dal punto di accesso e la successiva verifica in ingresso al punto di ricezione. Il messaggio originale (completo di header, testo ed eventuali allegati) è inserito come allegato all'interno di una busta di trasporto. La busta di trasporto firmata dal gestore mittente permette di verificare che il messaggio originale non sia stato modificato durante il suo percorso dal dominio mittente al dominio destinatario.*
>
> *La sicurezza del colloquio tra mittente e destinatario prevede un meccanismo di protezione per tutte le connessioni previste dall'architettura di posta certificata (tra utente e punto di accesso, tra gestore e gestore, tra punto di consegna ed utente) attuato tramite l'impiego di canali sicuri.*
>
> *L'integrità e la confidenzialità delle connessioni tra il gestore di posta certificata e l'utente devono essere garantite mediante l'uso di protocolli sicuri. A titolo esemplificativo, e non esaustivo, dei protocolli accettabili per l'accesso figurano quelli basati su TLS (es. IMAPS, POP3S, HTTPS), quelli che prevedono l'attivazione di un colloquio sicuro durante la comunicazione (es. SMTP STARTTLS, POP3 STLS), quelli che realizzano un canale di trasporto sicuro sul quale veicolare protocolli non sicuri (es. IPSec).*
>
> *Il colloquio tra i gestori deve avvenire con l'impiego del protocollo SMTP su trasporto TLS, come descritto nella RFC 3207. Il punto di ricezione deve prevedere ed annunciare il supporto per l'estensione STARTTLS ed accettare connessioni sia in chiaro (per la posta ordinaria) che su canale protetto. Riguardo il punto di accesso è invece possibile utilizzare unicamente connessioni su canale protetto.*

Ancora nel documento Regole tecniche del servizio di trasmissione di documenti informatici mediante posta elettronica certificata viene anche specificato che **il flusso di messaggi di PEC deve transitare su macchine appartenenti al circuito della PEC o gestite direttamente dai gestori**:

> *Al fine di garantire la completa tracciabilità nel flusso di messaggi di posta certificata, questi non devono transitare su sistemi esterni al circuito di posta certificata. Nello scambio di messaggi tra gestori diversi, tutte le transazioni devono avvenire tra macchine appartenenti al circuito della posta certificata od a conduzione diretta del gestore. Gli eventuali sistemi secondari di ricezione dei messaggi per il dominio di posta certificata devono essere sotto il controllo diretto del gestore. Ad ogni dominio di posta certificata dovrà essere associato un record di tipo "MX" definito all'interno del sistema di risoluzione dei nomi secondo le raccomandazioni della RFC 1912.*

Livelli di servizio e norme di garanzia

Per quanto riguarda i **livelli di servizio** nelle Regole Tecniche PEC (Allegato al DM 2 novembre 2005) sono fornite le seguenti indicazioni:

- **il gestore di PEC può fissare il numero massimo di destinatari e la dimensione massima del singolo messaggio**, sia per i messaggi che provengono da un suo titolare, sia per i messaggi che provengono da titolari di caselle di altri gestori di posta elettronica certificata;
- in ogni caso **il gestore di PEC deve garantire la possibilità dell'invio di un messaggio ad almeno cinquanta destinatari** per il quale **il prodotto del numero dei destinatari per la dimensione del messaggio non superi i trenta megabytes**;
- la **disponibilità nel tempo** del servizio di PEC **deve essere maggiore o uguale al 99,8% in un quadrimestre**, ovvero il tempo di indisponibilità non deve essere inferiore a circa 23 ore ogni 4 mesi;
- **la durata massima di un evento di indisponibilità** del servizio di PEC **deve essere minore o uguale al 50% del totale previsto per il quadrimestre**, ovvero circa 11,5 ore;
- per evitare ai gestori l'onere di dover comunicare formalmente non disponibilità di durata limitata, si ritiene **tollerabile l'assenza di comunicazioni per eventi che non superino i cinque minuti**;
- **la ricevuta di accettazione deve essere fornita al mittente entro un termine, da concordarsi tra gestore e titolare,** da calcolare a partire dall'inoltro del messaggio, non considerando i tempi relativi alla trasmissione.

Un secondo aspetto su cui le Regole Tecniche PEC (Allegato al DM 2 novembre 2005) forniscono indicazioni sono gli **avvisi di mancata consegna**:

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

Un terzo aspetto su cui le Regole Tecniche PEC (Allegato al DM 2 novembre 2005) forniscono indicazioni sono le **norme di garanzia sulla natura della posta elettronica ricevuta**:

- Il gestore di PEC del destinatario ha l'obbligo di **segnalare** a quest'ultimo **se la posta elettronica in arrivo non è qualificabile come PEC**;
- **I messaggi relativi all'invio e alla consegna** di documenti attraverso la PEC sono **rilasciati indipendentemente dalle caratteristiche e dal valore giuridico dei documenti trasmessi**.

Virus informatici

Per quanto riguarda l'eventualità di **rilevamento di virus informatici** il 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" fornisce le seguenti indicazioni:

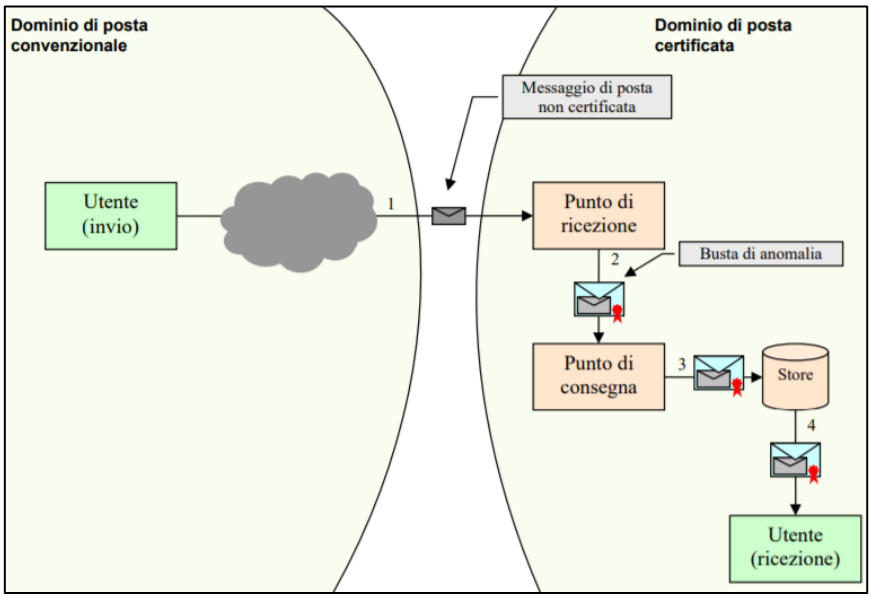
- **qualora il gestore del mittente riceva messaggi con virus informatici** è tenuto a **non accettarli**, **informando tempestivamente il mittente** dell'impossibilità di dar corso alla trasmissione; in tale caso il gestore conserva i messaggi ricevuti per trenta mesi;
- **qualora il gestore del destinatario riceva messaggi con virus informatici** è tenuto a **non inoltrarli** al destinatario, **informando tempestivamente il gestore del mittente**, affinché comunichi al mittente medesimo l'impossibilità di dar corso alla trasmissione; in tale caso il gestore del destinatario conserva i messaggi ricevuti per trenta mesi.

La gestione dei log dei messaggi contenti virus è poi stata dettaglia ulteriormente nel documento "Istruzioni per la conservazione dei log dei messaggi e dei messaggi di posta elettronica certificata con virus v.1" pubblicato dall'AgID il 14 luglio 2016 in cui tra le varie indicazioni si evidenzia che **il messaggio che trasporta un virus deve essere inviato in conservazione senza operare modifiche** al messaggio originale e che **il Responsabile della conservazione deve permettere ai soggetti autorizzati l'accesso ai messaggi con virus** attraverso la produzione di un Pacchetto di Distribuzione (PdD).

Quindi il sistema di PEC deve impedire che la presenza di virus possa compromettere la sicurezza dei messaggi gestiti prevedendo l'istallazione ed il costante aggiornamento di sistemi antivirus che impediscano quanto più possibile ogni infezione, senza però intervenire sul contenuto della posta.7

Invio di un messaggio da un dominio di posta convenzionale verso un dominio di PEC

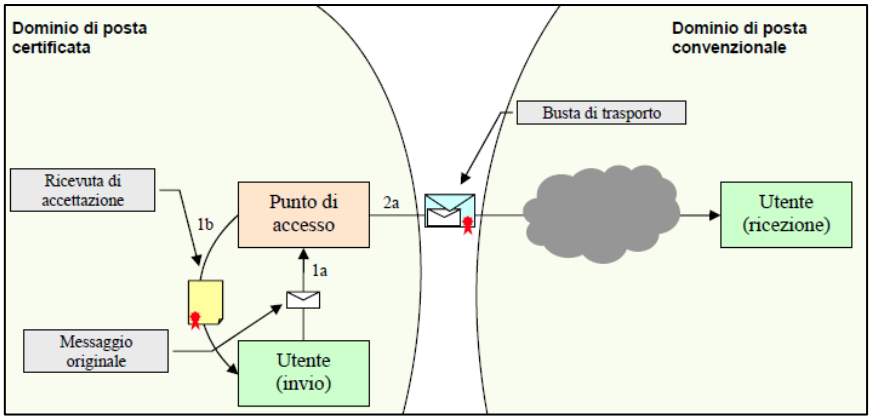
Come indicato nel documento Regole tecniche del servizio di trasmissione di documenti informatici mediante posta elettronica certificata l'accettazione di messaggio di posta ordinaria nel circuito di trattamento della PEC è a discrezione del gestore destinatario e i criteri adottati per gestire la posta ordinaria devono essere noti e condivisi dall'utente finale del servizio.



Ovviamente dal momento che non sarà possibile inviare una Ricevuta di presa in carico e la Ricevuta di avvenuta consegna in questo caso l'invio del messaggio non avrà valore legale. Il messaggio verrà inserito in una Busta di anomalia per segnalare all'utente la provenienza da un indirizzo non certificato.

Invio di un messaggio da dominio di PEC verso un dominio di posta convenzionale

Anche in questo caso dal momento sarà possibile inviare una Ricevuta di presa in carico, ma non la Ricevuta di avvenuta consegna l'invio del messaggio non avrà valore legale.



Requisiti tecnico funzionali di un client di un sistema di PEC

Come indicato nel documento Regole tecniche del servizio di trasmissione di documenti informatici mediante posta elettronica certificata i requisiti che devono essere rispettati da un client, per garantire ad un utente di un generico sistema di PEC, l'insieme minimo di funzionalità operative sono le seguenti:

- **colloquio con i punti di accesso e di consegna** mediante l'utilizzo di **canali sicuri**;
- **autenticazione dell'utente** in **fase di invio** e di **ricezione dei messaggi**;
- supporto del **formato MIME secondo RFC 2045 - RFC 2049**;
- gestione del **media type "message/rfc822"**;
- supporto del **set di caratteri "ISO-8859-1 (Latin-1)"**;
- supporto dello **standard S/MIME versione 3** come da **RFC 2633** per la verifica delle firme delle buste e delle ricevute

Conclusioni

La PEC ha subito negli anni un'evoluzione che l'ha portata ad essere non solo uno strumento informatico che lo **stesso valore legale di una raccomandata tradizionale**, ma è anche stata **eletta a domicilio digitale** anche se su questo aspetto il Legislatore nazionale dovrà esprimersi per stabilire come adempiere in modo completo ai requisisti del Regolamento eIDAS in materia di Servizio elettronico di recapito certificato (SERC) e il Servizio elettronico di recapito certificato qualificato.

La PEC ha avuto negli ultimi anni una grande diffusione sul territorio nazionale come risulta dalle statistiche che l'AgID si occupa anche di fornire e rendere disponibili nella seguente pagina Statistiche sull'utilizzo della PEC. Secondo tali statistiche nel bimestre gennaio-febbraio 2019 sono stati scambiati circa 5 milioni di messaggi al giorno e che le caselle sarebbero quasi 9 milioni di cui circa 6 milioni di professioni e imprese (fonte INI-PEC) e circa 123 mila di Pubbliche Amministrazioni (fonte IPA), quindi **circa il 32% delle PEC sono utilizzate da persone fisiche**.

Va precisato che **la PEC non è riconosciuta come standard internazionale** e per questo motivo sistemi di posta elettronica come Exchange non offrono supporto nativo alla PEC, esistono infatti altre tecniche di firma digitale e di tracciamento della consegna equivalenti (xes RFC 3798). Un altro aspetto da tenere presente è che **per la PEC devono essere usati domini dedicati**, ovvero un dominio di PEC non contiene caselle email non-PEC.

Riferimenti

- 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"
- DM 2 novembre 2005 “Regole tecniche per la formazione, la trasmissione e la validazione, anche temporale, della posta elettronica certificata”
- Allegato al DM 2 novembre 2005 “Regole tecniche del servizio di trasmissione di documenti informatici mediante posta elettronica certificata”
- Regole tecniche del servizio di trasmissione di documenti informatici mediante posta elettronica certificata
- Codice dell'Amministrazione Decreto Legislativo 7 marzo 2005, n. 82
- Regolamento Europeo 910/2014 eIDAS
- AgID - Posta elettronica certificata
- Ministero dello Sviluppo Economico - INI-PEC