

# **MANUALE OPERATIVO**

**Posta Elettronica Certificata ai sensi del DPR 68/05**

*Il presente documento è stato redatto in coerenza con il Codice Etico e i Principi Generali del Controllo Interno*

<b>IT Telecom</b>	<i>Tipo documento:</i> <b>Manuale Operativo</b>	<i>Emesso da:</i> <b>CAS</b>	<i>Codice documento</i> <b>MO.PEC.00.00</b>	<i>Data di emissione</i> <b>01.12.2005</b>
-------------------	--	---------------------------------	--	---

**Dati Identificativi del Documento**

<i>Redatto:</i>	<i>M. Donatone</i>	.....
<i>Verificato:</i>	<i>C. Villani</i>	.....

**REGISTRO DELLE MODIFICHE**

<b>Versione</b>	<b>Descrizione</b>	<b>Data di Emissione</b>
00	Prima Emissione	1 dicembre 2005

<b>IT Telecom</b>	<i>Tipo documento:</i> <b>Manuale Operativo</b>	<i>Emesso da:</i> <b>CAS</b>	<i>Codice documento</i> <b>MO.PEC.00.00</b>	<i>Data di emissione</i> <b>01.12.2005</b>
-------------------	--	---------------------------------	--	---

## Sommario

<b>DATI IDENTIFICATIVI DEL DOCUMENTO .....</b>	<b>2</b>
<b>SOMMARIO .....</b>	<b>3</b>
<b>PARTE I INFORMAZIONI GENERALI.....</b>	<b>6</b>
<b>1 Scopo del documento.....</b>	<b>7</b>
<b>2 Identificazione del Gestore e del Responsabile del Manuale Operativo .....</b>	<b>7</b>
<b>3 Riferimenti normativi .....</b>	<b>7</b>
<b>4 Standard.....</b>	<b>9</b>
4.1 Procedure e standard tecnologici e di sicurezza .....	9
4.2 Sistema di Qualità .....	10
<b>5 Definizioni, abbreviazioni e termini tecnici .....</b>	<b>10</b>
5.1 Definizioni.....	10
5.2 Abbreviazioni e termini tecnici.....	15
<b>PARTE II IL SERVIZIO DI POSTA ELETTRONICA CERTIFICATA .....</b>	<b>17</b>
<b>6 Natura del servizio PEC.....</b>	<b>18</b>
6.1 Aspetti generali del servizio di PEC IT Telecom – Livelli di servizio e Indicatori di qualità .....	18
6.1.1 <i>Livelli di servizio e Indicatori di qualità .....</i>	<i>18</i>
6.1.2 <i>Aspetti generali.....</i>	<i>18</i>
6.1.3 <i>I soggetti del servizio secondo la normativa .....</i>	<i>19</i>
6.1.4 <i>Funzionamento del servizio .....</i>	<i>19</i>
6.1.4.1 <i>Invio del messaggio da parte del mittente.....</i>	<i>19</i>
6.1.4.2 <i>Invio del messaggio al punto di ricezione.....</i>	<i>20</i>
6.1.4.3 <i>Invio del messaggio al punto di consegna .....</i>	<i>20</i>
6.1.4.4 <i>Problemi di consegna.....</i>	<i>20</i>
6.1.4.5 <i>Firma elettronica delle ricevute e delle buste di trasporto.....</i>	<i>21</i>
6.1.4.6 <i>Riferimento temporale .....</i>	<i>21</i>
6.1.4.7 <i>Tipologia delle Ricevute di Avvenuta Consegna .....</i>	<i>21</i>
<b>7 Riferimento Temporale e Marca Temporale del Gestore .....</b>	<b>22</b>
7.1 Generazione delle Chiavi di Marcatura Temporale .....	23

<b>IT Telecom</b>	<i>Tipo documento:</i> <b>Manuale Operativo</b>	<i>Emesso da:</i> <b>CAS</b>	<i>Codice documento</i> <b>MO.PEC.00.00</b>	<i>Data di emissione</i> <b>01.12.2005</b>
-------------------	--	---------------------------------	--	---

7.2	Marche Temporali .....	23
7.2.1	<i>Registrazione delle marche temporali</i> .....	24
7.2.2	<i>Validità delle marche temporali</i> .....	24
7.3	Sicurezza del sistema di Validazione Temporale .....	24
<b>8</b>	<b>La soluzione IT Telecom di Posta Elettronica Certificata .....</b>	<b>25</b>
8.1	Architettura del Servizio .....	25
8.2	Principali tecnologie utilizzate .....	27
8.3	Organizzazione del personale.....	27
<b>9</b>	<b>Modalità di generazione, conservazione, reperimento e presentazione dei log dei messaggi .....</b>	<b>28</b>
9.1	Generazione.....	28
9.2	Conservazione dei Log.....	30
9.2.1	<i>Conservazione dei log su Flat-files</i> .....	30
9.2.2	<i>Conservazione dei log su database</i> .....	31
9.3	Reperimento e presentazione dei Log .....	31
<b>10</b>	<b>Tipologie del servizio PEC offerte da IT Telecom.....</b>	<b>33</b>
10.1	Trattamento dei Domini di PEC.....	33
10.1.1	<i>Domini certificati di IT Telecom</i> .....	33
10.1.2	<i>Dominio del cliente</i> .....	33
10.2	Tipologie di Caselle di PEC.....	34
10.2.1	<i>Caselle istituzionali</i> .....	34
10.2.1.1	<i>Principali funzioni del servizio</i> .....	35
10.2.1.2	<i>Modalità di accesso alle caselle di PEC</i> .....	35
10.2.1.3	<i>Dimensioni delle caselle di PEC e traffico</i> .....	35
10.2.2	<i>Caselle individuali</i> .....	36
10.2.2.1	<i>Modalità di accesso</i> .....	36
10.2.2.2	<i>Dimensioni delle caselle di PEC e traffico</i> .....	36
10.3	Il portale PKI.....	36
<b>11</b>	<b>Cenni sulle infrastrutture del Gestore e sulle misure di sicurezza .....</b>	<b>37</b>
11.1	Infrastrutture.....	37
11.2	Misure di sicurezza .....	39
11.3	Servizi di emergenza.....	39
11.4	Disponibilità e Tempi di ripristino.....	40
	<b>PARTE III CONDIZIONI DI FORNITURA E DI UTILIZZO DEL SERVIZIO DI POSTA ELETTRONICA CERTIFICATA .....</b>	<b>42</b>

<b>IT Telecom</b>	<i>Tipo documento:</i> <b>Manuale Operativo</b>	<i>Emesso da:</i> <b>CAS</b>	<i>Codice documento</i> <b>MO.PEC.00.00</b>	<i>Data di emissione</i> <b>01.12.2005</b>
-------------------	--	---------------------------------	--	---

<b>12 Condizioni di fornitura del servizio PEC di IT Telecom .....</b>	<b>43</b>
<b>13 Obblighi, Responsabilità e Indennizzi .....</b>	<b>47</b>
13.1 Obblighi del Gestore .....	47
13.1.1 Polizza assicurativa .....	48
13.2 Obblighi del titolare .....	48
13.3 Definizione delle responsabilità e delle limitazioni agli indennizzi .....	49
13.4 Manleva del titolare .....	50
<b>PARTE IV PROCEDURA DI ATTIVAZIONE DEL SERVIZIO DI PEC .....</b>	<b>51</b>
<b>14 Procedura di attivazione .....</b>	<b>52</b>
<b>PARTE V PROTEZIONE DEI DATI .....</b>	<b>53</b>
<b>15 Modalità di Protezione dei Dati .....</b>	<b>55</b>
15.1 Definizione e identificazione di “Dati personali” .....	56
15.2 Tutela e diritti degli interessati .....	56
15.3 Applicazione del Codice per la protezione dei dati personali .....	56
15.3.1 Adempimenti generali .....	56
15.3.2 Adempimenti tecnici ed organizzativi .....	56
15.3.2.1 Registrazione .....	57
15.3.2.2 Elaborazione .....	57
15.3.2.3 Conservazione .....	57
15.3.2.4 Cancellazione/Distruzione .....	57
15.3.2.5 Protezione .....	58
15.4 Circostanze di comunicazione di dati personali .....	58

<b>IT Telecom</b>	<i>Tipo documento:</i> <b>Manuale Operativo</b>	<i>Emesso da:</i> <b>CAS</b>	<i>Codice documento</i> <b>MO.PEC.00.00</b>	<i>Data di emissione</i> <b>01.12.2005</b>
-------------------	--	---------------------------------	--	---

<p style="text-align: center;"><b>PARTE I</b></p> <p style="text-align: center;"><b>Informazioni Generali</b></p>
---

<b>IT Telecom</b>	<i>Tipo documento:</i> <b>Manuale Operativo</b>	<i>Emesso da:</i> <b>CAS</b>	<i>Codice documento</i> <b>MO.PEC.00.00</b>	<i>Data di emissione</i> <b>01.12.2005</b>
-------------------	--	---------------------------------	--	---

## 1 Scopo del documento

Questo documento illustra le regole generali e le procedure seguite dal Gestore del servizio di Posta Elettronica Certificata (PEC) IT Telecom s.r.l. nell'erogazione del servizio stesso.

Il presente documento:

- è pubblicato dal Gestore a garanzia dell'affidabilità del proprio servizio di PEC nei confronti degli utilizzatori finali e contiene le modalità operative del servizio indicato;
- costituisce documento pubblico secondo le disposizioni del DPR 68/2005 e delle normative attuative;
- è liberamente disponibile per la consultazione ed il download in formato PDF sul sito predisposto dal Gestore IT Telecom: <http://www.firmasicura.it>.

## 2 Identificazione del Gestore e del Responsabile del Manuale Operativo

La società I.T. Telecom s.r.l., con unico socio, Gruppo Telecom Italia – Direzione e coordinamento di Telecom Italia S.p.A., con sede in Milano (MI) – Via Cornelio Tacito, 14, 20137, oltre ad esercitare l'attività di certificazione della firma qualificata in qualità di Certificatore Accreditato ai sensi del DPR 28 dicembre 2000, n. 445, esercita anche l'attività di gestione di posta elettronica certificata quale iscritto nell'elenco pubblico dei gestori ai sensi dell'Art. 14 del DPR 11 febbraio 2005, n. 68.

Il responsabile del Manuale Operativo è Cinzia Villani, Responsabile dei Servizi di Certificazione Digitale nell'ambito della struttura organizzativa del Gestore.

## 3 Riferimenti normativi

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

<b>[L. 59/97]</b>	<b>Legge 15 marzo 1997, n. 59</b> - Delega al Governo per il conferimento di funzioni e compiti alle regioni ed enti locali, per la riforma della Pubblica Amministrazione e per la semplificazione amministrativa (Gazzetta Ufficiale n. 63 del 17 Marzo 1997, Supplemento ordinario) - Articolo 15, comma 2, relativo alla validità e rilevanza legale degli atti, dati e documenti formati dalla pubblica amministrazione e dai privati con strumenti informatici o
-------------------	--

<b>IT Telecom</b>	<i>Tipo documento:</i> <b>Manuale Operativo</b>	<i>Emesso da:</i> <b>CAS</b>	<i>Codice documento</i> <b>MO.PEC.00.00</b>	<i>Data di emissione</i> <b>01.12.2005</b>
-------------------	--	---------------------------------	--	---

	telematici, i contratti stipulati nelle medesime forme, nonché la loro archiviazione e trasmissione con strumenti informatici
<b>[TUDA]</b>	<b>Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445</b> – Testo Unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa (GU n. 42 del 20 febbraio 2001) e successive modifiche ed integrazioni, in particolare apportate con il decreto legislativo 23 gennaio 2002, n. 10, con la legge 16 gennaio 2003, n. 3 e il DPR 7 aprile 2003, n. 137.
<b>[Cod. PA Dig.]</b>	<b>Decreto Legislativo 7 marzo 2005, n. 82</b> - Codice dell'amministrazione digitale, recante le disposizioni in base alle quali lo Stato, le Regioni e le autonomie locali assicurano la disponibilità, la gestione, l'accesso, la trasmissione, la conservazione e la fruibilità dell'informazione in modalità digitale mediante le tecnologie dell'informazione e della comunicazione.
<b>[DLgs 196/03]</b>	<b>Decreto Legislativo n. 196 del 30 giugno 2003</b> - Codice in materia di protezione dei dati personali, pubblicato sul Supplemento ordinario n. 123 della Gazzetta Ufficiale n. 174 del 29 luglio 2003.
<b>[DPCM 2004]</b>	<b>Decreto del Presidente del Consiglio dei Ministri 13 gennaio 2004</b> – Regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici (Gazzetta Ufficiale n. 98 del 27 aprile 2004) e successive modifiche ed integrazioni.
<b>[DPR 68/05]</b>	<b>Decreto del Presidente della Repubblica 11 febbraio 2005, n. 68</b> – Regolamento recante disposizioni per l'utilizzo della posta elettronica certificata, a norma dell'articolo 27 della legge 16 gennaio 2003, n. 3.
<b>[DM 2/11/05]</b>	<b>Decreto 2 novembre 2005 della Presidenza del Consiglio dei Ministri Dipartimento per l'Innovazione e le Tecnologie</b> , recante Regole tecniche per la formazione, la trasmissione e la validazione, anche temporale, della posta elettronica certificata (GU n. 266 del 15-11-2005).
<b>[CNIPA RT]</b>	<b>Regole tecniche</b> del servizio di trasmissione di documenti informatici mediante posta elettronica certificata.

Il Cod. PA Dig. (in vigore dal 1° gennaio 2006, art. 48) abroga le disposizioni del TUDA relative alla trasmissione del documento informatico (art. 14) e sottopone la disciplina del servizio di PEC alle disposizioni contenute nel DPR 68/05.

<b>IT Telecom</b>	<i>Tipo documento:</i> <b>Manuale Operativo</b>	<i>Emesso da:</i> <b>CAS</b>	<i>Codice documento</i> <b>MO.PEC.00.00</b>	<i>Data di emissione</i> <b>01.12.2005</b>
-------------------	--	---------------------------------	--	---

## 4 Standard

### 4.1 Procedure e standard tecnologici e di sicurezza

Il servizio di PEC erogato da IT Telecom in base al presente documento è conforme agli standard di riferimento internazionalmente riconosciuti (e qui sotto riportati) secondo l'Art. 3 del DPR 68/05.

#### *Standard Tecnologici di riferimento*

<b>Codice</b>	<b>Titolo</b>
RFC 1847	Security Multiparts for MIME: Multipart/Signed and Multipart/Encrypted
RFC 1891	SMTP Service Extension for Delivery Status Notifications
RFC 1912	Common DNS Operational and Configuration Errors
RFC 2045	Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies
RFC 2049	Multipurpose Internet Mail Extensions (MIME) Part Five: Conformance Criteria and Examples
RFC 2252	Lightweight Directory Access Protocol (v3): Attribute Syntax Definitions
RFC 2315	PKCS #7: Cryptographic Message Syntax Version 1.5
RFC 2633	S/MIME Version 3 Message Specification
RFC 2660	The Secure HyperText Transfer Protocol
RFC 2821	Simple Mail Transfer Protocol
RFC 2822	Internet Message Format
RFC 2849	The LDAP Data Interchange Format (LDIF) - Technical Specification
RFC 3174	US Secure Hash Algorithm 1 (SHA1)
RFC 3207	SMTP Service Extension for Secure SMTP over Transport Layer Security
RFC 3280	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

<b>IT Telecom</b>	<i>Tipo documento:</i> <b>Manuale Operativo</b>	<i>Emesso da:</i> <b>CAS</b>	<i>Codice documento</i> <b>MO.PEC.00.00</b>	<i>Data di emissione</i> <b>01.12.2005</b>
-------------------	--	---------------------------------	--	---

In particolare, si riportano qui di seguito i riferimenti ai singoli paragrafi nei quali sono specificamente trattati gli aspetti relativi alle procedure e agli standard di sicurezza, nonché ad ulteriori standard tecnologici non nominati nella precedente tabella:

- Generazione delle Chiavi di Marcatura Temporale, par. 7.1;
- Marche Temporali, par. 7.2;
- Sicurezza del sistema di Validazione Temporale, par. 7.3;
- Canale sicuro di trasmissione, cap. 8;
- Architettura del Servizio, paragrafi 8.1 e 8.2;
- Generazione, conservazione, reperimento e presentazione dei log dei messaggi, cap. 9;
- Portale di accesso ai servizi, par. 10.3
- Infrastrutture del Gestore e misure di sicurezza, cap. 11.

## **4.2 Sistema di Qualità**

---

Il sistema di qualità del Gestore è conforme alla norma ISO 9001:2000 per le seguenti attività: Progettazione, Realizzazione, Erogazione e Assistenza di servizi telematici.

Il certificato è stato emesso in data 30 settembre 2003 da CISQ/IMQ-CSQ, partner italiano di IQNet.

Le attività di progettazione, erogazione ed assistenza del servizio di PEC, sono condotte dal Gestore nell'ambito del sistema di qualità IT Telecom che, come sopra riportato, è conforme alla norma ISO 9001:2000.

## **5 Definizioni, abbreviazioni e termini tecnici**

---

### **5.1 Definizioni**

---

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

I termini e le espressioni non definiti avranno il significato loro attribuito all'interno del paragrafo o sezione che li contiene. Fa eccezione il capitolo 15, nel quale valgono le convenzioni ivi indicate e desunte dal DLgs 196/03, Codice in materia di protezione dei dati personali.

**Avviso di mancata consegna.** Nel caso in cui il gestore di PEC sia impossibilitato a consegnare il messaggio nella casella di PEC del destinatario, il sistema emette un avviso di mancata consegna per indicare l'anomalia al mittente del messaggio originale.

**Avviso di non accettazione.** È l'avviso che viene emesso quando il gestore mittente è impossibilitato ad accettare il messaggio in ingresso. La motivazione per cui non è possibile accettare il messaggio è inserita all'interno del testo della ricevuta che

<b>IT Telecom</b>	<i>Tipo documento:</i> <b>Manuale Operativo</b>	<i>Emesso da:</i> <b>CAS</b>	<i>Codice documento</i> <b>MO.PEC.00.00</b>	<i>Data di emissione</i> <b>01.12.2005</b>
-------------------	--	---------------------------------	--	---

esplicita inoltre che il messaggio non potrà essere consegnato al destinatario. L'avviso di non accettazione è firmato con la chiave del gestore di PEC del mittente.

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

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

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

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

**Certificatore (Certification Authority, CA, Autorità di Certificazione):** prestatore di servizi di certificazione, la società I.T. Telecom S.R.L. Per certificatore, si intende il soggetto che presta servizi di certificazione delle firme elettroniche o che fornisce altri servizi connessi con queste ultime.

**Certificatore Accreditato:** È tale, ai sensi dell'art.2, comma 1, lettera c) del DL 10/02, il certificatore accreditato in Italia ovvero in altri Stati membri dell'Unione Europea ai sensi dell'art. 3, paragrafo 2, della direttiva 1999/93/CE nonché ai sensi del TUDA; IT Telecom S.R.L. è un certificatore accreditato in Italia ai sensi del TUDA, che emette, pubblica nel registro e revoca Certificati Qualificati operando in conformità alle regole tecniche e secondo quanto prescritto dal TUDA (art. 1, lett. u e z).

**Certificato Qualificato:** Un certificato emesso da un certificatore accreditato che risponde ai requisiti di cui all'allegato II della direttiva 1999/93/CE e conforme ai requisiti di cui all'allegato I della medesima direttiva, ai sensi del TUDA e successive modificazioni (art. 1, lett. aa).

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

**Chiavi asimmetriche:** La coppia di chiavi crittografiche una privata e una pubblica, correlate tra loro, e utilizzate nell'ambito dei sistemi di validazione di documenti informatici (art. 22, lett. b) del TUDA).

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

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

<b>IT Telecom</b>	<i>Tipo documento:</i> <b>Manuale Operativo</b>	<i>Emesso da:</i> <b>CAS</b>	<i>Codice documento</i> <b>MO.PEC.00.00</b>	<i>Data di emissione</i> <b>01.12.2005</b>
-------------------	--	---------------------------------	--	---

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

**Chiave Privata:** L'elemento della coppia di chiavi asimmetriche, destinato ad essere conosciuto soltanto dal soggetto titolare, mediante il quale si appone la firma digitale sul documento informatico (art. 22, lett. c del TUDA).

**Chiave Pubblica:** L'elemento della coppia di chiavi asimmetriche, destinato ad essere reso pubblico, con il quale si verifica la firma digitale apposta sul documento informatico dal titolare delle chiavi asimmetriche (art. 22, lett. d del TUDA).

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

**CNIPA - Centro nazionale per l'informatica nella pubblica amministrazione.** È l'organismo di cui all'articolo 4, comma 1, del decreto legislativo 12 febbraio 1993, n. 39, come modificato dall'articolo 176, comma 3, del decreto legislativo 30 giugno 2003, n. 196.

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

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

**Documento informatico.** È la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti (art. 1, lettera b del TUDA).

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

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

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

**Firma digitale.** Un particolare tipo di firma elettronica qualificata, basata su un sistema di chiavi asimmetriche a coppia, una pubblica e una privata, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici (art. 1, lett. n del TUDA).

<b>IT Telecom</b>	<i>Tipo documento:</i> <b>Manuale Operativo</b>	<i>Emesso da:</i> <b>CAS</b>	<i>Codice documento</i> <b>MO.PEC.00.00</b>	<i>Data di emissione</i> <b>01.12.2005</b>
-------------------	--	---------------------------------	--	---

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

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

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

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

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

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

**Manuale Operativo.** Il documento pubblico che definisce e descrive le procedure applicate dal Gestore del servizio di PEC nello svolgimento della sua attività (art. 23 del DM 2/11/05). Esso è depositato presso il CNIPA ed è reso disponibile presso il Gestore stesso.

**Manuale della Qualità.** Il manuale predisposto dal Gestore, finalizzato alla documentazione del proprio sistema di qualità certificato UNI EN ISO 9001:2000, come previsto dall'art. 20, comma 2 del DM 2/11/05.

**Marca temporale (Riferimento temporale).** È un'evidenza informatica con cui si attribuisce, ad uno o più documenti informatici, un riferimento temporale opponibile ai terzi (TUDA e DPCM 2004).

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

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

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

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

<b>IT Telecom</b>	<i>Tipo documento:</i> <b>Manuale Operativo</b>	<i>Emesso da:</i> <b>CAS</b>	<i>Codice documento</i> <b>MO.PEC.00.00</b>	<i>Data di emissione</i> <b>01.12.2005</b>
-------------------	--	---------------------------------	--	---

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

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

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

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

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

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

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

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

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

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

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

<b>IT Telecom</b>	Tipo documento: <b>Manuale Operativo</b>	Emesso da: <b>CAS</b>	Codice documento <b>MO.PEC.00.00</b>	Data di emissione <b>01.12.2005</b>
-------------------	---	--------------------------	---	--

## 5.2 Abbreviazioni e termini tecnici

**CC - Common Criteria.** Criteri per la valutazione della sicurezza nei sistemi informatici, con riconoscimento internazionale in quanto evoluzione dei criteri europei (ITSEC), americani (Federal Criteria), e canadesi (Canadian Criteria).

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

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

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

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

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

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

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

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

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

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

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

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

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

<b>IT Telecom</b>	<i>Tipo documento:</i> <b>Manuale Operativo</b>	<i>Emesso da:</i> <b>CAS</b>	<i>Codice documento</i> <b>MO.PEC.00.00</b>	<i>Data di emissione</i> <b>01.12.2005</b>
-------------------	--	---------------------------------	--	---

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

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

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

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

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

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

**X509.** Specifica ITU-T che definisce la struttura e la terminologia da utilizzare per la compilazione dei certificati e delle liste ad essi associate.

<b>IT Telecom</b>	<i>Tipo documento:</i> <b>Manuale Operativo</b>	<i>Emesso da:</i> <b>CAS</b>	<i>Codice documento</i> <b>MO.PEC.00.00</b>	<i>Data di emissione</i> <b>01.12.2005</b>
-------------------	--	---------------------------------	--	---

## **PARTE II**

### **Il servizio di Posta Elettronica Certificata**

<b>IT Telecom</b>	<i>Tipo documento:</i> <b>Manuale Operativo</b>	<i>Emesso da:</i> <b>CAS</b>	<i>Codice documento</i> <b>MO.PEC.00.00</b>	<i>Data di emissione</i> <b>01.12.2005</b>
-------------------	--	---------------------------------	--	---

## 6 Natura del servizio PEC

---

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

- fornisce al mittente la documentazione elettronica attestante l'invio e la consegna dei messaggi informatici, assicurandone il tracciamento mediante una serie di ricevute appositamente generata dai sistemi di posta certificata dai gestori del servizio. Per aumentare il livello di garanzia dell'avvenuta trasmissione dei messaggi, tali ricevute sono firmate e marcate elettronicamente dai sistemi di gestione, con l'ausilio di specifici certificati digitali, così da assegnare anche un riferimento temporale certo all'avvenuta trasmissione dei dati. La posta inoltrata tra domini di posta certificati, infatti, viene elaborata applicando criteri di inserimento e controllo della firma elettronica, fornendo così un meccanismo di certificazione dei messaggi scambiati tra mittenti e destinatari;
- dà al processo di trasmissione valore equivalente a quello della notifica a mezzo posta nei casi consentiti dalla legge.

### 6.1 Aspetti generali del servizio di PEC IT Telecom – Livelli di servizio e Indicatori di qualità

---

#### 6.1.1 Livelli di servizio e Indicatori di qualità

In relazione all'art. 12 del DM 2/11/05, di seguito sono individuati i livelli di servizio e gli indicatori di qualità del servizio di PEC IT Telecom:

- Limite del numero di **destinatari per messaggio**  $\geq 50$ ;
- Valore limite del **prodotto tra Numero dei destinatari e Dimensione del messaggio** (espresso in MB)  $\leq 30$ ;
- La **disponibilità nel tempo del servizio** è  $\geq 99,8\%$  del periodo temporale di riferimento che è **pari ad un quadrimestre**;
- La durata massima di ogni evento di **indisponibilità del servizio** è  $\leq 50\%$  del totale previsto per il periodo temporale di riferimento di cui al punto precedente;
- Nell'ambito dell'intervallo di disponibilità, la ricevuta di accettazione è fornita al mittente entro un termine concordato tra il gestore e il titolare e calcolato a partire dall'inoltro del messaggio, non considerando i tempi relativi alla trasmissione.

#### 6.1.2 Aspetti generali

L'**identificazione degli utenti** avviene mediante user-id e password (modificabile dall'utente), oppure mediante utilizzo di una smartcard con certificato di autenticazione.

<b>IT Telecom</b>	<i>Tipo documento:</i> <b>Manuale Operativo</b>	<i>Emesso da:</i> <b>CAS</b>	<i>Codice documento</i> <b>MO.PEC.00.00</b>	<i>Data di emissione</i> <b>01.12.2005</b>
-------------------	--	---------------------------------	--	---

L'**Accesso** alla casella di posta mediante protocollo POP3-S (Post Office Protocol), IMAP-S (Internet Message Access Protocol) e HTTP-S (Hyper Text Transfer Protocol) attraverso browser, oppure tutti i principali client di posta.

### 6.1.3 I soggetti del servizio secondo la normativa

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

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

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

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

### 6.1.4 Funzionamento del servizio

Il funzionamento generale dell'applicazione consiste nelle seguenti fasi secondo lo schema descritto nella Figura 1:

#### 6.1.4.1 Invio del messaggio da parte del mittente

Il **mittente** invia un messaggio attraverso il servizio di posta certificata. Il server di posta certificata del mittente (**punto di accesso**) esegue una serie di controlli formali sul messaggio pervenuto e provvede a generare una ricevuta di accettazione. I controlli formali accertano se i destinatari del messaggio appartengono all'infrastruttura di posta certificata o sono utenti esterni (es. posta Internet).

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

La **ricevuta di accettazione** è un messaggio di posta elettronica firmato dal gestore del mittente, nel quale sono riportati la data ed ora di accettazione, l'oggetto ed i dati del mittente e del destinatario. Nella ricevuta di accettazione è riportata la tipologia

<b>IT Telecom</b>	<i>Tipo documento:</i> <b>Manuale Operativo</b>	<i>Emesso da:</i> <b>CAS</b>	<i>Codice documento</i> <b>MO.PEC.00.00</b>	<i>Data di emissione</i> <b>01.12.2005</b>
-------------------	--	---------------------------------	--	---

dei vari destinatari per informare il mittente del differente flusso seguito dai due gruppi di messaggi.

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

#### **6.1.4.2 Invio del messaggio al punto di ricezione**

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

#### **6.1.4.3 Invio del messaggio al punto di consegna**

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

#### **6.1.4.4 Problemi di consegna**

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

Qualora il gestore del mittente riceva messaggi con virus informatici è tenuto a non accettarli informando tempestivamente il mittente dell'impossibilità di dar corso alla trasmissione. In tal caso il gestore conserva i messaggi ricevuti per trenta mesi secondo le modalità definite dall'art. 12, comma 1 del DPR 68/05. Qualora il gestore del destinatario riceva messaggi con virus informatici è tenuto a non inoltrarli al

---

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

<b>IT Telecom</b>	<i>Tipo documento:</i> <b>Manuale Operativo</b>	<i>Emesso da:</i> <b>CAS</b>	<i>Codice documento</i> <b>MO.PEC.00.00</b>	<i>Data di emissione</i> <b>01.12.2005</b>
-------------------	--	---------------------------------	--	---

destinatario informando tempestivamente il gestore del mittente, affinché comunichi al mittente medesimo l'impossibilità di dar corso alla trasmissione. In tal caso il gestore del destinatario conserva i messaggi ricevuti per trenta mesi secondo le modalità definite dall'art. 12, comma 2 del DPR 68/05.

In tutti questi casi vengono generati e inviati al mittente specifici avvisi con i motivi della mancata consegna.

#### **6.1.4.5 Firma elettronica delle ricevute e delle buste di trasporto**

Le ricevute e le buste di trasporto rilasciate dal Gestore sono sottoscritte dal medesimo mediante una firma elettronica avanzata ai sensi dell'articolo 1, comma 1, lettera dd), del TUDA, generata automaticamente dal sistema di posta elettronica e basata su chiavi asimmetriche a coppia, una pubblica e una privata, che consente di renderne manifesta la provenienza e assicurarne l'integrità e l'autenticità, secondo le modalità previste dalle regole tecniche (art. 9 del DPR 68/05).

#### **6.1.4.6 Riferimento temporale**

Su tutti gli eventi che costituiscono la transazione di elaborazione dei messaggi (generazione di ricevute, buste di trasporto, log, ecc.) il Gestore appone un riferimento temporale in conformità con l'art. 10 del DPR 68/05 e secondo le modalità che il Gestore utilizza nella sua attività di Certificazione Digitale (più oltre si riporta una sintesi del contenuto del Manuale Operativo dei Certificati Qualificati di Firma Digitale ai sensi del DPR 445/2000, Marcatura Temporale, Carta Nazionale dei Servizi del Certificatore, relativa a questo tema).

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

#### **6.1.4.7 Tipologia delle Ricevute di Avvenuta Consegna**

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

- la **Ricevuta Completa** è costituita da un messaggio di posta elettronica inviato al mittente che riporta in formato leggibile i dati di certificazione (mittente, destinatario, oggetto, riferimenti temporali, codice identificativo del messaggio). Gli stessi dati sono inseriti all'interno di un file XML allegato alla ricevuta. Per le consegne relative ai destinatari primari del messaggio, la ricevuta di avvenuta consegna **contiene anche il messaggio originale, completo di header, testo ed eventuali allegati**;
- la **Ricevuta Breve** ha lo scopo di ridurre i flussi di trasmissione della PEC, soprattutto in quei casi in cui la mole di documenti e di messaggi scambiati è molto consistente. Per questo, la Ricevuta Breve contiene il messaggio originale e gli hash crittografici degli eventuali allegati. Per permettere la verifica dei contenuti trasmessi, il mittente deve conservare gli originali non modificati degli allegati inseriti nel messaggio originale, a cui gli hash fanno riferimento;

- la **Ricevuta Sintetica** segue le regole di emissione della ricevuta completa, solo che nell'allegato contiene esclusivamente il file XML con i dati di certificazione descritti. La ricevuta sintetica è particolarmente utile in tutte quelle fattispecie di servizio che includono la PEC come strumento di trasporto a supporto di una forte automazione dei flussi di comunicazione.

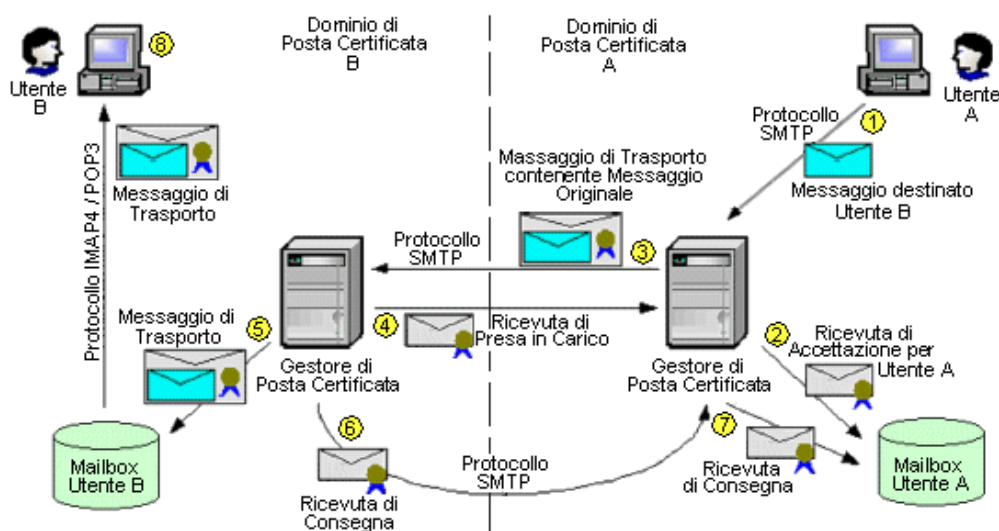


Figura 1: Schema di funzionamento del servizio di posta elettronica certificata

## 7 Riferimento Temporale e Marca Temporale del Gestore

In questo capitolo si descrivono le modalità di utilizzo del servizio di Validazione Temporale del Certificatore IT Telecom.

Il servizio è il risultato di una procedura informatica che attribuisce ad uno o più documenti informatici un riferimento temporale opponibile ai terzi, associando a qualsiasi evidenza informatica (intesa come sequenza di simboli binari) una data ed un'ora certe, validando temporalmente queste informazioni, mediante la generazione di una marca temporale (art. 1, comma 1, lett. f), g), h), i) e art. 44, comma 1 del DPCM 2004).

Per marca temporale si intende una struttura di dati (ovvero l'impronta del documento cui la marca si riferisce, ottenuta attraverso un'apposita funzione di hash) firmata digitalmente, così da poter attribuire al documento informatico in oggetto un riferimento temporale (data ed ora) sicuro e verificabile (art. 1, comma 1, lett. d ed e del DPCM 2004).

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

- l'**impronta del documento** (con l'indicazione dell'algoritmo impiegato) che rende univoca l'associazione dello stesso con la marca temporale;

<b>IT Telecom</b>	<i>Tipo documento:</i> <b>Manuale Operativo</b>	<i>Emesso da:</i> <b>CAS</b>	<i>Codice documento</i> <b>MO.PEC.00.00</b>	<i>Data di emissione</i> <b>01.12.2005</b>
-------------------	--	---------------------------------	--	---

- il **numero progressivo** seriale della marca che ne sancisce la esclusività della marcatura;
- **la data e l'ora** relative alla richiesta dell'utente al Certificatore.

Ciascuna marca temporale viene generata e firmata da un apposito sistema elettronico sicuro (TSA – *Time Stamping Authority*) del Certificatore IT Telecom, così da dimostrare l'esistenza del documento informatico, mediante il riferimento temporale indicato nella marca associata al documento stesso (art. 44, comma 2 del DPCM 2004).

## **7.1 Generazione delle Chiavi di Marcatura Temporale**

Il certificato della Time Stamping Authority (TSA) del Certificatore IT Telecom è reperibile nell'elenco pubblico dei Certificatori italiani Accreditati gestito dal CNIPA.

Si evidenzia, inoltre, l'impiego esclusivo della coppia di chiavi corrispondente al certificato suddetto per la certificazione delle chiavi delle marche temporali emesse, in quanto i certificati per i Titolari di chiavi di sottoscrizione sono firmati con una diversa coppia di chiavi (art. 4, comma 4 e 5 del DPCM 2004).

Il *Responsabile del sistema di riferimento temporale* del Certificatore è l'unico soggetto abilitato alla generazione delle chiavi di marcatura temporale impiegate per la sottoscrizione dei relativi certificati (art. 46, comma 3 e 4 del DPCM 2004). Ciascuna coppia di chiavi del Time Stamping Service (TSS) del Certificatore ha validità pari a tre (3) anni ed è generata all'interno di un apparato hardware crittografico sicuro (HSM – *Hardware Security Module*), utilizzando l'algoritmo asimmetrico RSA con chiavi non inferiori a 1.024 bit di lunghezza e sostituita ogni mese, al fine di limitare il numero delle marche generate con la medesima coppia, senza revocarne il corrispondente certificato (art. art. 46, comma 1 e 2 del DPCM 2004).

## **7.2 Marche Temporali**

Tutti i certificati per chiavi di marcatura temporale emessi dal Certificatore sono conformi alla normativa in vigore e contengono l'identificativo del sistema di marcatura temporale che utilizza le chiavi relative (art. 47, comma 1 e 2 del DPCM 2004).

Ancora in coerenza con la normativa vigente, il Certificatore si è basato sulle specifiche tecniche esposte dal gruppo di lavoro dello IETF (RFC 3161), relativo al protocollo TSP (Time Stamp Protocol), per definire il formato delle marche temporali nell'ambito del suo servizio di Validazione Temporale.

Riguardo al contenuto delle marche temporali, di seguito si riportano le informazioni sicuramente presenti al loro interno (art. 45, comma 1 del DPCM 2004):

- a) identificativo della CA emittente: IT Telecom Time Stamp Authority;
- b) numero di serie della marca;
- c) algoritmo impiegato per la sottoscrizione della marca: RSA;
- d) identificativo del certificato relativo alla chiave pubblica di verifica della marca;
- e) data ed ora di generazione della marca: in formato UTC;

<b>IT Telecom</b>	<i>Tipo documento:</i> <b>Manuale Operativo</b>	<i>Emesso da:</i> <b>CAS</b>	<i>Codice documento</i> <b>MO.PEC.00.00</b>	<i>Data di emissione</i> <b>01.12.2005</b>
-------------------	--	---------------------------------	--	---

- f) identificatore dell'algoritmo di hash impiegato per la generazione dell'impronta dell'evidenza informatica sottoposta a validazione temporale: SHA-1;
- g) valore dell'impronta dell'evidenza informatica.

### 7.2.1 Registrazione delle marche temporali

Il sistema di Validazione Temporale del Certificatore IT Telecom garantisce la conservazione di tutte le marche temporali emesse in un apposito archivio digitale non modificabile, per un periodo non inferiore ai cinque anni. Su richiesta dell'interessato, è possibile conservare le suddette marche per un periodo maggiore, secondo specifiche condizioni previste dal Certificatore medesimo (art. 50, comma 1 del DPCM 2004).

### 7.2.2 Validità delle marche temporali

Una marca temporale ha validità sino alla scadenza del certificato ad essa associato e per l'intero periodo della sua conservazione nell'apposito archivio del Certificatore (art. 50, comma 2 del DPCM 2004).

Il certificato di marcatura temporale di IT Telecom ha una durata di tre anni. Tuttavia, possono essere concordati con gli utenti periodi di validità maggiori. In alternativa, prima della scadenza del certificato, può essere associata una nuova marca all'evidenza informatica relativa alla marca precedente, così da dare continuità alla validità del documento originario.

Si ricorda che, per estendere nel tempo l'efficacia legale di un documento informatico firmato digitalmente, è sufficiente associare successivamente al medesimo documento nuove marche temporali (art. 52 del DPCM 2004).

## 7.3 Sicurezza del sistema di Validazione Temporale

Personale espressamente autorizzato dal certificatore provvede al buon funzionamento del servizio di Validazione Temporale.. Attraverso un sistema di monitoraggio interno viene effettuato un continuo controllo delle fonti di riferimento temporale esterne utilizzate, verificando lo stato dei server presenti nella Sala Sistemi del Certificatore. Mediante un dispositivo sw denominato TIME CHECK, infatti, è possibile richiedere, tramite protocollo SMNP, il riferimento temporale all'elemento di rete monitorato (server), confrontando i dati ricevuti con quelli del sistema di monitoraggio, sincronizzato con una terza parte esterna, lo IEN "Galileo Ferraris".

Il personale del Certificatore analizza eventuali anomalie accorse al servizio di Validazione Temporale, registrate automaticamente in un apposito registro operativo su di un supporto non riscrivibile (art. 49, comma 1 e 2 del DPCM 2004), come:

- asincronismo con la fonte esterna di riferimento (IEN);
- differenza oraria superiore a quella impostata come allarme;
- indisponibilità o manomissione del supporto non riscrivibile;
- tentativo di sabotaggio del sistema.

<b>IT Telecom</b>	<i>Tipo documento:</i> <b>Manuale Operativo</b>	<i>Emesso da:</i> <b>CAS</b>	<i>Codice documento</i> <b>MO.PEC.00.00</b>	<i>Data di emissione</i> <b>01.12.2005</b>
-------------------	--	---------------------------------	--	---

Al verificarsi dei suddetti accadimenti, il personale autorizzato provvede al blocco del sistema, prima della sua pronta risoluzione (art. 49, comma 3 del DPCM 2004).

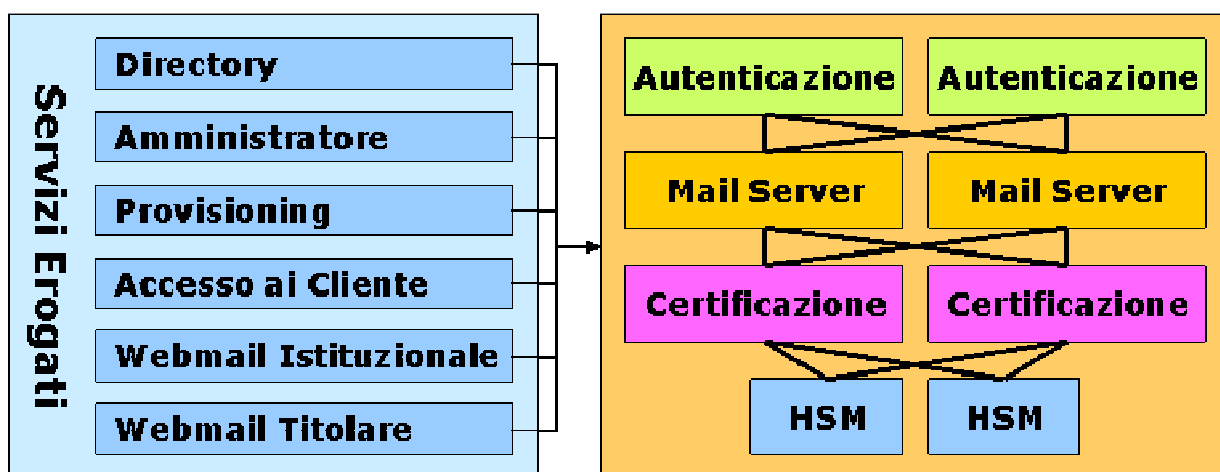
## 8 La soluzione IT Telecom di Posta Elettronica Certificata

La soluzione di PEC di IT Telecom si avvale di un'architettura modulare e scalabile, che consente di impiegare un client di posta elettronica sfruttando un canale sicuro di trasmissione come l'IMAP-S/POP3S e SMTPS<sup>2</sup>.

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

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

### 8.1 Architettura del Servizio



L'architettura della piattaforma di PEC IT Telecom prevede tre differenti gruppi tecnologici:

- **punti di accesso per l'utente finale** per i vari livelli di amministrazione ai differenti servizi erogati. I primi possono fruire della posta elettronica accedendo ad un'interfaccia Webmail online, differenziata fra utente titolare o

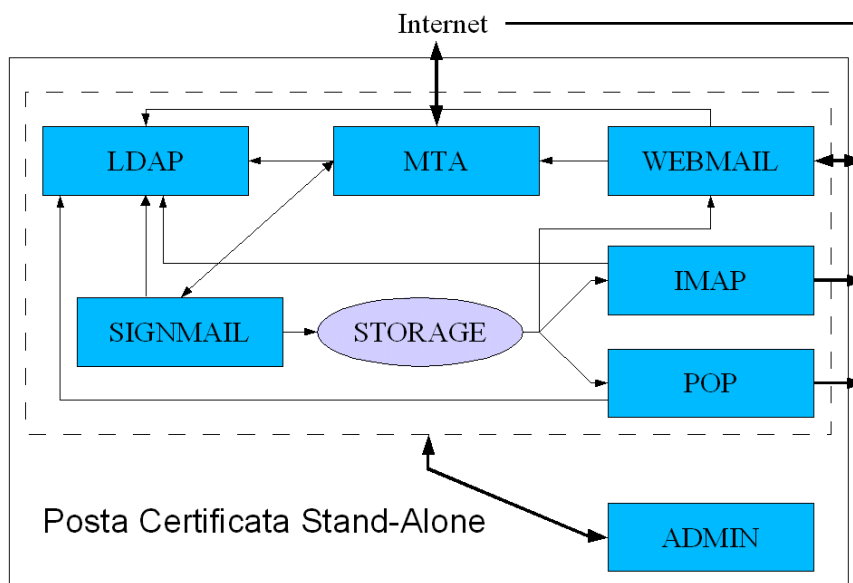
<sup>2</sup> Le Regole Tecniche allegate al DM 2/11/05 stabiliscono che l'integrità e la confidenzialità delle connessioni tra il gestore di posta certificata e l'utente devono essere garantite mediante l'uso di protocolli sicuri. A titolo esemplificativo, e non esaustivo, dei protocolli accettabili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

istituzionale, oppure utilizzando un comune Client di posta (Outlook, Eudora, ecc.). Il Provisioning invece consente un facile ed intuitivo livello di amministrazione dei servizi stessi da parte del Gestore dei ruoli e dell'Incaricato, laddove invece l'Amministratore della piattaforma tecnologica è dotato di un interfaccia di gestione personale.

- **sistema di gestione**, smistamento e transazione delle mail (Mailserver), il sistema di autorizzazione ed Autenticazione delle utenze e la parte dedicata alla Certificazione dei messaggi di posta.
- **moduli HSM**, macchine dedicate allo storage protetto delle chiavi private di firma.

Di seguito, alcune componenti presenti nell'architettura generale della PEC stand alone con l'aiuto di un grafico per evidenziarne le interrelazioni:

1. MTA - Server di posta che supporta il protocollo SMTP;
2. LDAP - Server Lightweight Directory per memorizzazione utenze e preferenze globali;
3. WEBMAIL - Client per accesso remoto tramite Web;
4. IMAP - Server per accesso remoto tramite MUA;
5. POP3 - Server per accesso remoto tramite MUA;
6. ADMIN - Client ad accesso riservato per l'amministrazione/gestione del sistema tramite Web;
7. SIGNMAIL - Plugin per la posta certificata.



<b>IT Telecom</b>	<i>Tipo documento:</i> <b>Manuale Operativo</b>	<i>Emesso da:</i> <b>CAS</b>	<i>Codice documento</i> <b>MO.PEC.00.00</b>	<i>Data di emissione</i> <b>01.12.2005</b>
-------------------	--	---------------------------------	--	---

## 8.2 Principali tecnologie utilizzate

Di seguito, l'indicazione delle principali tecnologie utilizzate per l'esercizio del servizio di PEC

- **Sistemi operativi di base:**
  - SUN Solaris
- **Storage:**
  - SUN Storage Disk Array
  - EMC2
- **Middleware:**
  - Sun One Webserver
  - Sun One Directory Server
  - Sun One Java WebContainer
  - Websphere Application Server
  - Oracle Database Client/Server
  - Apache Jakarta Tomcat
  - SMTP Postfix
  - Pop-Imap server Courier
  - CyrusSASL
  - Load-balancing Sureware Keyper Cybertrust
  - Sureware Keyper Cybertrust PKCS#11
- **Application Software Languages:**
  - Java
  - Ansi C
  - SS Javascript

## 8.3 Organizzazione del personale

L'organizzazione del personale addetto all'erogazione del servizio di PEC di IT Telecom prevede, tra le altre, le figure professionali di responsabile della registrazione dei titolari, responsabile dei servizi tecnici, responsabile delle verifiche e delle ispezioni (auditing), responsabile della sicurezza, responsabile della sicurezza dei log dei messaggi e responsabile del sistema di riferimento temporale (art. 21, comma 1 del DM 2/11/05). Tali figure professionali sono appositamente addestrate in funzione degli aggiornamenti subiti dal sistema di PEC (art. 22, comma 2 del DM 2/11/05) e posseggono una esperienza non inferiore a cinque anni nella analisi, progettazione, commercializzazione e conduzione di sistemi informatici. (art. 22, comma 1 del DM 2/11/05).

<b>IT Telecom</b>	<i>Tipo documento:</i> <b>Manuale Operativo</b>	<i>Emesso da:</i> <b>CAS</b>	<i>Codice documento</i> <b>MO.PEC.00.00</b>	<i>Data di emissione</i> <b>01.12.2005</b>
-------------------	--	---------------------------------	--	---

## **9 Modalità di generazione, conservazione, reperimento e presentazione dei log dei messaggi**

In questo capitolo sono descritte le modalità che il Gestore IT Telecom adotta per le attività di generazione, conservazione, reperimento e presentazione dei log dei sistemi. Ulteriori specificazioni relative alla sicurezza dei trattamenti, sono riportate nel Piano della Sicurezza del Gestore, depositato presso il CNIPA.

### **9.1 Generazione**

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

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

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

Le informazioni dei log durante il trattamento sono memorizzate da due specifiche componenti della piattaforma durante le fasi di trattamento :

- il sistema posizionato sulla rete di front-end della piattaforma che colloquia attraverso le strutture dei firewall con i sistemi esterni effettua le seguenti operazioni :
  - instaura il colloquio sicuro con gli utenti durante le fasi di ricezione o trasmissione dei messaggi
  - instaura il colloquio sicuro con i server di altri gestori di posta certificata
  - l'autenticazione degli utenti,
  - il controllo della presenza di virus nei messaggi
  - la trasmissione dei messaggi da e verso Internet
  - eliminazione di messaggi pericolosi ed indesiderati
  - sincronizzazione dell'indice (LDIF) interno della piattaforma utilizzato per la verifica dei messaggi con l'indice predisposto da CNIPA
  - predisposizione e disponibilità dell'indice del gestore I.T.Telecom aggiornato
  - Caching della CRL di CNIPA

<b>IT Telecom</b>	<i>Tipo documento:</i> <b>Manuale Operativo</b>	<i>Emesso da:</i> <b>CAS</b>	<i>Codice documento</i> <b>MO.PEC.00.00</b>	<i>Data di emissione</i> <b>01.12.2005</b>
-------------------	--	---------------------------------	--	---

- il sistema posizionato sulla rete di back-end della piattaforma che , ricevendo l'inoltro dei messaggi dalle componenti di front-end effettua le seguenti operazioni :
  - verifica ed identificazione della tipologia dei messaggi in ingresso (messaggi di trasporto, anomalia, ricevuta di presa in carico, ricevuta di avvenuta consegna completa, breve e sintetica , avviso di mancata consegna, ecc.)
  - firma dei messaggi di posta certificata
  - memorizzazione dei messaggi nelle mailbox degli utenti
  - Verifiche temporali sul completamento delle trasmissioni relative a ciascun messaggio (mancata consegna nelle 12 o 24 ore)

Tutti i sistemi della piattaforma sono sincronizzati temporalmente utilizzando il protocollo NTP; il riferimento temporale certo è costituito da due sorgenti in modo da garantire l'alta affidabilità dei sistemi (v. par. 7.3).

I sistemi sopraccitati generano log memorizzati con le due seguenti modalità:

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

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

- Instaurazione del colloqui sicuro (startup TLS – HTTPS etc.)
- Autenticazione ed identificazione degli utenti che accedono alla piattaforma
- Ricezione di messaggi da altri server di posta
- Intercettazione di virus : in questo caso il sistema '*marca*' il messaggio come infetto e lo trasmette per la memorizzazione ai sistemi di back-end senza alterarlo
- La eliminazione di messaggi indesiderati (spamming)
- Il tentativo di inoltro di messaggi senza la necessaria autenticazione (RELAY)
- Attività di sincronizzazione degli indici LDIF.

Questi log possono essere generati con diversi livelli di dettaglio di informazioni (debug) ma contengono per ciascun evento almeno : il tipo di evento , l'identificativo del messaggio trattato (se presente) , l'indirizzo elettronico del mittente e del destinatario (se presenti) , il sistema server della piattaforma che lo ha generato, il sistema server esterno alla piattaforma coinvolto nel trattamento, la data e l'ora dell'evento, la componente software di piattaforma che ha gestito l'evento, il risultato del trattamento.

<b>IT Telecom</b>	<i>Tipo documento:</i> <b>Manuale Operativo</b>	<i>Emesso da:</i> <b>CAS</b>	<i>Codice documento</i> <b>MO.PEC.00.00</b>	<i>Data di emissione</i> <b>01.12.2005</b>
-------------------	--	---------------------------------	--	---

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

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

- Identificazione del tipo messaggio: messaggio di trasporto, anomalia ecc.
- Verifica della firma e della CRL
- Identificazione del dominio mittente e dei domini destinatari del messaggio
- Identificazione del mittente e dei destinatari del messaggio
- Verifiche delle strutture formali: XML, header etc...
- Modalità di trattamento da effettuare: generazione ricevute ed anomalie, consegna messaggio, avvisi.

Per la memorizzazione dei log sono state dedicate alcune tabelle del database nelle quali sono contenuti i dati del trattamento e gli esiti dei trattamenti effettuati; in particolare:

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

## 9.2 Conservazione dei Log

### 9.2.1 Conservazione dei log su Flat-files

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

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

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

<b>IT Telecom</b>	<i>Tipo documento:</i> <b>Manuale Operativo</b>	<i>Emesso da:</i> <b>CAS</b>	<i>Codice documento</i> <b>MO.PEC.00.00</b>	<i>Data di emissione</i> <b>01.12.2005</b>
-------------------	--	---------------------------------	--	---

Il processo, immediatamente dopo la rotazione, prevede l'apposizione di una marca temporale generata dal server della Time Stamping Authority di IT Telecom.

L'integrità e l'inalterabilità dei log vengono garantite mediante l'apposizione della marca temporale (per una descrizione del sistema, si veda il cap. 7).

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

- backup giornaliero dei log marcati temporalmente con periodo di retention pari a trenta mesi;
- creazione di due copie dei log marcati temporalmente su dispositivo non riscrivibile (DVD worm) con cadenza almeno settimanale;
- invio con cadenza almeno mensile di una copia dei log su dispositivo non riscrivibile al sito di Disaster Recovery.

### 9.2.2 Conservazione dei log su database

I log sul database generati dalle componenti di back-end vengono estratti dal database stesso con cadenza almeno giornaliera e memorizzati su file con rappresentazioni congruenti con la tipologia di dati in essi contenuti (ad es. flat-file per dati VARCHAR o NUMBER, binary per dati di tipo Blob).

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

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

Il processo di estrazione comprende l'apposizione di una marca temporale generata dal server della Time Stamping Authority di IT Telecom.

L'integrità e l'inalterabilità dei log vengono garantite mediante l'apposizione della marca temporale (per una descrizione del sistema, si veda il cap. 7).

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

- backup giornaliero incrementale del database;
- backup full settimanale del database con retention pari a quattro settimane;
- copia di tutti i dati contenuti nel database mediante le funzionalità di replica on-change del database Oracle sul server di replica presente nel sito di Disaster Recovery.

## 9.3 Reperimento e presentazione dei Log

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

**Fase 1** - Le richieste di accesso ai Log sono effettuate dai seguenti soggetti, con le modalità indicate:

<b>IT Telecom</b>	<i>Tipo documento:</i> <b>Manuale Operativo</b>	<i>Emesso da:</i> <b>CAS</b>	<i>Codice documento</i> <b>MO.PEC.00.00</b>	<i>Data di emissione</i> <b>01.12.2005</b>
-------------------	--	---------------------------------	--	---

1. Il **Titolare** sottoscrive un documento cartaceo o informatico (mediante firma qualificata) con il quale richiede il recupero e la presentazione dei log. Il documento, che il Titolare può inviare sia per raccomandata A/R sia con posta elettronica certificata, deve contenere almeno i seguenti dati:
  - dati anagrafici del Titolare;
  - periodo temporale del quale si richiedono i log ed ulteriori dettagli utili alla loro estrazione, quali ad es. il message-ID, l'indirizzo e-mail, ecc.;
  - motivazione della richiesta;
  - indicazione della struttura richiesta per la rappresentazione dei dati contenuti dei log;
  - autorizzazione relativamente alla normativa sulla privacy, ove richiesta;
  - il recapito del Titolare per l'invio dei log in caso di trasmissione della richiesta tramite raccomandata A/R; ovvero in caso di trasmissione tramite PEC, l'indirizzo di PEC presso il quale il Titolare richiede l'invio.
2. I **soggetti autorizzati per legge**, con le stesse modalità previste per il Titolare;
3. Il **Gestore**, che è autorizzato in quanto Incaricato del trattamento dei dati

**Fase 2** - L'estrazione dei dati di riferimento è effettuata mediante ricerca sul database dei riferimenti necessari al recupero dei log o dei dati relativi allo specifico messaggio di cui si richiede il log del trattamento.

Poiché l'interfaccia web si avvale di dati indicizzati presenti su tabelle del database, le fasi di identificazione dei log sono molto veloci ed efficaci anche nel caso si conoscano solamente pochi dati relativi alla trasmissione (ad es. il solo Message-ID, l'indirizzo elettronico del mittente o del destinatario, il gestore ecc.).

**Fase 3** - L'estrazione dei log viene effettuata mediante accesso ai server o agli archivi WORM, presso i quali si reperiscono i file di log identificati nella fase 2.

**Fase 4:** La presentazione dei log avviene esclusivamente mediante l'invio al recapito indicato dal richiedente di un supporto non riscrivibile. Detto supporto contiene i log informativi firmati digitalmente dal Gestore (v. infra per le modalità), nei quali sono rappresentati in formato testuale i dati minimi di riferimento previsti dalla normativa ed eventualmente ulteriori informazioni<sup>3</sup>. In particolare, il documento è generato da un processo che prevede le seguenti fasi:

1. copia ed assemblaggio dei log richiesti in un unico archivio;
2. apposizione sull'archivio della firma digitale del responsabile sicurezza dei log dei messaggi (art. 21, comma 1, lettera e DM 2/11/05);
3. marcatura temporale dell'archivio firmato contenente i log;

<sup>3</sup> Il log è prodotto in formato ASCII base ed è strutturato secondo le indicazioni formulate dal Titolare nella richiesta.

<b>IT Telecom</b>	<i>Tipo documento:</i> <b>Manuale Operativo</b>	<i>Emesso da:</i> <b>CAS</b>	<i>Codice documento</i> <b>MO.PEC.00.00</b>	<i>Data di emissione</i> <b>01.12.2005</b>
-------------------	--	---------------------------------	--	---

4. produzione di due copie dell'archivio firmato e marcato su dispositivo non riscrivibile;
5. archiviazione della prima copia presso il Gestore IT Telecom;
6. invio della seconda copia al richiedente.

## **10 Tipologie del servizio PEC offerte da IT Telecom**

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

- **Dominio sul quale sono configurate le caselle di posta elettronica:** di IT Telecom o del Cliente
- **Tipologia di servizio:** casella privata, casella istituzionale
- **Modalità di utilizzo:** webmail o client di posta.

### **10.1 Trattamento dei Domini di PEC**

Il cliente per la gestione della propria corrispondenza certificata può avvalersi del dominio di posta certificata di IT Telecom oppure può utilizzare un proprio dominio (o sottodominio) avendone richiesto la configurazione come dominio (o sottodominio) di posta certificata.

#### **10.1.1 Domini certificati di IT Telecom**

In questo caso il cliente, per la gestione della sua corrispondenza certificata, si appoggia al dominio di Posta Certificata del Servizio IT Telecom.

Tutti gli scambi in entrata ed in uscita effettuati dalle caselle di posta del cliente configurate in questo dominio, sono trattati come scambi di messaggi di posta certificata. Coerentemente alla normativa vigente assumono quindi un valore equivalente alla notificazione per mezzo della posta nei casi consentiti dalla legge.

Per ogni messaggio inviato, il mittente riceverà una ricevuta di accettazione ed una ricevuta di consegna per ciascuno dei destinatari ai quali il messaggio è stato inviato (in caso di problemi di consegna o anomalie nell'utilizzo del servizio, riceverà i corrispondenti avvisi).

#### **10.1.2 Dominio del cliente**

In questa ipotesi, il cliente che già possiede un suo dominio o un sottodominio Internet, ne chiede la configurazione come dominio o sottodominio di posta certificata.

Tutti gli scambi in entrata ed in uscita effettuati dalle caselle di posta del cliente configurate nel dominio certificato sono trattati come scambi di messaggi di posta certificata. Coerentemente alla normativa vigente assumono quindi un valore equivalente alla notificazione per mezzo della posta nei casi consentiti dalla legge.

Per ogni messaggio inviato, il mittente riceverà una ricevuta di accettazione ed una ricevuta di consegna per ciascuno dei destinatari ai quali il messaggio è stato inviato

<b>IT Telecom</b>	Tipo documento: <b>Manuale Operativo</b>	Emesso da: <b>CAS</b>	Codice documento <b>MO.PEC.00.00</b>	Data di emissione <b>01.12.2005</b>
-------------------	---	--------------------------	---	--

(in caso di problemi di consegna o anomalie nell'utilizzo del servizio, riceverà i corrispondenti avvisi).

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

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

## 10.2 Tipologie di Caselle di PEC

### 10.2.1 Caselle istituzionali

La casella istituzionale prevede la possibilità che un gruppo di utenti (utenti operatori) possa accedere alla medesima casella per la gestione della corrispondenza scambiata attraverso di essa. Allo scopo di consentire al Cliente di mantenere il controllo sulla gestione delle utenze, è prevista l'attivazione di Incaricati della Registrazione degli utenti che effettuano la registrazione degli utenti stessi secondo le procedure indicate da IT Telecom, l'attivazione delle utenze e delle caselle di PEC, nonché la gestione dell'utenza (utente amministratore).

Con questo tipo di servizio IT Telecom intende soddisfare le esigenze di organizzazioni di grandi dimensione e di enti della Pubblica Amministrazione nei quali, normalmente, nell'ambito della posta certificata, gli indirizzi di posta corrispondono a punti di riferimento che ricevono i messaggi in entrata i quali, a loro volta, sono acquisiti da più operatori che provvedono a classificarli e smistarli verso le funzioni organizzative competenti. Gli stessi riferimenti centralizzati, si occupano anche di trattare la corrispondenza in uscita prodotta dalle varie funzioni interne.

Per soddisfare le esigenze legate a questo tipo di utilizzo, questo servizio, oltre a supportare chi opera nella gestione della corrispondenza, garantisce anche la possibilità di curare l'amministrazione delle utenze e di assicurare i necessari livelli di sicurezza nell'accesso e nella gestione dei contenuti, anche attraverso la presenza di una funzione di auditing interna al cliente, per il controllo dei flussi.

In modo particolare, la soluzione realizzata da IT Telecom prevede l'utilizzo di un'interfaccia Web dedicata alla gestione della corrispondenza scambiata che è in grado di soddisfare le esigenze seguenti:

- **Sicurezza nell'accesso e protezione dei contenuti:** l'accesso al servizio avviene attraverso autenticazione tramite certificato digitale. Anche se il servizio prevede che più utenti abilitati possano accedere ad una stessa casella di posta istituzionale, tutti sono identificati singolarmente ed il sistema registra tutte le operazioni effettuate da ciascuno di loro (replica, accesso alla corrispondenza elettronica, lavorazione ecc.).
- **Praticità di utilizzo:** attraverso un codice identificativo progressivo attribuito a ciascun messaggio, il sistema permette di gestire un consistente flusso di

<b>IT Telecom</b>	<i>Tipo documento:</i> <b>Manuale Operativo</b>	<i>Emesso da:</i> <b>CAS</b>	<i>Codice documento</i> <b>MO.PEC.00.00</b>	<i>Data di emissione</i> <b>01.12.2005</b>
-------------------	--	---------------------------------	--	---

corrispondenza elettronica in entrata ed in uscita, garantendo le funzionalità di visualizzazione, ordinamento e lavorazione della corrispondenza elettronica in entrata ed in uscita. Gli automatismi nell'assegnazione del codice identificativo e delle informazioni correlate (operatore che ha inviato il messaggio, casella di provenienza ecc.) sollevano l'utente da un complesso di attività ripetitive spesso fonte di errori. Le numerose funzioni d'uso permettono, infine, di snellire e velocizzare le operazioni di trattamento della corrispondenza elettronica.

### **10.2.1.1 Principali funzioni del servizio**

Come accennato, nel caso di una casella di posta istituzionale, diversi utenti utilizzano la medesima casella di posta elettronica certificata. La soluzione IT Telecom prevede un meccanismo di verifica dell'appartenenza dell'utente al gruppo di titolari che possono accedere alla casella istituzionale (userid e password, oppure certificato di autenticazione): solo le persone preventivamente autorizzate potranno accedervi. È inoltre previsto un meccanismo di controllo delle possibili sovrapposizioni tra i vari utenti appartenenti al gruppo, questo meccanismo rende impossibile modificare un messaggio di posta preso in carico da un'altro utente, fino al suo rilascio. L'utente che ha in carico il messaggio può decidere di rilasciarlo consentendo ad altri utenti di prenderlo in carico oppure può decidere di completarlo.

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

- Si può prendere in carico un messaggio solo quando nessun altro utente sta utilizzando in quel momento il messaggio stesso..
- Quando un altro utente sta già utilizzando un messaggio sarà impossibile prendere in carico lo stesso messaggio.

### **10.2.1.2 Modalità di accesso alle caselle di PEC**

Questo tipo di soluzione è utilizzabile esclusivamente attraverso l'utilizzo di un browser, raggiungibile via internet tramite il Portale PKI di IT Telecom all'indirizzo <https://portal.tipki.it>.

In sostituzione del precedente e su richiesta del Cliente in fase di definizione del contratto, è previsto un altro tipo di accesso sempre via browser, che prescinde totalmente dal portale PKI e quindi da una gestione accentrata dell'anagrafica; tale soluzione, se adottata, non permetterebbe al Cliente, in un momento successivo, di utilizzare i dati già esistenti e presenti presso altri servizi trusted forniti da IT Telecom (firma digitale a norma, time stamping, conservazione documentale e così via).

Allo scopo di consentire al Cliente di mantenere il controllo sulla gestione delle utenze, è prevista l'attivazione di Incaricati alla Registrazione degli utenti che effettuano la registrazione degli utenti secondo le procedure indicate da IT Telecom, l'attivazione delle utenze e delle caselle di PEC, nonché la gestione dell'utenza.

### **10.2.1.3 Dimensioni delle caselle di PEC e traffico**

Tutte le utenze di Posta Elettronica Certificata sono a traffico illimitato. Per le caselle istituzionali, il cliente può scegliere tra due diverse dimensioni della mailbox, da 200

<b>IT Telecom</b>	<i>Tipo documento:</i> <b>Manuale Operativo</b>	<i>Emesso da:</i> <b>CAS</b>	<i>Codice documento</i> <b>MO.PEC.00.00</b>	<i>Data di emissione</i> <b>01.12.2005</b>
-------------------	--	---------------------------------	--	---

MB e da 500 MB. L'attivazione di una casella istituzionale è subordinata all'acquisto di due utenze supplementari associate alla medesima.

## 10.2.2 Caselle individuali

La Casella Individuale è di esclusiva pertinenza di un singolo utente e non prevede la possibilità che altri possano visualizzarne il contenuto. La Casella Individuale prevede l'attivazione di un'unica utenza.

Il funzionamento delle caselle di posta titolare è simile a quello delle caselle di posta istituzionali eccetto che per la gestione della presa in carico/rilascio della mail che evidentemente risulta essere superflua in questo contesto.

### 10.2.2.1 Modalità di accesso

La casella di posta certificata individuale può essere fruita sia attraverso un normale client di posta che attraverso un browser raggiungibile via internet all'indirizzo del Portale PKI di IT Telecom <https://portal.tipki.it>.

In sostituzione del precedente e su richiesta del Cliente in fase di definizione del contratto, è previsto un altro tipo di accesso sempre via browser, che prescinde totalmente dal portale PKI e quindi da una gestione accentrata dell'anagrafica; tale soluzione, se adottata, non permetterebbe al Cliente, in un momento successivo, di utilizzare i dati già esistenti e presenti presso altri servizi trusted forniti da IT Telecom (firma digitale a norma, time stamping, conservazione documentale e così via)

In entrambi questi casi, l'accesso alla casella è di esclusiva pertinenza di un singolo utente ed il sistema non prevede la possibilità che altri utenti possano accedere al contenuto della casella stessa.

Allo scopo di consentire al Cliente di mantenere il controllo sulla gestione delle utenze, è prevista l'attivazione di Incaricati della Registrazione degli utenti che effettuano la registrazione degli utenti secondo le procedure indicate da IT Telecom, l'attivazione delle utenze e delle caselle di PEC, nonché la gestione dell'utenza.

### 10.2.2.2 Dimensioni delle caselle di PEC e traffico

Tutte le utenze di Posta Elettronica Certificata sono a traffico illimitato. Per le caselle individuali, il cliente può scegliere tra diverse dimensioni della mailbox: da 50 MB, da 100 MB, da 200 MB e da 500 MB.

## 10.3 Il portale PKI

Il Portale PKI è il portale applicativo mediante il quale i clienti di IT Telecom possono accedere a tutti i principali servizi offerti. In particolare, per il servizio di PEC:

- Gli Incaricati possono registrare i Richiedenti e gestire le utenze dei Titolari appartenenti alla propria struttura. In modo specifico possono:
  - ◆ visualizzare le informazioni registrate relative a ciascun Titolare;
  - ◆ effettuare il reset delle password di accesso dei Titolari in caso di smarrimento.

<b>IT Telecom</b>	<i>Tipo documento:</i> <b>Manuale Operativo</b>	<i>Emesso da:</i> <b>CAS</b>	<i>Codice documento</i> <b>MO.PEC.00.00</b>	<i>Data di emissione</i> <b>01.12.2005</b>
-------------------	--	---------------------------------	--	---

Il Portale PKI rappresenta inoltre l'opportunità per un eventuale ampliamento verso gli altri servizi offerti da IT Telecom, tra cui la Firma Digitale Qualificata ed il servizio di Cifratura dei messaggi di posta elettronica.

Il software di PKI è certificato, per il software core di CA, rispetto ai Common Criteria (CC) al livello EAL3 ed è conforme alle specifiche FIPS PUB 140-1.

## **11 Cenni sulle infrastrutture del Gestore e sulle misure di sicurezza**

Le caratteristiche di dettaglio della gestione della sicurezza da parte del Gestore sono contenute nel **Piano della Sicurezza** e non sono oggetto di divulgazione, per salvaguardarne l'efficacia. Copia del Piano della Sicurezza è depositato presso il CNIPA come organo di vigilanza e controllo.

### **11.1 Infrastrutture**

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

Inoltre adotta soluzioni hardware e software leader di mercato per interoperabilità, affidabilità e sicurezza:

- è basata su **standard SUN J2EE** ed è integrabile con sistemi e applicazioni di office automation, di posta elettronica, di workflow, di Directory (LDAP), ecc.;
- garantisce la **scalabilità** dell'applicazione al crescere del numero degli utenti o della complessità elaborativa;
- si fonda sui principali **standard "de facto"** disponibili sul mercato: HTTP, JAVA, JDBC, SSL, XA, LDAP, X.509, HTML, SOAP;
- fornisce il supporto per lo sviluppo di componenti **applicativi riutilizzabili** (javabean);
- tutte le piattaforme sono su **sistema operativo SUN SOLARIS**;
- utilizza **DBMS ORACLE 9i**;
- La continuità del servizio è garantita da sistemi di **ridondanza funzionale** e di **disaster recovery**.

IT Telecom dispone di un pool di risorse con uno specifico know-how sulle tecnologie utilizzate, continuamente aggiornato attraverso attività di scouting e di contatto con i principali vendor del settore. Il Competence Center IT Telecom può vantare una collaborazione pluriennale con il CNIPA (ex AIPA e Centro Tecnico RUPA) e con altri enti italiani e stranieri (Assocertificatori, ecc.) ed è a disposizione dei clienti che necessitano di un supporto tecnico e consulenziale.

<b>IT Telecom</b>	<i>Tipo documento:</i> <b>Manuale Operativo</b>	<i>Emesso da:</i> <b>CAS</b>	<i>Codice documento</i> <b>MO.PEC.00.00</b>	<i>Data di emissione</i> <b>01.12.2005</b>
-------------------	--	---------------------------------	--	---

In termini di accesso e interoperabilità, la soluzione proposta da IT Telecom consente di impiegare un qualunque client di posta elettronica in grado di usare IMAP-S/POP3S e SMTPS:

- Outlook Express 5.\* e 6.\*
- Microsoft Outlook 2000 e 2002
- Netscape 7.\*
- Mozilla 1.\*
- Opera 5.\*
- Eudora 5.\*
- Eudora 5.\* Email
- Internet Explorer 5.\* e 6.\*

L'utilizzo della posta certificata e dei certificati S/MIME di IT Telecom permette di crittografare i messaggi garantendone la assoluta riservatezza. L'utilizzo invece dei certificati qualificati di firma digitale di IT Telecom permettono di garantire l'autenticità e la non ripudiabilità dei documenti sottoscritti e trasferiti mediante il servizio di PEC. I certificati e le chiavi utilizzati per la certificazione dei messaggi sono memorizzati all'interno di dispositivi HSM ad alta sicurezza: SUREWARE KEYPER certificati secondo i criteri ITSEC.

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

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

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

La funzione di posta elettronica certificata è inoltre completata da funzioni aggiuntive fornite da sistemi integrati con il sistema di PEC:

<b>IT Telecom</b>	<i>Tipo documento:</i> <b>Manuale Operativo</b>	<i>Emesso da:</i> <b>CAS</b>	<i>Codice documento</i> <b>MO.PEC.00.00</b>	<i>Data di emissione</i> <b>01.12.2005</b>
-------------------	--	---------------------------------	--	---

- **sistema di profilazione, autorizzazione ed autenticazione** degli utenti/operatori del servizio, comprensivo di interfaccia di amministrazione dei profili. Il sistema di profilazione provvede a restringere le possibilità operative ed il dominio dei dati a quelli effettivamente definiti per l'utente in questione in fase di attivazione, in base al suo ruolo ed al contesto. L'accesso operativo alle funzioni messe a disposizione da questo sistema viene effettuato da utenti muniti di certificato digitale (SSLv3). Il sottosistema di autorizzazione ed autenticazione per l'accesso alle diverse funzioni opera strettamente in funzione del ruolo dell'utente, dell'attività (o funzione) e dell'area (o contesto) in cui opera. Tutte le funzioni (ed eventualmente le subfunzioni collegate) vengono abilitate solo agli utenti che ne hanno diritto in base al loro ruolo. Essi possono comunque operare solo sui dati che fanno riferimento al loro dominio. Sul sistema di profilazione è definito un ruolo specifico autorizzato alla consultazione di questa base dati (Auditor).
- **sistema di identificazione** dei messaggi di posta in ingresso ed uscita, secondo requisiti.

## 11.2 Misure di sicurezza

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

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

## 11.3 Servizi di emergenza

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

<b>IT Telecom</b>	<i>Tipo documento:</i> <b>Manuale Operativo</b>	<i>Emesso da:</i> <b>CAS</b>	<i>Codice documento</i> <b>MO.PEC.00.00</b>	<i>Data di emissione</i> <b>01.12.2005</b>
-------------------	--	---------------------------------	--	---

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

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

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

Per garantire la disponibilità dei servizi essenziali fra quelli offerti dal Gestore a fronte di un disastro di tale natura, è previsto un sito di Disaster Recovery (geograficamente distante) che permette di garantire i servizi minimi previsti dalla normativa. È previsto per tanto un Piano Operativo per l'attivazione del sito e delle procedure di Disaster Recovery e di ritorno alla normale operatività.

Le procedure descritte nei dettagli nel Piano Operativo consentono al personale di gestione del traffico di rete di cambiare le rotte di instradamento verso il nuovo sito di Disaster Recovery. Sempre nel Piano Operativo sono descritte le procedure che permettono in seguito alla riattivazione del sito principale di fare un allineamento dei dati dal sito di Disaster Recovery così da garantire una continuità degli eventi accaduti.

A fronte dell'evento disastroso, una procedura di urgenza coinvolge un gruppo di crisi composto dai responsabili delle funzioni centrali. Il gruppo di crisis management analizza la gravità dell'evento e predispone le azioni necessarie per minimizzare i danni e per fornire indicazioni sulle modalità e politiche da adottare per il ripristino del sito (Policy di Crisis Management).

## **11.4 Disponibilità e Tempi di ripristino**

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

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

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

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

<b>IT Telecom</b>	<i>Tipo documento:</i> <b>Manuale Operativo</b>	<i>Emesso da:</i> <b>CAS</b>	<i>Codice documento</i> <b>MO.PEC.00.00</b>	<i>Data di emissione</i> <b>01.12.2005</b>
-------------------	--	---------------------------------	--	---

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

<b>IT Telecom</b>	<i>Tipo documento:</i> <b>Manuale Operativo</b>	<i>Emesso da:</i> <b>CAS</b>	<i>Codice documento</i> <b>MO.PEC.00.00</b>	<i>Data di emissione</i> <b>01.12.2005</b>
-------------------	--	---------------------------------	--	---

### **PARTE III**

## **Condizioni di fornitura e di utilizzo del servizio di posta elettronica certificata**

<b>IT Telecom</b>	<i>Tipo documento:</i> <b>Manuale Operativo</b>	<i>Emesso da:</i> <b>CAS</b>	<i>Codice documento</i> <b>MO.PEC.00.00</b>	<i>Data di emissione</i> <b>01.12.2005</b>
-------------------	--	---------------------------------	--	---

## **12 Condizioni di fornitura del servizio PEC di IT Telecom**

Si riportano qui di seguito le condizioni di fornitura che IT Telecom sottopone ai clienti che facciano richiesta del servizio di PEC:

**Premesso** che:

- l'erogazione del servizio di Posta Elettronica Certificata (SERVIZIO, oppure PEC) è regolata da un'apposita normativa e da specificazioni tecniche emanate dal CNIPA (Centro Nazionale per l'Informatica nella Pubblica Amministrazione);
- il SERVIZIO può essere fornito solamente da gestori del servizio iscritti nell'Elenco Pubblico dei Gestori di Posta Elettronica Certificata tenuto dal CNIPA (ELENCO PUBBLICO);
- TELECOM ITALIA S.P.A., in quanto non iscritta all'ELENCO PUBBLICO intende avvalersi per la fornitura del SERVIZIO di I.T. TELECOM S.R.L., società interamente controllata da Telecom Italia, in qualità di Gestore del servizio di posta elettronica certificata, iscritta all'ELENCO PUBBLICO.

**Tutto quanto ciò premesso**, si riportano le seguenti Condizioni di Fornitura del Servizio (CONDIZIONI), tutte da ritenersi quali condizioni essenziali dell'offerta di fornitura e specificamente accettate dal TITOLARE, la cui inosservanza dà luogo all'applicazione dell'art. 1456 c.c.

### **Articolo 1 Soggetti del SERVIZIO**

Nell'ambito del SERVIZIO si identificano i soggetti di seguito indicati:

- **TELECOM ITALIA:** soggetto che stipula il contratto di vendita del SERVIZIO nei confronti dei TITOLARI e degli UTILIZZATORI.
- **GESTORE:** IT TELECOM S.R.L. che opera in qualità di Gestore di Posta Elettronica Certificata iscritto nell'elenco pubblico CNIPA e che gestisce DOMINI di posta elettronica certificata con i relativi punti di accesso, ricezione e consegna definiti dalla normativa vigente in materia;
- **TITOLARE:** il soggetto che acquista il SERVIZIO dal GESTORE per il tramite di TELECOM ITALIA, affinché sia utilizzato dai soggetti afferenti alla propria organizzazione;
- **UTILIZZATORE:** il soggetto cui il GESTORE ha rilasciato le credenziali di accesso per l'utilizzo del SERVIZIO. Nel caso il servizio sia richiesto da un TITOLARE per uso personale, il TITOLARE e l'UTILIZZATORE coincidono;
- **MITTENTE:** l'UTILIZZATORE che si avvale del SERVIZIO del GESTORE per la trasmissione di documenti prodotti mediante strumenti informatici;
- **DESTINATARIO:** l'UTILIZZATORE che si avvale del SERVIZIO del GESTORE per la ricezione di documenti prodotti mediante strumenti informatici;

Il GESTORE può demandare attività di registrazione ed amministrazione degli UTILIZZATORI ad incaricati indicati dal TITOLARE nell'ambito della propria organizzazione (INCARICATI).

### **Articolo 2 Subappalto**

<b>IT Telecom</b>	<i>Tipo documento:</i> <b>Manuale Operativo</b>	<i>Emesso da:</i> <b>CAS</b>	<i>Codice documento</i> <b>MO.PEC.00.00</b>	<i>Data di emissione</i> <b>01.12.2005</b>
-------------------	--	---------------------------------	--	---

Il TITOLARE accetta sin d'ora che il servizio di PEC sia in tutto o in parte subappaltato al GESTORE.

### **Articolo 3 Rapporti contrattuali**

Il TITOLARE accetta di svolgere il rapporto contrattuale direttamente con il GESTORE là dove specificato, e segnatamente per le previsioni di cui agli articoli 5,6,7,8,9, 10.

### **Articolo 4 Attività e obblighi del GESTORE**

Il GESTORE fornirà il SERVIZIO conformemente a quanto stabilito dalla normativa vigente in materia, con le modalità indicate nel MANUALE OPERATIVO e secondo le presenti CONDIZIONI.

In particolare, il GESTORE assume i seguenti obblighi:

- a. assicurare l'interoperabilità del SERVIZIO con gli altri operatori iscritti nell'elenco pubblico dei gestori di PEC;
- b. assicurare l'erogazione del SERVIZIO secondo i livelli minimi di servizio previsti dalla normativa vigente.

Il GESTORE si riserva il diritto di modificare le specifiche tecniche di erogazione del SERVIZIO in base all'evoluzione tecnologica e/o normativa, rendendole note attraverso la pubblicazione nel MANUALE OPERATIVO, ove tali modifiche risultassero essere di rilevante entità o la loro pubblicazione fosse richiesta dalla normativa vigente.

### **Articolo 5 Esclusioni**

Il GESTORE non sarà in alcun modo responsabile per quanto di seguito indicato:

- danni di qualsiasi natura, diretti od indiretti, o pregiudizi da chiunque patiti per eventi derivanti da atti della Pubblica Autorità, caso fortuito, forza maggiore ovvero da altra causa non imputabile al GESTORE (quali, in via puramente esemplificativa e non esaustiva, mancato o erroneo funzionamento di reti, apparecchiature o strumenti di carattere tecnico al di fuori della sfera di controllo del GESTORE, interruzioni nella fornitura di energia elettrica, terremoti, esplosioni, incendi), esclusi i casi di dolo o colpa grave;
- danni di qualsiasi natura, diretti od indiretti, o pregiudizi da chiunque patiti nella misura in cui tali danni derivino dalla violazione di obblighi che, in virtù di quanto previsto dal MANUALE OPERATIVO ovvero dalle vigenti disposizioni di legge, incombono all'UTILIZZATORE, al MITTENTE, al DESTINATARIO, a quanti ricevono messaggi trasmessi per il tramite del SERVIZIO;
- danni di qualsiasi natura, diretti od indiretti, o pregiudizi da chiunque patiti nella misura in cui questi avrebbero potuto essere evitati o limitati dalla conoscenza delle previsioni contenute nel MANUALE OPERATIVO da parte del TITOLARE, dell'UTILIZZATORE, del MITTENTE, del DESTINATARIO, da quanti ricevono messaggi trasmessi per il tramite del SERVIZIO;
- danni di qualsiasi natura, diretti od indiretti, o pregiudizi da chiunque patiti derivanti dall'erroneo utilizzo di codici identificativi da parte dell'UTILIZZATORE;

<b>IT Telecom</b>	<i>Tipo documento:</i> <b>Manuale Operativo</b>	<i>Emesso da:</i> <b>CAS</b>	<i>Codice documento</i> <b>MO.PEC.00.00</b>	<i>Data di emissione</i> <b>01.12.2005</b>
-------------------	--	---------------------------------	--	---

- danni di qualsiasi natura, diretti od indiretti, o pregiudizi da chiunque patiti derivanti dal mancato invio o dalla mancata consegna dei messaggi ove causati da anomalie segnalate, secondo i casi, al MITTENTE o al DESTINATARIO i quali non abbiano provveduto a riscontrare la comunicazione di anomalia inviata dal GESTORE;
- danni di qualsiasi natura, diretti od indiretti, o pregiudizi da chiunque patiti derivanti da ritardi, interruzioni, errori o malfunzionamenti del SERVIZIO non imputabili al GESTORE o derivanti dall'errata utilizzazione del SERVIZIO da parte del TITOLARE o dell'UTILIZZATORE;
- danni di qualsiasi natura, diretti od indiretti, o pregiudizi da chiunque patiti derivanti dall'applicazione delle previsioni normative in merito al trattamento dei messaggi con contenuto malevolo o contenenti virus informatici;
- danni di qualsiasi natura, diretti od indiretti, o pregiudizi da chiunque patiti al di fuori dei livelli minimi di servizio previsti dalla normativa vigente;
- danni di qualsiasi natura, diretti od indiretti, o pregiudizi da chiunque patiti derivanti dall'impiego del SERVIZIO al di fuori delle previsioni normative vigenti o dall'utilizzo di servizi di posta elettronica forniti da gestori non inclusi nell'elenco pubblico tenuta dal CNIPA.

I messaggi di posta elettronica possono subire dei ritardi nella loro trasmissione via Internet, pertanto il GESTORE non assume alcuna responsabilità, salvo eventuale dolo o colpa grave, per detti ritardi.

Il GESTORE è esonerato da ogni potere di controllo, di mediazione o di vigilanza sul contenuto dei messaggi inviati dagli UTILIZZATORI e non assume nessuna responsabilità riguardo al loro contenuto illecito o contrario alla morale o all'ordine pubblico, non sussistendo alcun obbligo di cancellazione in capo al GESTORE in merito alla cancellazione del contenuto dei messaggi.

Il GESTORE non assume nessun obbligo, garanzia o responsabilità ulteriori rispetto a quelle scaturenti dal contratto di fornitura del SERVIZIO per il tramite di Telecom Italia e dalla normativa vigente.

Il danneggiato decade dal diritto al risarcimento dei danni imputabili al GESTORE qualora non ne faccia motivata denuncia scritta al GESTORE entro il termine di 10 giorni dal verificarsi dell'evento dannoso.

La responsabilità del GESTORE non può in ogni caso essere superiore all'ammontare del corrispettivo del SERVIZIO pagato dal TITOLARE.

### **Articolo 6 Obblighi del TITOLARE**

Con l'accettazione di quanto stabilito in queste Condizioni di Fornitura il TITOLARE assume gli obblighi seguenti:

- a. consultare preventivamente il MANUALE OPERATIVO e conoscerne i contenuti;
- b. fornire tutte le informazioni e la documentazione richieste dal GESTORE, necessarie ad una corretta identificazione personale garantendone, sotto la propria responsabilità, l'attendibilità ai sensi del DPR n. 68/2005 e successive modifiche ed integrazioni;

<b>IT Telecom</b>	<i>Tipo documento:</i> <b>Manuale Operativo</b>	<i>Emesso da:</i> <b>CAS</b>	<i>Codice documento</i> <b>MO.PEC.00.00</b>	<i>Data di emissione</i> <b>01.12.2005</b>
-------------------	--	---------------------------------	--	---

- c. informare espressamente gli UTILIZZATORI riguardo agli obblighi da questi assunti in merito all'uso del SERVIZIO;
- d. ove richiesto, prestare il consenso al trattamento dei dati personali ai sensi del D.Lgs. n. 196 del 2003;
- e. conservare e far conservare agli UTILIZZATORI con la massima riservatezza e diligenza i codici di accesso al SERVIZIO;
- f. informare immediatamente il GESTORE in caso risulti compromessa la riservatezza dei codici di accesso per l'utilizzo del SERVIZIO.

Per quanto concerne l'attività degli INCARICATI, il TITOLARE garantisce che l'INCARICATO si atterrà alle procedure comunicate dal GESTORE ed indicate nel MANUALE OPERATIVO.

Il TITOLARE prende atto che alla scadenza del contratto o in caso di sua risoluzione, non sarà più possibile accedere al SERVIZIO ed al suo contenuto, pertanto si impegna a darne informativa agli UTILIZZATORI, sollevando il GESTORE da ogni responsabilità derivante dal mancato accesso.

#### **Articolo 7 Obblighi dell'UTILIZZATORE**

L'UTILIZZATORE, al momento della firma della documentazione di abilitazione all'uso del SERVIZIO assume i seguenti obblighi:

- a. consultare preventivamente il MANUALE OPERATIVO e conoscerne i contenuti;
- b. attenersi alle modalità di utilizzo del SERVIZIO indicate dal GESTORE nella guida all'utilizzo del SERVIZIO, pubblicata sul sito web del SERVIZIO;
- c. conservare con la massima riservatezza e diligenza i codici di accesso al SERVIZIO, obbligandosi a non cederli a terzi a nessun titolo ed impedendone ad essi l'utilizzo;
- d. informare immediatamente il TITOLARE in caso risulti compromessa la riservatezza dei codici di accesso per l'utilizzo del SERVIZIO.

#### **Articolo 8 Obblighi del TITOLARE e dell'UTILIZZATORE**

Il TITOLARE, e l'UTILIZZATORE al momento della firma della documentazione di abilitazione all'uso del SERVIZIO, assumono i seguenti obblighi:

- a. non utilizzare né a permettere a terzi di utilizzare il SERVIZIO per fini illeciti o per effettuare comunicazioni contrarie alla Legge, alla morale o all'ordine pubblico;
- b. non utilizzare il SERVIZIO con lo scopo di depositare, inviare, pubblicare, trasmettere e/o condividere applicazioni o documenti informatici che siano in contrasto o violino diritti di proprietà intellettuale, segreti commerciali, marchi, brevetti o altri diritti di proprietà di terzi;
- c. non consentire a terzi non autorizzati dal TITOLARE l'uso del SERVIZIO, di cui sarà comunque responsabile il TITOLARE.

#### **Articolo 9 Cessione**

<b>IT Telecom</b>	<i>Tipo documento:</i> <b>Manuale Operativo</b>	<i>Emesso da:</i> <b>CAS</b>	<i>Codice documento</i> <b>MO.PEC.00.00</b>	<i>Data di emissione</i> <b>01.12.2005</b>
-------------------	--	---------------------------------	--	---

Il TITOLARE non potrà cedere a terzi in tutto o in parte il SERVIZIO regolato dalle presenti CONDIZIONI, senza la preventiva autorizzazione scritta di Telecom Italia e/o del GESTORE.

### **Articolo 10 Responsabilità del TITOLARE**

Fatte salve le previsioni della normativa vigente, costituisce specifica responsabilità contrattuale del TITOLARE l'erronea o parziale indicazione da parte dell'UTILIZZATORE di dati rilevanti per l'attività, specificatamente riportati nell'Articolo 6 e nell'Articolo 7.

Pertanto il TITOLARE manleva il GESTORE da ogni responsabilità, spesa, danno o pregiudizio, diretto od indiretto, di cui il GESTORE fosse chiamato a rispondere nei confronti di terzi per fatto riconducibile alla erronea o parziale indicazione dei dati rilevanti di cui al comma precedente.

Inoltre il TITOLARE manleva il GESTORE da ogni responsabilità, spesa, danno o pregiudizio, diretto od indiretto, di cui il GESTORE fosse chiamato a rispondere nei confronti di terzi per fatto imputabile al TITOLARE o all'UTILIZZATORE in relazione all'uso del SERVIZIO.

### **Articolo 11 Rinvio al Manuale Operativo**

Per quanto non espressamente indicato negli articoli precedenti in tema di attività ed obblighi, si rinvia a quanto dispone il MANUALE OPERATIVO, che costituisce parte integrante e sostanziale del presente allegato.

### **Articolo 12 Foro Competente**

Per ogni e qualsiasi controversia relativa all'esecuzione o interpretazione del contratto di fornitura del servizio è competente in via esclusiva il foro di Roma.

## **13 Obblighi, Responsabilità e Indennizzi**

Questo capitolo definisce gli obblighi e le relative responsabilità del Gestore e del Richiedente/Titolare, nonché le eventuali limitazioni agli indennizzi che possono essere richiesti al Gestore.

Per ciò che non è espressamente stabilito nel presente capitolo, varrà, in relazione a ciascuno dei soggetti di volta in volta coinvolti, quanto previsto dalle disposizioni normative applicabili e, in particolare, dal DPR 68/05, dal DM 2/11/05, dal TUDA nonché dal DPCM 2004 e loro eventuali successive modificazioni ed integrazioni.

### **13.1 Obblighi del Gestore**

Il Gestore è tenuto ad attenersi a quanto stabilito dal DPR 68/05, dal DM 2/11/05 e, ove applicabili, dal TUDA e dal DPCM 2004 e alle altre normative vigenti in materia. In particolare:

- assicurare il livello minimo di servizio previsto dall'art. 12, comma 2 del DM 2/11/05 ;

<b>IT Telecom</b>	<i>Tipo documento:</i> <b>Manuale Operativo</b>	<i>Emesso da:</i> <b>CAS</b>	<i>Codice documento</i> <b>MO.PEC.00.00</b>	<i>Data di emissione</i> <b>01.12.2005</b>
-------------------	--	---------------------------------	--	---

- prevedere l'esistenza di servizi di emergenza che, in ogni caso, assicurino il completamento della trasmissione ed il rilascio delle ricevute (art. 11, comma 4 del DPR 68/05);
- descrivere nel presente Manuale Operativo le soluzioni tecniche ed organizzative che realizzano i servizi di emergenza, di cui al punto precedente, e consentano il rispetto dei vincoli definiti nell'art. 12 commi 4 e 5 del DM 2/11/05;
- assicurare l'interoperabilità dei servizi offerti, nel caso in cui la trasmissione del messaggio di posta elettronica certificata avvenga tra diversi gestori (art. 5, comma 2 del DPR 68/05 e art. 8, comma 1 del DM 2/11/05);
- segnalare al destinatario, in qualità di gestore del destinatario medesimo, se la posta elettronica in arrivo non è qualificabile come posta elettronica certificata secondo quanto prescritto dal DPR 68/05 e dall'art. 14, comma 1 del DM 2/11/05.

### 13.1.1 Polizza assicurativa

Il Gestore, nell'ambito della sua attività di Certificatore della Firma Digitale è dotato di polizza assicurativa a copertura dei rischi dell'attività e dei danni causati a terzi (art. 14, comma 6, lett. j del DPR 68/05). Tale polizza di assicurazione è estesa anche alle attività di esercizio della PEC, con le seguenti caratteristiche:

<b>Tipo di Risarcimento</b>	<b>Massimale annuo</b>	<b>Massimale per singolo sinistro</b>
Risarcimento di danni patrimoniali cagionati a Terzi in conseguenza di: <ul style="list-style-type: none"> <li>• fatto accidentale verificatosi in relazione allo svolgimento dell'attività di gestione della posta elettronica certificata ai sensi del DPR 68/2005</li> <li>• fatto doloso dei dipendenti addetti alla stessa attività</li> </ul>	€ 1.500.000,00	€ 1.500.000,00
Risarcimento per danni conseguenti alla diffusione di dati personali della persona fisica, giuridica, ente o associazione, che sia avvenuta involontariamente o per infedeltà del personale autorizzato, dipendente o non, dal Gestore	€ 500.000,00	€ 500.000,00

## 13.2 Obblighi del titolare

Il privato che intende avvalersi del servizio di posta elettronica certificata (titolare) deve:

<b>IT Telecom</b>	<i>Tipo documento:</i> <b>Manuale Operativo</b>	<i>Emesso da:</i> <b>CAS</b>	<i>Codice documento</i> <b>MO.PEC.00.00</b>	<i>Data di emissione</i> <b>01.12.2005</b>
-------------------	--	---------------------------------	--	---

- dichiarare espressamente e con chiarezza la propria volontà di utilizzare la posta elettronica certificata relativamente ad un procedimento con una pubblica amministrazione o ad un singolo rapporto intrattenuto con un altro soggetto privato (art. 5, comma 1 del DM 2/11/05 e art. 4, comma 4 del DPR 68/05);
- la dichiarazione di cui al punto precedente può essere resa (art. 5, comma 2, lett. a del DM 2/11/05) mediante l'utilizzo di strumenti informatici, nel qual caso la dichiarazione deve essere sottoscritta con la firma digitale di cui all'art. 1, comma 1, lettera n del TUDA, oppure (art. 5, comma 2, lett. b del DM 2/11/05) in calce ad un'istanza o dichiarazione concernente lo specifico procedimento o rapporto; nei rapporti con la pubblica amministrazione si applica l'articolo 38 del TUDA;
- rendere la dichiarazione di cui al primo punto anche nei casi di variazione dell'indirizzo di posta elettronica certificata o di cessazione della volontà di avvalersi della posta elettronica certificata medesima (art. 5, comma 3 del DM 2/11/05);
- consultare preventivamente il presente Manuale Operativo e conoscerne i contenuti. Il Gestore non sarà responsabile di eventuali danni o pregiudizi nella misura in cui tali danni e pregiudizi avrebbero potuto essere evitati o limitati dalla conoscenza delle previsioni contenute nel presente Manuale.

### **13.3 Definizione delle responsabilità e delle limitazioni agli indennizzi**

Nel presente paragrafo sono individuate sia le limitazioni della responsabilità assunta dal Gestore nell'ambito delle situazioni giuridiche relative allo svolgimento della propria attività, sia i correlati indennizzi, ferme restando le specifiche previsioni di cui ai precedenti paragrafi.

Il Gestore non è in alcun modo responsabile per quanto di seguito indicato:

- danni di qualsiasi natura, diretti od indiretti, da chiunque patiti per eventi derivanti da **atti della Pubblica Autorità, caso fortuito, forza maggiore** ovvero da altra **causa non imputabile al Gestore** (quali, in via puramente esemplificativa e non esaustiva, mancato o erroneo funzionamento di reti, apparecchiature o strumenti di carattere tecnico al di fuori della sfera di controllo del Gestore, interruzioni nella fornitura di energia elettrica, terremoti, esplosioni, incendi).
- danni di qualsiasi natura, diretti od indiretti, se non nei casi di **proprio dolo o colpa grave**.
- danni di qualsiasi natura, diretti od indiretti, da chiunque patiti nella misura in cui tali danni derivino dalla **violazione di obblighi** che, in virtù di quanto previsto dal presente Manuale Operativo ovvero dalle vigenti disposizioni di legge, incombono al titolare.

Il danneggiato decade dal diritto al risarcimento dei danni imputabili al Gestore qualora non ne faccia motivata denuncia scritta al Gestore entro il termine di 10 giorni dal verificarsi dell'evento dannoso.

<b>IT Telecom</b>	<i>Tipo documento:</i> <b>Manuale Operativo</b>	<i>Emesso da:</i> <b>CAS</b>	<i>Codice documento</i> <b>MO.PEC.00.00</b>	<i>Data di emissione</i> <b>01.12.2005</b>
-------------------	--	---------------------------------	--	---

Il Gestore non assume alcun ulteriore obbligo, garanzia e responsabilità rispetto a quelli previsti dal presente Manuale Operativo o dalle vigenti disposizioni normative.

### **13.4 Manleva del titolare**

---

Il **titolare** manleva il Gestore da ogni responsabilità, spesa, danno o pregiudizio, diretto od indiretto, di cui il Gestore sia chiamato a rispondere nei confronti di terzi per fatti imputabili al titolare.

<b>IT Telecom</b>	<i>Tipo documento:</i> <b>Manuale Operativo</b>	<i>Emesso da:</i> <b>CAS</b>	<i>Codice documento</i> <b>MO.PEC.00.00</b>	<i>Data di emissione</i> <b>01.12.2005</b>
-------------------	--	---------------------------------	--	---

## **PARTE IV**

### **Procedura di attivazione del servizio di PEC**

<b>IT Telecom</b>	<i>Tipo documento:</i> <b>Manuale Operativo</b>	<i>Emesso da:</i> <b>CAS</b>	<i>Codice documento</i> <b>MO.PEC.00.00</b>	<i>Data di emissione</i> <b>01.12.2005</b>
-------------------	--	---------------------------------	--	---

## 14 Procedura di attivazione

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

1. firma del contratto di fornitura fra il Titolare e Telecom Italia;
2. accettazione da parte del Titolare delle condizioni di fornitura del servizio IT Telecom e sottoscrizione della Scheda di Attivazione del Titolare (Modulo di adesione al servizio di PEC);
3. indicazione, da parte del Titolare, se intende utilizzare un dominio internet da adibire a dominio di posta certificata (un preesistente dominio attivo di posta convenzionale può anche essere adibito a dominio di posta certificata solo e soltanto con la perdita di tutte le caselle attestata su di esso);
4. registrazione ed attivazione del Richiedente;
5. attivazione delle caselle di PEC.

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

<b>Titolare</b>	Il soggetto che richiede l'attivazione del servizio di PEC a beneficio dei propri utilizzatori
<b>Utilizzatore</b>	Il soggetto per il quale viene attivata l'utenza di PEC.
<b>Incaricato alla gestione ed amministrazione degli utilizzatori</b>	La persona della struttura del Titolare che effettua: <ul style="list-style-type: none"> <li>• la registrazione degli utilizzatori collegandosi ad un portale applicativo raggiungibile attraverso Internet;</li> <li>• l'attivazione delle utenze di PEC per gli utilizzatori.</li> </ul>

**Attivazione del Titolare.** Una volta sottoscritto il contratto, il Titolare individua i propri referenti interni che agiranno in qualità di Incaricati per la gestione e l'amministrazione degli utenti e comunica i loro nominativi a IT Telecom inviandogli il **"Modulo di Adesione al servizio di PEC"**. Ricevuto tale modulo, IT Telecom verifica i dati per l'attivazione del cliente sulla piattaforma PEC, informa il Titolare e, tramite mail, invia agli Incaricati individuati:

- i **codici di accesso al Portale PKI**, per la registrazione dei dati degli utilizzatori del servizio di PEC da parte dell'Incaricato;
- Il **Manuale dell'Incaricato PEC**, per l'attivazione delle caselle da associare agli utenti.

**Registrazione degli utilizzatori e attivazione delle caselle.** L'Incaricato accede al portale PKI ed inserisce i dati degli utilizzatori, per i quali vengono automaticamente attivate le caselle di PEC associate.

<b>IT Telecom</b>	<i>Tipo documento:</i> <b>Manuale Operativo</b>	<i>Emesso da:</i> <b>CAS</b>	<i>Codice documento</i> <b>MO.PEC.00.00</b>	<i>Data di emissione</i> <b>01.12.2005</b>
-------------------	--	---------------------------------	--	---

<p style="text-align: center;"><b>PARTE V</b></p> <p style="text-align: center;"><b>Protezione dei Dati</b></p>
---

<b>IT Telecom</b>	<i>Tipo documento:</i> <b>Manuale Operativo</b>	<i>Emesso da:</i> <b>CAS</b>	<i>Codice documento</i> <b>MO.PEC.00.00</b>	<i>Data di emissione</i> <b>01.12.2005</b>
-------------------	--	---------------------------------	--	---

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

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

- i dipendenti che hanno ricevuto la nomina di incaricati ai sensi dell'art. 30 del DLgs 196/03, hanno ricevuto dettagliate istruzioni circa le modalità e le misure di sicurezza da adottare per il trattamento dei dati personali.
- il trattamento dei dati personali avviene sotto la supervisione di responsabili del trattamento, anch'essi formalmente nominati, i quali hanno a loro volta ricevuto le necessarie istruzioni ed indicazioni operative.
- apposite funzioni aziendali hanno il compito di definire le policy per la sicurezza delle informazioni e di verificare, con l'ausilio di funzioni di auditing interno, che esse siano effettivamente applicate.
- il sistema di policy si basa sulla corretta classificazione degli asset. Con l'ausilio di strumenti di risk assessment, sono individuate le misure di sicurezza più idonee alla tutela dei singoli asset, alla definizione dei controlli e all'applicazione dei sistemi di monitoraggio e verifica più appropriati.
- la tutela dei dati personali non si configura come un processo indipendente, ma risulta del tutto integrato nella gestione corrente della sicurezza degli asset aziendali.
- le politiche di sicurezza fisica e di tutela del patrimonio materiale dell'azienda e le politiche di gestione degli incidenti di sicurezza e delle crisi sono definite tenendo presenti i principi di tutela dei dati personali e le necessità di protezione di questi dati fissate dalla legge.

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

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

<b>IT Telecom</b>	<i>Tipo documento:</i> <b>Manuale Operativo</b>	<i>Emesso da:</i> <b>CAS</b>	<i>Codice documento</i> <b>MO.PEC.00.00</b>	<i>Data di emissione</i> <b>01.12.2005</b>
-------------------	--	---------------------------------	--	---

## 15 Modalità di Protezione dei Dati

Il presente capitolo del Manuale Operativo ha lo scopo di illustrare le procedure e le modalità operative adottate dal Gestore per il trattamento dei dati personali, nello svolgimento della propria attività di gestore del servizio di PEC.

I dati personali sono trattati, conservati e protetti dal Gestore conformemente a quanto previsto dal **Decreto legislativo n. 196 del 30 giugno 2003** "Codice in materia di protezione dei dati personali", pubblicato sul Supplemento ordinario n. 123 della G.U. n. 174 del 29 luglio 2003 e successive integrazioni e modificazioni.

La terminologia utilizzata nel presente capitolo è conforme a quella adottata dal DLgs 196/03, e parzialmente difforme da quella utilizzata nel TUDA e dal DPCM 2004. In particolare:

- a) per **Titolare**, si intende la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione o organismo cui competono le decisioni in ordine alle finalità ed alle modalità del trattamento di dati personali, ivi compreso il profilo della sicurezza (ovvero il Gestore);
- b) per **Responsabile** si intende la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal Titolare al trattamento di dati personali;
- c) per **Incaricato** si intende la persona fisica autorizzata a compiere operazioni di trattamento dal titolare o dal responsabile;
- d) per **"Interessato"**, si intende la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali.

In particolare, il Gestore, in qualità di Titolare ai sensi del DLgs 196/03:

- nomina, se del caso, un **Responsabile del trattamento dei dati**, individuandolo all'interno dell'organizzazione aziendale e comunicandogli analiticamente e per iscritto i compiti che dovrà assolvere, ai sensi dell'Art. 29 del DLgs 196/03;
- individua e nomina gli Incaricati del trattamento dei dati (ovvero gli Incaricati della gestione e dell'amministrazione dell'utenza e quanti altri tratteranno i dati attinenti il servizio), che operano sotto la diretta autorità del Cliente<sup>4</sup> o del Responsabile del Servizio<sup>5</sup> attenendosi alle istruzioni impartite, ai sensi dell'Art. 30 del DLgs 196/03;
- nomina eventuali **Responsabili esterni per il trattamento dei dati** specificando analiticamente i compiti per iscritto ed effettua, anche tramite verifiche periodiche, controlli sulla puntuale osservanza delle disposizioni di legge e delle proprie istruzioni.

<sup>4</sup> Il soggetto che richiede l'attivazione del servizio di PEC a beneficio dei propri utilizzatori.

<sup>5</sup> Il soggetto identificato come tale ai fini dell'attuazione del DLgs 196/03 nell'ambito dell'organizzazione del Gestore.

<b>IT Telecom</b>	<i>Tipo documento:</i> <b>Manuale Operativo</b>	<i>Emesso da:</i> <b>CAS</b>	<i>Codice documento</i> <b>MO.PEC.00.00</b>	<i>Data di emissione</i> <b>01.12.2005</b>
-------------------	--	---------------------------------	--	---

## **15.1 Definizione e identificazione di “Dati personali”**

Ai sensi dell’Art. 4, comma 2, lett. b) del DLgs 196/03, per *dato personale* si intende “qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale”; pertanto sono dati personali anche i codici identificativi forniti dal Gestore e i PIN.

Dati personali potranno inoltre essere quelli relativi all’utente ovvero ad eventuali terzi e contenuti nei campi informativi presenti sui moduli e negli archivi, elettronici o cartacei, di cui ai relativi capitoli del presente Manuale Operativo. Al fine di garantirne un trattamento adeguato, le misure di sicurezza predisposte dal Gestore e analiticamente descritte nel Piano per la Sicurezza, sono realizzate conformemente a quanto previsto dal DLgs 196/03.

## **15.2 Tutela e diritti degli interessati**

In materia di trattamento dei dati personali il Gestore garantisce la tutela degli interessati in ottemperanza al DLgs 196/03. In particolare:

- agli interessati sono fornite le necessarie informazioni ai sensi dell’Art. 13 (quali ad esempio il titolare, le modalità e finalità del trattamento, l’ambito di comunicazione e di diffusione, nonché i diritti di accesso ai suoi dati ai sensi dell’Art. 7);
- agli interessati viene richiesto, laddove necessario, il consenso scritto al trattamento dei propri dati personali.

## **15.3 Applicazione del Codice per la protezione dei dati personali**

### **15.3.1 Adempimenti generali**

Dal punto di vista generale il Gestore, in qualità di Titolare ai sensi del DLgs 196/03:

- predispone, conserva e aggiorna, nell’ambito delle attività di gestione del servizio di PEC, *archivi informatici e cartacei* contenenti dati personali, incorporati nelle Banche Dati del Titolare e utilizzati nella gestione di tutte le fasi del servizio;
- definisce e aggiornai compiti dei suoi incaricati in relazione al trattamento degli archivi suddetti, in conformità con le misure minime di sicurezza previste dal DLgs 196/03 (Parte I, Titolo V, capi I e II) e riportate nel Piano per la Sicurezza, nonché con le policy aziendali in materia di sicurezza e di tutela della riservatezza dei dati.

### **15.3.2 Adempimenti tecnici ed organizzativi**

Dal punto di vista tecnico il Gestore, (il Responsabile se nominato) tramite i suoi incaricati, adotta gli opportuni provvedimenti in relazione alla registrazione, elaborazione, conservazione, protezione dei dati personali, cancellazione/distruzione, secondo le modalità indicate qui di seguito.

<b>IT Telecom</b>	<i>Tipo documento:</i> <b>Manuale Operativo</b>	<i>Emesso da:</i> <b>CAS</b>	<i>Codice documento</i> <b>MO.PEC.00.00</b>	<i>Data di emissione</i> <b>01.12.2005</b>
-------------------	--	---------------------------------	--	---

### **15.3.2.1 Registrazione**

- garantisce la conservazione dei dati tecnici relativi a struttura e formato degli archivi informatici e cartacei contenenti dati personali, nonché alla loro locazione fisica;
- supervisiona l'organizzazione e classificazione in maniera univoca degli archivi, nonché delle loro copie di sicurezza (backup) curando di ridurre al minimo indispensabile le copie, totali o parziali, di ciascun archivio secondo le modalità descritte nel Piano per la Sicurezza del Gestore.
- supervisiona l'organizzazione e classificazione in maniera univoca della modulistica relativa al servizio contenente dati personali, curando di ridurre al minimo indispensabile le copie, totali o parziali, di ciascun archivio secondo le modalità descritte nel Piano per la Sicurezza del Gestore.

### **15.3.2.2 Elaborazione**

- controlla che l'elaborazione dei suddetti archivi e dei dati personali in essi contenuti sia effettuata esclusivamente per le finalità indicate nell'informativa resa ai sensi dell'Art. 13 del DLgs 196/03;
- verifica, in funzione del tipo di elaborazione, i formati di output e la destinazione finale dei dati al fine di garantirne la protezione, secondo quanto previsto nel seguito;
- rileva l'eventuale generazione di nuovi archivi nell'ambito delle fasi di elaborazione, supervisionando la loro classificazione.

### **15.3.2.3 Conservazione**

- supervisiona la classificazione degli eventuali archivi – e dei dati in essi contenuti - soggetti a pura e semplice conservazione (archivi storici e/o di backup), riportando la durata della conservazione (inclusa data iniziale e finale), la natura del supporto e la sede di conservazione;
- si assicura che siano trattati come archivi di conservazione dei dati personali tutti gli archivi appartenenti a procedure temporaneamente bloccate o sospese;
- verifica che le procedure di conservazione di tutti i documenti utilizzati nell'ambito del servizio di PEC siano coerenti con la tutela dei dati personali, nel rispetto di quanto disposto in tema di conservazione dalla normativa specifica del servizio.

### **15.3.2.4 Cancellazione/Distruzione**

- verifica la registrazione - eventualmente in maniera automatizzata - della cancellazione/distruzione di singoli dati personali dagli archivi, riportando la tipologia dei dati, l'archivio interessato, la data di cancellazione/distruzione, nonché l'origine della cancellazione/distruzione (su richiesta dell'interessato, procedurale, accidentale, ecc.);
- verifica la registrazione della cancellazione/distruzione di archivi interi, secondo le modalità illustrate al punto precedente ed in conformità a quanto previsto dal DLgs 196/03, curando inoltre l'aggiornamento degli *archivi informatici e cartacei*.

<b>IT Telecom</b>	<i>Tipo documento:</i> <b>Manuale Operativo</b>	<i>Emesso da:</i> <b>CAS</b>	<i>Codice documento</i> <b>MO.PEC.00.00</b>	<i>Data di emissione</i> <b>01.12.2005</b>
-------------------	--	---------------------------------	--	---

### **15.3.2.5 Protezione**

- protegge la confidenzialità dei dati personali stabilendo le modalità di accesso agli archivi informatici e cartacei da parte dei soggetti abilitati appartenenti all'organizzazione del Gestore. In particolare:
  - ✓ classifica i soggetti abilitati all'accesso in funzione delle loro mansioni. In particolare, si precisa che il Gestore ha definito ed attua specifiche policy di gestione delle credenziali di autenticazione e per la costruzione e l'utilizzo delle password
  - ✓ registra le modalità di protezione dei dati, sia per quanto concerne la sicurezza logica degli archivi informatici (software di sicurezza, modalità di generazione del log delle elaborazioni, ecc.) che fisica (vigilanza dei locali, archiviazione documenti, gestione delle copie di sicurezza);
  - ✓ assicura la confidenzialità dei dati personali contenuti nei diversi formati di output delle fasi di elaborazione (cartacei, su terminale, ecc.) stabilendo le modalità operative necessarie, sia manuali che automatizzate;
  - ✓ supervisiona la circolazione interna delle informazioni contenute negli stampati (tabulati) o in altri supporti;
  - ✓ assicura la distribuzione degli output su terminale in accordo con i profili utente designati dal responsabile della sicurezza;
- protegge l'integrità dei dati singolarmente considerati e degli archivi nel loro insieme, durante tutte le fasi di trattamento, stabilendo le modalità operative necessarie, sia manuali che automatizzate;
- garantisce la disponibilità dei dati, affinché il titolare possa adempiere alle richieste di consultazione/verifica da parte degli interessati previste dalla normativa vigente.

## **15.4 Circostanze di comunicazione di dati personali**

Fermo restando il diritto dell'interessato di richiedere ed ottenere dal Gestore informazioni relative ai propri dati personali, secondo quanto previsto dall'Art. 7 del DLgs 196/03, il Gestore, nello svolgimento delle proprie attività relative al servizio di PEC, può effettuare operazioni di comunicazione dei dati personali.

In particolare:

- i dati personali possono essere comunicati all'Autorità Giudiziaria, in conformità con quanto previsto dalla normativa vigente;
- particolari accordi contrattuali possono prevedere destinatari e forme di comunicazione ulteriori rispetto a quanto previsto dal TUDA e dal DPCM 2004. Tali comunicazioni avverranno comunque nel rispetto della normativa vigente.