

# Manuale Operativo

## Posta Elettronica Certificata

**REDATTO DA** F. D'AGAPITI, F. LUCCHETTA

**VERIFICATO DA** C. VOLLONO

**APPROVATO DA** G. ZAPPA

VERSIONE 3.1	DATA 29/04/2010	CODICE RISERVATEZZA PUBBLICO	CODIFICA PI_MO_PEC_v3.1_100429	Pagina 1/62
-----------------	--------------------	---------------------------------	-----------------------------------	-------------

LISTA DI DISTRIBUZIONE	
Documento pubblico (sul sito del gestore Poste Italiane S.p.A. <a href="http://www.poste.it">www.poste.it</a> e sul portale del servizio PostaCertificat@ <a href="http://www.postacertificata.gov.it">www.postacertificata.gov.it</a> )	
DigitPA	

## - INDICE -

<b>1</b>	<b>STORIA DELLE MODIFICHE .....</b>	<b>5</b>
<b>2</b>	<b>SCOPO.....</b>	<b>6</b>
2.1	PREMESSA.....	6
2.2	SERVIZIO POSTE ITALIANE.PEC@ PER I DIPENDENTI DI POSTE ITALIANE.....	6
2.3	SERVIZIO DI COMUNICAZIONE ELETTRONICA CERTIFICATA (POSTACERTIFICAT@) TRA CITTADINO E LA PUBBLICA AMMINISTRAZIONE.....	6
2.4	RIFERIMENTI NORMATIVI.....	7
<b>3</b>	<b>DEFINIZIONI .....</b>	<b>8</b>
<b>4</b>	<b>DATI IDENTIFICATIVI E RIFERIMENTI .....</b>	<b>12</b>
4.1	DATI DEL GESTORE.....	12
4.2	DATI IDENTIFICATIVI DEL MANUALE OPERATIVO.....	12
4.3	RIFERIMENTI DEL SITO WEB DEL GESTORE .....	13
<b>5</b>	<b>INDICE DEI CONTENUTI .....</b>	<b>13</b>
<b>6</b>	<b>DESCRIZIONE DEL SERVIZIO DI POSTE ITALIANE.PEC @.....</b>	<b>16</b>
6.1	CARATTERISTICHE GENERALI DEL SERVIZIO .....	16
6.2	DEFINIZIONE APPLICATIVA DELLE COMPONENTI IL SERVIZIO .....	19
6.3	RICEVUTE ED AVVISI RILASCIATI ALL'UTENTE.....	19
6.3.1	<i>Ricevute</i> .....	20
6.3.1.1	Ricevuta di accettazione .....	20
6.3.1.2	Ricevuta di avvenuta consegna.....	20
6.3.1.2.1	Ricevuta completa di avvenuta consegna.....	20
6.3.1.2.2	Ricevuta di avvenuta consegna breve.....	20
6.3.1.2.3	Ricevuta di avvenuta consegna sintetica .....	21
6.3.2	<i>Avvisi</i> .....	21
6.3.2.1	Avviso di non accettazione per errori formali.....	21
6.3.2.2	Avviso di mancata consegna per superamento dei tempi massimi previsti.....	21
6.3.2.3	Avviso di non accettazione per virus informatico.....	21
6.3.2.4	Avviso di rilevazione virus informatico.....	21
6.3.2.5	Avviso di mancata consegna per virus informatico.....	22
6.3.2.6	Avviso di mancata consegna.....	22
6.3.3	<i>Buste di anomalia</i> .....	22
6.4	RIFERIMENTI TEMPORALI DEI MESSAGGI.....	22
6.4.1	<i>Sincronizzazione e distribuzione del riferimento temporale</i> .....	23
<b>7</b>	<b>CONTENUTO DELL'OFFERTA POSTE ITALIANE.PEC @ .....</b>	<b>24</b>
7.1	TIPOLOGIE DI UTENTI.....	24
7.1.1	<i>Modalità di rilascio delle caselle</i> .....	24
7.2	LA TIPOLOGIA DEL SERVIZIO.....	24
<b>8</b>	<b>MODALITÀ DI ACCESSO AL SERVIZIO DI POSTE ITALIANE.PEC @.....</b>	<b>25</b>
<b>9</b>	<b>CONDIZIONI DI FORNITURA POSTE ITALIANE.PEC @.....</b>	<b>26</b>
<b>10</b>	<b>LIVELLI DI SERVIZIO ED INDICATORI DI QUALITÀ POSTE ITALIANE.PEC @ .....</b>	<b>27</b>
<b>11</b>	<b>DESCRIZIONE DEL SERVIZIO POSTACERTIFICAT@ .....</b>	<b>29</b>
11.1	CARATTERISTICHE GENERALI DEL SERVIZIO.....	29
11.2	DEFINIZIONE APPLICATIVA DELLE COMPONENTI IL SERVIZIO POSTACERTIFICAT@.....	30
11.3	RICEVUTE ED AVVISI RILASCIATI ALL'UTENTE .....	33
11.4	RIFERIMENTI TEMPORALI DEI MESSAGGI .....	33

<b>12 CONTENUTO DELL'OFFERTA POSTACERTIFICAT@ .....</b>	<b>34</b>
12.1 TIPOLOGIE DI UTENTI.....	34
<b>13 MODALITÀ DI RILASCIO DELLE CASELLE DI POSTACERTIFICAT@.....</b>	<b>34</b>
13.1 RICHIESTA ED ATTIVAZIONE DELLA CASELLA DEL CITTADINO.....	34
13.2 RICHIESTA ED ATTIVAZIONE DELLA CASELLA DELLA PA.....	35
13.3 LA TIPOLOGIA DEL SERVIZIO.....	35
<b>14 MODALITÀ DI ACCESSO AL SERVIZIO POSTACERTIFICAT@.....</b>	<b>35</b>
<b>15 CONDIZIONI DI FORNITURA DEL SERVIZIO POSTACERTIFICAT@.....</b>	<b>36</b>
<b>16 LIVELLI DI SERVIZIO ED INDICATORI DI QUALITÀ DEL SERVIZIO POSTACERTIFICAT@.....</b>	<b>36</b>
<b>17 TABELLA RIEPILOGATIVA DOCUMENTAZIONE DEL SERVIZIO PUBBLICATA SUL SITO POSTACERTIFICAT@ .....</b>	<b>37</b>
<b>18 OBBLIGHI E RESPONSABILITÀ.....</b>	<b>39</b>
18.1 OBBLIGHI DEL GESTORE.....	39
18.2 OBBLIGHI DEL SOGGETTO TITOLARE DEL SERVIZIO.....	40
18.3 OBBLIGHI DELL'UTENTE DELLA CASELLA, SE DISTINTO DAL TITOLARE DEL SERVIZIO .....	40
18.4 RESPONSABILITÀ.....	41
<b>19 ESCLUSIONI E LIMITAZIONI IN SEDE DI INDENNIZZO.....</b>	<b>41</b>
<b>20 PROCEDURE E STANDARD TECNOLOGICI E DI SICUREZZA.....</b>	<b>43</b>
20.1 STANDARD DI QUALITÀ E SICUREZZA DEL PROCESSO .....	43
20.1.1 <i>Standard di qualità</i> .....	43
20.1.2 <i>Standard tecnologici</i> .....	43
20.2 GESTIONE DEI SISTEMI TECNOLOGICI.....	44
20.2.1 <i>Attivazione della procedura di gestione</i> .....	45
20.2.2 <i>Aggiornamento della configurazione</i> .....	45
20.2.3 <i>Controllo dello stato di configurazione</i> .....	46
20.3 GESTIONE DELLE VERIFICHE AFFERENTI LA SICUREZZA .....	46
20.3.1 <i>Pianificazione e definizione degli assessment</i> .....	47
20.3.2 <i>Effettuazione dell'assessment</i> .....	47
<b>21 SOLUZIONI FINALIZZATE A GARANTIRE IL COMPLETAMENTO DELLA TRASMISSIONE .....</b>	<b>49</b>
21.1 APPROCCIO ORGANIZZATIVO.....	49
21.2 APPROCCIO TECNOLOGICO .....	51
21.2.1 <i>Connettività</i> .....	51
21.2.2 <i>Sistemi tecnologici servizio Poste Italiane.PEC @</i> .....	51
21.2.3 <i>Sistemi tecnologici servizio PostaCertificat@</i> .....	53
<b>22 REPERIMENTO E PRESENTAZIONE DELLE INFORMAZIONI DI LOG.....</b>	<b>56</b>
<b>23 MODALITÀ DI PROTEZIONE DEI DATI DEI TITOLARI .....</b>	<b>59</b>
23.1 AMBITO DEL TRATTAMENTO DEI DATI PERSONALI.....	60
23.1.1 <i>Accesso ai dati</i> .....	60
23.1.2 <i>Trattamento di dati sensibili</i> .....	60
23.1.3 <i>Trattamento di dati giudiziari</i> .....	61
23.2 SICUREZZA DEI DATI.....	61

## 1 Storia delle modifiche

Data	Versione	Descrizione modifiche	Codifica
5/12/2005	1.0	Prima versione	PI_MOPEC_v1.0_051205
25/07/2007	2.0	Revisione procedurale	PI_MOPEC_V2.0_250707
02/10/2007	2.1	Il documento è stato modificato a seguito di riorganizzazione interna. Sono stati aggiornati i paragrafi relativi all'individuazione dell'Amministratore. In particolare i paragrafi 2.1; 7.1.1, 7.2, 9.	PI_MOPEC_V2.1_021007
06/11/2007	2.2	Paragrafo 13.1.1 "Standard di Qualità": aggiornamento dei riferimenti normativi a seguito del recepimento delle osservazioni rilevate in sede di audit di terza parte svolto dall'Ente Certificatore TUV.	PI_MOPEC_V2.2_061107
31/10/2008	2.3	Rev. Par. 16.2 Politiche di riferimento Poste Italiane	PI_MO_PEC_v2.3_083110
04/09/2009	2.4	<ul style="list-style-type: none"> <li>• Allineamento del documento a seguito della nuova struttura organizzativa</li> <li>• Modificati schema architettura connettività e schema architettura fisica</li> <li>• Corretta periodicità audit</li> </ul>	PI_MO_PEC_v2.4_090904
26/04/2010	3.0	<ul style="list-style-type: none"> <li>• Revisionato intero documento per integrazione relative al servizio PostaCertificat@ e alla normativa di riferimento</li> <li>• Modificato Responsabile del Servizio e Responsabile della Registrazione dei Titolari</li> </ul>	PI_MO_PEC_v3.0_100426
29/04/2010	3.1	<ul style="list-style-type: none"> <li>• Aggiornato elenco dei riferimenti normativi (par. 2.4)</li> <li>• Corretto il riferimento email del responsabile del MO (par. 4.2)</li> <li>• Modificato cap. 5 (Indice dei contenuti)</li> </ul>	PI_MO_PEC_v3.1_100429

## 2 Scopo

### 2.1 Premessa

Il Manuale Operativo si riferisce ai servizi di Posta Elettronica Certificata implementati dalla Funzione Tecnologie dell'Informazione per conto di Poste Italiane S.p.A., in osservanza della normativa vigente elencata (cfr par.2.4) e definisce le procedure applicate da Poste Italiane (in qualità di gestore) per lo svolgimento della propria attività di erogazione dei sistemi di Posta Elettronica Certificata. Il gestore (TI per conto di Poste Italiane) pertanto si assume tutte le responsabilità connesse/derivanti l'operatività degli erogatori esterni coinvolti. Di seguito sono riportati i dati identificativi del Gestore.

Il gestore Poste Italiane gestisce due tipologie di servizi di Posta Elettronica Certificata, con caratteristiche specifiche:

### 2.2 Servizio Poste Italiane.PEC@ per i dipendenti di Poste Italiane

**Poste Italiane.PEC @**, è un servizio offerto ai soggetti appartenenti alla propria organizzazione o come componente di servizi integrati sempre offerti al personale interno. In quest'ottica i soggetti che entrano in relazione con il Gestore o che ne utilizzano i servizi sono quindi:

- Utenti che accedono alla casella di Posta Elettronica Certificata per spedire messaggi o per verificarne la ricezione;
- "Amministratori del Sistema", soggetti di interfaccia con il Gestore, con il compito di individuare e attivare, all'interno delle unità organizzative, dei Titolari delle caselle di posta elettronica certificata. Tali soggetti possono essere individuati o all'interno della struttura TI\Esercizio di Poste Italiane o individuati all'interno dell'Unità Organizzativa.

All'interno del presente Manuale, per i soggetti sopra elencati, sono definiti gli obblighi e le corrispondenti responsabilità.

Il servizio Poste Italiane.PEC @ è erogato dalla Funzione Tecnologie dell'Informazione con il supporto operativo dell'outsourcer PosteCom S.p.A.

### 2.3 Servizio di Comunicazione Elettronica Certificata (PostaCertificat@) tra Cittadino e la Pubblica Amministrazione

Il servizio **PostaCertificat@** è un servizio erogato in conformità al DPCM del 6 maggio 2009. Il servizio PostaCertificat@ è finalizzato a garantire la comunicazione elettronica certificata tra Cittadino e Pubblica Amministrazione e si rivolge ai seguenti soggetti:

VERSIONE 3.1	DATA 29/04/2010	CODICE RISERVATEZZA PUBBLICO	CODIFICA PI_MO_PEC_v3.1_100429	Pagina 6/62
-----------------	--------------------	---------------------------------	-----------------------------------	-------------

- tutti i cittadini italiani maggiorenni che ne facciano richiesta;
- cittadini dipendenti della PA, aventi diritto, esclusivamente per le comunicazioni tra dipendente e PA oltre che tra Cittadino e PA.
- tutte le amministrazioni pubbliche locali e centrali per i propri registri di protocollo, utilizzati per le comunicazioni tra PA e Cittadino.

Il servizio PostaCertificat@ è erogato dal Gestore Poste Italiane S.p.A., in qualità di mandataria del RTI, e da PosteCom S.p.A. e Telecom Italia S.p.A. in qualità di mandanti del suddetto RTI aggiudicatario della gara di affidamento del servizio in conformità all'art. 5 del DPCM del 6 maggio 2009.

## 2.4 Riferimenti normativi

<b>DLgs 82/2005</b>	Decreto Legislativo 7 marzo 2005, n° 82 - <i>Codice dell'amministrazione digitale.</i>
<b>DPR 68/2005</b>	Decreto del Presidente della Repubblica 11 febbraio 2005, n. 68 - <i>Regolamento recante disposizioni per l'utilizzo della posta elettronica certificata, a norma dell'articolo 27 della legge 16 gennaio 2003, n. 3</i>
<b>DM 2/11/2005</b>	Decreto del Ministro per l'Innovazione e le Tecnologie - <i>Decreto del Ministro per l'Innovazione e le Tecnologie recante Regole Tecniche per la formazione, la trasmissione e la validazione, anche temporale, della Posta Elettronica Certificata</i>
<b>CNIPA/CR/56 del 21 maggio 2010</b>	<i>Modalità per la presentazione della domanda di iscrizione nell'elenco pubblico dei gestori di posta elettronica certificata (PEC) di cui all'articolo 14 del decreto del Presidente della Repubblica 11 febbraio 2005, n. 68.</i>
<b>CNIPA 2006/51</b>	Espletamento della vigilanza e del controllo sulle attività esercitate dagli iscritti nell'elenco dei gestori di posta elettronica certificata (PEC), di cui all'articolo 14 del decreto del Presidente della Repubblica 11 febbraio 2005, n. 68, «Regolamento recante disposizioni per l'utilizzo della posta elettronica certificata, a norma dell'articolo 27 della legge 16 gennaio 2003, n. 3».
<b>DLgs 196/2003</b>	Decreto Legislativo 30 giugno 2003, n° 196 - <i>Codice in materia di protezione dei dati personali.</i>
<b>DPCM 06/05/2009</b>	Decreto del Presidente del Consiglio dei Ministri del 6 maggio 2009 recante disposizioni in materia di rilascio e di uso della casella di posta elettronica certificata ai cittadini.

**Tabella 1 - Riferimenti normativi**

## 3 Definizioni

Gestore di Posta Elettronica Certificata	Poste Italiane, gestisce il dominio di posta elettronica certificata che, nel rispetto della normativa vigente, si interfaccia con altri gestori di posta elettronica certificata per l'interoperabilità con altri titolari.
Utente di posta elettronica certificata	La persona fisica, che sia mittente o destinatario di posta elettronica certificata.
Amministratore del Sistema presso le unità organizzative richiedenti	Soggetto di interfaccia con il Gestore, qualora previsto, preposto all'individuazione ed attivazione dei Titolari delle caselle di posta elettronica certificata.

**Tabella 2 – Soggetti del Servizio**

Dominio di Posta Elettronica Certificata	Dominio di posta elettronica certificata che contiene unicamente caselle di posta elettronica certificata.
Casella di Posta Elettronica Certificata (PEC)	La casella di posta elettronica all'interno di un dominio di posta elettronica certificata ed alla quale è associata una funzione che rilascia ricevute di avvenuta consegna al ricevimento di messaggi di PEC.
Indice dei Gestori di Posta Elettronica Certificata	Il sistema, aggiornato dal DigitPA, che contiene l'elenco dei domini e dei gestori di posta elettronica certificata.

**Tabella 3 – Componenti del Servizio**

Punto di accesso	Il sistema che fornisce i servizi di accesso per l'invio e la lettura di messaggi di posta elettronica certificata, nonché i servizi di identificazione ed accesso dell'utente, di verifica della presenza di virus informatici all'interno del messaggio, di emissione della ricevuta di accettazione e di imbustamento del messaggio originale nella busta di trasporto.
Punto di ricezione	Il sistema che riceve il messaggio all'interno di un dominio di posta elettronica certificata, effettua i controlli sulla provenienza e sulla correttezza

	del messaggio ed emette la ricevuta di presa in carico, imbusta i messaggi errati in una busta di anomalia e verifica la presenza di virus informatici all'interno dei messaggi di posta ordinaria e delle buste di trasporto.
Punto di consegna	Il sistema che compie la consegna del messaggio nella casella PEC del titolare destinatario, verifica la provenienza e la correttezza del messaggio ed emette, a seconda dei casi, la ricevuta di avvenuta consegna o l'avviso di mancata consegna.

**Tabella 4 – Nodi del sistema**

Ricevuta di accettazione	La ricevuta, sottoscritta con la firma del gestore di posta elettronica certificata del mittente, contenente i dati di certificazione, rilasciata al mittente dal punto di accesso a fronte dell'invio di un messaggio di posta elettronica certificata.
Avviso di non accettazione	L'avviso, sottoscritto con la firma del gestore di posta elettronica certificata del mittente, che viene emesso quando il gestore mittente è impossibilitato ad accettare il messaggio in ingresso, recante la motivazione per cui non è possibile accettare il messaggio e l'esplicitazione che il messaggio non potrà essere consegnato al destinatario.

**Tabella 5 – Accettazione dei messaggi**

Ricevuta di presa in carico	La ricevuta, sottoscritta con la firma del gestore di posta elettronica certificata del destinatario, emessa dal punto di ricezione nei confronti del gestore di posta elettronica certificata 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 consentire l'associazione con il messaggio cui si riferisce.
-----------------------------	---

**Tabella 6 – Comunicazione tra i gestori**

Ricevuta di avvenuta consegna	La ricevuta, sottoscritta con la firma del gestore di posta elettronica certificata del destinatario, emessa dal punto di consegna al mittente nel momento in cui il messaggio è inserito nella casella di posta elettronica certificata del destinatario. Può essere in forma completa, breve oppure sintetica.
Ricevuta completa di avvenuta consegna	Forma completa della ricevuta di avvenuta consegna nella quale sono contenuti i dati di certificazione ed il messaggio originale.
Ricevuta breve di avvenuta consegna	Forma breve della ricevuta di avvenuta consegna nella quale sono contenuti i dati di certificazione ed un estratto (impronta) del messaggio originale.
Ricevuta sintetica di avvenuta consegna	Forma sintetica della ricevuta di avvenuta consegna nella quale sono contenuti i soli dati di certificazione.
Avviso di mancata consegna	L'avviso, emesso dal sistema, per indicare l'anomalia al mittente del messaggio originale nel caso in cui il gestore di posta elettronica certificata sia impossibilitato a consegnare il messaggio nella casella di posta elettronica certificata del destinatario.

**Tabella 7 – Consegna dei messaggi**

Messaggio originale	Il messaggio inviato da un utente di posta elettronica certificata prima del suo arrivo al punto di accesso e consegnato al titolare destinatario per mezzo di una busta di trasporto che lo contiene.
Busta di trasporto	La busta creata dal punto di accesso e sottoscritta con la firma del gestore di posta elettronica certificata mittente, all'interno della quale sono inseriti il messaggio originale inviato dall'utente di posta elettronica certificata ed i relativi dati di certificazione.
Busta di anomalia	La busta, sottoscritta con la firma del gestore di posta elettronica certificata del destinatario, nella quale è inserito un messaggio errato ovvero non di posta elettronica certificata e consegnata ad un titolare, per evidenziare al destinatario detta anomalia.

Dati di certificazione	I dati, quali ad esempio data ed ora di invio, mittente, destinatario, oggetto, identificativo del messaggio, che descrivono l'invio del messaggio originale e sono certificati dal gestore di posta elettronica certificata del mittente; tali dati sono inseriti nelle varie ricevute e sono trasferiti al titolare destinatario insieme al messaggio originale per mezzo di una busta di trasporto.
Marca Temporale	Evidenza informatica con cui si attribuisce, ad uno o più documenti informatici, un riferimento temporale opponibile ai terzi secondo quanto previsto dal decreto del Presidente del Consiglio dei Ministri 13 gennaio 2004.

**Tabella 8 – Componenti della trasmissione telematica**

## 4 Dati identificativi e riferimenti

### 4.1 Dati del Gestore

DENOMINAZIONE E RAGIONE SOCIALE	POSTE ITALIANE S.p.A.
Rappresentante Legale	Giovanni Ialongo
Responsabile della Direzione TI	Ing Agostino Ragosa
Sede Legale	Viale Europa, 190 00144 ROMA
Telefono	0039 06 59581
Sede Operativa	Viale Europa, 175 00144 ROMA
Telefono	0039 06 59581
Indirizzo Internet del Gestore	<a href="http://www.poste.it">http://www.poste.it</a>
Indirizzo Internet del servizio PostaCertificat@	<a href="http://www.postacertificata.gov.it">http://www.postacertificata.gov.it</a>
Call Center Poste Italiane	803 160
Call Center servizio PostaCertificat@	Call Center disponibile dalle 8:00 alle 20:00, dal lunedì al sabato, accessibile da rete fissa al numero verde gratuito 800.104.464 oppure da rete mobile al numero 199.135.191 (il costo della chiamata è legato al piano tariffario dell'operatore utilizzato)

Tabella 9 – Dati identificativi del Gestore

### 4.2 Dati identificativi del Manuale Operativo

Il presente Manuale Operativo, identificato attraverso il numero di versione 3.1 e dal nome “PI\_MO\_PEC\_v3.1\_100429”, è consultabile, per via telematica, sul sito del Gestore Poste Italiane S.p.A. all'indirizzo <http://www.poste.it>

Questo manuale si riferisce ai servizi di Posta Elettronica Certificata (Posteitaliane.PEC@ e PostaCertificat@) erogati dalla Funzione Tecnologie dell'Informazione per Poste Italiane S.p.A., in osservanza della normativa vigente elencata nell'apposito capitolo.

**RESPONSABILE DEL MANUALE OPERATIVO**

<b>NOME</b>	Giorgio
<b>COGNOME</b>	Zappa
<b>TELEFONO</b>	0039 06 59581
<b>EMAIL</b>	zappagi2@posteitaliane.it

**Tabella 10 – Dati identificativi del Responsabile del Manuale Operativo**

### 4.3 Riferimenti del sito web del gestore

Le informazioni relative al servizio, compreso il presente Manuale Operativo, sono disponibili all'indirizzo web [http://poste.it/online/MO\\_PEC.pdf](http://poste.it/online/MO_PEC.pdf)

## 5 Indice dei contenuti

<b>Contenuto</b>	<b>Riferimento servizio Poste Italiane.PEC @</b>	<b>Riferimento servizio PostaCertificat@</b>
Dati identificativi del gestore	§ 4.1	
Responsabile del Manuale Operativo	§ 4.2	
Riferimenti normativi per la verifica dei contenuti	§ 2.4	
Indirizzo web del Gestore Poste Italiane dove è presente il Manuale Operativo	§ 4.4	
Procedure e standard tecnologici e di sicurezza	§ 20	
Definizioni, abbreviazioni e termini tecnici	§ 3	
Descrizione sintetica del servizio offerto	§ 6	§ 11
Descrizione delle modalità di reperimento e di presentazione delle informazioni presenti nei <i>log</i>	§ 22	
Contenuto e modalità di offerta	§ 7	§ 12
Modalità di accesso al servizio	§ 8	§ 14
Indicazione dei livelli di servizio	§ 10	§ 16

Indicazione delle condizioni di fornitura	§ 9	§ 15
Indicazione delle modalità di protezione dei dati dei titolari	§ 23	
Obblighi, responsabilità e limitazioni in sede di indennizzo	§ 18, § 19	

**Tabella 11 – Contenuto in relazione alla circolare CNIPA/CR/56 del 21/05/2010**

## **SEZIONE I: SERVIZIO POSTE ITALIANE.PEC @**

VERSIONE 3.1	DATA 29/04/2010	CODICE RISERVATEZZA PUBBLICO	CODIFICA PI_MO_PEC_v3.1_100429	Pagina 15/62
-----------------	--------------------	---------------------------------	-----------------------------------	--------------

## 6 Descrizione del servizio di Poste Italiane.PEC @

### 6.1 Caratteristiche generali del servizio

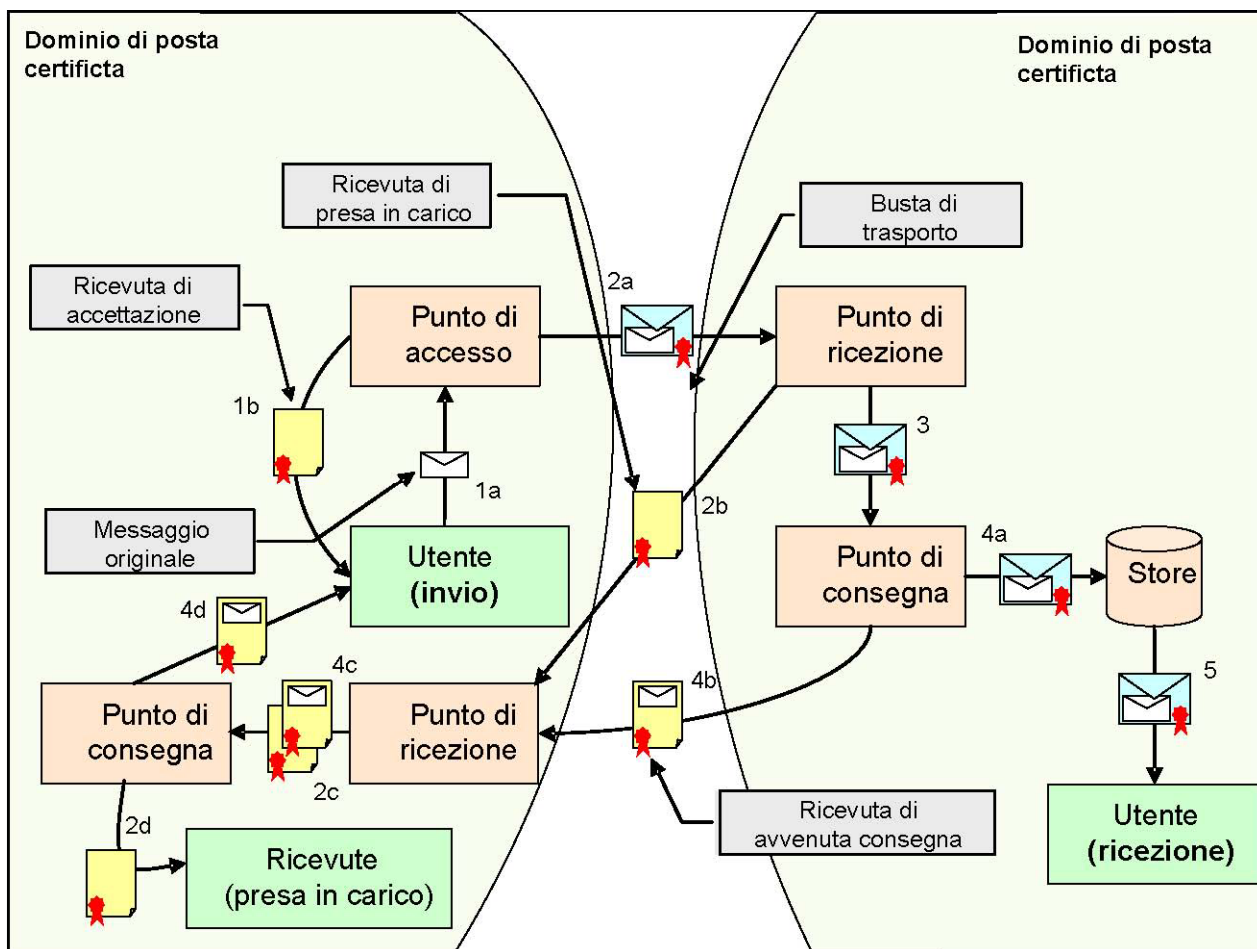
Poste Italiane.PEC @ è il servizio di Posta Elettronica Certificata di Poste Italiane che, nel rispetto della normativa vigente, consente di inviare e ricevere documentazione elettronica con un elevato livello di sicurezza e di dare valore legale al processo di consegna dei messaggi.

Le caselle di Poste Italiane.PEC @ consentono l'inoltro e la ricezione di messaggi in conformità con quanto previsto dal DPR 68/2005 e dal DM 2 novembre 2005.

Il servizio si basa su una classica infrastruttura di posta elettronica SMTP, ma il formato dei messaggi e l'elaborazione degli stessi sono diversi rispetto ad un normale messaggio di posta elettronica.

Tramite Poste Italiane.PEC @ l'utente mittente, utilizzando gli stessi client applicativi di posta elettronica comunemente adottati, invia il messaggio da un apposito account configurato sul dominio di posta certificata registrato. Una volta inviato il messaggio, il server provvede a fornire al mittente una ricevuta di accettazione sottoscritta mediante firma elettronica avanzata e ad inoltrare il messaggio al server di posta certificata del destinatario, che provvederà a fornire, a sua volta, al mittente la ricevuta di avvenuta consegna del messaggio sulla casella di posta certificata del destinatario. L'interazione fra due distinti Gestori, coinvolti nell'invio di un messaggio di posta certificata, è regolata dallo scambio di una ricevuta di presa in carico.

La figura seguente, tratta dall'Allegato Tecnico alle Regole Tecniche emanate con (DM 2 novembre 2005), propone una rappresentazione grafica degli elementi caratteristici di un dominio di posta certificata e delle sue interazioni con un altro dominio di posta certificata, nell'ipotesi di corretto invio e consegna con esito positivo.



**Figura 1 – elementi di un dominio di posta elettronica certificata**

- 1a** l'utente invia una e-mail al Punto di Accesso;
- 1b** il Punto di Accesso restituisce al mittente una Ricevuta di Accettazione;
- 2a** il Punto di Accesso crea una Busta di Trasporto (contenente il messaggio originale) e la inoltra al Punto di Ricezione del Gestore di Posta Certificata della casella del destinatario;
- 2b** il Punto di Ricezione verifica la Busta di Trasporto e crea una Ricevuta di Presa in Carico che viene inoltrata al Punto di ricezione del Gestore mittente;
- 2c** il Punto di Ricezione verifica la validità della Ricevuta di Presa in Carico e la inoltra al Punto di Consegna;
- 2d** il Punto di Consegna salva la Ricevuta di Presa in Carico nello store delle ricevute del Gestore;
- 3** il Punto di Ricezione inoltra la Busta di Trasporto al Punto di Consegna;
- 4a** il Punto di Consegna verifica il contenuto della Busta di Trasporto e la salva nello

store (mailbox del destinatario);

- 4b** il Punto di Consegna crea una Ricevuta di Avvenuta Consegna e la inoltra al Punto di Ricezione del Gestore mittente;
- 4c** il Punto di ricezione verifica la validità della Ricevuta di avvenuta consegna e la inoltra al Punto di Consegna;
- 4d** il Punto di Consegna salva la Ricevuta di Avvenuta Consegna nella mailbox del mittente;
- 5** l'utente destinatario ha a disposizione la e-mail inviata.

La trasmissione tra mittente e destinatario (e tra i due relativi server) avviene mediante messaggi di posta certificata sottoscritti con firma elettronica avanzata.

Durante le fasi di trattamento del messaggio, viene mantenuta traccia su un apposito registro delle operazioni.

## 6.2 Definizione applicativa delle componenti il servizio

Di seguito l'architettura applicativa del servizio.

### Posta Certificata

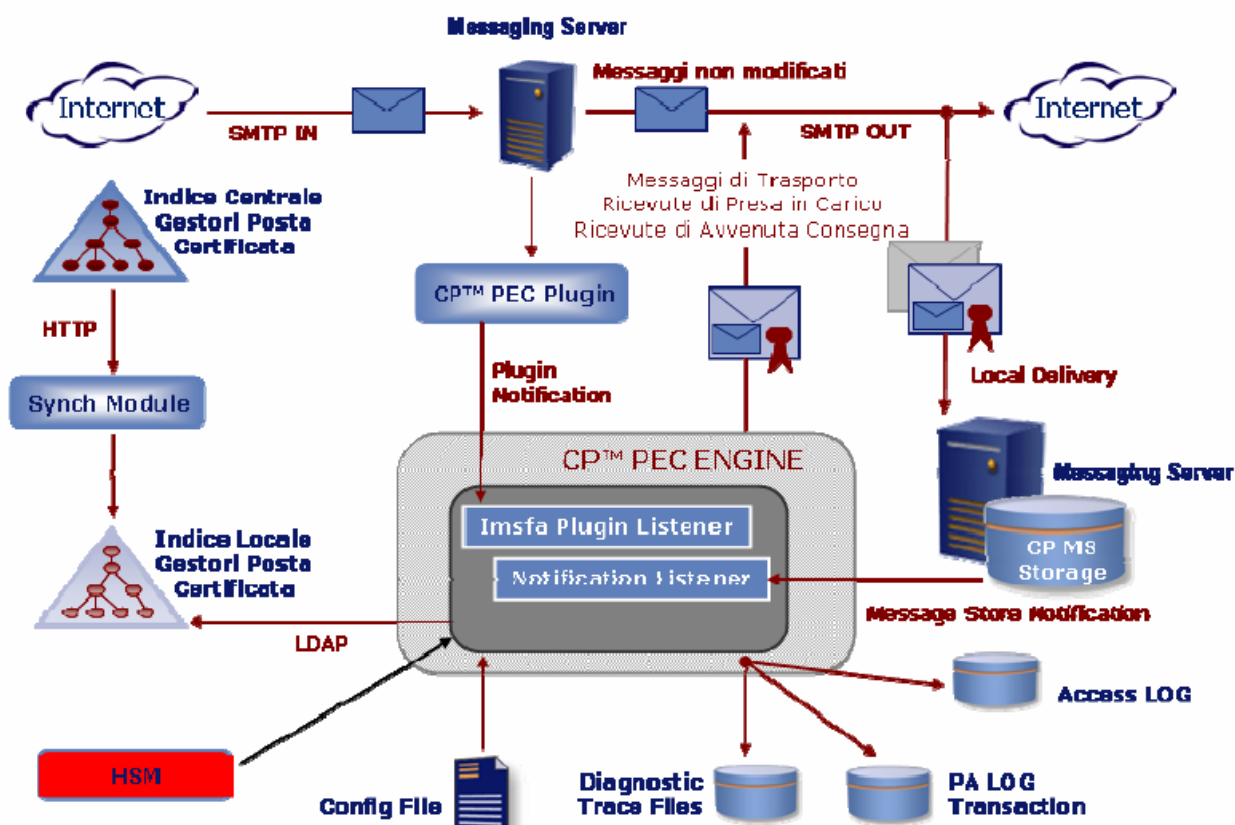


Figura 2 - Architettura applicativa del servizio

## 6.3 Ricevute ed avvisi rilasciati all'utente

La Posta Elettronica Certificata aggiunge ai normali sistemi di e-mail il valore derivante dalla trattazione di opportune ricevute od avvisi che rivestono valenza legale per la dimostrazione dell'avvenuta effettuazione delle diverse fasi di trasmissione telematica dei messaggi.

Per permettere una chiara contestualizzazione e specifica attribuzione di valenza alle diverse tipologie di ricevute ed avvisi, di seguito viene riportata una sintetica descrizione degli stessi.

### 6.3.1 Ricevute

#### 6.3.1.1 Ricevuta di accettazione

Le ricevute di accettazione rilasciate dal Gestore, sono costituite da un messaggio di posta elettronica inviato al mittente e riportante data ed ora di accettazione, dati del mittente e del destinatario ed oggetto.

Il corpo del messaggio è composto da un testo che costituisce la vera e propria ricevuta in formato leggibile e da un allegato in cui gli stessi dati di certificazione sono inseriti all'interno di un file XML per permettere una elaborazione automatica dei messaggi e delle relative ricevute.

#### 6.3.1.2 Ricevuta di avvenuta consegna

Le ricevute di avvenuta consegna rilasciate dal Gestore sono costituite da un messaggio di posta elettronica inviato al mittente che riporta la data e l'ora di avvenuta consegna, i dati del mittente e del destinatario e l'oggetto.

Il corpo del messaggio è composto da un testo che costituisce la vera e propria ricevuta in formato leggibile. Gli stessi dati di certificazione sono inseriti all'interno di un file XML per permettere la trattazione automatica dei messaggi e delle relative ricevute.

La ricevuta di avvenuta consegna è emessa per ognuno dei destinatari a cui è consegnato il messaggio.

##### 6.3.1.2.1 Ricevuta completa di avvenuta consegna

Nel rilascio delle ricevute di avvenuta consegna, il sistema distingue tra i messaggi consegnati ai destinatari primari ed i riceventi in copia. Esclusivamente per le consegne relative ai destinatari primari, all'interno della ricevuta di avvenuta consegna, oltre agli allegati descritti, è inserito il messaggio originale completo.

##### 6.3.1.2.2 Ricevuta di avvenuta consegna breve

Al fine di consentire uno snellimento dei flussi, è possibile, per il mittente, richiedere al Gestore, la ricevuta di avvenuta consegna in formato breve. Tale ricevuta inserisce al suo interno il messaggio originale, sostituendone gli allegati con le relative impronte univoche (hash crittografici) per ridurre le dimensioni della ricevuta. Per permettere la verifica dei contenuti trasmessi è indispensabile che il mittente conservi gli originali "immodificati" degli allegati inseriti nel messaggio originale cui le impronte (hash) fanno riferimento.

La ricevuta di consegna breve viene richiesta dal mittente mediante apposite applicazioni in grado di formare lo specifico messaggio di Posta Elettronica Certificata in aderenza alle relative specifiche definite dall'allegato tecnico al DM 2 novembre 2005.

### 6.3.1.2.3 Ricevuta di avvenuta consegna sintetica

Nel caso che il mittente richieda, mediante appositi applicativi e secondo la specifica definita dall'allegato tecnico al DM 2 novembre 2005, la ricevuta di consegna sintetica, questa riporta i soli dati di certificazione sia nel testo in chiaro che nell'allegato file XML.

### 6.3.2 Avvisi

I dati di certificazione riportati negli avvisi sono inseriti all'interno di un file XML allegato al messaggio.

#### 6.3.2.1 Avviso di non accettazione per errori formali

Qualora il punto di accesso al servizio del Gestore, non possa provvedere all'inoltro del messaggio, a causa del mancato superamento dei controlli formali, viene recapitato al mittente uno specifico avviso di non accettazione. L'avviso non contiene il messaggio originale.

#### 6.3.2.2 Avviso di mancata consegna per superamento dei tempi massimi previsti

Nei messaggi originati da caselle di Posta Elettronica Certificata fornita da Poste Italiane, qualora Poste Italiane stessa 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 effettuare la consegna del messaggio.

Qualora, entro ulteriori dodici ore, l'erogatore (per conto del gestore) non abbia ricevuto la ricevuta di avvenuta consegna del messaggio inviato, inoltra al mittente un ulteriore avviso relativo alla mancata consegna del messaggio.

#### 6.3.2.3 Avviso di non accettazione per virus informatico

Nei messaggi originati da caselle di Posta Elettronica Certificata fornite da Poste Italiane qualora Poste Italiane stessa riceva messaggi in accettazione con virus informatici non provvede all'accettazione ed informa tempestivamente il mittente dell'impossibilità di dar corso alla trasmissione.

In questo caso viene emesso l'avviso di non accettazione per virus informatico per dare chiara comunicazione al mittente dei motivi che hanno portato al rifiuto del messaggio.

#### 6.3.2.4 Avviso di rilevazione virus informatico

Qualora Poste Italiane riceva messaggi di Posta Elettronica Certificata, diretti ai propri utenti, che rilevino la presenza di virus informatici, non provvede all'inoltro, informando

tempestivamente il gestore del mittente affinché comunichi al mittente stesso l'impossibilità di dar corso alla consegna.

Il sistema genera un avviso di rilevazione virus che restituisce al gestore mittente indicando come indirizzo quello specificato per le ricevute nell'Indice dei gestori di posta certificata, con l'indicazione dell'errore riscontrato.

#### 6.3.2.5 Avviso di mancata consegna per virus informatico

Nel caso di messaggi originati da caselle di Posta Elettronica Certificata gestite da TI in cui la presenza di virus sia rilevata dal gestore del destinatario, TI attraverso l'erogatore, all'arrivo dell'avviso di rilevazione di virus informatico proveniente dal gestore destinatario, emette un avviso di mancata consegna che restituisce al mittente.

#### 6.3.2.6 Avviso di mancata consegna

Nel caso si verifichi un errore nella fase di consegna del messaggio, il sistema genera un avviso di mancata consegna da restituire al mittente con l'indicazione dell'errore riscontrato.

#### 6.3.3 Buste di anomalia

Nel caso in cui uno dei test evidenzi un errore nel messaggio in arrivo, oppure venga riconosciuto come un messaggio di posta ordinaria e lo specifico accordo contrattuale o modalità di conduzione preveda la propagazione verso il destinatario, il sistema lo inserisce in una busta di anomalia.

Nella busta di anomalia non sono inseriti allegati oltre al messaggio pervenuto al punto di ricezione (es. dati di certificazione) data l'incertezza sull'effettiva provenienza/correttezza del messaggio.

## 6.4 Riferimenti temporali dei messaggi

A ciascuna trasmissione è apposto un riferimento temporale, secondo le modalità indicate nell'allegato tecnico del DM 2 novembre 2005. Il riferimento temporale è generato con un sistema che garantisce stabilmente uno scarto non superiore ad un minuto secondo rispetto alla scala di tempo universale coordinato(UTC), determinata ai sensi dell'art. 3, comma 1, della legge 11 agosto 1991, n. 273.

Per tutte le operazioni effettuate durante i processi di elaborazione dei messaggi, ricevute, log, ecc. svolte dai punti di accesso/ricezione/consegna è disponibile il relativo riferimento temporale. Gli eventi (generazione di ricevute, buste di trasporto, log, ecc.) che costituiscono la transazione di elaborazione del messaggio presso i punti di accesso,

ricezione e consegna, impiegano il riferimento temporale rilevato all'interno della transazione stessa. In questo modo l'indicazione dell'istante di elaborazione del messaggio è univoca all'interno dei log, delle ricevute, dei messaggi, ecc. generati dal server.

Le indicazioni temporali fornite dal servizio in formato leggibile dall'utente (testo delle ricevute, buste di trasporto, ecc.) sono fornite con riferimento all'ora legale vigente al momento indicato per l'operazione. Per la data il formato impiegato è "gg/mm/aaaa" mentre per l'indicazione oraria si utilizza "hh:mm:ss", dove hh è in formato 24 ore. Al dato temporale è fatta seguire tra parentesi la "zona" ossia la differenza (in ore e minuti) tra l'ora legale locale ed UTC. La rappresentazione di tale valore è in formato "[+|-]hhmm", dove il primo carattere indica una differenza positiva o negativa.

#### 6.4.1 Sincronizzazione e distribuzione del riferimento temporale

La sorgente dell'informazione temporale deriva dall'orologio di sistema. La precisione dell'orologio di sistema è garantita dalla sua sincronizzazione con una sorgente esterna che mantiene un'informazione temporale corrispondente alla scala temporale UTC. Al fine di garantire la precisione e la sincronizzazione delle registrazioni di controllo (log) è implementato un sistema di sincronizzazione oraria realizzato mediante la implementazione del protocollo NTP. Tramite apposite applicazioni, la sorgente temporale viene distribuita ai sistemi che gestiscono la Posta Elettronica Certificata e assicurano l'apposizione del Riferimento Temporale opponibile ai terzi, come previsto dall'articolo 9 del DM 2 novembre 2005.

VERSIONE 3.1	DATA 29/04/2010	CODICE RISERVATEZZA PUBBLICO	CODIFICA PI_MO_PEC_v3.1_100429	Pagina 23/62
-----------------	--------------------	---------------------------------	-----------------------------------	--------------

## **7 Contenuto dell’offerta Poste Italiane.PEC @**

### **7.1 Tipologie di utenti**

Gli utenti che possono usufruire del servizio Poste Italiane.PEC @, sono i soggetti appartenenti alle Unità Organizzative interne di Poste Italiane o a soggetti comunque da queste individuati.

#### **7.1.1 Modalità di rilascio delle caselle**

Il rilascio di caselle a soggetti appartenenti alle Unità Organizzative interne a Poste Italiane, o a soggetti comunque da queste individuati, avviene secondo la modalità che prevede l’attivazione di un dominio dedicato di posta certificata e, qualora previsto, la contestuale individuazione dell’Amministratore. L’Amministratore del sistema, tramite l’interfaccia web di gestione del proprio dominio di Poste Italiane.PEC @, assume il compito di attivare, cancellare o gestire le caselle dei Titolari. Tale soggetto, può essere individuato o all’interno dell’Unità Organizzativa o all’interno di TI/Esercizio.

### **7.2 La Tipologia del servizio**

Le caselle avranno un proprio dominio a scelta, che dovrà essere dedicato all’inoltro di messaggi di posta elettronica certificata. La casella di Posta Elettronica Certificata standard ha una dimensione di 100 MB; è possibile acquistare ulteriori pacchetti di 100 MB l’uno, che possono essere distribuiti tra i vari Titolari con “slot” minimi di 10 MB. Gli specifici accordi contrattuali potranno riferirsi anche a diverse dimensioni o caratteristiche per la casella purché nel rispetto della normativa vigente ed espressamente indicate nell’accordo contrattuale raggiunto con il fornitore.

L’Amministratore, individuato all’interno dell’Unità Organizzativa o all’interno di Esercizio, ha possibilità di gestire direttamente la configurazione del servizio, tramite interfaccia web di gestione accedendo con le seguenti funzionalità:

- autenticazione tramite user-id e password;
- inserimento nuovi utenti;
- cancellazione utenti;
- disabilitazione utenti;
- reset password ad un valore impostato: nel caso in cui un utente abbia dimenticato la propria password l’Amministratore del sistema ha la possibilità di eseguire il reset del campo password ad un valore impostato dall’Amministratore;

**I tempi di attivazione del Servizio sono di 3 giorni lavorativi** dalla data di ricezione di tutta la documentazione necessaria compresa quella eventuale per la registrazione del nuovo dominio.

## **8 Modalità di accesso al servizio di Poste Italiane.PEC @**

Al servizio di Poste Italiane.PEC @ è possibile accedere secondo le seguenti modalità:

- via web (HTTPS) attraverso una applicazione webmail con le seguenti principali funzionalità:
  - gestione della posta in arrivo;
  - redazione di un nuovo messaggio;
  - organizzazione dei messaggi e delle cartelle che li contengono;
  - Rubrica dei destinatari;
  - ricerca messaggio;
  - opzioni;
  - cambio della password.
- utilizzando un client di posta elettronica (SMTP/S per l'invio e POP3/S e IMAP/S per la ricezione). In questo caso le funzionalità esposte sono quelle tipiche dello specifico client utilizzato dal Titolare. Per utilizzare questa modalità di accesso, è necessario configurare il proprio client con i parametri relativi:
  - server di posta in arrivo (POP3/S o IMAP/S);
  - server di posta in uscita (SMTP/S);
  - numeri porta server posta in arrivo;
  - numeri porta server posta in uscita.

L'autenticazione del titolare alla propria casella di posta elettronica certificata viene effettuata tramite credenziali riservate (userid e password) impostate dall'Amministratore del Sistema, individuato all'interno dell'unità organizzativa o all'interno di TI/Esercizio.

È necessario che il Titolare provveda al cambiamento della password la prima volta che accede alla propria utenza. L'interfaccia web di accesso al servizio, tra le diverse funzionalità esposte, consente anche quella di impostare una nuova password. Per un sicuro e corretto utilizzo della propria casella di Posta Elettronica Certificata, si consiglia di effettuare il cambiamento della password periodicamente.

## 9 Condizioni di fornitura Poste Italiane.PEC @

Le Caselle sono rilasciate per soggetti appartenenti a specifiche unità organizzative. Per aderire al servizio, l'Unità Organizzativa sottoscrive la Richiesta di servizio dove vengono riportate le clausole regolamentari relative al lotto di caselle richiesto. Tale Richiesta, sottoscritta dal Responsabile dell'Unità Organizzativa o da soggetto con potere di firma, individua la figura di "Amministratore del Sistema" (all'interno della stessa Unità Organizzativa richiedente o all'interno di TI/Esercizio) quale soggetto di interfaccia con il Gestore, preposto alla individuazione dei Titolari delle caselle di posta elettronica certificata.

**Il numero massimo di caselle richiedibili per tale modalità è 10.** E' possibile utilizzare un dominio specifico che dovrà essere utilizzato dall'unità organizzativa esclusivamente per l'inoltro/ricezione di messaggi di posta elettronica certificata.

In aggiunta a tali modalità il servizio potrà essere utilizzato come vettore certificato nell'ambito di servizi integrati di Poste Italiane. In tal caso sarà il servizio nel suo insieme ad essere oggetto di acquisizione da parte dell'utente finale.

Il servizio standard ha una durata annuale e, se non diversamente specificato, si rinnova tacitamente per la medesima durata originaria, salvo disdetta da comunicarsi - con un preavviso di almeno 30 (trenta) giorni rispetto alla data di scadenza - tramite richiesta formale dell'utente da inviare al Referente TI/Esercizio incaricato, che provvederà ad inoltrare la domanda a chi di competenza.

TI (per conto di Poste Italiane) potrà sospendere temporaneamente il Servizio, fermo restando gli obblighi di legge, per procedere alla manutenzione di impianti ed altre apparecchiature necessarie all'esecuzione del Servizio stesso, dandone comunicazione al Titolare tramite e-mail o avviso pubblicato sul sito Internet [www.postepernoi.poste](http://www.postepernoi.poste), con un preavviso di 1 (uno) giorno.

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

Nel caso in cui l'esecuzione del Servizio fosse ritardata, impedita od ostacolata da cause di forza maggiore, l'esecuzione medesima si intenderà sospesa per un periodo equivalente alla durata della causa di *forza maggiore*.

Per "**forza maggiore**" si intende qualsiasi circostanza al di fuori del ragionevole controllo di TI e, pertanto, in via esemplificativa e non esaustiva, si riferisce ad atti di pubbliche

autorità, guerre, rivoluzioni, insurrezioni o disordini civili, scioperi, serrate o altre vertenze sindacali, blocchi od embarghi, interruzioni nella fornitura di energia elettrica, inondazioni, disastri naturali, epidemie ed altre circostanze che esulino dal controllo di Poste Italiane.

## 10 Livelli di servizio ed indicatori di qualità Poste Italiane.PEC @

<b>Destinatari degli invii</b>	Numero massimo di destinatari per messaggi originati da caselle Poste Italiane.PEC@	<b>100</b>
<b>Dimensione dei messaggi</b>	Dimensione massima per il singolo messaggio accettabile da caselle Poste Italiane PEC @ (intesa come prodotto dei destinatari per la dimensione del messaggio stesso)	<b>30 Mb</b>
<b>Disponibilità</b>	Disponibilità del servizio nel periodo di riferimento (*)	<b>99,8 %</b>
	Durata massima di indisponibilità del servizio nel periodo (*)	<b>262,8 minuti</b>
	Durata massima per singola indisponibilità del servizio (*)	<b>131,4 minuti</b>
<b>Tempi</b>	Tempo di consegna delle ricevute	<b>30 minuti</b>

**Tabella 12 – Livelli di servizio ed indicatori di qualità**

(\*) Il periodo temporale di riferimento, per il calcolo della disponibilità del servizio di posta elettronica certificata, è pari ad un quadrimestre.

**SEZIONE II: SERVIZIO POSTACERTIFICAT@**

## 11 Descrizione del servizio PostaCertificat@

### 11.1 Caratteristiche generali del servizio

La PostaCertificat@ è un servizio di comunicazione elettronica sicura e certificata tra Pubblica Amministrazione e Cittadino. Attraverso la PostaCertificat@ ogni cittadino può dialogare in modalità sicura e certificata con la Pubblica Amministrazione comodamente da casa o con qualsiasi dispositivo in grado di connettersi ad internet senza recarsi presso gli Uffici della PA per:

- Richiedere o inviare informazioni alle Pubbliche Amministrazioni dotate di PostaCertificat@;
- inviare istanze/documentazione alle Pubbliche Amministrazioni dotate di PostaCertificat@;
- ricevere documenti, informazioni, comunicazioni dalle Pubbliche Amministrazioni dotate di PostaCertificat@.

Il servizio PostaCertificat@:

- fornisce tutte le garanzie di una posta elettronica certificata;
- permette di dare ad un messaggio di posta elettronica la piena validità legale nei casi previsti dalla normativa;
- garantisce data e ora riferiti all'accettazione e alla consegna del messaggio e l'integrità del contenuto trasmesso.

Il servizio si rivolge:

1. a tutti i cittadini italiani maggiorenni che ne facciano richiesta;
2. ai cittadini dipendenti della PA esclusivamente per le comunicazioni tra dipendente e PA oltre che tra Cittadino e PA. I dipendenti pubblici che attivano la casella PostaCertificat@ potranno attivare a proprio carico anche i servizi accessori previsti per i cittadini.
3. a tutte le amministrazioni pubbliche locali e centrali per i propri registri di protocollo, utilizzati per le comunicazioni tra PA e Cittadino

La PostaCertificat@ è rilasciata ai sensi del Decreto del Presidente del Consiglio dei Ministri del 6 maggio 2009 recante disposizioni in materia di rilascio e di uso della casella di posta elettronica certificata ai cittadini. L'utilizzo della PostaCertificat@ avviene ai sensi

del Codice dell'Amministrazione Digitale ed è aderente al Regolamento sulla Posta Elettronica Certificata DPR 11 febbraio 2005, n. 68 ed alle Regole Tecniche di cui al Decreto Ministeriale 2 Novembre 2005.

## 11.2 Definizione applicativa delle componenti il servizio PostaCertificat@

Di seguito una vista complessiva dell'architettura applicativa del servizio con focus, cerchiato in rosso, della piattaforma PEC:

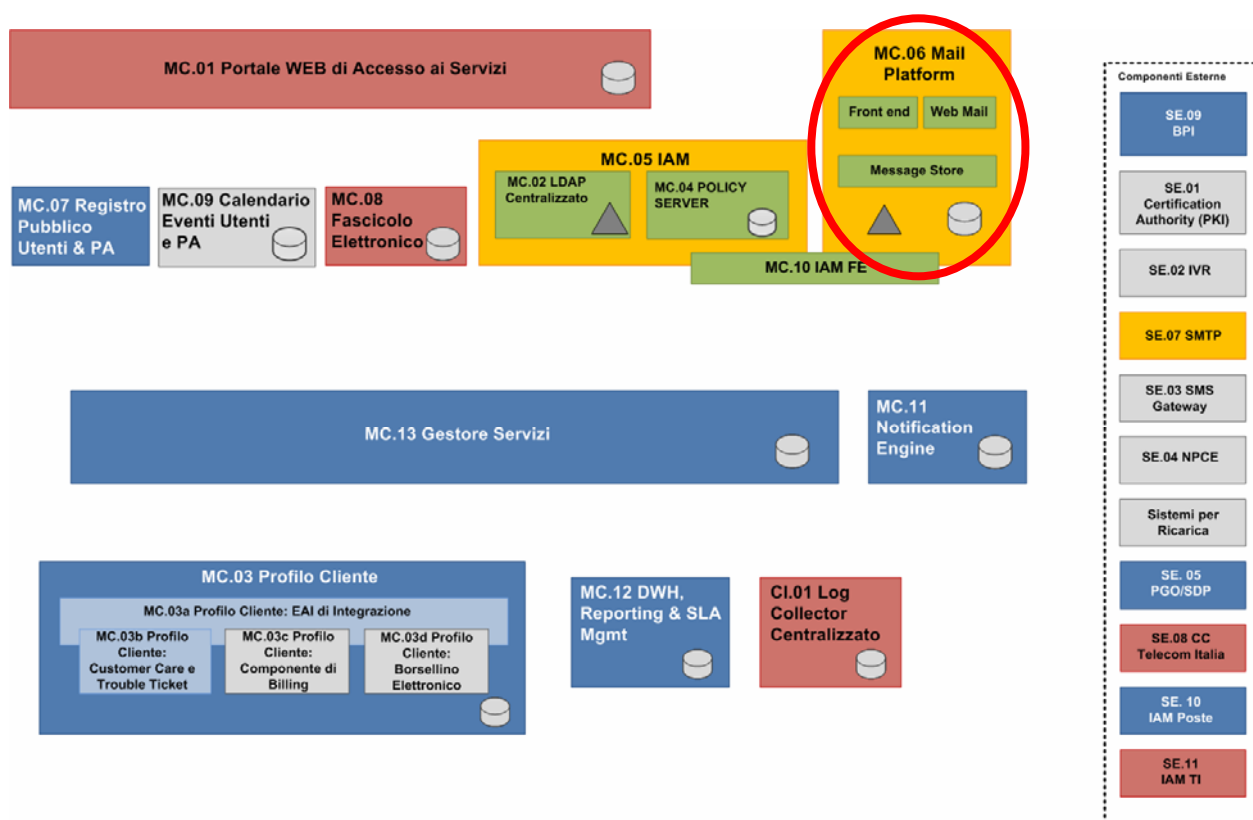


Figura 3 - Architettura applicativa della Piattaforma del servizio PostaCertificat@

Facendo riferimento alla figura successiva, si descrivono le funzionalità dei tre differenti elementi architettureali che compongono la Piattaforma PEC:

1. Punto di Accesso
2. Punto di Ricezione
3. Punto di Consegna

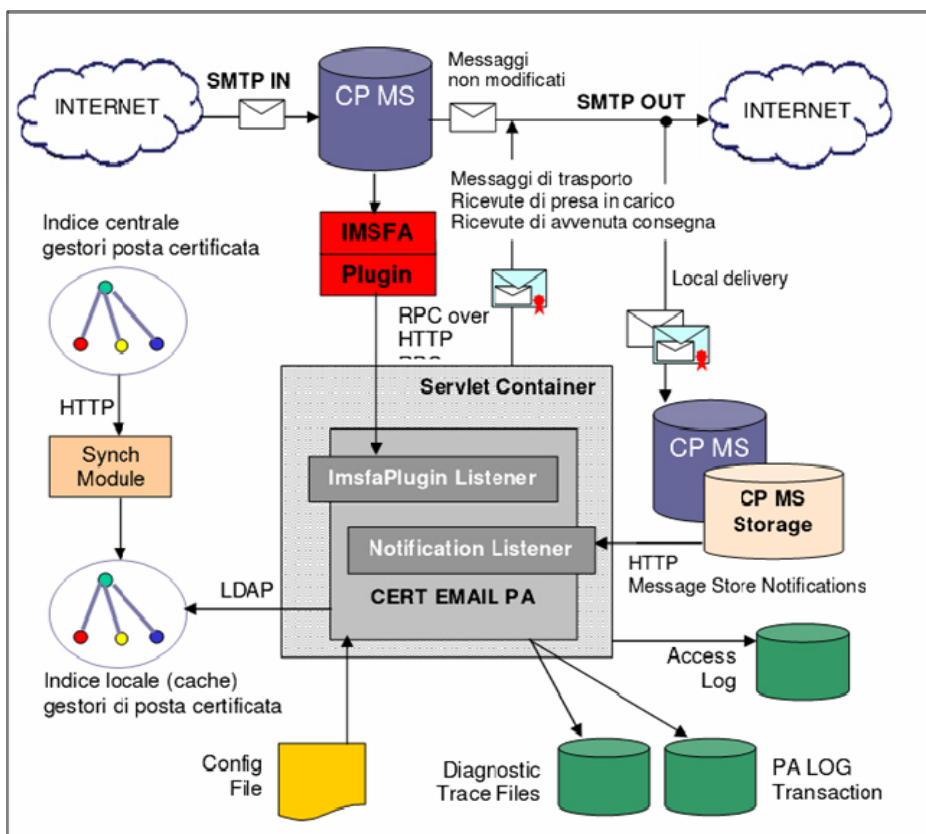


Figura 4 - Architettura funzionale della piattaforma PEC

- **Punto di accesso:** al momento dell'invio di un messaggio di posta certificata il punto di accesso accerta l'identità di chi effettua il collegamento mediante SMTP authentication. Alla ricezione di un messaggio originale, il punto di accesso:
  - effettua dei controlli formali sul messaggio in ingresso;
  - genera una ricevuta di accettazione;
  - imbusta il messaggio originale in un messaggio di trasporto.

La ricevuta di accettazione indica al mittente che il suo messaggio è stato accettato dal sistema e certifica la data e l'ora dell'evento. All'interno della ricevuta è presente un testo leggibile dall'utente, un allegato XML con i dati di certificazione in formato elaborabile ed eventuali altri allegati per funzionalità aggiuntive offerte dal gestore.

Il punto di accesso, utilizzando i dati dell'indice dei gestori di posta certificata, effettua un controllo per ogni destinatario del messaggio originale per verificare se appartengono all'infrastruttura di posta certificata o sono utenti esterni (es. posta Internet). La ricevuta di accettazione (ed i

relativi dati di certificazione) riporta quindi la tipologia dei vari destinatari per informare il mittente del differente flusso seguito dai due gruppi di messaggi (utenti di posta certificata, utenti esterni).

Il meccanismo di sicurezza per il colloquio tra i server partecipanti all'infrastruttura di posta certificata è realizzato mediante la firma dei messaggi in uscita dal punto di accesso e la loro verifica in ingresso al punto di ricezione. Il messaggio originale (completo di header, testo ed allegati) è inserito come allegato all'interno di un messaggio di trasporto. Il messaggio di trasporto firmato permette di verificare che il messaggio originale non sia stato modificato durante il suo percorso dal dominio mittente al dominio destinatario. La firma apposta sul messaggio dal sistema mittente è verificata all'arrivo sul server di destinazione.

L'implementazione di tale elemento è realizzata con un CP MailServer con funzionalità di Front End e con l'estensione IMSFA (Internet Mail Security Filter Agent) abilitata, estensione che permette di analizzare i messaggi in ingresso al sistema di posta e li sottopone mediante protocollo HTTP ad un'applicazione JAVA esterna (servlet Tomcat) che provvede alla generazione dei messaggi di trasporto e delle ricevute.

- **Punto di ricezione:** a fronte dell'arrivo di un messaggio, effettua la seguente serie di controlli ed operazioni:
  - verifica la correttezza/natura del messaggio in ingresso;
  - se il messaggio in ingresso è un messaggio di trasporto corretto:
  - emette una ricevuta di presa in carico verso il gestore mittente;
  - inoltra il messaggio di trasporto verso il punto di consegna ;
  - se il messaggio in ingresso è un messaggio di trasporto errato/non è un messaggio di trasporto:
    - imbusta il messaggio in arrivo in un messaggio di anomalia di trasporto
    - inoltra il messaggio di anomalia di trasporto verso il punto di consegna

La ricevuta di presa in carico è emessa dal gestore ricevente il messaggio nei confronti del gestore mittente. Il suo fine è quello di consentire il tracciamento del messaggio nel passaggio tra un gestore ed un altro.

L'implementazione di tale elemento è identica a quella del punto di accesso.

- **Punto di consegna:** all'arrivo del messaggio presso il punto di consegna, il sistema ne verifica la tipologia e stabilisce se deve inviare una ricevuta al mittente. La ricevuta di avvenuta consegna è emessa esclusivamente a fronte della ricezione di un messaggio di trasporto valido; in tutti gli altri casi (es. messaggi di anomalia di trasporto), la ricevuta di avvenuta consegna non è emessa.

La ricevuta di avvenuta consegna indica al mittente che il suo messaggio è stato effettivamente consegnato al destinatario specificato e certifica la data e l'ora dell'evento tramite un testo leggibile dall'utente ed un allegato XML con i dati di certificazione in formato elaborabile oltre ad eventuali allegati per funzionalità aggiuntive offerte dal gestore.

A fronte di un errore di consegna nella casella di destinazione (casella piena, messaggio troppo grande), il punto di consegna emette una ricevuta di errore di consegna.

L'implementazione di questo componente architetturale è realizzata tramite un CP MailServer con funzionalità di BackEnd.

### **11.3 Ricevute ed avvisi rilasciati all'utente**

La piattaforma applicativa utilizzata per il servizio PostaCertificat@ possiede le stesse caratteristiche e funzionalità della piattaforma applicativa utilizzata per il servizio Poste Italiane. PEC@). Per la descrizione puntuale di tali caratteristiche funzionalità si fa quindi riferimento al paragrafo 6.3 e relativi sottoparagrafi.

### **11.4 Riferimenti temporali dei messaggi**

Per il servizio PostaCertificat@, le modalità per la generazione e le caratteristiche del riferimento temporale sono analoghe a quelle adottate per il servizio Poste Italiane.PEC@ e quindi descritte al par. 6.4 del presente Manuale. Il riferimento temporale è in grado di garantire la precisione e la sincronizzazione delle registrazioni di controllo (log) e l'utilizzo di sistemi di PEC assicura l'apposizione del Riferimento Temporale opponibile ai terzi, come previsto dall'articolo 9 del DM 2 novembre 2005 come descritto nel paragrafo 6.4.1.

## **12 Contenuto dell’offerta PostaCertificat@**

### **12.1 Tipologie di utenti**

Il servizio è offerto a titolo gratuito e si rivolge:

1. a tutti i cittadini italiani maggiorenni che ne facciano richiesta (anche i cittadini italiani residenti all'estero);
2. ai cittadini dipendenti della PA esclusivamente per le comunicazioni tra dipendente e PA oltre che tra Cittadino e PA. I dipendenti pubblici che attivano la casella CEC PAC potranno attivare a proprio carico anche i servizi accessori previsti per i cittadini;
3. a tutte le amministrazioni pubbliche locali e centrali per i propri registri di protocollo, utilizzati per le comunicazioni tra PA e Cittadino.

## **13 Modalità di rilascio delle caselle di PostaCertificat@**

### **13.1 Richiesta ed Attivazione della casella del cittadino**

La richiesta di attivazione del servizio viene effettuata tramite il portale web dove il Cittadino ha a disposizione una procedura interattiva guidata che gli consente di inserire la richiesta in maniera semplice e veloce.

La procedura prevede:

1. Inserimento dei dati richiesti;
2. Verifica correttezza dei dati inseriti;
3. Selezione dei servizi accessori;
4. Scelta Password;
5. Presentazione Documentazione descrittiva del Servizio PostaCertificat@;
6. Accettazione da parte del cittadino delle condizioni contrattuali del servizio e delle implicazioni dell’adesione allo stesso nei rapporti con la Pubblica Amministrazione;
7. Finalizzazione della richiesta;
8. Comunicazione dell’esito della richiesta;
9. Lista degli uffici abilitati;

10. Memorizzazione della richiesta di attivazione;
11. Stampa riepilogativa della richiesta.

Il sito dedicato al servizio PostaCertificat@ ([www.postacertificata.gov.it](http://www.postacertificata.gov.it)) contiene tutte le informazioni utili per la richiesta e la successiva attivazione del servizio stesso.

### **13.2 Richiesta ed Attivazione della casella della PA**

Una volta sottoscritto il contratto, il processo di attivazione delle Caselle PA è simile al processo già descritto, con la differenza che la casella risulta associata non ad una persona fisica, ma ad una o più utenze che vi possono accedere. La responsabilità della creazione di una casella di protocollo è dell'utente di tipo AMPA che può creare una nuova casella, attraverso il portale, come se fosse una casella tradizionale.

- a. Richiesta attivazione casella: viene manifestata all'utente di tipo AMPA l'esigenza di creare una nuova casella di protocollo.
- b. Creazione casella inattiva: l'account AMPA, attraverso il portale, richiede la creazione di una nuova casella di tipo Protocollo. La casella verrà creata in stato inattivo.
- c. Creazione password per casella: viene creata una password per l'accesso alla casella di protocollo.
- d. Attivazione casella: la casella viene attivata.
- e. Comunicazione attivazione casella: viene inviata una comunicazione di avvenuta creazione ed attivazione di una nuova casella di protocollo. Tale comunicazione viene inviata solo all'utente di tipo AMPA.

### **13.3 La Tipologia del servizio**

La tipologia del servizio PostaCertificat@ è descritta definendo i servizi base ed i servizi avanzati forniti ai cittadini e alla PA. Tale descrizione di dettaglio è pubblicata sul sito dedicato del servizio ([www.postacertificata.gov.it](http://www.postacertificata.gov.it)).

### **14 Modalità di accesso al servizio PostaCertificat@**

E' possibile accedere al servizio di PostaCertificat@ secondo le seguenti modalità:

- tramite WebMail (HTTP/S), integrata all'interno del Portale Web;

- utilizzando un client di posta elettronica tradizionale (POP3/S o IMAP/S per il server di posta in arrivo e SMTP/S per il server di posta in uscita).

Le modalità e le condizioni specifiche per l'accesso al servizio sono descritte sul sito dedicato al servizio PostaCertificat@ ([www.postacertificata.gov.it](http://www.postacertificata.gov.it)).

## 15 Condizioni di fornitura del servizio PostaCertificat@

Le condizioni di fornitura del servizio sono dettagliate nelle Condizioni Generali del Servizio, nella Guida Utente Cittadino e nella Scheda di adesione pubblicati sul portale dedicato al servizio PostaCertificat@.

## 16 Livelli di servizio ed indicatori di qualità del servizio PostaCertificat@

<b>Destinatari degli invii</b>	Numero massimo di destinatari per messaggi originati da caselle PostaCertificat@ del Cittadino	<b>50</b>
	Numero massimo di destinatari per messaggi originati da caselle PostaCertificat@ della PA	-
<b>Dimensione dei messaggi</b>	Dimensione massima per il singolo messaggio accettabile da caselle PostaCertificat@ del Cittadino (intesa come prodotto dei destinatari per la dimensione del messaggio stesso)	<b>30 Mb</b>
	Dimensione massima per il singolo messaggio accettabile da caselle PostaCertificat@ della PA (intesa come prodotto dei destinatari per la dimensione del messaggio stesso)	-
<b>Disponibilità</b>	Disponibilità del servizio nel periodo di riferimento (*)	<b>99,8 %</b>
	Durata massima di indisponibilità del servizio nel periodo (*)	<b>262,8 minuti</b>
	Durata massima per singola indisponibilità del servizio (*)	<b>131,4 minuti</b>
<b>Tempi</b>	Tempo di consegna delle ricevute	<b>30 minuti</b>

## 17 Tabella riepilogativa documentazione del servizio pubblicata sul sito PostaCertificat@

Per le modalità operative di erogazione del servizio PostaCertificat@ ed ogni altro approfondimento si rimanda ai documenti pubblicati sul sito del servizio PostaCertificat@ ([www.postacertificata.gov.it](http://www.postacertificata.gov.it)) di seguito elencati:

SPECIFICHE	DOCUMENTI
<b>Caratteristiche generali del servizio</b>	Guida Cittadino
<b>Contenuto dell'offerta</b>	Condizioni generali del servizio
<b>Modalità di accesso al servizio di PostaCertificat@</b>	Home Page del Sito.
<b>Condizioni di fornitura</b>	Condizioni generali del servizio Guida Cittadino Contratto di adesione
<b>Obblighi e responsabilità</b>	Condizioni generali del servizio
<b>Esclusioni e limitazioni in sede di indennizzo</b>	Condizioni generali del servizio
<b>Reperimento e presentazione delle informazioni di log</b>	Procedura manuale descritta sul sito del servizio PostaCertificat@

Tabella 13 – Documentazione pubblicata sul portale del servizio PostaCertificat@

## SEZIONE III: OBBLIGHI E RESPONSABILITÀ

VERSIONE 3.1	DATA 29/04/2010	CODICE RISERVATEZZA PUBBLICO	CODIFICA PI_MO_PEC_v3.1_100429	Pagina 38/62
-----------------	--------------------	---------------------------------	-----------------------------------	--------------

## 18 Obblighi e responsabilità

### 18.1 Obblighi del Gestore

- Assicura l'interoperabilità con gli altri gestori di Posta Elettronica Certificata.
- Rilascia al mittente che utilizza i propri servizi la ricevuta di accettazione nella quale sono contenuti i dati di certificazione che costituiscono prova dell'avvenuta spedizione del messaggio di Posta Elettronica Certificata.
- Fornisce all'indirizzo del mittente le ricevute di avvenuta consegna.
- Nel caso di trasmissione tra caselle appartenenti a gestori diversi, rende disponibili, nei casi previsti dalla legge, i log inerenti le specifiche trasmissioni.
- Rilascia, se Gestore della casella di Posta Certificata del destinatario, la ricevuta di presa in carico del messaggio al Gestore della casella del mittente.
- Comunica al mittente, nei casi previsti e mediante un apposito avviso, la mancata consegna del messaggio.
- Sottoscrive con firma elettronica avanzata le ricevute rilasciate.
- Sottoscrive con firma elettronica avanzata le buste di trasporto, al fine di garantirne la provenienza, l'integrità e l'autenticità.
- Appone a ciascuna trasmissione un riferimento temporale generato con un sistema che garantisce uno scarto non superiore ad un minuto secondo rispetto alla scala di tempo universale coordinato (UTC), determinata ai sensi dell'art. 3, comma 1, della legge 11 agosto 1991, n. 273.
- Esegue, senza soluzione di continuità, il salvataggio dei log dei messaggi generati nell'intervallo temporale predefinito.
- Appone giornalmente la marcatura temporale al file dei log relativo al periodo.
- Tratta i virus secondo quanto previsto dal DM 2 novembre 2005, informando il mittente sul fatto che il messaggio inviato contiene un virus e conservando per 30 mesi i messaggi relativi.
- Garantisce i livelli di servizio previsti dal DM 2 novembre 2005 e riportati nel capitolo 10.
- Se Gestore mittente (nei casi di mancata ricezione, nelle 12 ore successive all'inoltro del messaggio, della 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 e, in assenza di comunicazioni nelle successive 12 ore, comunica al mittente avviso relativo alla mancata consegna del messaggio.

- Segnala al destinatario i messaggi non qualificabili come Posta Elettronica Certificata.
- Si attiene alle regole di cui al DM 2 novembre 2005 per l'accesso all'elenco pubblico dei gestori di posta elettronica certificata.

## 18.2 Obblighi del soggetto Titolare del servizio

- Fornisce in maniera veritiera e sotto la sua responsabilità le informazioni richieste dal Gestore ai fini dell'attivazione del servizio.
- Gestisce in maniera sicura le credenziali per l'accesso alla casella di Posta Elettronica Certificata.
- Si attiene alle normali regole di sicurezza nell'utilizzo della casella, al fine di evitare danni ai soggetti che utilizzano o gestiscono il servizio di Posta Certificata.
- Si avvale, per l'utilizzo della Posta Certificata, dei soggetti inclusi nell'Elenco dei Gestori accreditati gestiti da DigitPA.
- Nel caso intenda utilizzare il servizio di Posta Certificata nei rapporti con la Pubblica Amministrazione, dichiara espressamente il proprio indirizzo. Nei casi corrispondenti, revoca la dichiarazione con le stesse modalità.

## 18.3 Obblighi dell'utente della casella, se distinto dal Titolare del servizio

- Gestisce in maniera sicura le credenziali per l'accesso alla casella di Posta Elettronica Certificata.
- Si attiene alle normali regole di sicurezza nell'utilizzo della casella, al fine di evitare danni ai soggetti che utilizzano o gestiscono il servizio di Posta Certificata.

## 18.4 Responsabilità

Il Gestore è responsabile, verso gli utenti del servizio di Posta Elettronica Certificata, per l'adempimento degli obblighi derivanti dall'espletamento delle attività previste dal D.Lgs 82/2005, dal DPR 68/2005, dal DM 02/11/05 e successive loro modifiche e integrazioni.

Il Gestore non assume responsabilità per l'uso improprio delle caselle di Posta Elettronica Certificata.

Le limitazioni agli indennizzi stabilite dal Gestore sono riportate nell'apposito capitolo e nel contratto fornito al cliente.

Il titolare del contratto di servizio è responsabile della correttezza e completezza dei dati necessari per l'attivazione e la gestione delle caselle di Posta Elettronica Certificata.

## 19 Esclusioni e limitazioni in sede di indennizzo

In considerazione che l'utilizzo della casella di Posta Certificata relativa al servizio Poste Italiane.PEC@ viene concesso ai dipendenti per esclusivi motivi di lavoro non è previsto alcun tipo di indennizzo per qualsivoglia tipologia di problematica e/o contestazione.

Relativamente al servizio PostaCertificat@, le esclusioni e limitazioni in sede di indennizzo sono dettagliate nelle Condizioni Generali del Servizio pubblicate sul sito dedicato ([www.postacertificata.gov.it](http://www.postacertificata.gov.it)).

VERSIONE 3.1	DATA 29/04/2010	CODICE RISERVATEZZA PUBBLICO	CODIFICA PI_MO_PEC_v3.1_100429	Pagina 41/62
-----------------	--------------------	---------------------------------	-----------------------------------	--------------

**SEZIONE IV: STANDARD E PROCEDURE**

VERSIONE 3.1	DATA 29/04/2010	CODICE RISERVATEZZA PUBBLICO	CODIFICA PI_MO_PEC_v3.1_100429	Pagina 42/62
-----------------	--------------------	---------------------------------	-----------------------------------	--------------

## 20 Procedure e standard tecnologici e di sicurezza

### 20.1 Standard di qualità e sicurezza del processo

#### 20.1.1 Standard di qualità

Di seguito l'elencazione degli standard per la Gestione del Sistema di Qualità usati come riferimento per la definizione, gestione e controllo dei processi oppure come standard di certificazione.

CODICE DOCUMENTO	TITOLO
UNI EN ISO 9001:2008	Sistemi di gestione per la qualità. Requisiti
UNI EN ISO 9004:2009	Sistemi di gestione per la qualità. Linee guida per il miglioramento delle prestazioni
UNI EN ISO 9000:2005	Sistemi di gestione per la qualità. Fondamenti e vocabolario
UNI EN ISO 10007:2006	Gestione per la Qualità. Linee guida per la gestione della configurazione
UNI CEI ISO 90003:2005	Ingegneria del Sw e di sistema. Guida per l'applicazione della ISO 9001:2000 al software per elaboratore
UNI 10999:2002	Linee guida per la documentazione dei sistemi di gestione per la qualità
UNI EN ISO 19011:2003	Linee guida per gli audit dei sistemi di gestione per la qualità e/o di gestione ambientale
ISO IEC 27001:2005	Information security management system - Requirements
ISO IEC 20000:2005	ICT Service Management-Requirements

**Tabella 14 – Standard di qualità**

#### 20.1.2 Standard tecnologici

Relativamente ai processi ed alle applicazioni individuate dall'allegato tecnico al DM 2 novembre 2005, il servizio Poste Italiane.PEC @ è conforme agli standard elencati nella tabella che segue.

CODICE	TITOLO
RFC 1847	Security Multiparts for MIME: Multipart/Signed and Multipart/Encrypted
RFC 1891	SMTP Service Extension for Delivery Status Notifications
RFC 1912	Common DNS Operational and Configuration Errors
RFC 2045	Multipurpose Internet Mail Extensions (MIME) Part One: Format Of Internet Message Bodies
RFC 2049	Multipurpose Internet Mail Extensions (MIME) Part Five: Conformance Criteria and Examples
RFC 2252	Lightweight Directory Access Protocol (v3): Attribute Syntax Definitions
RFC 2315	PKCS #7: Cryptographic Message Syntax Version 1.5
RFC 2633	S/MIME Version 3 Message Specification
RFC 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
ISO/IEC 9594-8:2001	Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks

**Tabella 15 – Standard tecnologici**

## 20.2 Gestione dei sistemi tecnologici

Lo scopo delle procedure messe in atto dal Gestore Poste Italiane, per la conduzione dei sistemi di Posta Elettronica Certificata è quello di:

- rendere disponibili informazioni certe sulla configurazione del sistema e le relazioni che intercorrono tra i vari elementi anche al fine di apportare modifiche in modo controllato;
- assicurare il controllo delle modifiche alla configurazione nel rispetto dei ruoli come definiti dalla norma e che hanno competenza sulle attività di modifica agli elementi di configurazione;
- tracciare la storia della configurazione per ricostruire versioni del sistema di gestione della Posta Elettronica Certificata ed identificare cause di eventuali problemi verificatisi a seguito di modifiche ai sistemi per l'erogazione.

#### 20.2.1 Attivazione della procedura di gestione

La procedura è attivata dal Responsabile Servizi Tecnici, per la Posta Certificata:

- in caso di prima installazione dell'hardware e del software applicativo e dei successivi aggiornamenti,
- per controllare periodicamente lo stato della configurazione su base periodica o su specifica richiesta delle funzioni interessate.

#### 20.2.2 Aggiornamento della configurazione

L'aggiornamento della configurazione viene effettuato con l'ausilio di strumenti di sistema che generano una tracciatura completa dello stato di configurazione di ogni componente il sistema di Posta Elettronica Certificata.

Le informazioni contenute nella scheda tecnica sono generate dal sistema di configuration management. Le informazioni minime tracciate nella scheda tecnica sono:

- hardware: CPU, hard disk, porte;
- apparati di rete: switch, router;
- software di base: sistema operativo;
- software applicativo: versione installata.

Alla scheda tecnica sono associate informazioni aggiuntive relative al responsabile della gestione della risorsa di elaborazione e al Responsabile delle risorse dati, nonché la classificazione assegnata alla risorsa, necessaria per l'identificazione del livello di protezione attuabile, secondo lo schema che segue:

VERSIONE 3.1	DATA 29/04/2010	CODICE RISERVATEZZA PUBBLICO	CODIFICA PI_MO_PEC_v3.1_100429	Pagina 45/62
-----------------	--------------------	---------------------------------	-----------------------------------	--------------

- **Alta:** se la compromissione della risorsa impatta sulla Posta Certificata in maniera bloccante tale per cui una o più funzionalità critiche per l'utenza non sono disponibili;
- **Media:** se la compromissione della risorsa limita la funzionalità di Posta Certificata in alcune sue componenti secondarie tali da non impedirne comunque una fruizione anche se parziale;
- **Bassa:** se la compromissione della risorsa che fa parte del sistema di gestione della Posta Certificata può essere accomunata ai comuni malfunzionamenti e dunque non sono riscontrabili ripercussioni significative sulla fruizione del servizio.

### 20.2.3 Controllo dello stato di configurazione

Con periodicità mensile, o su richiesta della funzione responsabile del servizio di Posta Certificata viene effettuato il controllo dello stato della configurazione. Tali informazioni sono riportate in un apposito report contenente al minimo le seguenti informazioni:

- identificativo dell'item di configurazione;
- stato dell'item (attivo/non attivo);
- data (attivazione/disattivazione).

## 20.3 Gestione delle verifiche afferenti la sicurezza

Gli strumenti che sono implementati ai fini della sicurezza permettono di:

- individuare le vulnerabilità;
- classificare il grado di gravità delle situazioni di rischio;
- individuare le azioni correttive per minimizzare il rischio.

Lo stato dei processi relativamente alla sicurezza è monitorato mediante apposite verifiche formali.

La procedura è attivata dal Responsabile della Sicurezza a seguito di:

- **attività pianificate** e definite nel "Programma annuale Verifiche Ispettive Qualità e Sicurezza" con periodicità almeno semestrale;
- **attività non pianificate** ma che possono rendersi necessarie in forma occasionale;
- **mutamenti significativi** della infrastruttura di rete e dei sistemi;
- **sostanziali mutamenti dello scenario delle minacce** cui le reti ed i sistemi

sono soggetti;

- **incidenti di sicurezza**, quando (dopo averne eliminato gli effetti) sia necessario effettuare approfondite analisi per determinarne le possibili cause.

Il Responsabile della Sicurezza, per lo svolgimento delle attività, si avvale del Team di assessment che può essere formato da personale interno con specifiche competenze o da personale appartenente a società operanti nel settore della sicurezza.

### 20.3.1 Pianificazione e definizione degli assessment

Il Responsabile della Sicurezza predispone annualmente, per la parte di sua competenza, il Programma di Verifiche valutando le esigenze poste dai Clienti dei servizi erogati, i requisiti cogenti in merito alle verifiche da effettuare, il grado di copertura delle varie tematiche attinenti la sicurezza delle informazioni, gli esiti delle verifiche già effettuate nei periodi precedenti.

Il Responsabile della Sicurezza, ravvisata la necessità di effettuare una verifica, redige il documento “Specifica di Assessment” nella quale definisce almeno i seguenti aspetti: ambito (sistemi / reti da testare), obiettivi (tipologia di test e di attacchi, in funzione di cosa si vuole verificare nel dettaglio), impatto sui sistemi e sui servizi, risorse e tool necessari; team (interno o esterno), modalità operative; finestre temporali.

La Specifica di Assessment è condivisa con il Responsabile Servizi Tecnici e con TI a cui fa capo il servizio di Posta Elettronica Certificata.

Nel caso di affidamento dell’attività di assessment ad un Team di esperti esterni, gli accordi contrattuali prevedono esplicitamente il rispetto della riservatezza delle informazioni, la definizione ed il rispetto puntuale della Specifica di Assessment (ambito, tempistica e modalità operative) e la restituzione di tutti gli elaborati e dei risultati intermedi.

I tool di audit sono localizzati su sistemi diversi da quelli dedicati alla gestione/erogazione del servizio di Posta Elettronica Certificata.

### 20.3.2 Effettuazione dell’assessment

Le evidenze delle attività di assessment sono registrate nel “Rapporto della verifica ispettiva”, nel quale è riportata una scheda sintetica dei risultati ottenuti.

Nella fase di assessment il Team:

- rileva le vulnerabilità e definisce il fattore di rischio assoluto e quello reale (al fine di eliminare i falsi positivi);
- attribuisce ad ogni vulnerabilità una valutazione del grado di SEVERITA’ (Alta /

Media / Bassa). La severità delle vulnerabilità prese in considerazione viene valutata ispirandosi alle classificazioni più diffuse in ambito internazionale (CVE, OSVDB, NESSUS ecc.);

- raggruppa, ove possibile, le varie vulnerabilità in classi omogenee.

In questa fase il Responsabile della Sicurezza produce una sintesi dei risultati per le strutture coinvolte nella valutazione, nel quale sono riassunte le principali vulnerabilità riscontrate.

Per ogni famiglia di vulnerabilità, sono riportati in una griglia, il grado di diffusione (in termini di numerosità dei riscontri ottenuti sulle diverse macchine che fanno parte del perimetro) e il livello di severità associato.

In funzione dei risultati ottenuti i Responsabili delle strutture coinvolte avviano i trattamenti atti ad eliminare le vulnerabilità riscontrate. Il Responsabile della Sicurezza o i Responsabili delle strutture coinvolte avviano l'attuazione di Azioni Correttive.

Il Responsabile della Sicurezza utilizza i risultati delle attività di verifica come parte delle informazioni necessarie all'effettuazione delle analisi del rischio.

## 21 Soluzioni finalizzate a garantire il completamento della trasmissione

### 21.1 Approccio organizzativo

La continuità del servizio, anche al fine di assicurare il completamento delle fasi di trasmissione dei messaggi, è assicurata attraverso procedure di escalation che mirano alla gestione affidabile e controllata del servizio di Posta Certificata.

Per processo di escalation si intende l'esecuzione delle attività correlate alla risoluzione dei malfunzionamenti/guasti sui prodotti/entità, impiegate nel sistema di produzione, per i quali sia necessario un passaggio al livello di competenza/responsabilità superiore.

Il processo di escalation viene attivato nel momento in cui è accertata l'impossibilità di risolvere l'inconveniente a quel livello di competenze/responsabilità (se il problema risulta chiaramente identificato ed esistono le condizioni per procedere alla sua risoluzione, il caso non viene scalato).

Nel seguito viene delineata la modalità operativa adottata quando la risoluzione del problema o la correzione dell'anomalia richiede l'intervento di altre entità, al fine di garantire l'efficacia e efficienza sia delle attività di ripristino che del flusso informativo.

Responsabilità e tempi della procedura di escalation sono schematizzate di seguito.

TEMPI	ESCALATION
<p>Completamento entro <b>60 minuti</b> dal malfunzionamento</p>	<p><b>Il personale interessato, che riferisce al Responsabile dei Servizi Tecnici</b>, rilevato il verificarsi del guasto/anomalia, identifica ed attiva le contromisure opportune.</p> <p>In base ai risultati della diagnosi effettuata, il personale provvede a:</p> <ul style="list-style-type: none"> <li>• <b>richiedere l'intervento di ulteriori risorse specialistiche</b> (altri sistemisti o reperibile di secondo livello se in orario di reperibilità), se non in grado di procedere autonomamente;</li> <li>• <b>coinvolgere immediatamente il fornitore del prodotto</b> interessato dal malfunzionamento, se necessario in relazione alla tipologia di problema emerso;</li> <li>• <b>informare immediatamente il Responsabile dei Servizi Tecnici Poste Italiane</b> per mail e per telefono, avendo cura di specificare se il problema può essere di natura</li> </ul>

applicativa;

- **Il Responsabile dei Servizi Tecnici Poste Italiane**, una volta ricevuta la comunicazione, provvede a:
  - informare immediatamente il Responsabile della funzione TI
  - il responsabile del servizio di Posta Elettronica Certificata;
  - nel caso il problema sia di natura applicativa, deve coinvolgere, appena possibile, gli sviluppatori e/o il fornitore del prodotto (se applicativo acquistato).

**Tabella 16 – Identificazione**

TEMPI	ESCALATION
<p>Completamento entro <b>120 minuti</b> dal malfunzionamento</p>	<p><b>Il personale interessato, che riferisce al Responsabile dei Servizi Tecnici</b>, analizzato il guasto, provvede a coordinare l'attuazione di contromisure aggiuntive.</p> <p>Qualora, queste ultime si dimostrassero efficaci, il personale provvede a:</p> <ul style="list-style-type: none"> <li>• chiudere l'intervento registrando le contromisure adottate;</li> <li>• informare <b>il Responsabile dei Servizi Tecnici Poste Italiane</b>, precedentemente coinvolto, attraverso <b>mail e telefono</b>;</li> <li>• <b>Il Responsabile dei Servizi Tecnici Poste Italiane</b>, una volta ricevuta la comunicazione di chiusura del guasto , provvede ad informare immediatamente il Responsabile del servizio di Posta Elettronica Certificata;</li> </ul> <p>In caso di inefficacia e trascorsi i tempi previsti, <b>il Responsabile dei Servizi Tecnici</b> ed il <b>Responsabile del servizio</b> provvedono ad informare, attraverso gli strumenti ritenuti più efficaci:</p> <ul style="list-style-type: none"> <li>• <b>Il Direttore di TI</b>, al fine di consentirgli l'individuazione delle</li> </ul>

azioni più opportune;

**Il Responsabile dei Servizi Tecnici** informa le figure sopra elencate del tipo di malfunzionamento, nonché fornisce una stima dei tempi necessari al superamento del problema.

**Il Responsabile** del servizio di Posta Elettronica Certificata ricevuta la comunicazione **provvede ad attivare il processo informativo mediante le funzioni aziendali e gli strumenti opportuni, verso i Clienti coinvolti.**

Tabella 17 – Attuazione

Non appena il malfunzionamento è stato risolto il **Responsabile Servizi Tecnici** provvede a darne informazione alle seguenti funzioni, **attraverso mail**:

- **Il Responsabile del servizio**
- **Il Direttore TI;**

Il Responsabile del servizio, ricevuta la notizia della soluzione del problema, **provvede ad attivare il processo informativo mediante le funzioni aziendali e gli strumenti opportuni, verso i Clienti coinvolti.**

Il processo termina con la completa risoluzione del malfunzionamento; la chiusura (data ed ora) del processo viene registrata dallo strumento stesso.

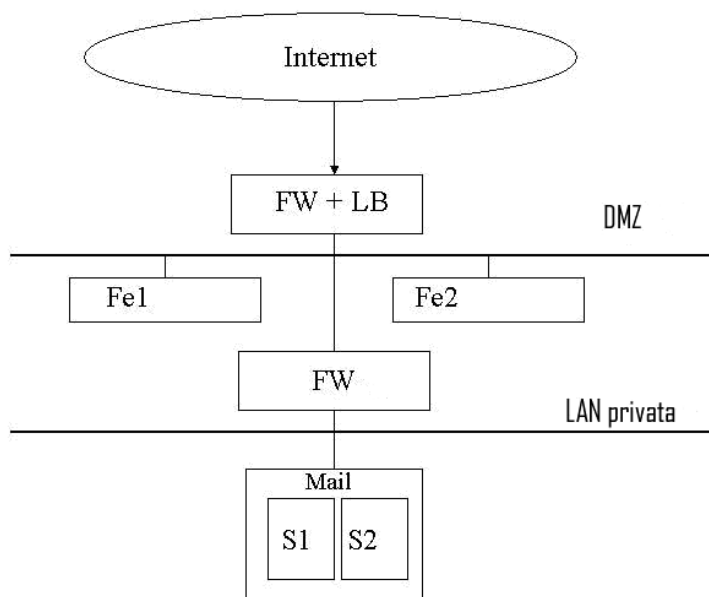
## 21.2 Approccio tecnologico

### 21.2.1 Connettività

I collegamenti alla rete dei Data Center sono opportunamente ridondati al fine di assicurare la connettività dei sistemi in tutte le occasioni possibili, consentendo così il completamento delle trasmissioni telematiche dei messaggi di Posta Elettronica Certificata anche nelle situazioni critiche.

### 21.2.2 Sistemi tecnologici servizio Poste Italiane.PEC @

Nella seguente figura è illustrato uno schema semplificato dell'architettura fisica del servizio Poste Italiane.PEC @ :



**Figura 5 - schema semplificato architettura fisica Poste Italiane.PEC@**

Il sistema è costituito da server che realizzano funzioni di front-end denominati FEx ed un sistema di back-end costituito da ulteriori server denominati Sx. I server di front-end e quelli di back-end sono posizionati su 2 LAN distinte ognuna protetta tramite Firewall in ridondanza che assicurano la continuità di servizio anche in caso di fault di uno di essi. Sono inseriti dispositivi di load-balancing (anche essi in ridondanza) che permettono di re-dirigere il traffico verso un dato servizio su più di un server fisico.

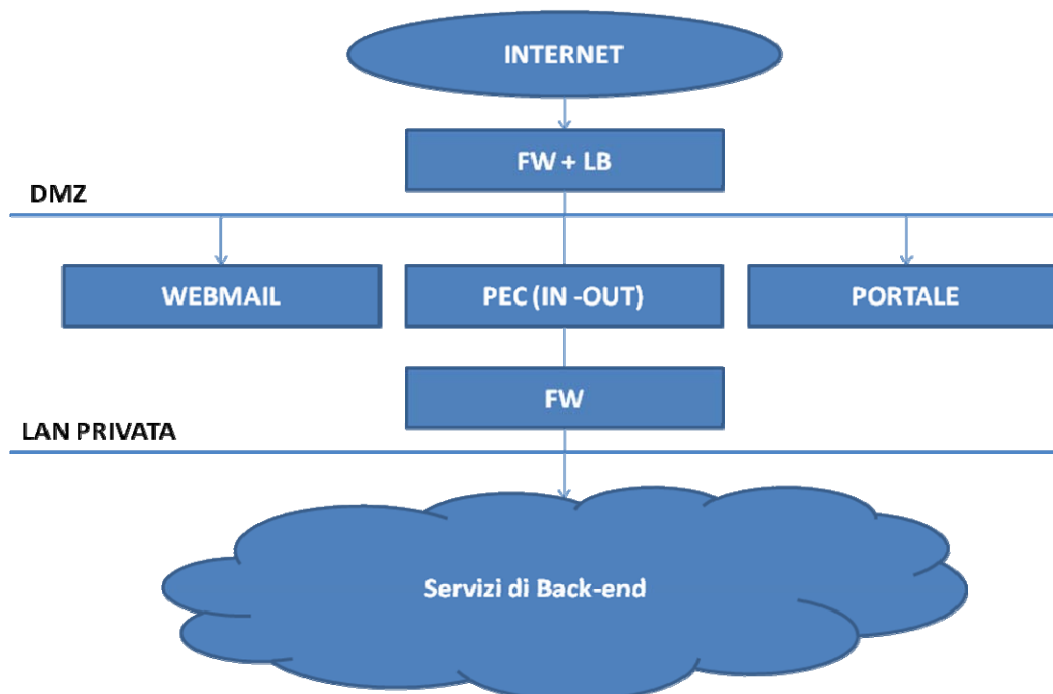
Tale architettura garantisce le seguenti funzionalità:

- **affidabilità:** in caso di fault di un elemento del servizio, questo non ne risente in quanto:
  - in caso di fault di un server di front-end, tutto il traffico viene re-diretto dagli apparati di load-balancing verso i server attivi;
  - in caso di fault di un server di back-end, il server “superstite” prenderà automaticamente in carico tutte le attività e le risorse del server malfunzionante. Tutte le informazioni rilevanti (caselle, configurazioni, etc.) sono memorizzate su dispositivi di memoria di massa dedicati collegati ai server tramite collegamenti in fibra ottica.
  - in caso di fault di un firewall o di un apparato di load-balancing, il funzionamento del sistema verrà garantito da un secondo elemento attivato tramite i meccanismi interni dello specifico apparato.

- **sicurezza:** l'introduzione di elementi di load-balancing permette di implementare facilmente funzionalità di NAT e conseguentemente di disaccoppiare la corrispondenza tra un servizio ed i server fisici che lo erogano, diminuendo quindi i rischi in caso di attacco informatico.
- **scalabilità:** l'architettura permette di scalare facilmente sia in modalità orizzontale che in modalità verticale. In particolare la scalabilità orizzontale è utilizzata soprattutto sui front-end in quanto, a seguito del rilevamento di una crescita delle attività dai parte dei singoli server di front-end, è sufficiente mettere in linea ulteriori server con le stesse caratteristiche degli altri e aggiungere nella configurazione degli apparati di load-balancing tali server nella lista di quelli abilitati per il servizio. Sui server di back-end viene garantita la scalabilità verticale, adottando specifici server le cui risorse -CPU, RAM, disco - possono essere aggiornati a caldo, sino ad una certa soglia oltre la quale vengono attivati meccanismi di scalabilità orizzontale compatibili con il software utilizzato

### 21.2.3 Sistemi tecnologici servizio PostaCertificat@

Nella seguente figura è illustrato uno schema semplificato dell'architettura fisica della piattaforma PostaCertificat@:



**Figura 6 - Architettura Fisica della Piattaforma PostaCertificat@**

L'architettura di fisica della piattaforma si fonda su principi derivati dalle best practices disponibili in letteratura e dall'esperienza maturata da Telecom Italia nello sviluppo e realizzazione dei propri IDC. Gli obiettivi raggiunti possono essere sintetizzati in:

- **elevata velocità:** sistemi e cablaggi adeguati a supportare la massima velocità offerta dagli standard di mercato attuali e futuri;
  - **alta affidabilità tramite la completa ridondanza:** sistemi e cablaggi completamente ridondati in modo da ridurre al minimo i tempi di disservizio provocati da guasti ed in grado di consentire interventi di manutenzione programmata anche invasiva (sostituzione apparati, aggiornamento hw/sw etc) in modo trasparente all'utente finale; la ridondanza è presente a tutti i livelli.
- **scalabilità orizzontale e verticale:** strutture di trasporto dati e sicurezza realizzate in modo da essere adattabili a necessità specifiche determinate da tipologie di servizi di volta in volta allocati (banda, numero di porte etc). Per i sistemi si utilizzano architetture in grado di scalare verticalmente, cioè in grado di crescere nel numero di processori, di memoria RAM e dischi; qualora tale crescita risulti insufficiente, si interverrà scalando l'architettura in senso orizzontale utilizzando più sistemi in parallelo e meccanismi di bilanciamento di traffico hardware. Il limite tra l'utilizzo delle due modalità, si delinea in fase di test e di esercizio;
- **strutturazione secondo domini a sicurezza diversa:** l'architettura è suddivisa in domini logici a sicurezza diversa con livelli di fiducia crescente (First Layer, Application/DB Layer, MGT/BCK Layer); la costituzione, a confine di ogni perimetro, di punti di concentrazione del traffico su cui vincolare il transito dei dati inter-dominio consente da una parte la migliore gestione degli instradamenti e dei flussi e dall'altra una più efficace definizione di politiche di protezione. Gli unici punti di accesso ai servizi erogati dai singoli domini, sono controllati dai sistemi di protezione perimetrale (firewall, intrusion detection systems);
- **flessibilità nella distribuzione del traffico:** struttura di rete e sicurezza realizzata in modo da poter consentire l'instradamento del traffico secondo schemi diversi in funzione dell'evoluzione delle applicazioni.

L'architettura della piattaforma del servizio PostaCertificat@ è strutturata secondo diversi domini logici, pensati per ospitare servizi progettati in ottica distribuita, su più sistemi fisici

VERSIONE 3.1	DATA 29/04/2010	CODICE RISERVATEZZA PUBBLICO	CODIFICA PI_MO_PEC_v3.1_100429	Pagina 54/62
-----------------	--------------------	---------------------------------	-----------------------------------	--------------

(multi-tier) indipendentemente dai contributi che ciascun componente è chiamato a svolgere (presentazione servizi, archiviazione dati, gestione).

VERSIONE 3.1	DATA 29/04/2010	CODICE RISERVATEZZA PUBBLICO	CODIFICA PI_MO_PEC_v3.1_100429	Pagina 55/62
-----------------	--------------------	---------------------------------	-----------------------------------	--------------

## 22 Reperimento e presentazione delle informazioni di log

Il servizio di Posta Elettronica Certificata offerto dal Gestore Poste Italiane garantisce la tracciatura dei messaggi in tutte le fasi significative. In particolare, in funzione delle singole operazioni interessate alla tracciatura, sono memorizzati i seguenti dati significativi: codice identificativo univoco assegnato al messaggio originale (Message-ID);

- data ora dell'evento interessato al processo di tracciatura;
- mittente del messaggio originale;
- destinatari del messaggio originale;
- oggetto del messaggio originale;
- tipo di evento interessato al processo di tracciatura (accettazione del messaggio, ricezione, consegna, emissione delle ricevute di errore, ogni altra operazione rilevante ai fini della trasmissione telematica definita dal DM 2 novembre '05;
- codice identificativo (Message-ID) dei messaggi correlati (ricevute, errori, etc.);
- i dati identificativi del gestore mittente.

I dati afferenti i log sono registrati su idonei supporti e sottoposti con cadenza giornaliera al processo di marcatura temporale secondo lo schema indicato di seguito.

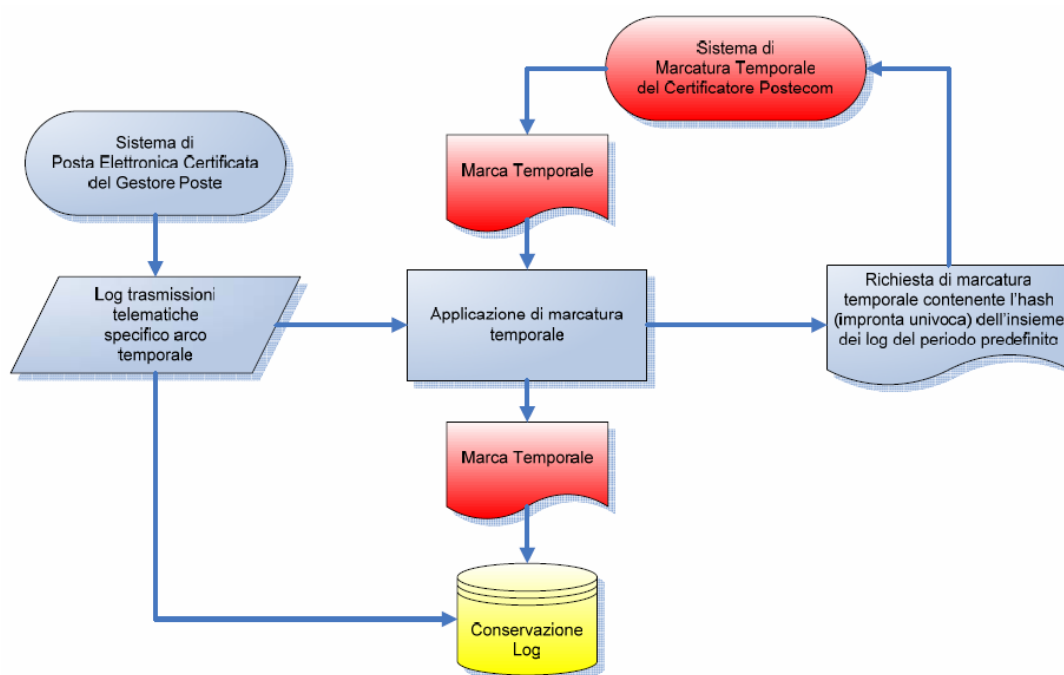


Figura 7 - processo di marcatura temporale

I log dei messaggi sono conservati per 30 mesi a cura del Gestore.

Il Gestore del servizio di Posta Certificata, conserva in un apposito registro tutte le informazioni significative, attinenti la trasmissione dei messaggi PEC.

Per il servizio Poste Italiane.PEC@, l'accesso ai log da parte dell'interessato avviene attraverso invio di una e-mail di richiesta all'indirizzo di posta certificata [supporto@pec.posteitaliane.it](mailto:supporto@pec.posteitaliane.it),

Per quanto riguarda il servizio PostaCertificata@, le modalità di richiesta di accesso e di presentazione dei log sono descritte in apposita procedura pubblicata sul sito dedicato al servizio ([www.postacertificata.gov.it](http://www.postacertificata.gov.it)).

La richiesta sarà evasa previo accertamento dell'autenticità e della legittimità della richiesta stessa. I dati dei log vengono individuati attraverso i seguenti identificativi:

- data della trasmissione;
- codice identificativo della trasmissione;
- coppia mittente/destinatario

In ogni caso l'accesso può avvenire previo richiesta dell'autorità giudiziaria. A richiesta ed in relazione allo specifico evento, ai soggetti aventi diritto, sono rese disponibili le informazioni contenute nei log, come previsto dall'allegato tecnico al DM 2 novembre 2005 al paragrafo §6.2 (il codice identificativo univoco assegnato al messaggio originale, la data e l'ora dell'evento, il mittente del messaggio originale, i destinatari del messaggio originale, l'oggetto del messaggio originale, il tipo di evento oggetto del log, il codice identificativo dei messaggi correlati generati e il gestore mittente).

## SEZIONE V: PROTEZIONE DATI PERSONALI

VERSIONE 3.1	DATA 29/04/2010	CODICE RISERVATEZZA PUBBLICO	CODIFICA PI_MO_PEC_v3.1_100429	Pagina 58/62
-----------------	--------------------	---------------------------------	-----------------------------------	--------------

## 23 Modalità di protezione dei dati dei titolari

La normativa in tema di trattamento dei dati personali è stata introdotta con la legge 31 dicembre 1996, n.675 a tutela della riservatezza e dell'identità personale. La materia è stata riunita ed armonizzata in un Testo Unico, approvato con Decreto Legislativo del 30 giugno 2003, n.196, che ha così sostituito la legge 675 ed i decreti connessi.

Le figure a cui sono attribuiti specifici ruoli e responsabilità nel trattamento dei dati personali sono:

- Titolare;
- Responsabile;
- Incaricato.

Il Titolare è il soggetto cui compete la scelta in ordine alle finalità e modalità del trattamento.

Il Responsabile è la persona fisica, la persona giuridica, la pubblica amministrazione o qualsiasi altro ente, associazione od organismo preposti dal Titolare al trattamento dei dati personali (art. 4 D. Lgs 196/03), che agisce sotto la sua diretta vigilanza.

Ai fini dell'adempimento degli obblighi imposti dal Codice<sup>1</sup>, in Poste Italiane è stata individuata la figura del Titolare nella società stessa, Poste Italiane S.p.A. Le figure dei Responsabili sono state invece individuate nelle persone dei responsabili delle strutture di primo livello, ognuno per i trattamenti effettuati nel proprio ambito.

Il Titolare si avvale della Funzione Tutela Aziendale per lo svolgimento degli adempimenti formali e organizzativi derivanti dal Codice e per la redazione del documento programmatico della sicurezza e delle procedure correlate (con la responsabilità di definire e realizzare un sistema di sicurezza adeguato per la protezione dei dati trattati e di verificarne la corretta implementazione).

Per ognuna delle strutture di primo livello di Poste Italiane S.p.A. sono individuate le tipologie dei dati trattati e le operazioni di trattamento consentite; l'individuazione è effettuata a livello di funzioni all'interno della singola struttura.

Le figure degli Incaricati sono state individuate nel personale di Poste Italiane S.p.A., per i trattamenti propri della funzione d'appartenenza. I Responsabili procedono al trattamento

---

<sup>1</sup> Si precisa che, in riferimento al servizio PostaCertificat@, la Presidenza del Consiglio dei Ministri - Dipartimento per la digitalizzazione della pubblica amministrazione e l'innovazione tecnologica, in qualità di titolare dei dati personali relativi ai servizi di base, ha emesso il decreto di nomina del concessionario quale responsabile del trattamento.

dei dati secondo le istruzioni impartite dal Titolare stesso.

### **23.1 Ambito del trattamento dei dati personali**

Il trattamento di dati personali, è consentito per le finalità proprie aziendali, nei limiti stabiliti dalle leggi e dai regolamenti. Ogni richiesta di comunicazione di dati personali rivolta da privati deve essere scritta e motivata e deve indicare le norme di legge o di regolamento su cui si basa.

E' vietato mettere a disposizione o far consultare i dati contenuti in banche dati da soggetti terzi, ad eccezione delle ipotesi di indagini di pubblica sicurezza, tramite la struttura "Servizi Sicurezza".

Con riferimento alla comunicazione dei dati il Responsabile dovrà informare il Titolare, tramite la struttura "Servizi Sicurezza", di qualsiasi richiesta pervenuta.

#### 23.1.1 Accesso ai dati

Ai dati possono avere accesso solo i dipendenti a ciò autorizzati. La designazione è effettuata anche per categoria sulla base delle medesime mansioni ricoperte all'interno di una stessa unità organizzativa.

#### 23.1.2 Trattamento di dati sensibili

Nel trattamento dei dati sensibili gli Incaricati si attengono ai seguenti principi:

- massimo rispetto della dignità dell'interessato;
- i dati sensibili sono raccolti, ove possibile, presso l'interessato mediante compilazione di un apposito modulo ove è presente l'informativa di cui all'art.13 e richiesto il consenso scritto all'interessato (art.26);
- tutti i dati da cui si evince lo stato di salute e la vita sessuale dell'interessato, contenuti in elenchi o banche dati informatiche, sono criptati o separati dagli altri dati dell'interessato, in modo da poter identificare gli interessati solo in caso di assoluta necessità;
- sono trattati solo dati essenziali, cioè non sostituibili con dati comuni in relazione agli scopi per i quali sono raccolti, verificandone periodicamente la pertinenza, non eccedenza e la necessità rispetto alle finalità perseguite;
- sono svolte soltanto operazioni di trattamento strettamente necessarie al perseguimento delle finalità sottese al trattamento stesso;
- sono impartite, da parte della struttura "Servizi Sicurezza" apposite *istruzioni*

*organizzative e tecniche* per la custodia e l'uso dei supporti rimuovibili sui cui sono memorizzati i dati al fine di evitare accessi non autorizzati;

I dati sensibili sono oggetto di trattamento solo con il *consenso scritto* dell'interessato e previa *autorizzazione del Garante*<sup>2</sup>, nell'osservanza dei presupposti e dei limiti stabiliti dalla legge e dai regolamenti.

*I dati idonei a rivelare lo stato di salute non sono diffusi.*

### 23.1.3 Trattamento di dati giudiziari

Il trattamento di dati giudiziari è consentito solo se autorizzato da espressa disposizione di legge o provvedimento del Garante, sul presupposto della rilevante finalità di interesse pubblico.

Le garanzie che la società stabilisce in favore del trattamento dei dati sensibili si applicano anche al trattamento di dati giudiziari.

## 23.2 Sicurezza dei dati

Come previsto dalle norme, il Titolare adotta idonee e preventive misure di sicurezza al fine di ridurre al minimo:

- i rischi di distruzione o perdita, anche accidentale, dei dati, di danneggiamento delle risorse hardware su cui sono registrati e dei locali ove vengono custoditi;
- l'accesso non autorizzato ai dati stessi;
- modalità di trattamento non consentite dalla legge o dai regolamenti aziendali.

Le misure di sicurezza adottate assicurano:

---

<sup>2</sup> Le autorizzazioni del Garante possono essere rilasciate anche per determinate categorie di titolari o di trattamenti e sono rinnovate annualmente. Sino ad oggi il Garante ha emanato 7 autorizzazioni a carattere collettivo relative:

- 1) al trattamento dei dati sensibili nei rapporti di lavoro;
- 2) al trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale;
- 3) al trattamento dei dati sensibili da parte degli organismi di tipo associativo e delle Fondazioni;
- 4) al trattamento dei dati sensibili da parte dei liberi professionisti;
- 5) al trattamento dei dati sensibili da parte di diverse categorie di titolari (settore bancario, assicurativo, turistico, del trasporto, dei sondaggi, delle ricerche, dell'elaborazione dei dati, della selezione del personale, della mediazione a fini matrimoniali);
- 6) al trattamento di alcuni dati sensibili da parte degli investigatori privati;
- 7) al trattamento di dati a carattere giudiziario da parte di privati, di enti pubblici economici e di soggetti pubblici.

- l'integrità dei dati, da intendersi come salvaguardia dell'esattezza dei dati, difesa da manomissioni o modifiche da parte di soggetti non autorizzati;
- la disponibilità dei dati, da intendersi come la certezza che l'accesso sia sempre possibile quando necessario; indica quindi la garanzia di fruibilità dei dati e dei servizi, evitando la perdita o la riduzione dei dati e dei servizi;
- la confidenzialità/riservatezza dei dati, da intendersi come garanzia che le informazioni siano accessibili solo da persone autorizzate e come protezione delle trasmissioni e controllo degli accessi stessi.

Il Sistema di Gestione Qualità e Sicurezza è stato strutturato per garantire, nel corso del ciclo di vita di un progetto, il rispetto degli adempimenti previsti dal Codice.

In merito all'utilizzo di risorse informatiche, il Titolare ha emanato le *“Norme per il corretto utilizzo delle risorse informative aziendali”*.

**\*\*\*QUESTA È L'ULTIMA PAGINA DEL DOCUMENTO\*\*\***

VERSIONE 3.1	DATA 29/04/2010	CODICE RISERVATEZZA PUBBLICO	CODIFICA PI_MO_PEC_v3.1_100429	Pagina 62/62
-----------------	--------------------	---------------------------------	-----------------------------------	--------------