



**MANUALE OPERATIVO  
DEL SERVIZIO DI POSTA ELETTRONICA CERTIFICATA  
AI SENSI DEL D.P.R. N. 68/2005**

Compilato : GIS – P. Iorio

Rivisto : DZA – S. Acanfora  
DZF – G. Gasbarrini  
DZS – F. Gerbino

Approvato : AD – M. Bonamico

Versione : 04

## INDICE

<b>1. INTRODUZIONE</b> .....	<b>6</b>
<b>1.1 SCOPO</b> .....	<b>6</b>
<b>1.2 CAMPO DI VALIDITÀ</b> .....	<b>6</b>
<b>1.3 PROPRIETÀ INTELLETTUALE</b> .....	<b>6</b>
<b>1.4 CORRISPONDENZA CIRC. CNIPA/49/2005 – MANUALE OPERATIVO</b> .....	<b>7</b>
<b>2. DATI DEL GESTORE</b> .....	<b>8</b>
<b>2.1 DATI IDENTIFICATIVI</b> .....	<b>8</b>
<b>2.2 RESPONSABILE DEL MANUALE OPERATIVO</b> .....	<b>8</b>
<b>3. RIFERIMENTI</b> .....	<b>9</b>
<b>3.1 RIFERIMENTI NORMATIVI</b> .....	<b>9</b>
<b>3.2 RIFERIMENTI TECNICI</b> .....	<b>10</b>
<b>4. DEFINIZIONI E ACRONIMI</b> .....	<b>12</b>
<b>4.1 DEFINIZIONI</b> .....	<b>12</b>
<b>4.2 ACRONIMI</b> .....	<b>21</b>
<b>5. DATI DEL MANUALE OPERATIVO</b> .....	<b>22</b>
<b>5.1 VERSIONE</b> .....	<b>22</b>
<b>5.2 INDIRIZZO INTERNET</b> .....	<b>22</b>
<b>6. SERVIZIO OFFERTO</b> .....	<b>23</b>
<b>6.1 DESCRIZIONE SINTETICA DEL SERVIZIO DI PEC COME DA NORMATIVA IN VIGORE</b>	<b>23</b>

<b>7. SERVIZIO OFFERTO DAL GESTORE .....</b>	<b>26</b>
<b>7.1 SERVIZI DI REGISTRAZIONE TITOLARI.....</b>	<b>26</b>
<b>7.2 MODALITÀ DI GESTIONE DELLE CASELLE .....</b>	<b>27</b>
<b>7.2.1 ASSEGNAZIONE DELLE CASELLE AGLI UTENTI TITOLARI .....</b>	<b>28</b>
<b>7.2.2 DISATTIVAZIONE DELLE CASELLE DI PEC.....</b>	<b>28</b>
<b>7.2.3 RIATTIVAZIONE DI UNA CASELLA DI PEC DISATTIVATA .....</b>	<b>28</b>
<b>7.2.4 REVOCA DI UNA CASELLA DI PEC .....</b>	<b>29</b>
<b>7.2.5 RIASSEGNAZIONE DI CASELLE DI PEC.....</b>	<b>29</b>
<b>7.2.6 INFORMAZIONI AL TITOLARE.....</b>	<b>29</b>
<b>7.3 FORMATO DELLE RICEVUTE DEL GESTORE .....</b>	<b>30</b>
<b>8. MODALITÀ DI ACCESSO AL SERVIZIO E NORME DI UTILIZZO.....</b>	<b>31</b>
<b>8.1 ATTIVAZIONE E ACQUISIZIONE DEL SERVIZIO.....</b>	<b>31</b>
<b>8.1.1 CREDENZIALI UTENTI TITOLARI .....</b>	<b>31</b>
<b>8.1.2 CREDENZIALI AMMINISTRATORI DEI TITOLARI .....</b>	<b>32</b>
<b>8.1.3 PRIMO ACCESSO ALLA CASELLA DI PEC .....</b>	<b>32</b>
<b>8.1.4 GESTIONE DELLE CREDENZIALI .....</b>	<b>32</b>
<b>8.1.5 RACCOMANDAZIONI DI UTILIZZO .....</b>	<b>33</b>
<b>9. MODALITÀ DELL'OFFERTA .....</b>	<b>35</b>
<b>9.1 CONTRAENTE PRIVATO .....</b>	<b>35</b>
<b>9.2 CONTRAENTE ORGANIZZAZIONE .....</b>	<b>35</b>
<b>9.3 ACCORDO DI SERVIZIO.....</b>	<b>35</b>
<b>9.3.1 DOMINI DI PEC DEI CLIENTI .....</b>	<b>36</b>
<b>10. MODALITÀ DI REPERIMENTO DEL LOG.....</b>	<b>38</b>
<b>11. LIVELLI DI SERVIZIO E INDICATORI DI QUALITÀ .....</b>	<b>39</b>

11.1	CONDIZIONI NORMALI DI FUNZIONAMENTO .....	39
11.2	SERVIZI DI EMERGENZA .....	40
11.3	OPERAZIONI IN CASO DI DISASTRO.....	40
11.4	INDICATORI DI QUALITÀ.....	41
11.5	INTEROPERABILITÀ CON GLI ALTRI GESTORI DI PEC.....	41
12.	MODALITÀ PER L'APPOSIZIONE E LA DEFINIZIONE DEL RIFERIMENTO TEMPORALE .....	42
13.	CONDIZIONI DI FORNITURA DEL SERVIZIO.....	43
14.	MODALITÀ DI PROTEZIONE DEI DATI DEI TITOLARI .....	44
15.	OBBLIGHI.....	45
15.1	OBBLIGHI DEL GESTORE .....	45
15.2	OBBLIGHI DEL TITOLARE .....	48
15.3	OBBLIGHI DELL'ORGANIZZAZIONE CUI FANNO CAPO I TITOLARI .....	49
15.4	RESPONSABILITÀ DEL GESTORE .....	49
15.5	ASSICURAZIONE .....	50
15.6	LIMITAZIONI DELLE RESPONSABILITÀ .....	50
16.	DESCRIZIONE SINTENTICA PROCEDURE ADOTTATE .....	51
16.1	CARATTERISTICHE DI SICUREZZA .....	51
16.2	SINTESI DELLE PROCEDURE PRINCIPALI .....	52
16.2.1	INSTALLAZIONE DELLE APPARECCHIATURE .....	52
16.2.2	CAPACITY PLANNING.....	52
16.2.3	GENERAZIONE DELLE CHIAVI DI FIRMA, LORO GESTIONE.....	52
16.2.4	GESTIONE DEI DISPOSITIVI DI FIRMA.....	54

<b>16.2.5</b>	<b>PROTEZIONE DEI MESSAGGI DI PEC.....</b>	<b>54</b>
<b>16.2.6</b>	<b>UTILIZZO IGPEC.....</b>	<b>54</b>
<b>16.2.7</b>	<b>GESTIONE DEL LOG DI PEC.....</b>	<b>55</b>
<b>16.2.8</b>	<b>ADDESTRAMENTO DEL PERSONALE.....</b>	<b>55</b>
<b>16.2.9</b>	<b>CESSAZIONE DELLE OPERAZIONI.....</b>	<b>56</b>

## **1. INTRODUZIONE**

### **1.1 SCOPO**

Il presente documento è il Manuale Operativo nel quale sono descritte le procedure applicate da SOGEI s.p.a. (d'ora innanzi Gestore) per offrire il servizio di posta elettronica certificata, in conformità con quanto previsto dal decreto del Presidente della Repubblica 11 febbraio 2005, n. 68 [6] e con i relativi dispositivi giuridici attuativi.

Tale documento è depositato presso il Centro Nazionale per l'Informatica e la Pubblica Amministrazione (d'ora innanzi CNIPA) ed è pubblicato all'indirizzo indicato nel paragrafo § 5.2, ove è consultabile per via telematica. Esso è conforme con:

- l'articolo 23 del decreto del Ministro per l'innovazione e la tecnologia del 2 novembre 2005 [8];
- l'articolo 2, comma 1, "Manuale Operativo" della Circolare del CNIPA n. CR/49 del 24 novembre 2005 [10];
- le Linee Guida Domanda iscrizione PEC [11].

### **1.2 CAMPO DI VALIDITÀ**

Quanto riportato nel presente documento si applica al Gestore nel suo insieme, cioè:

- alle sue infrastrutture logistiche e tecniche;
- al suo personale;
- a società ed enti eventualmente da esso incaricati di svolgere per suo conto alcune mansioni relative alla registrazione utenti titolari, al rilascio e alla gestione di caselle di posta elettronica certificata;
- agli utenti titolari delle caselle di posta elettronica certificata da esso rilasciate.

### **1.3 PROPRIETÀ INTELLETTUALE**

Il presente Manuale Operativo è di esclusiva proprietà del Gestore che è titolare di ogni relativo diritto intellettuale.

Quanto fornito dal Gestore ai titolari, agli addetti e agli eventuali fornitori per utilizzare le funzioni della posta elettronica certificata da esso gestita, è tutelato dai diritti sulla proprietà intellettuale.

#### 1.4 CORRISPONDENZA CIRC. CNIPA/49/2005 – MANUALE OPERATIVO

Vengono indicate nella tabella seguente le corrispondenze tra i punti dell'art. 2.1 della Circolare [10] e i capitoli del presente Manuale Operativo.

<b>Punti dell'art. 2.1 della circolare CNIPA/CR/49</b>	<b>Manuale Operativo</b>
a. Dati identificativi del Gestore	§ 2.1
b. Responsabile del Manuale Operativo	§ 2.2
c. Riferimenti normativi per la verifica dei contenuti	§ 3.1
d. Indirizzo Internet ove il Manuale Operativo è reperibile	§ 5.2
e. Procedure e standard tecnologici e di sicurezza	§ 3.2 e 16
f. Definizioni, abbreviazioni e termini tecnici	§ 4
g. Descrizione sintetica del servizio offerto	§ 6 e § 7
h. Modalità di reperimento dei log	§ 10
i. Contenuto e modalità di offerta	§ 9
j. Modalità di accesso al servizio	§ 8
k. Indicazione dei livelli di servizio	§ 11
l. Indicazione delle condizioni di fornitura	§ 13
m. Indicazione delle modalità di protezione dei dati dei titolari	§ 14
n. Obblighi, responsabilità e limitazioni in sede di indennizzo	§ 15
Requisito art. 12.7 D.M.I.T 2/11/2005 (soluzioni tecniche / organizzative che realizzano i servizi di emergenza)	§ 11.2
Modalità per l'apposizione e definizione del riferimento temporale	§ 12

## 2. DATI DEL GESTORE

### 2.1 DATI IDENTIFICATIVI

Dati identificativi del Gestore	
Denominazione Sociale:	SOGEI – Società Generale d'Informatica s.p.a.
Indirizzo sede legale:	Via M. Carucci, 99 - 00143 Roma (RM)
Indirizzo sede operativa:	Via M. Carucci, 99 - 00143 Roma (RM)
Legale rappresentante:	Presidente - Amministratore Delegato e Direttore Generale pro tempore
Registro delle Imprese di Roma:	N. Iscrizione 02327910580
N° Partita IVA:	01043931003
N° Telefono:	+39 06 50251
N° Fax:	+39 06 50957270
Indirizzo e-mail:	<a href="mailto:pec.sogei.it@sogei.it">pec.sogei.it@sogei.it</a>
Indirizzo di pubblicazione del presente Manuale Operativo:	<a href="http://ca.sogei.it">http://ca.sogei.it</a>
Indirizzo sito Internet:	<a href="http://ca.sogei.it">http://ca.sogei.it</a>

Il Gestore è in possesso dei requisiti previsti per le società di capitali dall'art. 14 del D.P.R. n. 68/2005 [6], e ottempera a quanto previsto dagli articoli 16, 21 e 22 e 23 del decreto del Ministro per l'innovazione e le tecnologie del 2 novembre 2005.

### 2.2 RESPONSABILE DEL MANUALE OPERATIVO

La responsabilità del Manuale Operativo è assegnata al Responsabile della registrazione dei Titolari.

### 3. RIFERIMENTI

#### 3.1 RIFERIMENTI NORMATIVI

Il presente documento fa riferimento alle norme italiane elencate di seguito.

- [1] Legge 7 agosto 1990, n. 241 – Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi, e successive integrazioni e modificazioni
- [2] Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 e successive integrazioni e modificazioni - Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa (Gazzetta Ufficiale n. 42 del 20 febbraio 2001)  

Nota: gli articoli di questo D.P.R. relativi alla posta elettronica certificata sono stati abrogati e sostituiti dal Decreto legislativo 7 marzo 2005, n. 82
- [3] Decreto legislativo 30 giugno 2003, n. 196– e successive integrazioni e modificazioni - Codice in materia di protezione dei dati personali (Legge delega n. 127/2001), pubblicato sulla Gazzetta Ufficiale n. 174 del 29 luglio 2003
- [4] Decreto del Presidente del Consiglio dei Ministri del 13 gennaio 2004 – Regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici
- [5] Deliberazione CNIPA n. 11/2004 del 10 febbraio 2004 – Regole tecniche per la riproduzione e conservazione di documenti su supporto ottico idoneo a garantire la conformità dei documenti agli originali - articolo 6, commi 1 e 2, del Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa, di cui al decreto del Presidente della Repubblica 28 dicembre 2000, n. 445
- [6] Decreto del Presidente della Repubblica 11 febbraio 2005, n. 68 e successive integrazioni e modificazioni – Regolamento recante disposizioni per l'utilizzo della posta elettronica certificata, a norma dell'articolo 27 della legge 16 gennaio 2003, n. 3. (Gazzetta Ufficiale n. 97 del 28 aprile 2005)
- [7] Decreto legislativo 7 marzo 2005, n. 82 e successive integrazioni e modificazioni – Codice dell'amministrazione digitale, pubblicato sulla Gazzetta ufficiale n. 112 del 16 maggio 2005
- [8] Decreto del Ministro per l'innovazione e la tecnologia del 2 novembre 2005 pubblicato sulla Gazzetta Ufficiale n. 266 del 15 novembre 2005

- [9] Allegato Tecnico al Decreto del Ministro per l'innovazione e le tecnologie del 2 novembre 2005 – Regole tecniche del servizio di trasmissione di documenti informatici mediante posta elettronica certificata (Gazzetta Ufficiale del 15 novembre 2005, n. 266)
- [10] CNIPA/CR/49 – Circolare 24 novembre 2005, n. 49, Modalità per la presentazione delle domande di iscrizione nell'elenco pubblico dei gestori di posta elettronica certificata (PEC), di cui all'articolo 14 del decreto del Presidente della Repubblica 11 febbraio 2005, n. 68. (Gazzetta Ufficiale 5 dicembre 2005, n. 283)
- [11] Linee guida - Raccomandazioni in merito alla predisposizione della documentazione prevista per l'iscrizione nell'Elenco pubblico dei gestori di posta elettronica certificata – 13 febbraio 2006
- [12] MO\_Certificazione\_Server – Manuale operativo per il servizio “CNIPA CERTIFICATI SERVER” – Certification Practice Statement - pubblicato sul sito CNIPA

### 3.2 RIFERIMENTI TECNICI

Il presente documento fa riferimento ai seguenti standard riconosciuti a livello internazionale. Ove nel seguente elenco non sia indicata una specifica versione di uno standard, il riferimento si applica a ogni sua versione.

- [a] ISO/IEC 9594-8; 2001 – INTERNATIONAL STANDARD ISO/IEC 9594-8:2001 – Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks
- [b] RFC 1847 – Security Multiparts for MIME: Multipart/Signed and Multipart / Encrypted
- [c] RFC 1891 – SMTP Service Extension for Delivery Status Notifications
- [d] RFC 1912 – Common DNS Operational and Configuration Errors
- [e] RFC 2045 – Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies
- [f] RFC 2049 – Multipurpose Internet Mail Extensions (MIME) Part Five: Conformance Criteria and Examples
- [g] RFC 2252 – Lightweight Directory Access Protocol (v3): Attribute Syntax Definitions
- [h] RFC 2315 – PKCS #7: Cryptographic Message Syntax Version 1.5

- [i] RFC 2633 – S/MIME Version 3 Message Specification
- [j] RFC 2821 – Simple Mail Transfer Protocol
- [k] RFC 2822 – Internet Message Format
- [l] RFC 2828 - Internet Security Glossary
- [m] RFC 2849 – The LDAP Data Interchange Format (LDIF) - Technical Specification
- [n] RFC 3174 – US Secure Hash Algorithm 1 (SHA1)
- [o] RFC 3207 – SMTP Service Extension for Secure SMTP over Transport Layer Security
- [p] RFC 3280 – Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
- [q] RFC 3647 - Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework
- [r] UNI EN ISO 9001:2000 – Sistemi di gestione per la qualità - Requisiti
- [s] ANSI X9.17 - Financial Institution Key Management

Nota: le specifiche RFC sono emesse dallo IETF – Internet Engineering Task Force

Le procedure di sicurezza seguite dal Gestore nella fornitura del servizio di PEC sono indicate al capitolo 16.

## 4. DEFINIZIONI E ACRONIMI

### 4.1 DEFINIZIONI

Vengono qui riportati i significati di termini specifici, compresi quelli indicati agli articoli 1 e 2 del D.P.R. n. 68/2005 [6], all'articolo 1 del D.M.I.T. 2 novembre 2005 [8], all'articolo 5 delle Regole Tecniche allegate a quest'ultimo.

Non vengono riportati i significati di termini specifici ormai di uso comune.

Termine	Significato	Riferimento
Amministratori dei titolari	Addetti alla registrazione dei titolari e alla gestione delle caselle di PEC. Possono essere dipendenti del Gestore o di Organizzazioni esterne, le quali possono essere a loro volta Organizzazioni clienti del Gestore o Organizzazioni con le quali il Gestore ha in essere un accordo apposito	
Avviso di mancata consegna	l'avviso, emesso dal sistema, per indicare l'anomalia al mittente del messaggio originale nel caso in cui il Gestore di posta elettronica certificata sia impossibilitato a consegnare il messaggio nella casella di posta elettronica certificata del destinatario	Art. 1.1 lettera n) D.M.I.T 2/11/2005 [8]
Avviso di non accettazione	l'avviso, sottoscritto con la firma del Gestore di posta elettronica certificata del mittente, che viene emesso quando il Gestore mittente è impossibilitato ad accettare il messaggio in ingresso, recante la motivazione per cui non è possibile accettare il messaggio e l'esplicitazione che il messaggio non potrà essere consegnato al destinatario	Art. 1.1 lettera f) D.M.I.T 2/11/2005 [8]
Busta di anomalia	la busta, sottoscritta con la firma del Gestore di posta elettronica certificata del destinatario, nella quale è inserito un messaggio errato ovvero non di posta elettronica certificata e consegnata ad un titolare, per evidenziare al destinatario detta anomalia	Art. 1.1 lettera q) D.M.I.T 2/11/2005 [8]
Busta di trasporto	il documento informatico che contiene il messaggio di posta elettronica certificata  la busta creata dal punto di accesso e sottoscritta con la firma del Gestore di posta elettronica certificata mittente, all'interno della quale sono inseriti il messaggio originale inviato dall'utente di posta	DPR 68/2005 [6]  Art. 1.1 lettera p) D.M.I.T 2/11/2005 [8]

Termine	Significato	Riferimento
	elettronica certificata ed i relativi dati di certificazione La busta di trasporto è consegnata immodificata nella casella di posta elettronica certificata di destinazione per permettere la verifica dei dati di certificazione da parte del ricevente	Allegato [9]
Casella di posta elettronica certificata	la casella di posta elettronica posta all'interno di un dominio di posta elettronica certificata ed alla quale è associata una funzione che rilascia ricevute di avvenuta consegna al ricevimento di messaggi di posta elettronica certificata  Una casella di posta elettronica certificata può essere definita esclusivamente all'interno di un dominio di posta elettronica certificata	Art. 1.1 lettera z) D.M.I.T 2/11/2005 [8]  Allegato [9]
Casella di posta elettronica certificata Applicativa	la casella di posta elettronica certificata la cui gestione dei messaggi (invio e scarico) è delegata ad apposita applicazione; l'accesso alla casella è effettuato automaticamente dall'applicazione attraverso le credenziali del titolare	
Centro nazionale per l'informatica nella pubblica amministrazione	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	DPR 68/2005 [6]
Certificate Revocation List	Un elenco firmato che riporta un insieme di certificati non più considerati validi dal certificatore che li ha emessi <i>(A signed list indicating a set of certificates that are no longer considered valid by the certificate issuer)</i>	ISO 9594-8 2001 [a]
Certificati elettronici	Ai sensi dell'articolo 1, comma 1, lettera e), del decreto legislativo 7 marzo 2005, n. 82, sono attestati elettronici che collegano i dati utilizzati per verificare le firme elettroniche ai titolari e confermano l'identità informatica dei titolari stessi	D.gs. n. 82/2005 [7]
Certificato qualificato	Certificato elettronico conforme ai requisiti di cui all'allegato 1 della direttiva n. 1999/93/CE, rilasciati da certificatori che rispondono ai requisiti di cui all'allegato 2 della medesima direttiva	Art. 1.1 lettera f) D.lgs. n. 82/2005 [7]

Termine	Significato	Riferimento
Certification Authority	Autorità considerata affidabile da uno o più utenti per creare e assegnare PKC <i>(Certification Authority (CA) - An authority trusted by one or more users to create and assign public key certificates)</i> In Italia viene usato il termine "Certificatore", come definito dall'art. 1, comma 1, lettera g), del D.lgs. n. 82/2005 [7]: al "soggetto che presta servizi di certificazione delle firme elettroniche"	ISO/IEC 9594-8: 2001 [a]
Certification Practice Statement	Una dichiarazione delle prassi seguite da un Certificatore nell'emettere (e gestire) certificati <i>(A statement of the practices which a certification authority employs in issuing certificates)</i>	RFC 3647 [q]
Certificatore	Vedere Certification Authority	
Chiavi asimmetriche	Chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consent[ono] al titolare [di una firma digitale] 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	D.lgs. n. 82/2005 [7] Art. 1.1.s (si veda la definizione di firma digitale)
Dati di certificazione	I dati inseriti nelle ricevute indicate dal presente regolamento, relativi alla trasmissione del messaggio di posta elettronica certificata I dati, quali ad esempio data ed ora di invio, mittente, destinatario, oggetto, identificativo del messaggio, che descrivono l'invio del messaggio originale e sono certificati dal Gestore di posta elettronica certificata del mittente; tali dati sono inseriti nelle ricevute e sono trasferiti al titolare destinatario insieme al messaggio originale per mezzo di una busta di trasporto	DPR 68/2005 [6] Art. 1.1 lettera r) D.M.I.T 2/11/2005 [8]
Digest crittografico ("Digest")	Si veda "Hash crittografico"	
Disastro	Incidente di sicurezza le cui conseguenze siano tali da rendere impossibile al Gestore la prosecuzione delle attività nel rispetto dei livelli di servizio previsti all'art. 12 del D.M.I.T. [8]. Si distinguono due tipi di disastro: disastro per il quale vi sia un preavviso sufficiente a consentire di spostare le operazioni nella sede di disaster recovery, disastro improvviso (si veda).	
Disastro improvviso	Disastro che si verifichi senza alcun preavviso, come ad esempio un terremoto o un attentato.	

Termine	Significato	Riferimento
Dispositivo sicuro per la creazione della firma	Apparato strumentale usato per la creazione della firma elettronica, rispondente ai requisiti di cui all'articolo 35 del D.lgs. n. 82/2005 [7]	
Domain Name System	Il principale database delle operazioni di Internet, distribuito su una serie di server e utilizzato dal software client per vari scopi, quali ad esempio la traduzione di un indirizzo di tipo "host name. domain name" in un indirizzo IP (ad esempio "rosslyn.bbn.com" viene trasformato in 192.1.7.10"), oppure l'individuazione di un host che accetta e-mail per un determinato indirizzo di e-mail <i>(The main Internet operations database, which is distributed over a collection of servers and used by client software for purposes such as translating a domain name-style host name into an IP address (e.g., "rosslyn.bbn.com" is "192.1.7.10") and locating a host that accepts mail for some mailbox address.)</i>	RFC 2828 [1]
Dominio di posta elettronica certificata	L'insieme di tutte e sole le caselle di posta elettronica certificata il cui indirizzo fa riferimento, nell'estensione, ad uno stesso dominio della rete Internet, definito secondo gli standard propri di tale rete  Dominio di posta elettronica certificata che contiene unicamente caselle di posta elettronica certificata  Corrisponde ad un dominio DNS dedicato alle caselle di posta elettronica dei titolari. All'interno di un dominio di posta elettronica certificata tutte le caselle di posta elettronica certificata devono appartenere a titolari. L'elaborazione dei messaggi di posta elettronica certificata (ricevute, buste di trasporto, ecc.) deve avvenire anche nel caso in cui il mittente ed il destinatario appartengano allo stesso dominio di posta elettronica certificata	DPR 68/2005 [6]  D.M.I.T 2/11/2005 [8]  Allegato [9]
Firma del Gestore di posta elettronica certificata	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, generata attraverso una procedura informatica che garantisce la connessione univoca al Gestore e la sua univoca identificazione, creata automaticamente con mezzi che garantiscano il	D.M.I.T 2/11/2005 [8]

Termine	Significato	Riferimento
	controllo esclusivo da parte del Gestore	
Firma digitale	Particolare tipo di firma elettronica qualificata basata su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, 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, comma 1, lettera s), del D.lgs n. 82/2005 [7]
Firma elettronica qualificata	Firma elettronica ottenuta attraverso una procedura informatica che garantisce la connessione univoca al firmatario e la sua univoca autenticazione informatica, 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, che sia basata su un certificato qualificato e realizzata mediante un dispositivo sicuro per la creazione della firma, quale l'apparato strumentale usato per la creazione della firma elettronica	Art. 1, comma 1, lettera r), del D.lgs n. 82/2005 [7]
Gestore di posta elettronica certificata	Il soggetto che gestisce uno o più domini di posta elettronica certificata con i relativi punti di accesso, di ricezione e di consegna, titolare della chiave usata per la firma delle ricevute e delle buste e che si interfaccia con altri gestori di posta elettronica certificata per l'interoperabilità con altri titolari	D.M.I.T 2/11/2005 [8]
Hash crittografico ("hash")	FUNZIONE DI HASH: una funzione matematica che genera, a partire da una generica sequenza di simboli binari (bit), una impronta in modo tale che risulti di fatto impossibile, a partire da questa, determinare una sequenza di simboli binari (bit) per le quali la funzione generi impronte uguali	DPCM 13 gennaio 2004 [4]
Hypertext Transfer Protocol	Un protocollo Internet client-server, basato sul TCP, application-layer, usato per trasportare richieste di dati e relative risposte nel World Wide Web ( <i>A TCP-based, application-layer, client-server, Internet protocol used to carry data requests and responses in the World Wide Web</i> )	RFC 2828 [I]
Incidente di sicurezza	Evento che violi le misure di sicurezza senza causare un'interruzione di servizio superiore al massimo previsto dall'art. 12.5 del D.M.I.T [8]	
Indice dei gestori di posta elettronica	Il sistema che contiene l'elenco dei domini e dei gestori di posta elettronica certificata, con i relativi certificati corrispondenti alle chiavi usate per la firma delle	D.M.I.T 2/11/2005 [8]

Termine	Significato	Riferimento
certificata	ricevute, degli avvisi e delle buste, realizzato per mezzo di un server Lightweight Directory Access Protocol, di seguito denominato LDAP, posizionato in un'area raggiungibile dai vari gestori di posta elettronica certificata e che costituisce, inoltre, la struttura tecnica relativa all'elenco pubblico dei gestori di posta elettronica certificata	
Internet Message Access Protocol, version 4 (IMAP4)	Un protocollo Internet tramite il quale una workstation client può accedere dinamicamente a una casella di posta su un server host per gestire e accedere a messaggi di posta che il server ha ricevuto e sta conservando per il client <i>(An Internet protocol by which a client workstation can dynamically access a mailbox on a server host to manipulate and retrieve mail messages that the server has received and is holding for the client)</i>	RFC 2828 [1]
Log dei messaggi	Il registro informatico delle operazioni relative alle trasmissioni effettuate mediante posta elettronica certificata tenuto dal Gestore	DPR 68/2005 [6]
Marca temporale	Evidenza informatica che consente la validazione temporale  Un'evidenza informatica con cui si attribuisce, ad uno o più documenti informatici, un riferimento temporale opponibile ai terzi secondo quanto previsto dal decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 e dal decreto del Presidente del Consiglio dei Ministri 13 gennaio 2004, pubblicato nella Gazzetta Ufficiale del 27 aprile 2004, n. 98	Art. 1, comma 1, lettera i), DPCM 13 gennaio 2004 [4] D.M.I.T 2/11/2005 [8]
Messaggio di posta elettronica certificata	Un documento informatico composto dal testo del messaggio, dai dati di certificazione e dagli eventuali documenti informatici allegati	DPR 68/2005 [6]
Messaggio originale	Il messaggio inviato da un utente di posta elettronica certificata prima del suo arrivo al punto di accesso e consegnato al titolare destinatario per mezzo di una busta di trasporto che lo contiene	D.M.I.T 2/11/2005 [8]

Termine	Significato	Riferimento
Post Office Protocol, version 3 (POP3)	Un protocollo standard Internet tramite il quale una workstation client può accedere dinamicamente a una casella di posta per accedere a messaggi di posta che il server ha ricevuto e conserva per il client <i>(An Internet Standard protocol by which a client workstation can dynamically access a mailbox on a server host to retrieve mail messages that the server has received and is holding for the client)</i>	RFC 2828 [I]
Posta elettronica certificata	Ogni sistema di posta elettronica nel quale è fornita al Mittente documentazione elettronica attestante l'invio e la consegna di documenti informatici	DPR 68/2005 [6]
Posta elettronica	Un sistema elettronico di trasmissione di documenti informatici	DPR 68/2005 [6]
Public Key Certificate	La chiave pubblica di un utente, insieme con altre informazioni, resa inalterabile mediante la firma digitale apposta con la chiave privata del certificatore che l'ha rilasciato <i>(The public key of a user, together with some other information, rendered unforgeable by digital signature with the private key of the certification authority which issued it.)</i> Nota: il significato attribuito al termine "Firma digitale" è diverso a seconda che si faccia riferimento alla normativa tecnica o a quella quella giuridica italiana. Per quanto concerne quest'ultima si veda la definizione data precedentemente. In ambito tecnico si intende per firma digitale il risultato di una procedura informatica di tipo crittografico con la quale un oggetto informatico, o meglio una sua sintesi crittografica, viene cifrato con la chiave privata di un'entità. Quest'ultima risulterà essere l'autore di questa firma digitale	ISO/IEC 9594-8: 2001 [a]
Punto di accesso	Il sistema che fornisce i servizi di accesso per l'invio e la lettura di messaggi di posta elettronica certificata, nonché i servizi di identificazione ed accesso dell'utente, di verifica della presenza di virus informatici all'interno del messaggio, di emissione della ricevuta di accettazione e di imbustamento del messaggio originale nella busta di trasporto	D.M.I.T 2/11/2005 [8]
Punto di consegna	Il sistema che compie la consegna del messaggio nella casella di posta elettronica certificata del titolare destinatario, verifica la provenienza e la correttezza del messaggio ed emette, a seconda dei casi, la ricevuta di avvenuta consegna o l'avviso di mancata consegna	D.M.I.T 2/11/2005 [8]

<b>Termine</b>	<b>Significato</b>	<b>Riferimento</b>
Punto di ricezione	Il sistema che riceve il messaggio all'interno di un dominio di posta elettronica certificata, effettua i controlli sulla provenienza e sulla correttezza del messaggio ed emette la ricevuta di presa in carico, imbusta i messaggi errati in una busta di anomalia e verifica la presenza di virus informatici all'interno dei messaggi di posta ordinaria e delle buste di trasporto	D.M.I.T 2/11/2005 [8]
Revoca del certificato	L'operazione, non retroattiva, con cui il certificatore annulla la validità del certificato da un dato momento in poi	
Ricevuta breve di avvenuta consegna	La ricevuta nella quale sono contenuti i dati di certificazione ed un estratto del messaggio originale	D.M.I.T 2/11/2005 [8]
Ricevuta completa di avvenuta consegna	La ricevuta nella quale sono contenuti [ <i>in allegato</i> ] i dati di certificazione ed il messaggio originale	D.M.I.T 2/11/2005 [8] <i>Allegato</i> [9]
Ricevuta di accettazione	La ricevuta, sottoscritta con la firma del Gestore di posta elettronica certificata del mittente, contenente i dati di certificazione, rilasciata al mittente dal punto di accesso a fronte dell'invio di un messaggio di posta elettronica certificata	D.M.I.T 2/11/2005 [8]
Ricevuta di avvenuta consegna	La ricevuta, sottoscritta con la firma del Gestore di posta elettronica certificata del destinatario, emessa dal punto di consegna al mittente nel momento in cui il messaggio è inserito nella casella di posta elettronica certificata del destinatario	D.M.I.T 2/11/2005 [8]
Ricevuta di presa in carico	La ricevuta, sottoscritta con la firma del Gestore di posta elettronica certificata del destinatario, emessa dal punto di ricezione nei confronti del Gestore di posta elettronica certificata mittente per attestare l'avvenuta presa in carico del messaggio da parte del sistema di posta elettronica certificata di destinazione, recante i dati di certificazione per consentirne l'associazione con il messaggio a cui si riferisce	D.M.I.T 2/11/2005 [8]
Ricevuta sintetica di avvenuta consegna	La ricevuta che contiene [ <i>in allegato</i> ] i dati di certificazione	D.M.I.T 2/11/2005 [8] <i>Allegato</i> [9]
Riferimento temporale	L'informazione contenente la data e l'ora che viene associata ad un messaggio di posta elettronica certificata	DPR 68/2005 [6]

Termine	Significato	Riferimento
Security Policy	Insieme di regole e norme che specificano o regolamentano le modalità con cui un sistema o un'organizzazione fornisce servizi di sicurezza per proteggere risorse di sistema critiche o riservate <i>(A set of rules and practices that specify or regulate how a system or organization provides security services to protect sensitive and critical system resources)</i>	RFC 2828 [L]
Simple Mail Transfer Protocol (SMTP)	Un protocollo standard Internet, basato su TCP, application-layer, utilizzato per spostare messaggi di posta da un computer a un altro	RFC 2828 [I]
Titolare	Il soggetto a cui è assegnata una casella di posta elettronica certificata	D.M.I.T 2/11/2005 [8]
Universal Time Coordinated	Misura di tempo, basata sui secondi, come stabilito e raccomandato dallo International Radio Consultative Committee (CCIR) e gestito dal Bureau International des Poids et Mesures (BIPM) <i>[Time scale, based on the second, as defined and recommended by the International Radio Consultative Committee (CCIR), and maintained by the Bureau International des Poids et Mesures (BIPM)]</i>	American National Standard for Telecommunications - Telecom Glossary 2000 <a href="http://www.its.bldrdoc.gov/projects/t1glossary2000/t1g2k.html">http://www.its.bldrdoc.gov/projects/t1glossary2000/t1g2k.html</a>
Utente di posta elettronica certificata	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 posta elettronica certificata	DPR 68/2005 [6]
Validazione temporale	Il risultato della procedura informatica con cui si attribuiscono, ad uno o più documenti informatici, una data ed un orario opponibili a terzi	D.lgs n. 82/2005 [7]
Virus informatico	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	DPR 68/2005 [6]

## 4.2 ACRONIMI

Acronimo	Descrizione
CNIPA	Centro Nazionale per l'Informatica nella Pubblica Amministrazione
CRL	Certificate Revocation List
D.M.I.T	Decreto del Ministro per l'innovazione e la tecnologia
DNS	Domain Name System
DPCM	Decreto Presidente del Consiglio dei Ministri
DPR	Decreto Presidente della Repubblica
http	Hypertext Transfer Protocol
IGPEC	Indice dei Gestori di PEC
IMAP4	Internet Message Access Protocol, version 4
LDAP	Lightweight Directory Access Protocol
LDIF	LDAP Data Interchange Format
MIME	Multipurpose Internet Mail Extensions
PEC	Posta Elettronica Certificata
PKCS	Public Key Cryptography Standard
POP3	Post Office Protocol, version 3
RFC	Request For Comment
S/MIME	Secure/MIME
SMTP	Simple Mail Transfer Protocol
TLS	Transport Layer Security
URL	Uniform Resource Locator
UTC	Universal Time Coordinated

## **5. DATI DEL MANUALE OPERATIVO**

### **5.1 VERSIONE**

Il presente documento costituisce la versione 1.0, rilasciata l'8/05/2006, del Manuale Operativo del Gestore in conformità con la normativa vigente.

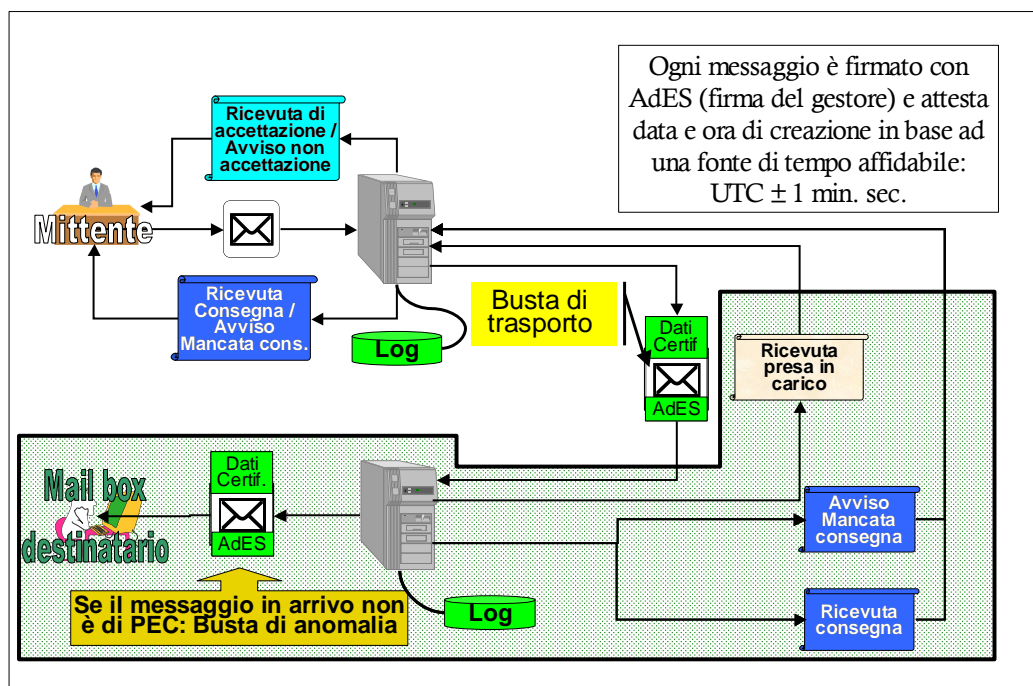
### **5.2 INDIRIZZO INTERNET**

Il presente "Manuale Operativo" è stato depositato presso il CNIPA ed è consultabile per via telematica all'indirizzo Internet del Gestore: [ca.sogei.it](http://ca.sogei.it). La pubblicazione di versioni aggiornate del Manuale Operativo avverrà sul sito sopra indicato dopo il loro inoltro al CNIPA.

## 6. SERVIZIO OFFERTO

### 6.1 DESCRIZIONE SINTETICA DEL SERVIZIO DI PEC COME DA NORMATIVA IN VIGORE

Il servizio di Posta Elettronica Certificata fornito dal Gestore è conforme con la normativa in vigore e opera come schematizzato nella figura seguente.



In sintesi il servizio opera come descritto di seguito.

Il mittente, dopo essersi autenticato, invia al proprio Gestore il messaggio che viene esaminato per controllare se è conforme con i requisiti tecnici e se contiene virus. Se la verifica ha esito sfavorevole, il Gestore invia al mittente un avviso di non accettazione con l'indicazione del motivo del rifiuto. In caso di esito favorevole il Gestore invia una ricevuta di accettazione.

Se il messaggio è indirizzato a destinatari presenti presso domini di altri gestori di PEC viene controllata la effettiva presenza di questi ultimi nell'Indice dei Gestori di PEC tenuto dal CNIPA.

La busta di trasporto viene inviata al Gestore del destinatario se esso è diverso da quello del mittente. In questo caso il Gestore del destinatario, dopo aver verificato l'autenticità della firma del Gestore del mittente mediante il rispettivo certificato presente nello IGPEC, invia immediatamente al Gestore del mittente una ricevuta di presa in carico del messaggio.

Il messaggio viene quindi depositato nella casella di posta del destinatario.

A seguito di ciò viene generata dal Gestore del destinatario una ricevuta di avvenuta consegna (o un avviso di mancata consegna se del caso) che viene inoltrata al mittente, eventualmente per il tramite del relativo Gestore se diverso da quello del destinatario.

Qualora entro le 22 ore successive all'invio del messaggio il Gestore che opera in qualità di Gestore del mittente non riceva una tale comunicazione, o non abbia potuto provvedere direttamente alla consegna del messaggio, ne informa il mittente.

Un pre-allarme viene dato nel caso in cui entro le 12 ore successive all'inoltro del messaggio al Gestore del destinatario il Gestore del mittente non abbia ricevuto né la ricevuta di avvenuta consegna né quella di presa in carico.

Nel caso in cui un Gestore accetti un messaggio da un mittente esterno al circuito di PEC, può inoltrarlo al destinatario, se questa è la sua prassi, solo se in esso risultano assenti virus. Il messaggio, se viene recapitato, viene depositato nella casella di PEC del destinatario dopo essere stato inserito in quella che si chiama "busta di anomalia".

Nel caso in cui un Gestore riceva una busta di trasporto ove sia presente un virus è tenuto a non consegnarla al destinatario e ad informarne il Gestore del mittente.

Qualora un Gestore riceva da altro Gestore segnalazione che una busta di trasporto da lui creata contiene un virus ne informa il mittente ed attiva le opportune azioni per evitare il ripetersi dell'evento.

Tutti gli eventi vengono registrati dai vari gestori sui rispettivi log che al massimo una volta al giorno vengono estratti per essere conservati in modo sostitutivo conformemente con la Deliberazione CNIPA n. 11/2004 [5].

In pratica la PEC replica con modalità elettroniche il meccanismo della Raccomandata con Avviso di Ricevuta della posta ordinaria, al quale aggiunge i seguenti ulteriori benefici:

- a) certezza della provenienza del messaggio da una determinata casella di PEC e certezza che esso è stato depositato nella corretta casella di PEC;

Nota: a meno di compromissione delle credenziali, l'autenticazione al servizio di PEC del mittente e del destinatario impedisce che una persona fisica o giuridica diversa dal titolare della casella, e che non sia da esso delegata, possa inviare posta in suo nome, e che una persona diversa dal destinatario o da un suo delegato possa accedere ai messaggi di PEC a lui destinati;

- b) in aggiunta alla celerità di consegna tipica della posta elettronica si ha anche una celere comunicazione di un'eventuale mancata consegna, che viene recapitata nella casella di PEC del mittente entro 24 ore dall'invio del messaggio;
- c) possibilità di ottenere copia del log di PEC che costituisce prova, valida a tutti gli effetti di legge, dell'avvenuta spedizione e consegna di un messaggio di PEC di cui si sia persa la relativa ricevuta;
- d) impossibilità da parte del destinatario di contestare il contenuto di un messaggio PEC per il quale sia stata richiesta una ricevuta di avvenuta consegna completa o breve, in quanto, oltre al messaggio originale inviato, la ricevuta completa contiene al proprio interno gli allegati, e la ricevuta breve contiene i digest degli allegati (e quindi conservando gli allegati è possibile dimostrare l'invio); analoga possibilità non sussiste se viene richiesta soltanto una ricevuta sintetica (si veda § 7.3) in quanto essa contiene soltanto l'identificativo del messaggio.

## 7. SERVIZIO OFFERTO DAL GESTORE

Il Gestore fornisce servizi di PEC sia a singoli individui, sia ad Organizzazioni.

La struttura del Gestore a disposizione dell'utenza fornisce i seguenti servizi erogati sia direttamente sia tramite le Organizzazioni clienti:

1. Servizi di registrazione titolari.
2. Servizi di gestione caselle di PEC.
3. Servizi di assistenza in condizioni normali e di emergenza

### 7.1 SERVIZI DI REGISTRAZIONE TITOLARI

La struttura organizzativa degli addetti alla registrazione utenti titolari è indicata nella figura seguente. Al suo vertice c'è il Responsabile della registrazione dei titolari, previsto all'articolo 21, comma 1, lettera a), del citato D.M.I.T. [8].

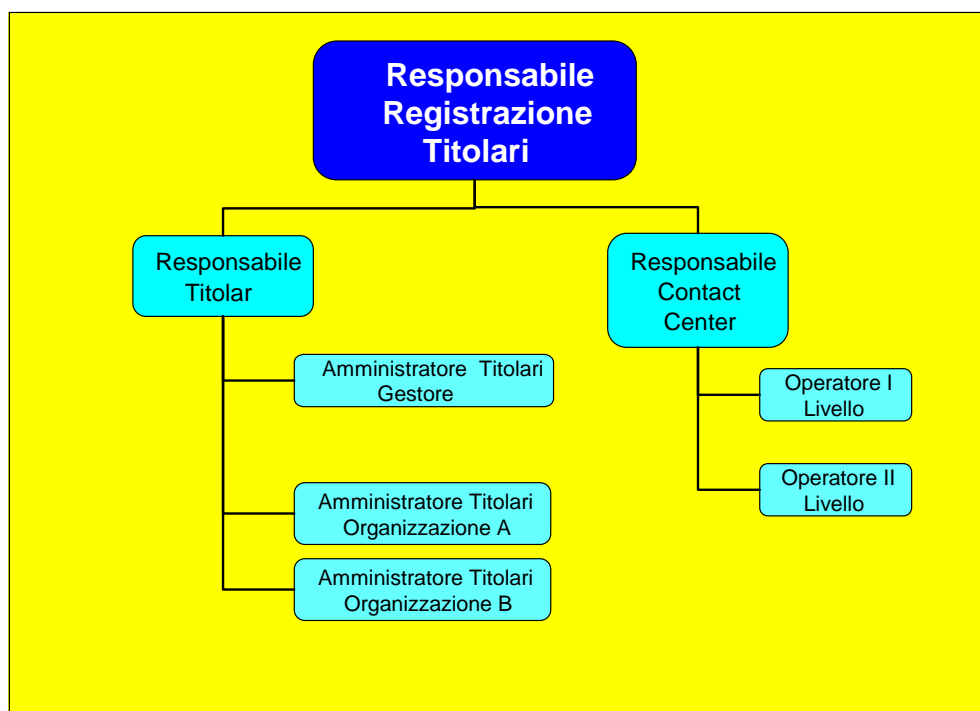


Figura 1 - Schema organizzativo relativo agli addetti alla registrazione titolari

Più in dettaglio sono previste le seguenti mansioni:

- il Responsabile Titolari, il quale coordina gli Amministratori dei Titolari;
- gli Amministratori dei Titolari:
  - sono nominati dal Responsabile Titolari se dipendenti SOGEI, oppure dal Cliente all'interno della propria Organizzazione;
  - gestiscono l'assegnazione e la eventuale, disattivazione, riattivazione e revoca in condizioni normali delle caselle di PEC dei titolari nonché eventuali funzioni amministrative relative alle caselle e/o agli utenti titolari laddove gli accordi di servizio lo prevedano;
- il *Responsabile del contact center* è responsabile dei servizi di informazioni per gli utenti titolari;
- gli *Operatori di I livello* sono abilitati a fornire le informazioni generali sul servizio;
- gli *Operatori di II livello* possono svolgere funzioni amministrative relative alle caselle e/o alle utenze dei titolari.

La registrazione degli utenti titolari viene fatta direttamente dal personale del Gestore nel caso di utenti titolari privati e da personale dell'Organizzazione Cliente, appositamente incaricato, nel caso di utenti titolari di caselle di PEC ad essa attribuite e del cui utilizzo essa, pertanto, è responsabile.

Gli addetti alla registrazione, cioè gli Amministratori dei titolari, verificano l'esistenza di accordi di servizio che diano diritto al richiedente di disporre di una casella di PEC del Gestore e gli attribuiscono tale casella con le modalità descritte di seguito.

Gli Amministratori dei titolari sono responsabili dell'identificazione dei Titolari che ricadono sotto la loro competenza nel rispetto degli accordi.

Gli Amministratori dei titolari del Gestore dovranno anche verificare all'atto della registrazione del titolare l'esistenza di accordi validi.

Nel caso in cui Amministratori dei titolari e addetti di contact center appartengano a società o ad organizzazioni esterne al Gestore, essi sono obbligati a rispettare le norme di sicurezza riportate nell'atto che regola l'accordo di servizio.

## **7.2 MODALITÀ DI GESTIONE DELLE CASELLE**

Il servizio di gestione delle caselle di PEC riguarda la loro sospensione, riattivazione e revoca da parte del Gestore sia su richiesta dell'assegnatario (persona fisica o giuridica), che dell'Amministratore di riferimento sia su iniziativa del Gestore stesso.

### **7.2.1 ASSEGNAZIONE DELLE CASELLE AGLI UTENTI TITOLARI**

La registrazione dei titolari avviene presso il relativo Amministratore dei titolari.

La registrazione dell'utente titolare da parte degli Amministratori dei titolari avviene comunicando alle funzioni apposite del Gestore gli estremi identificativi delle caselle di posta assegnate nel rispetto della nomenclatura concordata e previa verifica del Gestore.

### **7.2.2 DISATTIVAZIONE DELLE CASELLE DI PEC**

Le caselle di PEC possono essere disattivate su richiesta del titolare o dell'Amministratore dei Titolari competente.

Il Gestore in caso di disattivazione impedisce ogni accesso a tale casella.

Il contenuto di una casella di posta assegnata a un titolare in virtù della sua appartenenza ad un'Organizzazione cliente è da ritenersi di proprietà della medesima Organizzazione e non può essere considerata documentazione privata del titolare.

Pertanto, nel caso in cui un titolare lasci l'Organizzazione di appartenenza, il relativo Amministratore dei titolari ha il diritto di chiedere l'attribuzione a un altro titolare di tale casella, senza che ne venga svuotato il contenuto, né modificato l'indirizzo.

Il Gestore può disattivare d'autorità una casella di PEC qualora si verifichino le condizioni che prevedano tali misure, qualora abbia fondata notizia di impedimento temporaneo o definitivo del Titolare o su disposizione delle Autorità competenti.

### **7.2.3 RIATTIVAZIONE DI UNA CASELLA DI PEC DISATTIVATA**

La richiesta di riattivazione di una casella deve pervenire al Gestore dal richiedente originario della disattivazione o, se la casella è stata disattivata su richiesta di un Amministratore, dall'Amministratore originario o da chi è a lui subentrato formalmente nella gestione della specifica casella di PEC.

In caso di riattivazione il Gestore consentirà nuovamente l'accesso alla casella e ove previsto negli accordi di servizio ripristinerà le credenziali al valore consegnato inizialmente al titolare. In caso di smarrimento di tali credenziali il titolare ne richiederà di nuove al proprio Amministratore dei titolari.

#### **7.2.4 REVOCA DI UNA CASELLA DI PEC**

Una casella di PEC può essere revocata. In caso di revoca i messaggi di posta eventualmente in essa contenuti andranno perduti.

L'Amministratore dei titolari può chiedere la revoca di una casella di PEC assegnata a un titolare che a lui afferisca.

In tal caso il Gestore provvederà alla cancellazione della casella di PEC e delle credenziali associate.

Il Gestore può revocare d'autorità una casella di PEC qualora si verificano le condizioni che prevedano tali misure, qualora abbia fondata notizia di impedimento temporaneo o definitivo del Titolare o su disposizione delle Autorità competenti.

Una casella revocata non può essere riattivata. L'indirizzo di posta elettronica attribuito ad una casella revocata e l'utenza ad essa associata potranno essere riutilizzate.

#### **7.2.5 RIASSEGNAZIONE DI CASELLE DI PEC**

Le caselle di PEC, ove previsto dagli accordi in essere con lo specifico cliente, possono essere riassegnate nel tempo a titolari diversi. Questo può verificarsi:

1. Nel caso di caselle di pec attribuite a un'organizzazione cliente che assegni a persone fisiche diverse, successivamente nel tempo, una casella di pec corrispondente a una specifica funzione aziendale.
2. Nel caso di caselle di pec attribuite a persone fisiche che intendano legittimamente cedere o delegare in modo formale, in via definitiva o temporanea, ad altre persone la gestione di una casella di posta che sia stata ad esse assegnata. nel caso di caselle di pec attribuite a un'organizzazione cliente e gestite dagli amministratori dei titolari della medesima organizzazione, quest'ultima è totalmente responsabile di conservare storia delle attribuzioni delle varie caselle di pec nel tempo a differenti persone fisiche.

Nel caso di caselle di PEC attribuite a un cliente individuale, sarà quest'ultimo, all'atto della scadenza contrattuale, ad autorizzare eventualmente la riassegnazione dell'indirizzo e-mail a un nuovo assegnatario.

#### **7.2.6 INFORMAZIONI AL TITOLARE**

In ogni caso il titolare di una casella sospesa, revocata o riattivata viene informato dell'evento dal Gestore tramite l'Amministratore dei titolari di riferimento.

### 7.3 FORMATO DELLE RICEVUTE DEL GESTORE

La normativa prevede tre tipi diversi di ricevuta:

1. Completa: contiene in allegato i dati di certificazione del messaggio a cui fa riferimento ed il messaggio stesso comprensivo di eventuali allegati.
2. Breve: contiene in allegato i dati di certificazione, il messaggio originale, privo degli allegati che sono sostituiti dai relativi hash crittografici;
3. Sintetica: contiene in allegato solo i dati di certificazione.

Le buste di trasporto prodotte dal Gestore prevedono la richiesta di ricevute di avvenuta consegna complete per gli utenti titolari del proprio sistema mentre le ricevute destinate ad utenti titolari di altri gestori verranno prodotte secondo quanto richiesto.

Nell'eventualità che si voglia avere la possibilità di variare il livello di completezza della ricevuta a fronte di un messaggio inviato questo dovrà essere oggetto di specifici accordi con il Gestore non essendo previsto dal servizio base.

## **8. MODALITÀ DI ACCESSO AL SERVIZIO E NORME DI UTILIZZO**

Il servizio di PEC è fornito dal Gestore sia in modalità client sia in modalità webmail.

Prerequisito per l'utente è quindi la conoscenza delle procedure per connettersi ai server che espongono il servizio.

I protocolli utilizzati dai client sono protocolli di tipo sicuro e possono essere, a titolo esemplificativo, POP3S e IMAPS.

I titolari sono tenuti a provvedere autonomamente a scaricare frequentemente i messaggi e a conservarne copia ove lo ritengano necessario (si veda Nota del § 8.1.5).

Il Gestore conserva, come richiesto dall'articolo 11, comma 3, del D.M.I.T. [8], le registrazioni del log di PEC per trenta mesi nel rispetto delle procedure definite nella Deliberazione CNIPA n. 11/2004 [5], da dove è possibile estrarne i dati con le modalità indicate al § 10.

### **8.1 ATTIVAZIONE E ACQUISIZIONE DEL SERVIZIO**

Le istruzioni operative dettagliate necessarie per accedere al sistema di PEC del Gestore sono indicate in un documento che viene reso disponibile al titolare all'atto della sua registrazione.

Con la registrazione il titolare entra in possesso delle credenziali necessarie per autenticarsi al sistema di PEC del Gestore e può di conseguenza accedere alla propria casella di posta.

#### **8.1.1 CREDENZIALI UTENTI TITOLARI**

La modalità di autenticazione alla casella di posta elettronica certificata avviene mediante l'identificativo utente e password le norme della cui composizione sono indicate in specifiche Security Policy e riprese negli accordi di servizio.

All'utente viene consegnata dall'Amministratore di riferimento secondo modalità che ne garantiscono la riservatezza, una password iniziale che serve per l'attivazione della casella. La stessa viene utilizzata per eventuali riattivazioni successive, come indicato al § 7.2.3.

### **8.1.2 CREDENZIALI AMMINISTRATORI DEI TITOLARI**

Ad ogni Amministratore dei titolari, in aggiunta a quella eventualmente assegnatagli come utente generico, viene assegnata una casella di servizio.

Questa casella serve per le comunicazioni inerenti le caselle di PEC dei titolari di cui è responsabile.

All'Amministratore vengono consegnate, con modalità atte a garantirne la riservatezza, le credenziali di accesso alla casella di servizio con funzioni e caratteristiche del tutto analoghe a quelle della casella di un titolare.

### **8.1.3 PRIMO ACCESSO ALLA CASELLA DI PEC**

Il titolare si identifica al sistema di PEC mediante l'identificativo utente assegnatogli per la propria casella e la password iniziale, forniti al completamento delle operazioni di registrazione.

Immediatamente dopo la prima autenticazione il sistema di PEC chiederà al titolare di sostituire la password iniziale con un'altra che dovrà rispettare le norme di composizione indicate nelle istruzioni operative.

Nelle citate istruzioni operative del servizio sarà indicata la periodicità con la quale il titolare dovrà provvedere a sostituire la password con altra, tenendo conto del fatto che il sistema non consente il riutilizzo delle password utilizzate per un periodo anch'esso indicato nelle istruzioni.

### **8.1.4 GESTIONE DELLE CREDENZIALI**

Nel caso in cui l'utente dimentichi la password corrente può tramite contact center ove gli accordi lo prevedano, o tramite l'Amministratore di riferimento richiederne il ripristino. In tal caso la password verrà ripristinata al valore iniziale consegnato all'utente al momento dell'attivazione della casella.

L'utente titolare dovrà sostituire la password iniziale con un'altra alla prima connessione e ad ogni eventuale ripristino delle credenziali di accesso alla casella di PEC.

Il titolare inoltre potrà comunque in ogni momento modificare la password corrente a proprio piacimento.

Si ricorda che ogni password scelta dal titolare deve rispettare le norme di composizione che saranno comunicate al completamento della registrazione.

Relativamente alla casella di PEC applicativa (vedi tabella definizioni al § 4.1), in qualsiasi momento potrà essere modificata la modalità di gestione della password secondo le seguenti opzioni:

1. password gestita direttamente dal Titolare (modalità manuale)
2. password gestita direttamente dal sistema (modalità automatica)

ed in particolare potrà essere attivato il ripristino della modalità manuale del cambio password utilizzando la password inizialmente assegnata al Titolare.

Nel caso in cui l'utente abbia smarrito o dimenticato o ritenga compromessa la segretezza della password iniziale può richiedere all'Amministratore dei titolari l'attribuzione di una nuova password di attivazione, che sostituirà la password iniziale originariamente fornitagli e che gli verrà consegnata o inviata per posta ordinaria con modalità tali da garantirne la riservatezza.

Pertanto la password iniziale, ricevuta dal titolare in modo segreto al completamento della registrazione e associata al suo codice identificativo, o quella ricevuta come indicato al capoverso precedente, deve essere usata nei seguenti casi:

1. Prima attivazione della casella di posta: l'utente dovrà immettere, oltre all'identificativo utente la password iniziale e sostituirla immediatamente con un'altra che dovrà custodire in modo segreto. Qualora il titolare comunichi la nuova password ad altre persone, egli sarà ritenuto pienamente responsabile nei confronti di terzi di quanto fatto da tali persone con la casella di posta in questione.
2. Primo accesso alla casella di posta in seguito a riattivazione o ripristino da parte del Gestore come indicato al § 7.2.3.
3. Per ripristinare la modalità manuale del cambio password.

### **8.1.5 RACCOMANDAZIONI DI UTILIZZO**

Un titolare deve utilizzare la propria casella di PEC nel rispetto degli obblighi indicati al § 15.2.

Ogni titolare è tenuto a scaricare frequentemente la propria posta dal server PEC del Gestore.

Nota: Questo requisito discende dal dettato dell'art. 45.2 del D.lgs. n. 82/2005 [7] il quale prevede che: "Il documento informatico trasmesso per via telematica ... si intende consegnato al destinatario se reso disponibile all'indirizzo elettronico da questi dichiarato, nella casella di posta elettronica del destinatario messa a disposizione dal Gestore".

Da questa presunzione deriva che un titolare che non acceda di frequente alla propria casella di PEC non può addurre questo suo comportamento come scusante per una eventuale intempestiva o mancata azione a fronte di messaggi ricevuti e depositati nella citata casella di PEC.

Per le modalità di gestione in caso di disastro si veda il § 11.3.

## **9. MODALITÀ DELL'OFFERTA**

### **9.1 CONTRAENTE PRIVATO**

L'utente privato si identifica di persona esibendo un documento d'identità ufficiale dello Stato di appartenenza riconosciuto valido in Italia, oppure inviandone una fotocopia firmata autenticata.

Il contratto può essere sottoscritto in forma autografa o utilizzando la firma digitale, come previsto dal D.lgs. n. 82/2005 [7].

Il Gestore conserva copia del documento d'identificazione del contraente.

### **9.2 CONTRAENTE ORGANIZZAZIONE**

Il rappresentante legale dell'Organizzazione identifica se stesso e l'Organizzazione che rappresenta secondo la normativa vigente. In particolare qualora l'Organizzazione non abbia già in essere un contratto con il Gestore il rappresentante legale dovrà presentare:

- a) documento attestante l'iscrizione dell'Organizzazione alla Camera di Commercio;
- b) documentazione comprovante il proprio incarico a rappresentare l'Organizzazione in tale stipula;
- c) un documento d'identità ufficiale dello Stato di appartenenza riconosciuto valido in Italia.

Il contratto può essere sottoscritto in forma autografa o utilizzando la firma digitale, come previsto al D.lgs n. 82/2005 [7].

### **9.3 ACCORDO DI SERVIZIO**

Il contratto di cui al precedente punto 9.1.2 è costituito dai singoli atti regolanti le condizioni economiche e normative e dall' "accordo di servizio", riguardante le sole modalità e regole di erogazione del servizio e si intende costituito ad ogni effetto dal presente documento denominato "Manuale operativo del servizio di posta elettronica certificata", pubblicato sul sito internet di SOGEI (<http://ca.sogei.it>), e dal documento denominato "Manuale utente", di volta in volta consegnato ai singoli utenti".

Prima della sottoscrizione del citato contratto, con il quale il cliente accetta le condizioni di servizio ed i propri obblighi, lo stesso deve essere identificato come indicato nei paragrafi precedenti.

La documentazione, comprensiva della sottoscrizione delle condizioni, è archiviata in formato cartaceo, in archivi ad accesso fisico controllato, oppure è conservata in formato digitale in conformità con la Deliberazione CNIPA n. 11/2004 [5] e con l'articolo 23 del D.lgs. n. 82/2005 [7], per il periodo di tempo previsto dalla normativa civilistica.

Nel caso di Organizzazioni, il rappresentante legale, o un suo delegato, nell'accettare le condizioni contenute nell'accordo di servizio può:

1. Indicare una o più persone interne all'Organizzazione cliente quali Amministratori dei titolari, incaricati di mantenere i rapporti con il Gestore (il rappresentante legale o delegato dell'Organizzazione può successivamente modificare tale scelta).
2. Indicare i nominativi delle persone a cui assegnare le caselle di posta avvalendosi della struttura di Amministratori dei titolari del Gestore o segnalarli con comunicazioni successive.

L'assegnazione delle caselle di posta può essere modificata nel tempo.

### 9.3.1 DOMINI DI PEC DEI CLIENTI

Il cliente, all'atto della definizione dell'accordo di servizio, può richiedere al Gestore di attivare proprie caselle di PEC su uno o più domini di PEC a lui attribuiti.

In tal caso, nell'accordo si definiranno gli aspetti tecnici e organizzativi quali, a titolo di esempio, se saranno a carico del Cliente o del Gestore la registrazione di questi domini e l'eventuale gestione dei medesimi.

Tali domini potranno essere utilizzati solo per la PEC.

L'indirizzo delle caselle di posta elettronica certificata relative a questi domini del Cliente sarà del tipo seguente:

identificativo\_utente@dominio.xx.

Ove:

“identificativo\_utente”: avrà la struttura concordata con il cliente

“dominio.xx” sarà il nome di dominio concordato con il cliente

Un cliente potrà, all'interno del proprio dominio, amministrare le caselle, cioè crearle, disattivarle, riattivarle, cancellarle, e gestire i propri utenti titolari con strumenti che saranno assegnati agli Amministratori dei titolari nel rispetto di procedure definite negli accordi di servizio.

Eventuali ulteriori richieste di personalizzazioni al riguardo (ad esempio: l'aspetto grafico per accessi webmail etc...), saranno definiti negli accordi di servizio.

## 10. MODALITÀ DI REPERIMENTO DEL LOG

Sono autorizzati a formulare richieste di acquisizione dei dati presenti nel log, relativi a messaggi che siano stati gestiti negli ultimi 30 mesi dal Gestore: le autorità competenti, i mittenti o destinatari (purché utenti titolari del Gestore) dei messaggi interessati e gli Amministratori dei titolari per quanto riguarda i messaggi relativi ai titolari ad essi afferenti, limitatamente alle caselle revocate.

La richiesta deve essere inviata al Gestore mediante messaggio di PEC all'indirizzo che sarà comunicato all'atto della registrazione del titolare.

Nella richiesta dovranno essere indicati alcuni tra i seguenti parametri di ricerca:

1. Data (aaaa-mm-gg): obbligatoria;
2. Mittente e destinatario: obbligatorio;
3. Tipo di evento (accettazione, ricezione, consegna, emissione ricevute, errore, ecc.).

Ulteriori modalità della richiesta possono essere indicate negli accordi di servizio.

Una volta verificata la legittimità della richiesta, il Gestore estrarrà i dati richiesti, dal file di log corrente o dagli archivi della conservazione sostitutiva, e li invierà, a scelta del Gestore, o con messaggio PEC o su supporto non riscrivibile per lettera raccomandata. Ove venga utilizzato questo secondo mezzo i dati saranno inviati all'Amministratore dei titolari competente.

Qualora il richiedente sia l'Autorità giudiziaria la richiesta potrà essere inviata tramite lettera raccomandata A/R all'indirizzo indicato al paragrafo "Dati identificativi del Gestore" § 2.

Ulteriori modalità di richiesta potranno essere rese note attraverso il sito del Gestore.

## 11. LIVELLI DI SERVIZIO E INDICATORI DI QUALITÀ

Il Gestore garantisce l'alta affidabilità del servizio; le condizioni di ripristino del servizio in caso di disastro e/o disastro improvviso sono definite negli specifici accordi di servizio.

### 11.1 CONDIZIONI NORMALI DI FUNZIONAMENTO

Il Gestore, salvo che nel caso dei disastri che sono trattati nel § 11.3, opera nel rispetto dei livelli di servizio richiesti dall'articolo 12, commi 2, 3, 4, 5, 6 e 7, del D.M.I.T. [8], di cui si riprendono gli argomenti adattandoli all'offerta effettiva del Gestore.

1. Si garantisce la possibilità dell'invio di un messaggio, salvo diversi accordi con il singolo cliente:
  - a) almeno fino a cinquanta destinatari;
  - b) per il quale il prodotto del numero dei destinatari per la dimensione del messaggio stesso non superi i trenta megabytes.
    - In base ad accordi con i singoli clienti la disponibilità per questi ultimi di inviare messaggi di posta elettronica certificata può eventualmente essere limitata nell'orario e nei giorni.
    - I messaggi di posta elettronica certificata destinati agli utenti titolari del Gestore saranno da quest'ultimo accettati e depositati nelle relative caselle di posta elettronica certificata con una disponibilità di servizio maggiore o uguale al 99,8% (novantanovevirgolaottopercento) del periodo temporale di riferimento che, stante la normativa in vigore all'atto della redazione del presente Manuale Operativo, è pari ad un quadrimestre.
    - La durata massima di ogni evento di indisponibilità del servizio di posta elettronica certificata è minore, o uguale, al 50% (cinquantapercento) del totale previsto per l'intervallo di tempo di riferimento.
    - Nell'ambito dell'intervallo di disponibilità di cui sopra, la ricevuta di accettazione viene fornita al mittente entro un termine, da concordarsi tra Gestore e cliente, da calcolare a partire dall'inoltro del messaggio, non considerando i tempi relativi alla trasmissione.

Il Gestore assicura la sicurezza e l'affidabilità del proprio servizio e, ad eccezione dei casi di disastro di cui al § 11.3 il completamento della trasmissione ed il rilascio delle ricevute entro i termini sopra indicati.

A tal fine il servizio di PEC del Gestore opera, nel rispetto di adeguate procedure di sicurezza logica e fisica, con apparecchiature ridondate, custodite in locali il cui accesso è riservato al personale addetto avente esperienza professionale rispondente ai requisiti normativi in vigore e si avvale di apparati di firma anch'essi ridondate.

I principali dati del sistema sono copiati, a scopo di backup, presso il sito principale e, con continuità, conservati in altra località. In particolare, in situazione di normale svolgimento delle funzioni di PEC, il Gestore copia con continuità su tale località i dati del log. Solo in caso di disastro improvviso i dati relativi alle ultime transazioni potrebbero perdersi.

Pertanto, in caso di incidente che non sia configurabile come disastro, è assicurata la continuità del servizio o, al massimo, un'interruzione contenuta entro i limiti sopra indicati.

## **11.2 SERVIZI DI EMERGENZA**

Allo scopo di assicurare che in caso di incidenti, di sicurezza o di altro tipo, siano rispettati i livelli di servizio richiesti dall'articolo 12 del D.M.I.T. [8] e, in particolare, il completamento della trasmissione ed il rilascio delle ricevute di cui al comma 7 del medesimo articolo, sono in essere misure dei seguenti tipi:

1. La continuità dell'alimentazione elettrica è assicurata per un periodo di tempo coerente con i requisiti citati.
2. I sistemi del servizio di PEC, come anche i dispositivi di firma e i sistemi di rete, sono ridondate in tutte le parti principali. Le caselle di PEC sono registrate su sistemi SAN (Storage Area Network) e quindi sono accessibili da più sistemi.

Queste misure assicurano anche la continuità delle operazioni di copia di sicurezza presso il sito di disaster recovery.

Nei casi invece di disastro improvviso, nei quali si renda necessario attivare il sito di disaster recovery, i citati livelli di servizio non potranno essere rispettati. Le modalità e il tempo di ripristino del servizio saranno definiti negli accordi di servizio.

## **11.3 OPERAZIONI IN CASO DI DISASTRO**

In una località remota rispetto alla sede principale sono presenti sistemi atti a consentire la ripartenza del servizio in caso di disastro che colpisca la sede principale. In tale sito remoto vengono copiati con continuità i dati del sistema di PEC atti a consentire tale ripartenza. Non viene conservato il contenuto delle caselle di posta.

In caso di disastro i titolari verranno tempestivamente informati di quanto avvenuto e delle misure specifiche da attivare nel caso particolare.

Va comunque tenuto presente quanto segue:

1. Le caselle di PEC, una volta fatto ripartire il sistema, non conterranno alcun messaggio; le modalità di ripristino del contenuto delle caselle saranno indicati negli accordi di servizio.
2. Nel caso di disastro che richieda l'attivazione del sito di disaster recovery, la nuova URL ove sarà reperibile il file LDIF sarà attivata non appena reso nuovamente operativo il servizio di PEC, previa comunicazione al CNIPA fatta in modo analogo a quanto previsto nelle Linee Guida [10] per la prima attivazione.
3. A seconda del tipo di disastro il Gestore valuterà quali eventuali ulteriori misure devono essere attivate.

#### **11.4 INDICATORI DI QUALITÀ**

Come richiesto dalla normativa (articolo 20 comma 1 del D.M.I.T [8]), il sistema del Gestore è sottoposto a certificazione di qualità UNI EN ISO 9001: 2000 [r].

Questo obiettivo viene raggiunto in quanto i vari componenti organizzativi, infrastrutturali, tecnici e le registrazioni ad essi relative sono sottoposti periodicamente ed estemporaneamente a controlli svolti internamente ai reparti interessati, a verifiche formali e informali a cura dei Responsabili della sicurezza e dell'auditing, previsti al comma 1 dell'articolo 21 del D.M.I.T [8], e infine a verifica periodica relativa alla citata certificazione di qualità.

Il manuale della qualità è depositato presso il CNIPA e reso disponibile presso il Gestore, come previsto dall'articolo 20, comma 2 del D.M.I.T [8].

Al capitolo 16 sono indicate sinteticamente, nei vari paragrafi, le misure di sicurezza adottate per le varie procedure.

#### **11.5 INTEROPERABILITÀ CON GLI ALTRI GESTORI DI PEC**

Come richiesto dalla normativa (articolo 5 comma 2 del DPR [6]) il Gestore "effettua le verifiche sufficienti e necessarie a garantire gli aspetti di correttezza formale necessari per l'interoperabilità" (articolo 6, comma 4 dell'Allegato [9]).

Il Gestore ha quindi predisposto una casella di PEC specifica per l'effettuazione di test di interoperabilità con gli altri gestori.

## 12. MODALITÀ PER L'APPOSIZIONE E LA DEFINIZIONE DEL RIFERIMENTO TEMPORALE

Il Gestore utilizza una sorgente sicura di tempo da cui ottiene il dato UTC determinato ai sensi dell'articolo 3, comma 1, della legge 11 agosto 1991, n. 273, come previsto dall'articolo 9, comma 2, del D.M.I.T [8]; tale sorgente è ridondata per garantire la continuità del servizio.

Il segnale, emesso dallo Istituto Elettrico Nazionale (IEN) Galileo Ferraris di Torino, è captato via radio con un sistema di ricezione ridonato, formalmente tarato e certificato.

Tale segnale relativo al tempo UTC viene trasmesso in sicurezza al sistema di PEC.

Le procedure adottate e le caratteristiche della rete di trasmissione del segnale UTC assicurano che l'ora riportata nei riferimenti temporali non si discosta da quella rilevata dal sistema di rilevazione UTC di più di un minuto secondo.

### **13. CONDIZIONI DI FORNITURA DEL SERVIZIO**

1. Il Gestore può demandare le mansioni di registrazione utenti Titolari, descritte al §7.1, e quelle di revoca, disattivazione, riattivazione e riassegnazione delle caselle di PEC, descritte al § 7.2, a Organizzazioni esterne, siano esse clienti o fornitori del Gestore in virtù di specifici accordi.
2. Il Titolare accetta di operare con il Gestore, per le predette funzioni, tramite gli Amministratori dei titolari che il Gestore gli indicherà.
3. Il Gestore si obbliga al rispetto di quanto indicato nel presente Manuale Operativo e in particolare a quanto indicato al § 15.1.
4. Il Gestore potrà modificare le modalità di erogazione del servizio di PEC a seguito dell'evoluzione della tecnologia e in adeguamento di variazioni della normativa.
5. Le responsabilità del Gestore sono descritte al § 15.4, nei limiti indicati al § 15.6.
6. Il Titolare si obbliga al rispetto di quanto indicato nel presente Manuale Operativo e in particolare a quanto indicato al § 15.2.
7. L'Organizzazione cliente si obbliga al rispetto di quanto indicato nel presente Manuale Operativo e in particolare a quanto indicato al § 15.3.
8. L'accordo di fornitura si intende applicabile solo al Contraente, sia esso Contraente Privato (§ 9.1) o Contraente Organizzazione (9.2).
9. Nel caso di Contraente Privato, la casella di PEC relativa potrà essere trasferita ad altro contraente solo con il consenso delle parti interessate, e cioè il Gestore, il precedente contraente e il nuovo contraente.
10. Per ogni controversia è competente esclusivamente il Foro di Roma.

#### 14. MODALITÀ DI PROTEZIONE DEI DATI DEI TITOLARI

La gestione dei dati personali che ricadono sotto il D.lgs. n. 196/2003 [3] e successive integrazioni e modificazioni, nonché l'invio al Garante per la protezione dei dati personali delle comunicazioni relative avvengono secondo le modalità previste dalle norme vigenti.

In particolare:

1. All'atto della registrazione l'Amministratore dei Titolari, per conto del Gestore o direttamente per conto dell'Organizzazione cliente, sottopone al titolare l'informativa prevista dall'articolo 13, comma 1, del citato D.lgs. n. 196/2003;
2. Sono adottate le misure minime di sicurezza previste dagli articoli 33 – 36 del citato D.lgs. n. 196/2003 e, in particolare:
  - a) l'accesso ai dati soltanto da parte di persone autorizzate dietro autenticazione;
  - b) la gestione delle credenziali di accesso del personale autorizzato;
  - c) la protezione dei dati contro accessi illeciti anche quando essi sono esportati per motivi di backup;
  - d) la tenuta di un documento programmatico sulla sicurezza nell'ambito dell'organizzazione di cui il Gestore fa parte.

Non sono gestiti dati sensibili nel significato attribuito a questo termine dal citato D.lgs. 196/2003.

## 15. OBBLIGHI

Nello svolgimento della sua attività, il Gestore opera in conformità con quanto richiesto dalle normative di legge in vigore. In particolare, sono osservate le disposizioni seguenti:

- D.lgs. n. 82/2005 [7]<sup>1</sup>;
- D.P.R. n. 68/2005 [6];
- D.M.I.T. del 2 novembre 2005 [8] e relativo Allegato Tecnico [9];
- Circolare CNIPA n. 49/2005 [10];
- Deliberazione CNIPA n. 11/2004 [5].

### 15.1 OBBLIGHI DEL GESTORE

Il Gestore è responsabile nei confronti di terzi di quanto è eseguito per quanto riguarda il servizio di PEC dal proprio personale e da quello di altre organizzazioni che operino per proprio conto e in proprio nome. Il Gestore non potrà essere ritenuto responsabile di quanto fatto dai Titolari tramite le caselle di PEC ad essi assegnate dal Gestore stesso.

Esso mette in atto le seguenti misure tecnico/organizzative, conformi con la citata normativa in vigore e, in particolare:

- impiega personale dotato delle conoscenze specifiche, dell'esperienza e delle competenze necessarie, in conformità con quanto disposto all'articolo 22, comma 1 del D.M.I.T [8];
- attribuisce al citato personale gli incarichi di responsabilità previsti dall'articolo 21 del D.M.I.T [8];
- applica procedure e metodi amministrativi e di gestione adeguati e tecniche consolidate;
- assicura la segretezza della corrispondenza trasmessa tramite il proprio servizio di PEC, come previsto dall'articolo 49 del D.lgs. n. 82/2005 [7];
- adotta protocolli sicuri, come previsto all'articolo 8, comma 3, dell'Allegato tecnico [9]<sup>2</sup>, atti a garantire l'integrità, l'autenticità e la riservatezza delle comunicazioni:

---

<sup>1</sup> Il D.lgs. n. 82/2005 [7] ha abrogato e sostituito gli articoli del D.P.R. n. 445/2000 [2] relativi alla posta elettronica certificata

<sup>2</sup> Il citato passo dell'Allegato [9] cita a titolo esemplificativo: "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)."

- tra titolare e Gestore;
  - tra Gestore e CNIPA;
  - con gli altri gestori di PEC;
- assicura il rispetto delle norme previste dal D.M.I.T [8] e dall'Allegato tecnico al D.M.I.T [9], compresi gli standard tecnici ivi indicati, per il raggiungimento dell'interoperabilità con gli altri gestori di PEC;
  - adotta misure atte a impedire l'introduzione di codici eseguibili dannosi (ad es. virus) nel circuito di PEC;
  - prevede servizi di emergenza che assicurano il completamento della trasmissione anche in caso di incidente, tranne nel caso in cui si verifichi un evento improvviso dagli esiti disastrosi (terremoto, attentato, ecc.). In questo caso, vengono seguite procedure di disaster recovery Management che consentono di ripristinare il servizio presso altra sede, ove necessario;
  - assicura il rispetto dei livelli di servizio richiesti dalla normativa in vigore anche al verificarsi di incidenti non configurabili come disastri improvvisi;
  - salvo casi di disastri improvvisi, assicura la consegna delle ricevute di accettazione al mittente;
  - salvo casi di disastri improvvisi, segnala al mittente l'eventuale mancata ricezione della ricevuta di presa in carico o di avvenuta consegna entro i termini previsti dall'articolo 13 del D.M.I.T [8] e dall'articolo 6, comma 3, dell'Allegato tecnico [9];
  - entro i dodici mesi successivi al suo inserimento nell'elenco pubblico dei Gestori di PEC, in conformità con quanto previsto dall'articolo 7, comma 5, dell'Allegato Tecnico [9], provvede alla certificazione del sistema di qualità relativo al proprio processo di erogazione di PEC in base alle norme UNI EN ISO 9001: 2000 [r], successive evoluzioni o a norme equivalenti;
  - è assicurato contro i rischi dell'attività e i danni causati a terzi;
  - assicura che le proprie chiavi di firma siano generate dai responsabili dei server che le utilizzeranno, in conformità con quanto indicato nell'apposito Manuale Operativo CNIPA [12];
  - con una tempistica tale da non creare interruzioni di servizio attiva la procedura di sostituzione di un certificato elettronico relativo alle proprie chiavi di firma;
  - gestisce i dati personali di cui viene in possesso nel rispetto del "Codice in materia di protezione dei dati personali", di cui al decreto legislativo 30 giugno 2003, n. 196 [3],
  - nel caso di clienti che siano persone fisiche identifica il richiedente con certezza al momento della sottoscrizione del più volte citato accordo di servizio;

- nel caso in cui il cliente sia una persona fisica lo informa, con un mezzo di comunicazione durevole, sugli obblighi da lui assunti con la sottoscrizione dell'accordo di servizio, in particolare su ciò che riguarda la riservatezza delle sue credenziali e la sua responsabilità per quanto fatto con la casella di PEC a lui assegnata;
- nel caso in cui il cliente sia una persona giuridica lo informa del suo dovere di comunicare ai titolari che a lui fanno capo gli obblighi da essi assunti, come indicato al precedente punto;
- conserva le informazioni e i dati relativi agli accordi di servizio stipulati con i clienti secondo la vigente normativa civilistica;
- previa verifica dell'autenticità della richiesta, effettua la revoca, la sospensione o la riattivazione di una casella di PEC;
- comunica al Titolare l'avvenuta revoca, sospensione o riattivazione della sua casella di PEC tramite l'Amministratore dei titolari di riferimento;
- comunica al CNIPA ogni variazione significativa delle soluzioni tecnico-organizzative adottate entro quindici giorni dalla modifica (articolo 14, comma 11, del D.P.R. n. 68/2005 [6]);
- comunica la cessazione della propria attività ai propri clienti come previsto negli specifici accordi e ne informa tempestivamente il CNIPA;
- in caso di compromissione delle chiavi private utilizzate per firmare i messaggi indicati all'articolo 6, comma 2, del D.M.I.T [8] e per realizzare le connessioni sicure con il sito CNIPA, richiede con urgenza la revoca dei corrispondenti certificati con le modalità indicate al § 10.9 del Manuale operativo CNIPA [11];
- rende accessibile per via telematica:
  - le istruzioni su come chiedere l'accesso alle informazioni contenute nei record di log;
  - il presente Manuale operativo, o i suoi aggiornamenti, all'indirizzo Internet specificato al § 5.2 e con le modalità ivi indicate, in particolare:
    - ♦ all'inizio della propria operatività;
    - ♦ ad ogni variazione del Manuale stesso;
- consente l'accesso ai sistemi e dispositivi di PEC esclusivamente alle persone autorizzate, identificate attraverso una opportuna procedura di riconoscimento da parte del sistema al momento di apertura di ciascuna sessione;
- utilizza, per la propria *firma del Gestore di posta elettronica certificata*, dispositivi di firma conformi a criteri di sicurezza riconosciuti in ambito europeo o internazionale;
- opera in modo che non sia consentita la copia delle chiavi private di firma o dei dispositivi di firma che le contengono;

- consente l'esportazione delle chiavi private di firma, effettuata con modalità che non riducano il livello di sicurezza, solo allo scopo di consentire la ripartenza dopo incidenti di sicurezza nel caso di disastri che non richiedano lo spostamento delle operazioni presso il sito di disaster recovery;
- non consente l'uso della chiave usata per apporre le firme del Gestore per funzioni diverse da quella;
- dispone di un sistema di riferimento temporale che garantisce stabilmente uno scarto non superiore ad un minuto secondo rispetto alla scala di Tempo Universale Coordinato (UTC), determinata ai sensi dell'articolo 3, comma 1, della legge 11 agosto 1991, n. 273;
- associa un riferimento temporale a ciascuna registrazione annotata nel log e ai dati di certificazione associati ai messaggi di cui all'articolo 6 del D.M.I.T [8];
- garantisce la riservatezza, la sicurezza, l'integrità e l'inalterabilità nel tempo delle registrazioni di log, come richiesto dall'articolo 11 del D.P.R. n. 68/2005 [6], nel rispetto delle norme definite all'articolo 10 del D.M.I.T [8], e ne cura la conservazione sostitutiva, in conformità con quanto previsto dalla Deliberazione n. 11/2004 [5], per almeno 30 mesi.

## 15.2 OBBLIGHI DEL TITOLARE

Il Titolare di una casella di PEC è responsabile di tutto quanto venga effettuato tramite la casella di posta assegnatagli.

Il Titolare deve:

1. Fornire al Gestore o all'Amministratore dei titolari tutte le informazioni richieste, garantendone l'attendibilità sotto la propria responsabilità.
2. Comunicare al Gestore o all'Amministratore dei titolari, secondo le modalità comunicategli, eventuali variazioni alle informazioni già fornite.
3. Conservare con la massima diligenza le credenziali di attivazione e di ripristino della casella di PEC fornitigli.
4. Modificare tali credenziali subito dopo averle utilizzate.
5. Aggiornare con la periodicità indicata nell'accordo di servizio le credenziali di accesso alla propria casella di PEC.
6. Usare cautela nell'uso della casella e nel proteggerne l'accesso da parte di persone non autorizzate poiché è responsabile del suo contenuto e del suo utilizzo.

7. Sostituire le proprie credenziali con la massima celerità nel caso in cui ritenga che la loro segretezza sia stata compromessa.
8. Mettere in atto tutte le misure necessarie per evitare l'introduzione di virus e altro codice dannoso nel circuito di PEC.
9. Accedere in lettura alla propria casella di PEC il più frequentemente possibile (si veda Nota al § 8.1.5).
10. Richiedere immediatamente la sospensione della propria casella di PEC nel caso ritenga compromessa la segretezza delle credenziali di accesso e non sia in grado di modificarle prontamente.

### **15.3 OBBLIGHI DELL'ORGANIZZAZIONE CUI FANNO CAPO I TITOLARI**

Un'Organizzazione cui fanno capo i titolari ha i seguenti obblighi a cui ottempera tramite i propri Amministratori dei titolari. Questi ultimi costituiscono l'unica interfaccia responsabile dei contatti con il Gestore riguardanti la gestione dei titolari e sono tenuti a:

1. Identificare i titolari a cui assegna le caselle di PEC.
2. Assegnare la responsabilità di una casella di posta a una sola persona per volta.
3. Tenere traccia dell'assegnazione di una casella di PEC ai vari responsabili.
4. Porre i Titolari che ad essa fanno riferimento a conoscenza dei rispettivi obblighi (si veda § 15.2).

Eventuali ulteriori obblighi saranno indicati nello specifico accordo tra l'Organizzazione e il Gestore, quale, ad esempio, quello di comunicare tempestivamente al Gestore le variazioni di assegnazione delle caselle di PEC a persone fisiche.

### **15.4 RESPONSABILITÀ DEL GESTORE**

Il Gestore è responsabile verso i Titolari, per l'adempimento di tutti gli obblighi discendenti dall'espletamento delle attività previste dalla normativa in vigore, solo nei casi di dolo o colpa grave.

Il Gestore non potrà essere ritenuto responsabile delle conseguenze di eventi ad esso non imputabili, quali, a solo titolo di esempio: calamità naturali, disfunzioni tecniche e logistiche al di fuori del suo controllo, interventi dell'autorità, attentati, rivolte o atti di guerra che colpiscano anche o solo i soggetti delle cui attività il Gestore si avvale per la prestazione dei propri servizi di PEC.

Il Gestore non assume altresì responsabilità per le conseguenze derivanti dal mancato rispetto delle modalità operative specificate nel presente Manuale Operativo da parte di un suo cliente.

Il Gestore non è responsabile per le conseguenze derivanti da disfunzioni tecniche, organizzative o funzionali di altri enti.

#### **15.5 ASSICURAZIONE**

Il Gestore, in conformità con quanto disposto all'articolo 16, comma 2, del D.P.R. n. 68/2005 [6], ha stipulato un contratto assicurativo per la copertura dei rischi dell'attività e dei danni causati a terzi.

#### **15.6 LIMITAZIONI DELLE RESPONSABILITÀ**

Il Gestore non risponderà di eventi ad esso non imputabili ed esclude ogni responsabilità per danni subiti dagli utenti titolari o da terzi in conseguenza:

- del mancato rispetto delle procedure e delle regole stabilite dal Gestore;
- del danno causato da disservizio non imputabile al Gestore;
- della mancata assunzione da parte degli utenti titolari o di terzi delle misure di speciale diligenza, che si richiedono al fruitore di servizi di PEC, idonee ad evitare l'evento dannoso;
- di fatti ed atti illeciti svolti da parte degli utenti titolari o di terzi.

Il Gestore non sarà responsabile di qualsiasi inadempimento o comunque di qualsiasi evento dannoso determinato da caso fortuito o da eventi di forza maggiore.

## 16. DESCRIZIONE SINTENTICA PROCEDURE ADOTTATE

### 16.1 CARATTERISTICHE DI SICUREZZA

Presso il Gestore sono in vigore opportune misure per garantire la maggior sicurezza possibile.

Infatti, in base alle attività di Risk Assessment, condotte periodicamente o quando necessario, possono venire adeguate le Security Policy in vigore. Il tutto viene gestito dal Responsabile della sicurezza e dal team da esso coordinato previsto dall'articolo 21, comma 1, del D.M.I.T [8].

I compiti assegnati alla struttura coordinata dal responsabile della sicurezza sono tra gli altri quelli di:

- proporre, definire e assicurare l'applicazione dei criteri di sicurezza logica di tutti i sistemi informativi;
- assicurare la tutela dei dati personali e la riservatezza di dati e documenti gestiti verificandone l'adozione e l'attuazione attraverso le opportune procedure organizzative, informatiche e tecnologiche, con particolare riguardo all'accessibilità dei dati e alla prevenzione da intrusioni.
- coordinarsi con le strutture operative per quanto riguarda gli aspetti sistemistica e gestionali, nonché di sicurezza del CED.

Il piano di disaster recovery è gestito dal disaster recovery Manager sotto il controllo del responsabile della Sicurezza.

L'infrastruttura fisica, le apparecchiature, la competenza del personale e le procedure adottate sono tali da garantire un'operatività senza interruzioni nel rispetto dei livelli di servizio indicati all'articolo 12 del D.M.I.T [8].

L'accesso a strumenti, infrastrutture e a quant'altro utilizzato per erogare i servizi di PEC è strettamente limitato ai soli addetti ed è controllato.

Le modalità di messa in esercizio di nuovi prodotti (HW e SW) e procedure segue norme interne atte a prevenire malfunzionamenti e ad impedire intrusioni logiche nei sistemi e nella rete.

Sono inoltre in essere le misure previste dalla normativa per prevenire l'introduzione di virus informatici nel circuito PEC.

Il Gestore nell'eventualità di cessazione dell'attività chiederà a CNIPA la revoca dei propri certificati elettronici di firma e gestirà poi l'evento in modo da rendere di fatto impossibile ogni utilizzo abusivo delle proprie chiavi di firma.

## **16.2 SINTESI DELLE PROCEDURE PRINCIPALI**

Come dichiarato nella domanda di iscrizione consegnata a CNIPA in ottemperanza a quanto specificato all'articolo 1 del D.M.I.T 2 novembre 2005 [8], il sistema di PEC del Gestore è conforme ai requisiti indicati dal D.P.R. n. 68/2005 [6] e dal citato D.M.I.T.

Vengono di seguito indicate sinteticamente le procedure attuate per ottenere tale conformità.

### **16.2.1 INSTALLAZIONE DELLE APPARECCHIATURE**

Le apparecchiature per la prestazione dei servizi di PEC, comprese le apparecchiature di rete, sono installate dal personale appositamente autorizzato ad operare sui sistemi che svolgono i servizi di PEC.

Il disegno architettuale del sistema ha portato alla definizione di un sistema con un alto grado di affidabilità, con tutte le componenti hardware e software ridondate sia di sistema che di rete per consentire il raggiungimento degli elevati livelli di servizio previsti dalla normativa.

Il software necessario all'erogazione dei servizi di PEC viene installato e configurato, dopo essere stato verificato in un ambiente funzionalmente analogo, dal personale appositamente autorizzato a operare sui sistemi che svolgono i servizi di PEC.

Le regole di configurazione dei singoli sistemi HW e SW necessari all'erogazione dei servizi di PEC incluse quelle che riguardano le apparecchiature di rete, sono documentate preventivamente e una copia del documento relativo viene conservata in modo sicuro per consentire verifiche successive.

Le configurazioni in esercizio degli apparati e del software sono documentate.

### **16.2.2 CAPACITY PLANNING**

Periodicamente viene fatta una valutazione delle future necessità in termini di HW, SW, locali, personale e, ove necessario, si provvede ad adeguare il servizio.

### **16.2.3 GENERAZIONE DELLE CHIAVI DI FIRMA, LORO GESTIONE**

Le coppie di chiavi di firma utilizzate per apporre la firma del Gestore sono generate, da parte del personale addetto in regime di job separation e di dual control, direttamente all'interno di dispositivi di firma rispondenti ai requisiti di certificazione indicati all'articolo 14, lettera e), del D.P.R. n. 68/2005 [6]. Le

coppie di chiavi di firma vengono generate in conformità con quanto previsto all'Allegato C della norma ANSI X9.17 [s].

Copia a scopo di backup delle chiavi private viene effettuata subito dopo la loro generazione con procedure per le quali il dispositivo ha ottenuto la certificazione di sicurezza. Queste copie di backup sono custodite solo nel sito principale del Gestore e possono essere attivate soltanto nel rispetto delle procedure per le quali il dispositivo ha ottenuto la certificazione di sicurezza.

Per ogni coppia di chiavi viene richiesto al CNIPA il certificato elettronico della chiave pubblica corrispondente in conformità con le procedure indicate nel Manuale Operativo CNIPA [12]

Il certificato ricevuto da CNIPA viene quindi inserito in un file LDIF generato dal Gestore come previsto all'articolo 7, comma 5, dell'Allegato [9]; in tale file sono inseriti i certificati corrispondenti a tutte le coppie di chiavi di firma utilizzate dal Gestore per apporre le proprie firme.

Come indicato nelle Linee Guida [11], almeno 48 ore prima dell'effettiva attivazione del proprio servizio il Gestore comunica al CNIPA la data in cui il proprio file LDIF sarà disponibile. Tale comunicazione è inviata alla casella di posta elettronica indicata nella lettera con cui CNIPA ha comunicato al Gestore il suo accreditamento.

Il file LDIF di cui ai capoversi precedenti viene acquisito con cadenza almeno giornaliera dal CNIPA che ne inserisce il contenuto in un file LDIF, firmato da CNIPA, che costituisce l'Indice Generale dei Gestori di PEC. Questo file LDIF viene utilizzato dal Gestore come indicato al § 16.2.6.

Il Gestore inserisce ogni certificato nelle firme generate tramite la chiave privata corrispondente ai tipi di messaggio indicati all'articolo 6 del D.M.I.T. [8], in conformità con quanto definito all'articolo 6, comma 1, dell'Allegato tecnico [9].

In conformità con quanto indicato all'articolo 7, comma 5, dell'Allegato [9] il Gestore opera nel modo seguente all'approssimarsi della scadenza di ogni certificato di firma e, in particolare:

1. Con una tempestività tale da consentire alle funzioni di PEC di operare senza soluzioni di continuità, viene ripetuta per la coppia di chiavi il cui certificato è in scadenza l'operazione di generazione di una nuova coppia di chiavi e di richiesta di certificato a CNIPA.
2. Aggiunge il nuovo certificato nel proprio file LDIF indicato sopra senza rimuoverne i certificati scaduti.

#### 16.2.4 GESTIONE DEI DISPOSITIVI DI FIRMA

I dispositivi di firma sono custoditi in modo sicuro a cura del personale responsabile.

In caso di malfunzionamento dei dispositivi di firma, essi verranno re-inizializzati e le chiavi ripristinate.

In caso di una eventuale cessazione da parte del Gestore delle attività di PEC i dispositivi di firma saranno inizializzati in modo da cancellare ogni traccia delle chiavi private ivi conservate. Ove necessario si procederà alla distruzione di quei dispositivi o supporti dai quali non sia possibile eliminare le chiavi private.

#### 16.2.5 PROTEZIONE DEI MESSAGGI DI PEC

Il Gestore opera in modo da proteggere la riservatezza dei messaggi di posta da esso conservati da accessi effettuati da chiunque non sia in possesso di valide credenziali. Questo è in ottemperanza con quanto disposto dall'articolo 49 del D.lgs. n. 82/2005 [7].

Per un'analoga protezione nei collegamenti del Gestore con i titolari e con gli altri gestori vengono usati protocolli resi sicuri mediante l'uso dell'autenticazione basata su crittografia asimmetrica seguita da cifratura simmetrica dei messaggi scambiati tra i due estremi del collegamento, per esempio i protocolli elencati al capitolo 8.3 dell'Allegato tecnico [9]<sup>3</sup>.

#### 16.2.6 UTILIZZO IGPEC

L'Indice Generale dei gestori di PEC "contiene i dati dei gestori e dei relativi domini di posta certificata" (Allegato [9], articolo 7, comma5). In particolare questo Indice consiste di un file LDIF generato dal CNIPA, contenente i certificati corrispondenti alle chiavi private utilizzate dai vari gestori per generare le *Firme del Gestore di posta elettronica certificata* ed è autenticato dalla firma del CNIPA.

Il file LDIF di cui al capoverso precedente, aggiornato con cadenza almeno giornaliera dal CNIPA, viene tempestivamente scaricato dal Gestore che ne controlla l'autenticità verificando la firma appostavi da CNIPA mediante verifica dell'autenticità del certificato utilizzato da CNIPA<sup>4</sup>. I certificati in esso contenuti

---

<sup>3</sup> Il capitolo 8.3 dell'Allegato tecnico [9] recita: "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)."

<sup>4</sup> Questo è agevolmente possibile in quanto il certificato utilizzato da CNIPA, come indicato al capitolo 7.1 del Manuale Operativo CNIPA [11], è emesso da una CA il cui certificato radice è riconosciuto automaticamente dai prodotti di mercato.

sono utilizzati dal Gestore per verificare l'autenticità delle firme apposte dagli altri gestori ai messaggi indicati all'articolo 6 del D.M.I.T. [8].

#### **16.2.7 GESTIONE DEL LOG DI PEC**

Conformemente con quanto richiesto dalla normativa di cui all'articolo 11, comma 3, del D.P.R. 68/2005 [6], durante le fasi di trasmissione del messaggio di posta elettronica certificata il Gestore mantiene traccia delle operazioni svolte su un apposito log dei messaggi.

Con frequenza conforme con i requisiti indicati dall'articolo 10 del D.M.I.T. [8] i dati contenuti in tale log vengono estratti e su di essi viene apposta una marca temporale conforme con quanto previsto dal Titolo IV del D.P.C.M. 13 gennaio 2004 [4].

I dati così estratti vengono conservati in modo conforme con la Deliberazione CNIPA n. 11/2004 [5].

In aggiunta a quanto prescritto nella citata Deliberazione, alla firma digitale che il Responsabile della conservazione appone alla chiusura di ogni periodo di conservazione ai dati conservati in tale periodo viene apposta una marca temporale. Questo fa sì che, anche in presenza di eventuali successive revoche del certificato qualificato di firma e comunque dopo la scadenza di quest'ultimo, sia possibile verificare positivamente le firme apposte in regime di validità del certificato stesso.

Il Gestore ottempera a tutti i requisiti della Deliberazione CNIPA 11/2004 [5], in particolare, onde "consentire l'esibizione di ciascun documento conservato"<sup>5</sup> durante tutto il periodo richiesto anche al verificarsi di casi di incidente o di disastro, produce regolarmente copie di quanto conservato, le quali sono custodite in modo sicuro sia presso la sede principale sia presso una sede alternativa. In analogo modo sono conservate copie dei programmi necessari per accedere e elaborare i record di log onde renderne accessibile il contenuto.

Quanto conservato in modo conforme con quanto sopra viene custodito per il tempo previsto dall'articolo 11, comma 3, del D.M.I.T [8] e cioè per almeno trenta mesi.

#### **16.2.8 ADDESTRAMENTO DEL PERSONALE**

Il personale del Gestore e delle organizzazioni che cooperino con il medesimo alla gestione delle caselle di PEC viene addestrato costantemente sulle

---

<sup>5</sup> Art. 5.1.lettera a)

procedure ivi incluse le procedure di sicurezza e, ove del caso, sui sistemi e sui SW interessati.

Tale personale viene anche mantenuto costantemente aggiornato sulle procedure da seguire al verificarsi di incidenti di sicurezza.

#### **16.2.9 CESSAZIONE DELLE OPERAZIONI**

Qualora il Gestore intenda cessare l'attività di fornitura di caselle di PEC, comunicherà con un anticipo di almeno 30 giorni tale decisione ai propri clienti e al CNIPA indicando a quale Organizzazione consegnerà la documentazione la cui conservazione è prevista a norma di legge (in particolare la documentazione relativa a clienti e titolari, e i log). Chiederà inoltre che i certificati di firma ad esso assegnati siano revocati in data e ora compatibili con quella prevista per la cessazione delle operazioni. Successivamente all'emissione dell'ultima firma del Gestore verranno chiusi i collegamenti con i titolari e con gli altri gestori.

I titolari sono tenuti a seguire le procedure indicate dal Gestore per la cessazione del servizio e a rispettare i tempi indicati.

Una volta trascorso il tempo indicato ai Titolari per terminare queste operazioni:

1. Il Gestore:

- a) cancellerà in modo sicuro tutte le chiavi private di firma da esso utilizzate per fornire il servizio di PEC ed eventuali loro copie, distruggendo i dispositivi per i quali non esistano altri mezzi per garantire la cancellazioni delle chiavi private;
- b) chiederà la revoca dei propri certificati di firma: la richiesta di revoca sarà formulata seguendo una tempistica tale da evitare un indebolimento delle misure di sicurezza relative alla chiave privata di firma;
- c) prima di cessare le proprie attività provvederà ad acquisire la documentazione sullo stato dei propri certificati di firma PEC (CRL o risposte di OCSP server) nella quale essi risultino tutti revocati;
- d) consegnerà la documentazione di cui al punto precedente e quella di cui è prevista la conservazione all'Organizzazione che avrà indicato nelle sue precedenti comunicazioni ai clienti e al CNIPA.