Manuale Operativo

Posta Elettronica Certificata

Copia Archiviata Elettronicamente	File: MOP_PEC_01_1.1

Copia Controllata in distribuzione ad enti esterni	N°: 1
Rilasciata al *Centro Nazionale per l'Informatica nella Pubblica Amministrazione*	

Versione	Pagina n.	Motivo della revisione	Data
1.0	tutte	Approvazione	05/12/2005
1.1	tutte	Aggiornamento Rif. Temporale, Rif. Standard di sicurezza, Messaggi massivi, Dimensione massima messaggio garantita, aggiornamento connettività, Responsabili privacy, Adeguamento riferimenti normativi	18/03/2008

Versione	Redazione	Verifica	Approvazione	Data
1.0	Marilli Rupi	Stefano Carbone Renzo Ullucci	Dario Cassinelli Roberto Palumbo	05/12/2005
1.1	Marilli Rupi	Renzo Ullucci Carlo Vona	Dario Cassinelli Roberto Palumbo	18/03/2008

Indice

SEZIONE I: DATI GENERALI

1 Introduzione

1.1 Premessa

Il Manuale Operativo definisce le procedure applicate da Postecom nello svolgimento della propria attività di Gestore di Posta Elettronica Certificata ed è rivolto a tutti i soggetti che entrano in relazione con il Gestore o che ne utilizzano i servizi:

- ⇒ Soggetti che sottoscrivono il contratto d'uso del servizio;
- ⇒ Organizzazioni che sottoscrivono il contratto d'uso del servizio al fine di fornire la casella ad i propri appartenenti o a soggetti terzi;
- ⇒ "Amministratori del Sistema" quale soggetti di interfaccia con il Gestore, preposti alla individuazione ed all'attivazione dei Titolari delle caselle di posta elettronica certificata, nei contesti organizzativi;
- ⇒ Utenti che accedono alla casella di Posta Elettronica Certificata per spedire messaggi o per verificarne la ricezione.

All'interno del presente Manuale, per i soggetti sopra elencati, sono definiti gli obblighi e le corrispondenti responsabilità. Il Manuale Operativo riporta i dati identificativi del Gestore.

1.2 Riferimenti normativi

DLvo 82/2005	Decreto Legislativo 7 marzo 2005, n° 82 - *Codice dell'amministrazione digitale*
DPR 68/2005	Decreto del Presidente della Repubblica 11 febbraio 2005, n. 68 - *Regolamento recante disposizioni per l'utilizzo della posta elettronica certificata, a norma dell'articolo 27 della legge 16 gennaio 2003, n. 3*
DM 2/11/2005	Decreto del Ministro per l'Innovazione e le Tecnologie - *Decreto del Ministro per l'Innovazione e le Tecnologie recante Regole Tecniche per la formazione, la trasmissione e la validazione, anche temporale, della Posta Elettronica Certificata*
CNIPA/CR/49	Circolare CNIPA 24 novembre 2005, n° CNIPA/CR/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.*
Circolare Cnipa del 7 dicembre 2006, n. 51	Circolare per la vigilanza sui Gestori di Posta Elettronica Certificata
DLvo 196/2003	Decreto Legislativo 30 giugno 2003, n° 196 - *Codice in materia di protezione dei dati personali*

2 Definizioni

Soggetti del servizio

Gestore di Posta Elettronica Certificata	Postecom che gestisce uno o più domini di posta elettronica certificata che, nel rispetto della normativa vigente, si interfaccia con altri gestori di posta elettronica certificata per l'interoperabilità con altri titolari.
Utente di posta elettronica certificata	La persona fisica, 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.
Organizzazione	Il soggetto, pubblico o privato, che stipula un contratto di servizio per la posta certificata, finalizzato al rilascio di caselle a propri appartenenti o a soggetti terzi.
Amministratore del Sistema presso le organizzazioni	Soggetto di interfaccia con il Gestore, preposto alla individuazione ed attivazione dei Titolari delle caselle di posta elettronica certificata nei contesti amministrativi.
CNIPA	Centro Nazionale per l'Informatica nella Pubblica Amministrazione.

Componenti del servizio

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

Nodi del sistema

Punto di accesso	Il sistema che fornisce i servizi di accesso per l'invio e la lettura di messaggi di posta elettronica certificata, nonché i servizi di identificazione ed accesso dell'utente, di verifica della presenza di virus informatici all'interno del messaggio, di emissione della ricevuta di accettazione e di imbustamento del messaggio originale nella busta di trasporto.
Punto di ricezione	Il sistema che riceve il messaggio all'interno di un dominio di posta elettronica certificata, effettua i controlli sulla provenienza e sulla correttezza del messaggio ed emette la ricevuta di presa in carico, imbusta i messaggi errati in una busta di anomalia e verifica la presenza di virus informatici all'interno dei messaggi di posta ordinaria e delle buste di trasporto.
Punto di consegna	Il sistema che compie la consegna del messaggio nella casella PEC del

	titolare destinatario, verifica la provenienza e la correttezza del messaggio ed emette, a seconda dei casi, la ricevuta di avvenuta consegna o l'avviso di mancata consegna.

Accettazione dei messaggi

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

Comunicazioni tra i gestori

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.

Consegna dei messaggi

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

Componenti della trasmissione telematica

Messaggio originale	Il messaggio inviato da un utente di posta elettronica certificata prima del suo arrivo al punto di accesso e consegnato al titolare destinatario per mezzo di una busta di trasporto che lo contiene.
Busta di trasporto	La busta creata dal punto di accesso e sottoscritta con la firma del gestore di posta elettronica certificata mittente, all'interno della quale sono inseriti il messaggio originale inviato dall'utente di posta elettronica certificata ed i relativi dati di certificazione.
Busta di anomalia	La busta, sottoscritta con la firma del gestore di posta elettronica certificata del destinatario, nella quale è inserito un messaggio errato ovvero non di posta elettronica certificata e consegnata ad un titolare, per evidenziare al destinatario detta anomalia.
Dati di certificazione	I dati, quali ad esempio data ed ora di invio, mittente, destinatario, oggetto, identificativo del messaggio, che descrivono l'invio del messaggio originale e sono certificati dal gestore di posta elettronica certificata del mittente; tali dati sono inseriti nelle varie ricevute e sono trasferiti al titolare destinatario insieme al messaggio originale per mezzo di una busta di trasporto.
Marca Temporale	Evidenza informatica con cui si attribuisce, ad uno o più documenti informatici, un riferimento temporale opponibile ai terzi.

3 Dati identificativi e riferimenti

3.1 Dati del Gestore

Denominazione e Ragione sociale	**Postecom S.p.A.**
Rappresentante legale	*Dott. Dario Cassinelli*
Sede legale	*Viale Europa n.175, 00144 Roma*
Telefono	*+39 06 59581*
Sede operativa	*Viale Europa n.175, 00144 Roma*
Telefono	*+39 06 59581*
Indirizzo E-mail	*pecmanager@postecom.it*
Indirizzo Internet	*http://www.poste.it*
Call Center	*803160*

3.2 Dati identificativi del Manuale Operativo

Il presente Manuale Operativo è identificato attraverso il numero di versione 1.1.

Il corrispondente file in formato elettronico, conservato presso i locali del Gestore e depositato presso il CNIPA è identificabile dal nome “MOP_PEC_01_1.1” ed è consultabile per via telematica all’indirizzo Internet: http://www.poste.it nella sezione “Postecert - Servizi di Posta Elettronica Certificata”.

Questo manuale si riferisce ai servizi di Posta Elettronica Certificata come implementati da Postemail Certificata del Gestore Postecom S.p.A., in osservanza della normativa vigente elencata nell’apposito capitolo.

3.3 Responsabile

Responsabile del Manuale Operativo	
Nome	**Renzo**
Cognome	**Ullucci**
Telefono	**+39 06 59581**
E-mail	**renzo.ullucci@postecom.it**

3.4 Riferimenti del sito web del gestore

I riferimenti del sito web di Postecom sono:

- ⇒ indirizzo web *http://www.poste.it* dove è possibile trovare le informazioni relative al servizio, compreso il presente Manuale Operativo;
- ⇒ *https://pec.poste.it* (o altro indirizzo segnalato sul sito *www.poste.it*) per l'accesso al servizio di Postemail Certificata nella Modalità Base;
- ⇒ *https://gestionepec.poste.it* (o altro indirizzo comunicato direttamente al titolare del contratto di fornitura) per le funzionalità di gestione delle utenze di posta elettronica certificata nella Modalità Avanzata.

4 Indice dei contenuti

Contenuto in relazione alla circolare CNIPA/CR/49 del 24/11/2005	**Descrizione nel Manuale Operativo**
Dati identificativi del gestore	§ 3.1
Responsabile del Manuale Operativo	§ 3.3
Riferimenti normativi per la verifica dei contenuti	§ 1.2
Indirizzo web del Gestore Postecom dove è presente il Manuale Operativo	§ 3.2
Procedure e standard tecnologici e di sicurezza	§ 12
Definizioni, abbreviazioni e termini tecnici	§ 2
Descrizione sintetica del servizio offerto	§ 5
Descrizione delle modalità di reperimento e di presentazione delle informazioni presenti nei *log*	§ 14
Contenuto e modalità di offerta	§ 6
Modalità di accesso al servizio	§ 7
Indicazione dei livelli di servizio	§ 9
Indicazione delle condizioni di fornitura	§ 8
Indicazione delle modalità di protezione dei dati dei titolari	§ 15
Obblighi, responsabilità e limitazioni in sede di indennizzo	§ 10 § 11

SEZIONE II: POSTEMAIL CERTIFICATA

5 Descrizione del servizio di Posta Elettronica Certificata

5.1 Caratteristiche generali del servizio

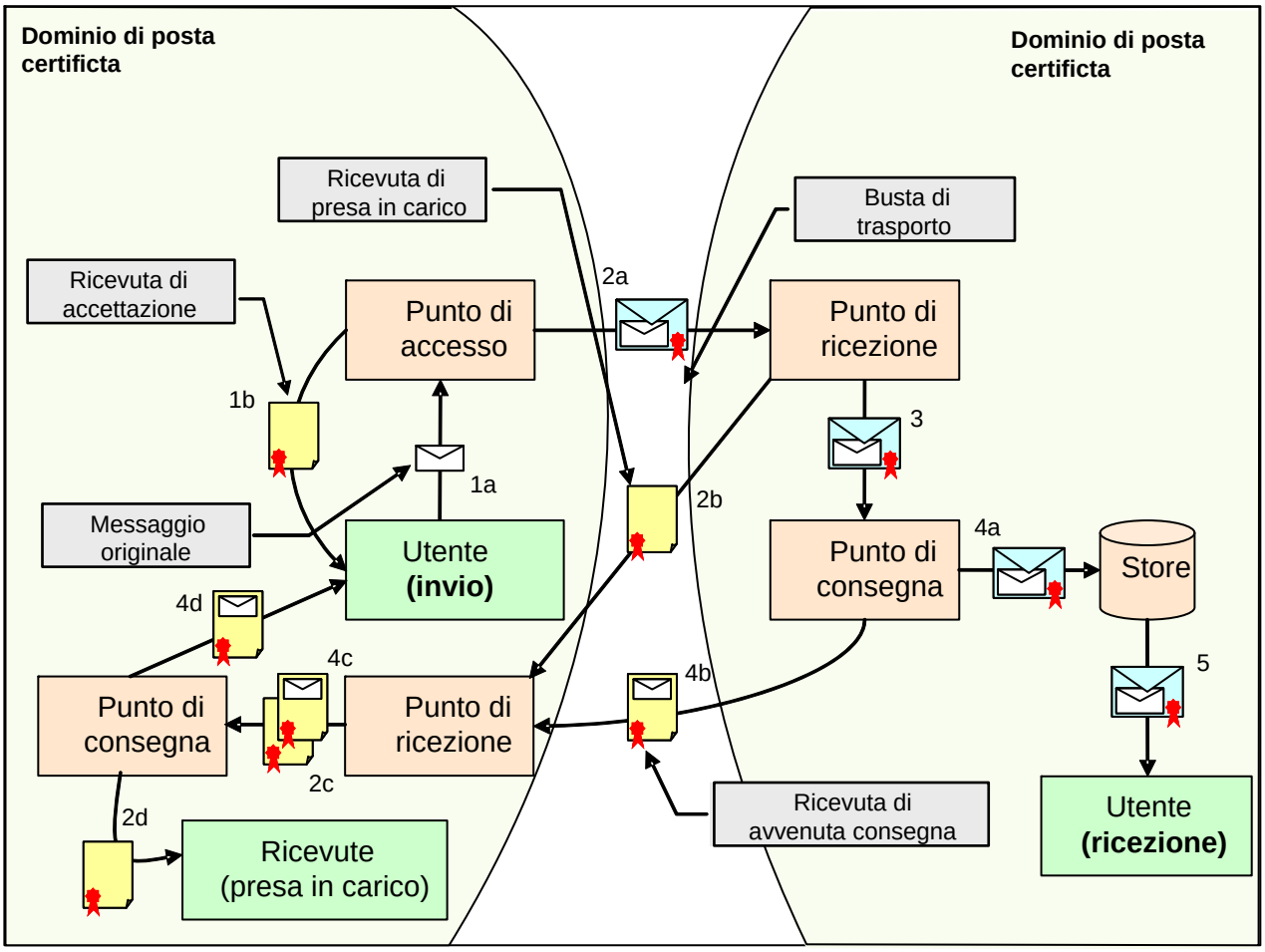
Postemail Certificata è il servizio di Posta Elettronica Certificata di Postecom che consente di inviare e ricevere documentazione elettronica con un elevato livello di sicurezza e di dare valore legale al processo di consegna dei messaggi, nel rispetto della normativa vigente.

Le caselle di Postemail Certificata consentono l'inoltro e la ricezione di messaggi in conformità con quanto previsto dal **DPR 68/2005** e dal **DM 2 novembre 2005**.

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

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

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



⇒ 1a - l'utente invia una e-mail al Punto di Accesso;

⇒ 1b - il Punto di Accesso restituisce al mittente una Ricevuta di Accettazione;

⇒ 2a - il Punto di Accesso crea una Busta di Trasporto (contenente il messaggio originale) e la inoltra al Punto di Ricezione del Gestore di Posta Certificata della casella del destinatario;

⇒ 2b - il Punto di Ricezione verifica la Busta di Trasporto e crea una Ricevuta di Presa in Carico che viene inoltrata al Punto di ricezione del Gestore mittente;

⇒ 2c - il Punto di Ricezione verifica la validità della Ricevuta di Presa in Carico e la inoltra al Punto di Consegna;

⇒ 2d - il Punto di Consegna salva la Ricevuta di Presa in Carico nello store delle ricevute del Gestore;

⇒ 3 - il Punto di Ricezione inoltra la Busta di Trasporto al Punto di Consegna;

⇒ 4a - il Punto di Consegna verifica il contenuto della Busta di Trasporto e la salva nello store (mailbox del destinatario);

⇒ 4b - il Punto di Consegna crea una Ricevuta di Avvenuta Consegna e la inoltra al Punto di Ricezione del Gestore mittente;

⇒ 4c - il Punto di ricezione verifica la validità della Ricevuta di avvenuta consegna e la inoltra al Punto di Consegna;

⇒ 4d - il Punto di Consegna salva la Ricevuta di Avvenuta Consegna nella mailbox del mittente;

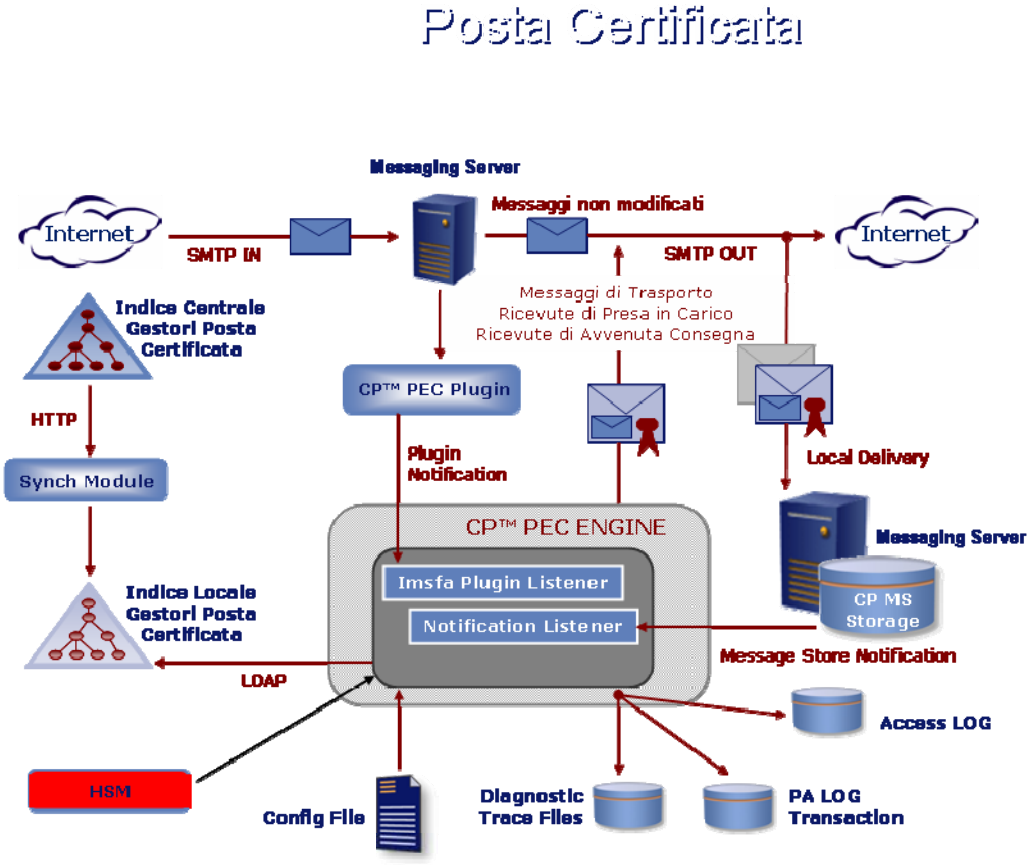
⇒ 5 - l'utente destinatario ha a disposizione la e-mail inviata.

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

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

5.2 Definizione applicativa delle componenti il servizio

Di seguito l'architettura applicativa del servizio.



5.3 Ricevute ed avvisi rilasciati all'utente

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

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

5.3.1 Ricevute

5.3.1.1 Ricevuta di accettazione

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

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

5.3.1.2 Ricevuta di avvenuta consegna

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

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

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

5.3.1.2.1 Ricevuta completa di avvenuta consegna

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

5.3.1.2.2 Ricevuta di avvenuta consegna breve

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

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

5.3.1.2.3 Ricevuta di avvenuta consegna sintetica

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

5.3.2 Avvisi

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

5.3.2.1 Avviso di non accettazione per errori formali

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

5.3.2.2 Avviso di mancata consegna per superamento dei tempi massimi previsti

Nei messaggi originati da caselle di Posta Elettronica Certificata fornire da Postecom, qualora Postecom stessa non abbia ricevuto dal gestore del destinatario, nelle dodici ore successive all'inoltro del messaggio, la ricevuta di presa in carico o di avvenuta consegna del messaggio inviato, comunica al mittente che il gestore del destinatario potrebbe non essere in grado di effettuare la consegna del messaggio.

Qualora, entro ulteriori dodici ore, Postecom non abbia ricevuto la ricevuta di avvenuta consegna del messaggio inviato, inoltra al mittente un ulteriore avviso relativo alla mancata consegna del messaggio.

5.3.2.3 Avviso di non accettazione per virus informatico

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

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

5.3.2.4 Avviso di rilevazione virus informatico

Qualora Postecom riceva messaggi di Posta Elettronica Certificata diretti a propri utenti e che rilevino la presenza di virus informatici non provvede all'inoltro, informando tempestivamente il gestore del mittente affinché comunichi al mittente stesso l'impossibilità di dar corso alla consegna.

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

5.3.2.5 Avviso di mancata consegna per virus informatico

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

5.3.2.6 Avviso di mancata consegna

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

5.3.3 Buste di anomalia

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

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

5.4 Riferimenti temporali dei messaggi

A ciascuna trasmissione e' apposto un riferimento temporale, secondo le modalità indicate nell'allegato tecnico del DM 2 novembre 2005.

Il riferimento temporale è generato con un sistema che garantisce stabilmente uno scarto non superiore ad un minuto secondo rispetto alla scala di tempo universale coordinato (UTC), determinata ai sensi dell'art. 3, comma 1, della legge 11 agosto 1991, n. 273.

Per tutte le operazioni effettuate durante i processi di elaborazione dei messaggi, ricevute, log, ecc. svolte dai punti di accesso/ricezione/consegna è disponibile il relativo riferimento temporale. Gli eventi (generazione di ricevute, buste di trasporto, log, ecc.) che costituiscono la transazione di elaborazione del messaggio presso i punti di accesso, ricezione e consegna, impiegano il riferimento temporale rilevato all'interno della transazione stessa. In questo modo l'indicazione dell'istante di elaborazione del messaggio è univoca all'interno dei log, delle ricevute, dei messaggi, ecc. generati dal server.

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

5.4.1 Sincronizzazione e distribuzione del riferimento temporale

La sorgente dell'informazione temporale deriva dall'orologio di sistema. La precisione dell'orologio di sistema è garantita dalla sua sincronizzazione con una sorgente esterna che mantiene un'informazione temporale corrispondente alla scala temporale UTC. Al fine di garantire la precisione e la sincronizzazione delle registrazioni di controllo (log) è implementato un sistema di sincronizzazione oraria realizzato mediante la implementazione del protocollo NTP.

Tramite apposite applicazioni, la sorgente temporale viene distribuita ai sistemi che gestiscono la Posta Elettronica Certificata e assicurano l'apposizione del Riferimento Temporale opponibile ai terzi, come previsto dall'articolo 9 del DM 2 novembre 2005.

6 Contenuto dell'offerta Postemail Certificata

6.1 Tipologie di utenti

6.1.1 Caselle per appartenente ad una Organizzazione

Il rilascio di caselle a soggetti appartenenti ad una Organizzazione o utenti da essa individuati, può avvenire secondo due modalità:

⇒ **Modalità Base**: L'Organizzazione sottoscrive un accordo contrattuale per il servizio in cui viene individuato il soggetto di riferimento dell'Organizzazione, che assume il compito di raccogliere i dati identificativi dei Richiedenti, compilare le richieste di emissione delle caselle e inviarle al Gestore nelle modalità indicate da Postecom. L'attivazione delle caselle viene effettuata direttamente dal Gestore una volta in possesso della documentazione necessaria. In questo caso il dominio di posta certificata è quello standard (eventualmente personalizzato con un terzo livello dedicato, identificativo della specifica Organizzazione).

⇒ **Modalità Avanzata**: L'Organizzazione sottoscrive un accordo contrattuale per il servizio in cui viene specificato il dominio dedicato di posta certificata dell'Organizzazione e viene individuato il soggetto di riferimento dell'Organizzazione ("Amministratore del sistema"), che assume il compito, tramite l'interfaccia web di gestione del proprio dominio di Postemail Certificata, di attivare, cancellare o gestire le caselle dei Titolari.

6.1.2 Caselle per persona fisica

Il rilascio di caselle a persone fisiche, può avvenire secondo le seguenti modalità:

⇒ **Modalità Base**: il Richiedente sottoscrive un accordo contrattuale per la fornitura del servizio in cui vengono riportate le informazioni necessarie per l'attivazione della casella Postemail Certificata. In questo caso il dominio di posta certificata è quello standard del Gestore Postecom. La documentazione di riferimento viene messa a disposizione sul sito *www.poste.it* nella sezione Servizi di Posta Elettronica Certificata.

6.1.3 Accordi con i terzi per la veicolazione del servizio

Postecom si riserva la possibilità di veicolare i propri servizi attraverso appositi accordi di rivendita nel rispetto della normativa vigente e delle indicazioni del presente Manuale Operativo.

6.2 Tipologie di servizi

6.2.1 Modalità Base

⇒ La casella base di Posta Elettronica Certificata ha una dimensione standard di 100 MB. Eventuali ulteriori tipologie di caselle (dimensioni, accesso, ecc.) sono definite sul sito *www.poste.it* nella sezione Servizi di Posta Elettronica Certificata.

⇒ I domini di Posta Elettronica Certificata standard sono *postecert.it* e *postemailcertificata.it.*

Per le Organizzazioni potrà essere concordato un dominio dedicato di terzo livello del tipo:

organizzazione.postecert.it.

oppure

organizzazione.postemailcertificata.it.

Postecom si riserva di accettare i domini proposti dai richiedenti.

⇒ L'indirizzo di Posta Elettronica Certificata è del tipo *username@postecert.it* oppure *username@postemailcertificata.it.* Il valore della username può essere proposto dal richiedente ma deciso dal Gestore (a titolo puramente esemplificativo, alcune cause di rifiuto potranno essere casi di omonimia, nomi molto lunghi, ecc.).

⇒ Per l'attivazione, disattivazione e configurazione delle caselle, il richiedente dovrà produrre richiesta a Postecom.

I tempi di attivazione del Servizio sono di 5 giorni lavorativi dal completo ricevimento della documentazione richiesta.

6.2.2 Modalità Avanzata

⇒ Le caselle avranno un proprio dominio a scelta, che dovrà essere dedicato all'inoltro di messaggi di posta elettronica certificata.

- Nel caso di registrazione di un dominio ex-novo, questa potrà essere effettuata al NIC da Postecom, previa avvenuta ricezione da parte del richiedente della necessaria documentazione, correttamente compilata.
- Nel caso in cui il richiedente, a fronte di un proprio dominio già registrato, voglia utilizzare per la posta elettronica certificata un dominio di terzo livello dedicato, tale nuovo dominio non dovrà essere registrato al NIC ma dovrà essere utilizzato esclusivamente per l'inoltro di messaggi di posta elettronica certificata.

⇒ La casella di Posta Elettronica Certificata standard ha una dimensione di 100 MB; è possibile acquistare ulteriori pacchetti di 100 MB l'uno, che possono essere distribuiti tra i vari Titolari con "slot" minimi di 10 MB. Gli specifici accordi contrattuali od offerte del servizio comunicati sul sito *www.poste.it* potranno riferirsi anche a diverse dimensioni o caratteristiche per la casella purché nel rispetto della normativa vigente ed espressamente indicate nell'accordo contrattuale.

⇒ L'Organizzazione intestataria delle caselle ha la possibilità di gestire direttamente la configurazione del servizio, tramite interfaccia web accessibile all'indirizzo *https://gestionepec.poste.it* (o altro indirizzo fornito al cliente al momento dell'accordo contrattuale). Personale individuato dall'Organizzazione ("l'Amministratore del sistema") potrà accedere all'interfaccia web di gestione con le seguenti funzionalità:

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

I tempi di attivazione del Servizio sono di 5 giorni lavorativi dalla intendersi dalla data di ricezione di tutta la documentazione necessaria compresa quella eventuale per la registrazione del nuovo dominio.

6.2.3 Invii massivi

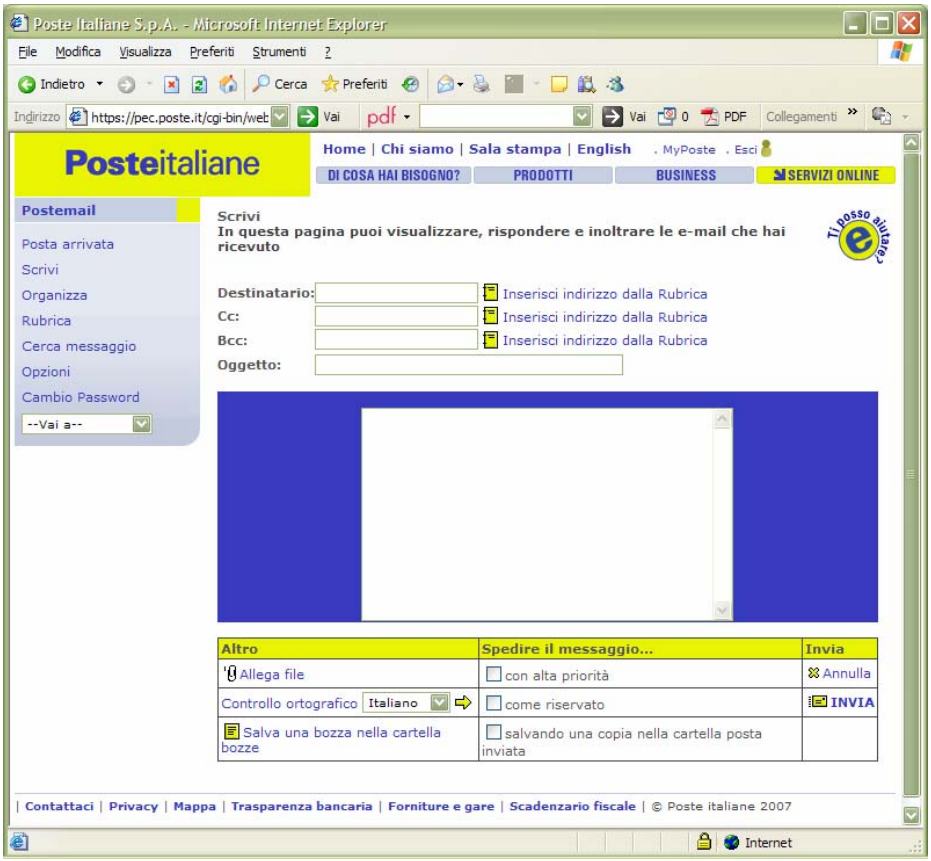
Salvo diverse indicazioni in specifici accordi contrattuali, la casella posta certificata si intende per un utilizzo standard equivalente al normale utilizzo della posta elettronica, per un utilizzo comunque equivalente a quello di una normale casella di posta elettronica, fino ad un massimo previsto di 200 invii giornalieri.

7 Modalità di accesso al servizio di Posta Elettronica Certificata

Al servizio di Postemail Certificata è possibile accedere secondo le seguenti modalità:

⇒ via web (HTTPS) attraverso una applicazione webmail, all'indirizzo *https://pec.poste.it* (o altro indirizzo segnalato sul sito *www.poste.it*) con le seguenti principali funzionalità:

- gestione della posta in arrivo;
- redazione di un nuovo messaggio;
- organizzazione dei messaggi e delle cartelle che li contengono;
- Rubrica dei destinatari;
- ricerca messaggio;
- opzioni;
- cambio della password.



⇒ utilizzando un client di posta elettronica (SMTP/S per l'invio e POP3/S e IMAP/S per la ricezione). In questo caso le funzionalità esposte sono quelle tipiche dello specifico client utilizzato dal Titolare. Per utilizzare questa modalità di accesso, è necessario configurare il proprio client con i parametri relativi:

- server di posta in arrivo (POP3/S o IMAP/S);
- server di posta in uscita (SMTP/S);
- numeri porta server posta in arrivo;
- numeri porta server posta in uscita.

I valori utili per il settaggio sono riportati sul sito *www.poste.it*.

L'autenticazione del titolare alla propria casella di posta elettronica certificata viene effettuata tramite credenziali riservate (userid e password):

⇒ fornite da Postecom per la Modalità Base;

⇒ impostate dall'Amministratore del Sistema per la Modalità Avanzata.

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

8 Condizioni di fornitura

Il servizio nelle modalità Base ed Avanzata prevede un canone annuo anticipato per il lotto di caselle prescelto.

Per aderire al Servizio sono possibili differenti modalità a seconda della tipologia di utenza interessata.

⇒ **Caselle per appartenente ad una Organizzazione** – l'Organizzazione sottoscrive con Postecom un Contratto di Servizio dove vengono riportate le clausole regolamentari relative al lotto di caselle richiesto. Tale Contratto, sottoscritto dal Legale Rappresentante o da soggetto con potere di firma, individua la figura di "Amministratore del Sistema" quale soggetto di interfaccia con il Gestore, preposto alla individuazione dei Titolari delle caselle di posta elettronica certificata. Relativamente alla documentazione da fornire in aggiunta al Contratto sopra menzionato, occorre distinguere due situazioni, a seconda che il Servizio sia fornito nella Modalità Base piuttosto che in quella Avanzata.

Modalità Base

- **dominio standard** – per ogni Titolare della casella viene redatta una scheda di registrazione al servizio.
- **dominio di terzo livello dedicato** - per ogni Titolare della casella viene redatta una scheda di registrazione al servizio.

Modalità Avanzata

Il numero minimo di caselle richiedibili per tale modalità è 5.

- **dominio da registrare** - Postecom potrà effettuare la registrazione al NIC del nuovo dominio di posta elettronica certificata per conto dell'Organizzazione che fornirà la documentazione necessaria per completare tale procedura.
- **dominio già registrato** - in questo caso non è necessaria la registrazione al NIC del nuovo dominio creato a partire da uno già registrato dall'Organizzazione. Lo specifico dominio dovrà essere utilizzato dall'Organizzazione esclusivamente per l'inoltro/ricezione di messaggi di posta elettronica certificata. Oltre al contratto di Servizio già sottoscritto dall'Organizzazione non è prevista altra documentazione aggiuntiva. Per poter utilizzare il Servizio, il *mantainer* del dominio dell'Organizzazione dovrà

Indirizzare la risoluzione del dominio di posta certificata verso i sistemi messi a disposizione da Postecom.

⇒ **Caselle per persona fisica** – il singolo Richiedente sottoscrive il Contratto di Servizio e comunica i dati necessari per l'attivazione della propria utenza.

Il contratto standard ha durata annuale, biennale o triennale e, se non diversamente specificato, si rinnova tacitamente per la medesima durata originaria, salvo disdetta da comunicarsi a Postecom - con un preavviso di almeno 30 (trenta) giorni rispetto alla data di scadenza - tramite raccomandata a/r, all'indirizzo: Postecom S.p.A. - Amministrazione Contratti, via Cordusio 4, 20123 Milano.

La disdetta potrà, inoltre, essere inoltrata attraverso casella di posta certificata, con richiesta firmata digitalmente e trasmessa all'indirizzo `gestionepec@postecert.it`.

Negli specifici accordi che non prevedano la clausola di tacito rinnovo, il Titolare dovrà espressamente richiedere l'estensione del Servizio per la medesima durata e con un preavviso minimo che consenta le normali operazioni di configurazione tecnica. Alla scadenza del contratto, qualora non rinnovato dal Titolare, Postecom provvederà al blocco del servizio e, trascorsi 30 giorni, si riserva il diritto di effettuare la cancellazione dei dati.

Postecom S.p.A. potrà, fermi restando gli obblighi di legge, sospendere temporaneamente il Servizio per procedere alla manutenzione di impianti ed altre apparecchiature necessarie all'esecuzione del Servizio stesso, dandone comunicazione al Titolare tramite e-mail o avviso pubblicato sul sito Internet *www.poste.it*, con un preavviso di 1 (uno) giorno.

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

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

Per "f*orza maggiore*" si intende qualsiasi circostanza al di fuori del ragionevole controllo di Postecom e, pertanto, in via esemplificativa e non esaustiva, si riferisce ad atti di pubbliche autorità, guerre, rivoluzioni, insurrezioni o disordini civili, scioperi, serrate o altre vertenze sindacali, blocchi od embarghi, interruzioni nella fornitura di energia elettrica, inondazioni, disastri naturali, epidemie ed altre circostanze che esulino dal controllo di Postecom.

Qualora la sospensione si protragga per un predeterminato intervallo temporale, sarà in facoltà di ciascuna delle Parti di recedere immediatamente dal rapporto contrattuale, dandone comunicazione scritta all'altra parte tramite raccomandata a/r (per Postecom S.p.A. all'indirizzo: Postecom S.p.A. – Amministrazione Contratti, via Cordusio 4, 20123 – Milano), fermo restando l'obbligo del Titolare a pagare il corrispettivo per il Servizio erogato sino alla data di efficacia del recesso.

Fermo restando quanto previsto dalle clausole del Contratto di Servizio, il rapporto contrattuale tra Postecom e il Titolare si intenderà risolto di diritto ai sensi e per gli effetti dell'art. 1456 cc, senza necessità di disdetta o preavviso, qualora il Titolare utilizzi il Servizio per finalità contrarie a leggi, regolamenti, altre disposizioni normative in generale o disposizioni di pubbliche autorità, o comunque per la violazione degli obblighi di cui alle precedenti clausole contrattuali, fermo restando il diritto di Postecom a ricevere il pagamento del corrispettivo del Servizio erogato sino alla data della risoluzione, oltre al risarcimento di tutti i danni eventualmente subiti.

In caso di ritardato pagamento del corrispettivo oltre 30 giorni dalla data di scadenza del pagamento indicato nella fattura, Postecom S.p.A. avrà facoltà di risolvere il rapporto contrattuale, dandone comunicazione scritta al Titolare a mezzo raccomandata a/r, con un preavviso di almeno 15 (quindici) giorni rispetto alla data in cui la risoluzione sarà efficace, fermo restando l'obbligo del Titolare di provvedere al pagamento del corrispettivo dovuto per il Servizio erogato sino alla predetta data.

9 Livelli di servizio ed indicatori di qualità

Destinatari degli invii

Numero massimo di destinatari per messaggi originati da caselle Postemail Certificata	100

Dimensione dei messaggi

Dimensione massima garantita per il singolo messaggio accettabile da caselle Postemail Certificata (intesa come prodotto del numero dei destinatari per la dimensione del messaggio stesso)	30 MB

Disponibilità

Disponibilità del servizio nel periodo di riferimento (*)	99,8 %
Durata massima di indisponibilità del servizio nel periodo (*)	262,8 minuti
Durata massima per singola indisponibilità del servizio (*)	131,4 minuti

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

Tempi

Tempo di consegna delle ricevute	30 minuti

SEZIONE III: OBBLIGHI E RESPONSABILITÀ

10 Obblighi e responsabilità

10.1 Obblighi del Gestore

- ⇒ Assicura l'interoperabilità con gli altri gestori di Posta Elettronica Certificata.
- ⇒ Rilascia al mittente che utilizza i propri servizi la ricevuta di accettazione nella quale sono contenuti i dati di certificazione che costituiscono prova dell'avvenuta spedizione del messaggio di Posta Elettronica Certificata.
- ⇒ Fornisce all'indirizzo del mittente le ricevute di avvenuta consegna.
- ⇒ Nel caso di trasmissione tra caselle appartenenti a gestori diversi, rende disponibili, nei casi previsti dalla legge, i log inerenti le specifiche trasmissioni.
- ⇒ Rilascia, se Gestore della casella di Posta Certificata del destinatario, la ricevuta di presa in carico del messaggio al Gestore della casella del mittente.
- ⇒ Comunica al mittente, nei casi previsti e mediante un apposito avviso, la mancata consegna del messaggio.
- ⇒ Sottoscrive con firma elettronica avanzata le ricevute rilasciate.
- ⇒ Sottoscrive con firma elettronica avanzata le buste di trasporto, al fine di garantirne la provenienza, l'integrità e l'autenticità.
- ⇒ Appone a ciascuna trasmissione un riferimento temporale generato con un sistema che garantisce uno scarto non superiore ad un minuto secondo rispetto alla scala di tempo universale coordinato (UTC), determinata ai sensi dell'art. 3, comma 1, della legge 11 agosto 1991, n. 273.
- ⇒ Esegue, senza soluzione di continuità, il salvataggio dei log dei messaggi generati nell'intervallo temporale predefinito.
- ⇒ Appone giornalmente la marcatura temporale al file dei log relativo al periodo.
- ⇒ Tratta i virus secondo quanto previsto dal DM 2 novembre 2005, informando il mittente sul fatto che il messaggio inviato contiene un virus e conservando per 30 mesi i messaggi relativi.
- ⇒ Garantisce i livelli di servizio previsti dal DM 2 novembre 2005 e riportati nel capitolo 9.
- ⇒ Se Gestore mittente (nei casi di mancata ricezione, nelle 12 ore successive all'inoltro del messaggio, della ricevuta di presa in carico o di avvenuta consegna del messaggio inviato) comunica al mittente che il Gestore del destinatario

potrebbe non essere in grado di realizzare la consegna del messaggio e, in assenza di comunicazioni nelle successive 12 ore, comunica al mittente avviso relativo alla mancata consegna del messaggio.

⇒ Segnala al destinatario i messaggi non qualificabili come Posta Elettronica Certificata.

⇒ Si attiene alle regole di cui al DM 2 novembre 2005 per l'accesso all'elenco pubblico dei gestori di posta elettronica certificata.

10.2 Obblighi del soggetto Titolare del servizio

⇒ Fornisce in maniera veritiera e sotto la sua responsabilità le informazioni richieste dal Gestore ai fini dell'attivazione del servizio.

⇒ Gestisce in maniera sicura le credenziali per l'accesso alla casella di Posta Elettronica Certificata.

⇒ Si attiene alle normali regole di sicurezza nell'utilizzo della casella, al fine di evitare danni ai soggetti che utilizzano o gestiscono il servizio di Posta Certificata.

⇒ Si avvale, per l'utilizzo della Posta Certificata, dei soggetti inclusi nell'Elenco dei Gestori accreditati gestiti dal Centro Nazionale per l'Informatica nella pubblica Amministrazione.

⇒ Nel caso intenda utilizzare il servizio di Posta Certificata nei rapporti con la Pubblica Amministrazione, dichiara espressamente il proprio indirizzo. Nei casi corrispondenti, revoca la dichiarazione con le stesse modalità.

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

⇒ Gestisce in maniera sicura le credenziali per l'accesso alla casella di Posta Elettronica Certificata.

⇒ Si attiene alle normali regole di sicurezza nell'utilizzo della casella, al fine di evitare danni ai soggetti che utilizzano o gestiscono il servizio di Posta Certificata.

10.4 Responsabilità

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

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

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

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

11 Esclusioni e limitazioni in sede di indennizzo

Qualsiasi contestazione relativa all'esecuzione del Servizio dovrà essere comunicata dal Titolare a Postecom S.p.A. - a pena di decadenza - entro il termine di (30) giorni, dalla data dell'evento ovvero da quella in cui ne venga accertata l'esistenza, tramite raccomandata a/r (all'indirizzo: Postecom S.p.A. - Amministrazione Contratti, via Cordusio 4, 20123 – Milano).

La responsabilità di Postecom S.p.A. nei confronti del Titolare per ogni tipo di danni, diretti, indiretti, consequenziali e comunque derivanti dall'esecuzione del Servizio (inclusi, in via esemplificativa e non esaustiva, danni per mancati profitti, per interruzione dell'attività, per perdita di dati o, in generale, per perdite economiche) sarà limitata - fatti salvi i casi di dolo o colpa grave – ad un importo pari al corrispettivo pagato e/o dovuto dal Titolare in base allo specifico accordo contrattuale nel caso di Titolari singoli o a quanto previsto dallo specifico contratto rivolto ad Organizzazioni.

Postecom S.p.A. non sarà in ogni caso responsabile verso il Titolare per ritardi, malfunzionamenti e interruzioni del Servizio causati da: eventi di forza maggiore, comunicazione errata, incompleta o non veritiera da parte del Titolare dei dati necessari per l'esecuzione del Servizio, presenza di virus o errori nei documenti elettronici o file in generale allegati ai messaggi consegnati dal Titolare a Postecom S.p.A. per l'esecuzione del Servizio, errata utilizzazione del Servizio da parte del Titolare o dei destinatari dei messaggi, malfunzionamento dei terminali utilizzati dal Titolare o dai destinatari dei messaggi, interruzione totale o parziale del servizio di accesso fornito dall'operatore di telecomunicazioni.

SEZIONE IV: STANDARD E PROCEDURE

12 Procedure e standard tecnologici e di sicurezza

12.1 Standard di qualità e sicurezza dei processo

12.1.1 Standard di qualità

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

Codice Documento	Titolo
UNI EN ISO 9001:2000	Sistemi di gestione per la qualità. Requisiti
UNI EN ISO 9004:2000	Sistemi di gestione per la qualità. Linee guida per il miglioramento delle prestazioni
UNI EN ISO 9000:2000	Sistemi di gestione per la qualità. Fondamenti e terminologia
UNI EN ISO 10007:1997	Gestione per la Qualità. Guida per la gestione della configurazione
UNI EN 29400-2:1994	Elementi di gestione per la qualità e del sistema. Guida per i servizi
UNI EN ISO 9000-3:1998	Norme di gestione per la qualità e di assicurazione della qualità. Guida per l'applicazione della ISO 9001:1994 allo sviluppo, alla fornitura, all'installazione ed alla manutenzione del software per elaboratore
UNI 10999:2002	Linee guida per la documentazione dei sistemi di gestione per la qualità
UNI EN ISO 19011:2003	Linee guida per gli audit dei sistemi di gestione per la qualità e/o di gestione ambientale

12.1.2 Standard di sicurezza

Si riportano di seguito i requisiti della norma ISO27001:2005 soddisfatti dal servizio di Posta Elettronica Certificata del Gestore Postecom**.**

Punto norma	Requisito richiesto dalla norma
4.3.1 a	Documented statements of the ISMS policy and objectives
4.3.1 b	Lo scopo del Sistema di Gestione per la sicurezza delle informazioni
4.3.1 c	Procedure e controlli a supporto del SGSI
4.3.1 d	Descrizione della metodologia di risk assessment
4.3.1 e	Report prodotto in fase di risk assessment
4.3.1 f	Piano di trattamento del rischio
4.3.1 g	Procedure documentate atte ad assicurare una efficace pianificazione, gestione e controllo dei suoi processi sulla sicurezza delle informazioni e atte a descrivere come misurare l'efficacia dei controlli
4.3.1 h	Registrazioni richieste dall'SGSI
4.3.1 i	Dichiarazione di Applicabilità

12.1.3 Standard tecnologici

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

Codice	Titolo
RFC 1847	Security Multiparts for MIME: Multipart/Signed and Multipart/Encrypted
RFC 1891	SMTP Service Extension for Delivery Status Notifications
RFC 1912	Common DNS Operational and Configuration Errors
RFC 2045	Multipurpose Internet Mail Extensions (MIME) Part One: Format Of Internet Message Bodies
RFC 2049	Multipurpose Internet Mail Extensions (MIME) Part Five: Conformance Criteria and Examples
RFC 2252	Lightweight Directory Access Protocol (v3): Attribute Syntax Definitions
RFC 2315	PKCS #7: Cryptographic Message Syntax Version 1.5
RFC 2633	S/MIME Version 3 Message Specification
RFC 2660	The Secure HyperText Transfer Protocol
RFC 2821	Simple Mail Transfer Protocol
RFC 2822	Internet Message Format
RFC 2849	The LDAP Data Interchange Format (LDIF) - Technical Specification
RFC 3174	US Secure Hash Algorithm 1 (SHA1)
RFC 3207	SMTP Service Extension for Secure SMTP over Transport Layer Security
RFC 3280	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
ISO/IEC 9594-8:2001	Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks

12.2 Gestione dei sistemi tecnologici

Lo scopo delle procedure messe in atto dal Gestore Postecom per la conduzione dei sistemi di Posta Elettronica Certificate è quello di:

- ⇒ rende1re disponibili informazioni certe sulla configurazione del sistema e le relazioni che intercorrono tra i vari elementi anche al fine di apportare modifiche in modo controllato;
- ⇒ assicurare il controllo delle modifiche alla configurazione nel rispetto dei ruoli come definiti dalla norma e che hanno competenza sulle attività di modifica agli elementi di configurazione;
- ⇒ tracciare la storia della configurazione per ricostruire versioni del sistema di gestione della Posta Elettronica Certificata ed identificare cause di eventuali problemi verificatisi a seguito di modifiche ai sistemi per l'erogazione.

12.2.1 Attivazione della procedura di gestione

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

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

12.2.2 Aggiornamento della configurazione

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

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

Le informazioni minime tracciate nella scheda tecnica sono:

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

Alla scheda tecnica sono associate informazioni aggiuntive relative al responsabile della gestione della risorsa di elaborazione ed al responsabile delle risorse dati, nonché la

classificazione assegnata alla risorsa, necessaria per l'identificazione del livello di protezione attuabile, secondo lo schema che segue:

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

12.2.3 Controllo dello stato di configurazione

Con periodicità mensile, o su richiesta della funzione responsabile del servizio di Posta Certificata viene effettuato il controllo dello stato della configurazione.

Tali informazioni sono riportate in un apposito report contenente al minimo le seguenti informazioni:

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

12.3 Gestione delle verifiche afferenti la sicurezza

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

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

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

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

- ⇒ **attività pianificate** e definite nel "Programma annuale Verifiche Ispettive Qualità e Sicurezza" con periodicità almeno annuale;
- ⇒ **attività non pianificate** ma che possono rendersi necessarie in forma occasionale;

- ⇒ **mutamenti significativi** della infrastruttura di rete e dei sistemi;
- ⇒ **sostanziali mutamenti dello scenario delle minacce** cui le reti ed i sistemi sono soggetti;
- ⇒ **incidenti di sicurezza**, quando (dopo averne eliminato gli effetti) sia necessario effettuare approfondite analisi per determinarne le possibili cause.

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

12.3.1 Pianificazione e definizione degli assessment

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

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

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

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

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

12.3.2 Effettuazione dell’assessment

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

Nella fase di assessment il Team:

- ⇒ rileva le vulnerabilità e definisce il fattore di rischio assoluto e quello reale (al fine di eliminare i falsi positivi);
- ⇒ attribuisce ad ogni vulnerabilità una valutazione del grado di SEVERITA' (Alta / Media / Bassa). La severità delle vulnerabilità prese in considerazione viene valutata ispirandosi alle classificazioni più diffuse in ambito internazionale (CVE, OSVDB, NESSUS ecc.);
- ⇒ raggruppa, ove possibile, le varie vulnerabilità in classi omogenee.

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

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

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

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

13 Soluzioni finalizzate a garantire il completamento della trasmissione

13.1 Approccio organizzativo

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

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

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

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

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

Tempi	Escalation
Completamento della fase entro 60 minuti dal malfunzionamento	**Il personale del Datacenter, coordinato dal Responsabile dei Servizi Tecnici**, rilevato il verificarsi del guasto/anomalia identifica ed attiva le contromisure opportune. In base ai risultati della diagnosi effettuata, il personale provvede a: ⇒ **richiedere l'intervento di ulteriori risorse specialistiche** (altri sistemisti o reperibile di secondo livello se in orario di reperibilità), se non in grado di procedere autonomamente; ⇒ **coinvolgere immediatamente il fornitore del prodotto** interessato dal malfunzionamento, se necessario in relazione ala tipologia di problema emerso; ⇒ **informare immediatamente il Responsabile del sevizio Postemail Certificata** per **mail** e per **telefono**, avendo cura di specificare se il problema può essere di natura applicativa; ⇒ **informare il Customer Care** (assistenza tecnica telefonica) attraverso **mail;** ⇒ se il malfunzionamento è imputabile ad un attacco/incidente di sicurezza, attivare la **Procedura di Gestione degli incidenti di sicurezza**; ⇒ Il **Responsabile del servizio Postemail Certificata**, una volta ricevuta la comunicazione, provvede a: ▪ informare immediatamente il **Manager dell'Unità Organizzativa (Business Unit)** responsabile del servizio di Posta Elettronica Certificata; ▪ nel caso il problema sia di natura applicativa, deve **coinvolgere, appena possibile, gli sviluppatori** e/o **il fornitore del prodotto** (se applicativo acquistato) attivando la **Procedura di Manutenzione del sw applicativo**.

Tempi	Escalation
Completamento della fase entro 120 minuti dal malfunzionamento	**Il personale del Datacenter, coordinato dal Responsabile dei Servizi Tecnici,** analizzato il guasto, provvede a coordinare l'attuazione di contromisure aggiuntive. Qualora, queste ultime si dimostrassero efficaci, il personale provvede a: ⇒ chiudere l'intervento registrando le contromisure adottate; ⇒ informare il **Responsabile del servizio Postemail Certificata,** precedentemente coinvolto, attraverso **mail e telefono**; ⇒ informare il **Customer Care** attraverso **mail**. Il **Responsabile del servizio Postemail Certificata**, una volta ricevuta la comunicazione di chiusura del guasto dal Data Center, provvede ad informare immediatamente il **BU Manager.** In caso di inefficacia e trascorsi i tempi previsti, **il Responsabile dei Servizi Tecnici** ed il **BU Manager** provvedono ad informare, attraverso gli strumenti ritenuti più efficaci: ⇒ l'**Amministratore Delegato**, al fine di consentirgli l'individuazione delle azioni più opportune; Il **Responsabile dei Servizi Tecnici** informa le figure sopra elencate del tipo di malfunzionamento, nonché fornisce una stima dei tempi necessari al superamento del problema. Il **BU Manager**, ricevuta la comunicazione **provvede ad attivare il processo informativo mediante le funzioni aziendali e gli strumenti opportuni, verso i Clienti coinvolti**.

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

- ⇒ **Responsabile del servizio Postemail Certificata**;
- ⇒ **Customer Care** (assistenza tecnica telefonica);
- ⇒ **al BU Manager;**
- ⇒ **all'Amministratore Delegato**.

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

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

13.2 Approccio tecnologico

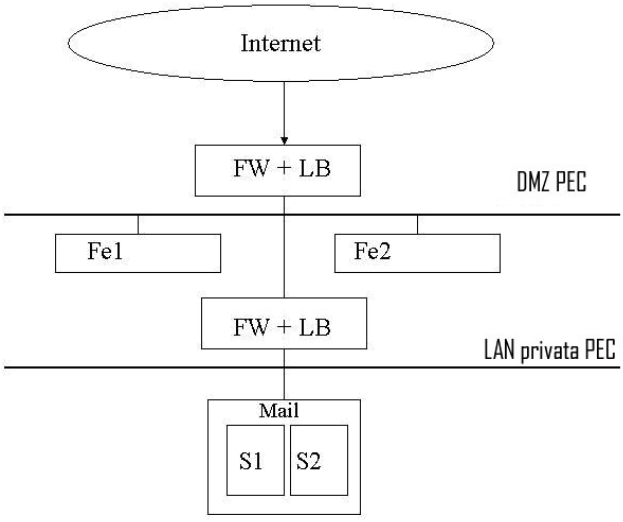
13.2.1 Connettività

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

Carrier	Banda (Mbps)	Tipologia accesso Internet	Tecnologie di accesso alla rete
Fastweb (NAMEX*)	100	Banda Nazionale	LinkEoSHD verso NAMEX
COLT	34	Banda Nazionale e Internazionale	Synchronous Digital Hierarchy (SDH)

13.2.2 Sistemi tecnologici

Nella seguente figura è illustrato uno schema semplificato dell'architettura fisica del servizio PosteMail Certificata



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

Tale architettura garantisce le seguenti funzionalità:

- ⇒ **affidabilità**: in caso di fault di un elemento del servizio, questo non ne risente in quanto:
  - in caso di fault di un server di front-end, tutto il traffico viene re-diretto dagli apparati di load-balancing verso i server attivi;
  - in caso di fault di un server di back-end, il server "superstite" prenderà automaticamente in carico tutte le attività e le risorse del server malfunzionante. Tutte le informazioni rilevanti (caselle, configurazioni, etc.) sono memorizzate su dispositivi di memoria di massa dedicati collegati ai server tramite collegamenti in fibra ottica.
  - in caso di fault di un firewall o di un apparato di load-balancing, il funzionamento del sistema verrà garantito da un secondo elemento attivato tramite i meccanismi interni dello specifico apparato.
- ⇒ **sicurezza**: l'introduzione di elementi di load-balancing permette di implementare facilmente funzionalità di NAT e conseguentemente di disaccoppiare la corrispondenza tra un servizio ed i server fisici che lo erogano, diminuendo quindi i rischi in caso di attacco informatico.
- ⇒ **scalabilità**: l'architettura permette di scalare facilmente sia in modalità orizzontale che in modalità verticale. In particolare la scalabilità orizzontale è utilizzata soprattutto sui front-end in quanto, a seguito del rilevamento di una crescita delle attività dai parte dei singoli server di front-end, è sufficiente mettere in linea ulteriori server con le stesse caratteristiche degli altri e aggiungere nella configurazione degli apparati di load-balancing tali server nella lista di quelli abilitati per il servizio. Sui server di back-end viene garantita la scalabilità verticale, adottando specifici server le cui risorse - CPU, RAM, disco - possono essere aggiornati a caldo, sino ad una certa soglia oltre la quale vengono attivati meccanismi di scalabilità orizzontale compatibili con il software utilizzato.

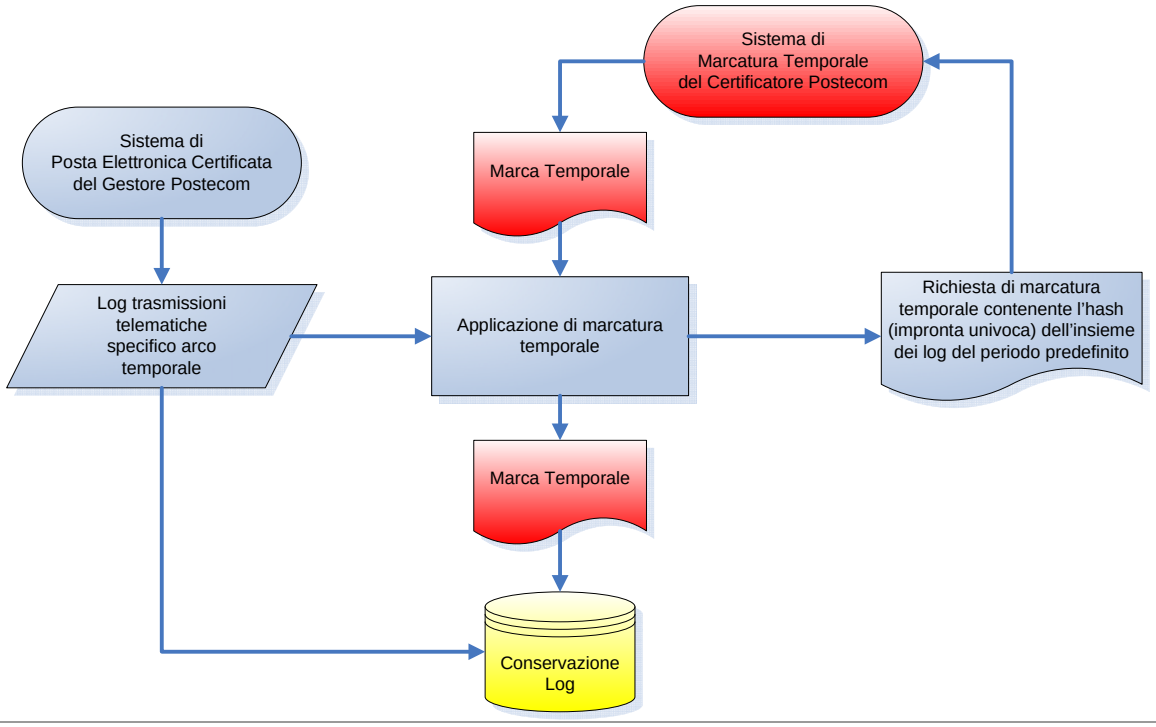
14 Reperimento e presentazione delle informazioni di log

Il servizio Postemail Certificata garantisce la tracciatura dei messaggi in tutte le fasi significative.

In particolare, in funzione delle singole operazioni interessate alla tracciatura, sono memorizzati i seguenti dati significativi:

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

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



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

L'accesso ai log da parte dell'interessato avente diritto avviene previo richiesta scritta, valutata dalla funzione sicurezza e dalla funzione legale.

A seguito dell'autorizzazione, i dati dei log afferenti la richiesta vengono individuati attraverso i seguenti identificativi:

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

In ogni caso l'accesso può avvenire previo richiesta dell'autorità giudiziaria.

Le richieste possono essere inoltrate all'indirizzo `supportopec@postecert.it` e vi verrà dato corso previo accertamento dei requisiti di autenticità e legittimità.

Ulteriori, eventuali, modalità di richiesta saranno comunicate sul sito del Gestore.

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

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

SEZIONE V: PROTEZIONE DATI PERSONALI

15 Modalità di protezione dei dati dei titolari

La normativa in tema di trattamento dei dati personali è stata introdotta con la legge 31 dicembre 1996, n.675 a tutela della riservatezza e dell'identità personale.

La materia è stata riunita ed armonizzata in un Testo Unico, approvato con Decreto Legislativo del 30 giugno 2003, n.196, che ha così sostituito la legge 675 ed i decreti connessi.

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

- ⇒ Titolare;
- ⇒ Responsabile;
- ⇒ Incaricato.

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

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

Ai fini dell'adempimento degli obblighi imposti dal Codice, in Postecom è stata individuata la figura del Titolare nella società stessa, Postecom S.p.A.

Le figure dei Responsabili sono state invece individuate nelle persone dei responsabili delle strutture di primo livello delle Business Unit e delle altre strutture organizzative previste nell'apposita Relazione sulla Struttura Organizzativa, ognuno per i trattamenti effettuati nel proprio ambito.

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

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

Le figure degli Incaricati sono state individuate nel personale di Postecom S.p.A., per i trattamenti propri della funzione d'appartenenza.

I Responsabili procedono al trattamento dei dati secondo le istruzioni impartite dal Titolare stesso.

15.1 Ambito del trattamento dei dati personali

Il trattamento di dati personali, è consentito per le finalità proprie aziendali, nei limiti stabiliti dalle leggi e dai regolamenti.

Ogni richiesta di comunicazione di dati personali rivolta da privati deve essere scritta e motivata e deve indicare le norme di legge o di regolamento su cui si basa.

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

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

15.1.1 Accesso ai dati

Ai dati possono avere accesso solo i dipendenti a ciò autorizzati.

La designazione è effettuata anche per categoria sulla base delle medesime mansioni ricoperte all'interno di una stessa unità organizzativa.

15.1.2 Trattamento di dati sensibili

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

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

⇒ sono impartite, da parte della struttura "Servizi Sicurezza" apposite *istruzioni organizzative e tecniche* per la custodia e l'uso dei supporti rimuovibili sui cui sono memorizzati i dati al fine di evitare accessi non autorizzati;

I dati sensibili possono sono oggetto di trattamento solo con il *consenso scritto* dell'interessato e previa *autorizzazione del Garante*[1], nell'osservanza dei presupposti e dei limiti stabiliti dalla legge e dai regolamenti.

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

15.1.3 Trattamento di dati giudiziari

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

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

15.2 Sicurezza dei dati

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

⇒ i rischi di distruzione o perdita, anche accidentale, dei dati, di danneggiamento delle risorse hardware su cui sono registrati e dei locali ove vengono custoditi;

⇒ l'accesso non autorizzato ai dati stessi;

⇒ modalità di trattamento non consentite dalla legge o dai regolamenti aziendali.

Le misure di sicurezza adottate assicurano:

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

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

Il Garante, in vista dell'entrata in vigore del nuovo "Codice privacy", ha rinnovato le suddette autorizzazioni fino al 30 giugno 2004.

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

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

In merito all'utilizzo di risorse informatiche personali il Titolare ha emanato le "*Politiche di Sicurezza per l'utilizzo delle postazioni informatiche personali*".