Manuale Operativo
del Servizio di Posta Elettronica Certificata

Conformità al Decreto Presidente della Repubblica n. 68 11/02/05
e al Decreto Presidente Consiglio dei Ministri 02/11/05

Codice documento: MO-PEC

Redazione: Antonio Raia

Approvazione: Franco Tafini

Data emissione: 16/05/2016

Revisione: 04

An IBM Company
intesa
DIGITAL
BUSINESS SOLUTIONS

REVISIONI

Revisione n°:	**00**	**Data Revisione:**	**07/07/2006**
Descrizione modifiche:	**Nessuna**		
Motivazioni:	**Prima emissione**		

Revisione n°:	**01**	**Data Revisione:**	**31/07/2007**
Descrizione modifiche:	**Cambiamento infrastruttura server farm** **Cambio sede operativa e legale** **Aggiornamento dati servizio**		
Motivazioni:	**Trasloco server farm** **Trasloco sede operativa e legale** **Adeguamento struttura tecnica**		

Revisione n°:	**02**	**Data Revisione:**	**1/12/2009**
Descrizione modifiche:	**Modifica infrastruttura tecnica** **Aggiornamento dati societari**		
Motivazioni:	**Adeguamento descrizione infrastruttura tecnica** **Cambio Amministratore Delegato** **Aggiornamento procedura emissione**		

Revisione n°:	**03**	**Data Revisione:**	**27/06/2014**
Descrizione modifiche:	**Aggiornamento dati societari e sedi periferiche** **Aggiornamento denominazione Agenzia per l'Italia Digitale** **Aggiornamento infrastruttura tecnica, PAR C.3**		
Motivazioni:	**Cambio Amministratore Delegato e ricollocazione filiali** **Dlgs 1 dicembre 2009, n. 177** **Adeguamento descrizione infrastruttura tecnica**		

Revisione n°:	**04**	**Data Revisione:**	**16/05/2016**
Descrizione modifiche:	**Adeguamento SLA relativo alla dimensione massima dei messaggi PEC gestiti (100MB)** **I controlli AV/AS sono implementati direttamente nei nodi di ricezione ed accettazione e non più attraverso apparati fisici.** **Aggiornamento dati societari**		
Motivazioni:	**Proposta AGID di elevare a 100 MB la dimensione dei msg PEC gestiti** **Aggiornamento sistema AV/AS** **Variazione sede legale e sede filiale Roma**		

Prefazione

Il *Manuale Operativo del Servizio di Posta Elettronica Certificata* vuole essere uno strumento attraverso il quale IN.TE.S.A. S.p.A., nella propria veste di *Gestore di Posta Elettronica Certificata*, fornisce gli elementi attraverso i quali l'utenza può valutare il servizio offerto.

Il documento segue un'impostazione basata su tre sezioni omogenee nel contenuto, allo scopo di guidare il lettore nella descrizione del servizio di Posta Elettronica Certificata.

La prima sezione è dedicata all'elencazione di quegli elementi che consentono l'identificazione del presente Manuale Operativo, i termini e i riferimenti tecnico/normativi, gli acronimi e le abbreviazioni utilizzate. Infine, attraverso una tabella di corrispondenza, è possibile identificare gli elementi che il Gestore di Posta Elettronica Certificata ha l'obbligo di precisare e descrivere dettagliatamente.

Nella seconda sezione vengono forniti, in sintesi, i principali elementi tecnici, normativi e organizzativi del servizio. Successivamente sono fornite le caratteristiche necessarie al Gestore di Posta Elettronica Certificata per poter essere iscritto nel registro dei Gestori curato da *AgID – Agenzia per l'Italia Digitale* (già *DigitPA - Ente nazionale per la digitalizzazione della pubblica amministrazione)*. Finalmente, sono proposte alcune applicazioni del servizio tramite scenari esemplificativi e formulate ipotesi di sviluppo e ottimizzazioni nell'ambito dei processi comunicativi tra operatori economici e istituzionali.

La terza e ultima sezione descrive:

- le funzionalità e le caratteristiche specifiche del servizio del Gestore Intesa;
- l'offerta del servizio;
- le condizioni di fornitura e di assunzione di responsabilità, con relativi indennizzi e limitazioni;
- una sintesi delle principali componenti tecnologiche e infrastrutturali in termini di piattaforme hardware e software utilizzati;
- la citazione degli standard di qualità e tecnici, internazionali e nazionali, utilizzati per rendere ottimale la progettazione, la realizzazione e il delivery del servizio.

Alla stesura del documento hanno attivamente partecipato le direzioni tecniche direttamente coinvolte nell'erogazione del servizio e le altre funzioni aziendali che forniscono supporto generale di tipo amministrativo, legale, qualità e marketing/commerciale.

IN.TE.S.A. S.p.A.

Pagina lasciata intenzionalmente bianca

Sommario

INDICE DELLE FIGURE

A. SEZIONE I - Dati Generali

A.1. Premessa alla Sezione

La presente Sezione contiene tutti gli elementi generali e particolari inerenti l'identificazione sia del presente documento, denominato *Manuale Operativo del Servizio di Posta Elettronica Certificata*, sia del Gestore IN.TE.S.A. S.p.A. Sono successivamente elencati e descritti tutti i termini e i riferimenti tecnico/normativi, gli acronimi e le abbreviazioni utilizzati nel documento.

Infine, viene presentata una Tabella di Corrispondenza che consente al lettore una rapida e chiara ricerca all'interno del Manuale Operativo degli elementi essenziali che il Gestore di Posta Elettronica Certificata ha l'obbligo di precisare e descrivere nel dettaglio.

A.2. Generalità del documento

Il presente *Manuale Operativo del Servizio di Posta Elettronica Certificata* (nel seguito anche solo *Manuale Operativo*) descrive le regole generali e le procedure operative seguite da IN.TE.S.A. S.p.A. (nel seguito anche solo *Gestore Intesa* o *Intesa*) nello svolgimento della propria attività di Gestore di Posta Elettronica Certificata (nel seguito anche solo *PEC*). Il Manuale Operativo è pubblicato a garanzia dell'affidabilità dei servizi offerti ai propri utenti e ai loro corrispondenti.

A.2.1. Scopo e campo d'applicazione

Il presente documento costituisce il Manuale Operativo del Servizio di Posta Elettronica Certificata della società IN.TE.S.A. S.p.A., già iscritta nell'elenco pubblico dei Certificatori ed è redatto in conformità all'Art.23 - *Manuale Operativo* del DM 02/11/05.

Il presente Manuale Operativo contiene le indicazioni previste nella Circolare CNIPA 14/11/05 nel Cap.2 - *Requisiti tecnico-organizzativi* e tiene conto del documento CNIPA *Raccomandazioni per iscrizione IGPEC* del 13 febbraio 2006.

A.2.2. Proprietà intellettuale

Il presente Manuale Operativo è di esclusiva proprietà di IN.TE.S.A. S.p.A., che è Titolare di ogni relativo diritto intellettuale.

Quanto fornito da IN.TE.S.A. S.p.A. ai propri titolari e addetti per utilizzare la funzioni del servizio di Posta Elettronica Certificata gestito da IN.TE.S.A. S.p.A. è coperto da diritti sulla proprietà intellettuale.

A.2.3. Procedure per l'aggiornamento

Gli aggiornamenti al presente documento saranno sottoposti ad approvazione di AgID e, successivamente, pubblicati sul sito del Gestore.

L'utente è tenuto a verificare periodicamente sul sito del Gestore la presenza di una eventuale nuova versione del manuale operativo.

A.2.4. Validità

Quanto descritto in questo documento si applica a IN.TE.S.A. S.p.A., cioè alle sue infrastrutture logistiche e tecniche, al suo personale, e ai Titolari delle caselle del servizio di Posta Elettronica Certificata.

A.2.5. Dati identificativi della versione del Manuale Operativo

Il presente documento costituisce la Versione n.04 del *Manuale Operativo del Gestore di Posta Elettronica Certificata IN.TE.S.A S.p.A.* rilasciata il 16 maggio 2016 in conformità con l'Art.23 del DM 02/11/05.

Il presente Manuale Operativo è pubblicato e consultabile per via telematica presso l'indirizzo Internet:

http://trustedmail.intesa.it/documentazione/Manuale Operativo PEC.pdf

A.2.6. Responsabile del Manuale Operativo

Il Responsabile del Manuale Operativo è:

Antonio Raia

IN.TE.S.A. S.p.A.

Indirizzo: Strada Pianezza, 289 - 10151 Torino

N. Telefono: +39-011-192.16.111

N. Fax: +39-011-192.16.375

Indirizzo di Posta Elettronica: ***uff_pec@intesa.it***

A.2.7. Responsabile dell'approvazione del Manuale Operativo

Il Responsabile dell'approvazione del Manuale Operativo è:

Franco Tafini

Indirizzo: Strada Pianezza, 289 - 10151 Torino

N. Telefono: +39-011-192.16.111

N. Fax: +39-011-192.16.375

A.3. Generalità del Gestore

A.3.1. Dati identificativi del Gestore

Il Gestore - di cui il presente documento costituisce il Manuale Operativo ai sensi dell'Art.23 del DM 02/11/05 - è la società IN.TE.S.A. S.p.A., di cui di seguito sono forniti i dati identificativi e una breve presentazione.

Denominazione sociale	IN.TE.S.A. S.p.A.
Indirizzo della sede legale	Strada Pianezza, 289 - 10151 Torino
Legale Rappresentante	Amministratore Delegato
Registro delle Imprese di Torino	N. Iscrizione 1692/87
N. di Partita I.V.A.	05262890014
N. di telefono (centralino)	+39-011-192.16.111
Indirizzo delle sede operativa	Strada Pianezza, 289 - 10151 Torino
Sito Internet	***www.intesa.it***
N. di fax	+39-011-192.16.375
Indirizzo di posta elettronica	***marketing@intesa.it***
ISO Object Identifier (OID)	1.3.76.21.1

IN.TE.S.A. S.p.A. opera sul mercato dal 1987 come fornitore di soluzioni per l'e-business, che facilitano e rendono possibile la comunicazione e la collaborazione in rete di comunità aziendali. Basandosi su tecnologie all'avanguardia nei settori organizzativo, gestionale e operativo, offre soluzioni a valore aggiunto personalizzate, nel quadro di un'offerta di servizio globale al Cliente.

Nel corso degli ultimi anni ha rafforzato la propria presenza nell'offerta di soluzioni per la Business Process Integration, proponendosi quale partner in grado di gestire un'attività di business nel suo complesso per conto del cliente.

Dal marzo 2001 è iscritta all'albo dei Certificatori Accreditati tenuto da AgID.

IN.TE.S.A. S.p.A. è composta da circa 150 dipendenti dislocati nella sede centrale di Torino e negli uffici tecnico/commerciali distribuiti in Italia.

Le unità periferiche sono dislocate a:

- MILANO – Piazzale Biancamano, 8 - 20121 Milano

- ROMA - Piazza Marconi, 15 - 00144 Roma

Il pacchetto azionario della società IN.TE.S.A. S.p.A. è attualmente interamente posseduto dalla società IBM Italia S.p.A. della quale fanno parte anche altre società specializzate in servizi informatici. In tale contesto, Intesa si occupa dei servizi innovativi e della gestione delle relative infrastrutture sotto la direzione e il controllo di IBM Italia S.p.A.

In questo ambito, Intesa, come società facente parte del gruppo IBM, ha pertanto conseguito la certificazione UNI EN ISO 9001:2000 per *Sales, Design, Development, Consultancy, Delivery, Services, Installation and Support of all activities culminating in the provisions of IT and business solutions*. Tale certificazione è relativa a tutti i processi aziendali. In tale specifico ambito, il servizio di PEC è stato progettato, realizzato ed è erogato e assistito nel pieno rispetto dei processi di qualità di cui sopra.

In conformità con l'Art.21 del DM 02/11/05, il personale responsabile delle attività di gestione del servizio di Posta Elettronica Certificata, è articolato nelle figure seguenti:

- Responsabile della sicurezza;
- Responsabile della registrazione dei titolari;
- Responsabile della sicurezza dei log dei messaggi;
- Responsabile dei servizi tecnici;
- Responsabile delle verifiche e ispezioni (auditing);
- Responsabile del sistema di riferimento temporale.

Tali figure professionali sono appositamente addestrate anche in funzione degli aggiornamenti subiti dal sistema di Posta Elettronica Certificata (Art.22, comma 2 del DM 2/11/05) e posseggono un’esperienza non inferiore ai cinque anni nelle attività di analisi, progettazione, commercializzazione e conduzione di sistemi informatici (Art.22, comma 1 del DM 2/11/05).

Le figure sopra elencate possono avvalersi, per lo svolgimento delle funzioni di loro competenza, di addetti e operatori specializzati.

Intesa ha definito inoltre una figura specifica che svolge la funzione di *Responsabile del servizio di PEC*. Tale figura avrà, fra gli altri, i compiti di:

- fare da punto di riferimento aziendale per le comunicazioni e le problematiche di ordine tecnico/normativo da e verso AgID, recependo e riportando all'interno del team di lavoro Intesa gli eventuali adeguamenti tecnico/organizzativi derivanti da aggiornamenti, modifiche e integrazioni normative. Parteciperà ad eventuali riunioni, convocazioni e attività tecnico/istituzionali organizzate da AgID;
- fare da punto di riferimento operativo di tipo tecnico/organizzativo nell'ambito del team di lavoro PEC di Intesa in coordinamento con i responsabili delle attività di cui all'Art.21 DM 2/11/05. Inoltre interagirà con ciascuna delle altre diverse strutture di riferimento aziendali qualora il loro coinvolgimento sia di supporto nell’attività inerente il servizio di PEC;

- fare da punto di riferimento per i clienti sulle problematiche di carattere tecnico e progettuale operando, per quest'ultimo argomento, in sinergia con gli architetti addetti all'offering;
- fare da punto di riferimento per gli altri Gestori di PEC per le problematiche legate all'interoperabilità fra i Gestori stessi.

A.3.2. Sito WEB del Gestore

Le informazioni relative ai servizi di Posta Elettronica Certificata offerti da Intesa sono disponibili on-line all'URL:

http://trustedmail.intesa.it/

A.3.3. Metodi di comunicazione con il Gestore

L'utente può contattare il Gestore, per ottenere informazioni o supporto, scrivendo o telefonando ai recapiti riportati ai paragrafi precedenti, ovvero tramite:

Posta Elettronica

Scrivendo all'indirizzo di posta elettronica: ***uff_pec@intesa.it***, chiunque lo desideri può ottenere supporto e informazioni relativamente al servizio Trusted Mail

N° verde 800-80.50.93

Allo scopo di fornire un supporto più tempestivo e indipendente dalla piattaforma tecnologica, Intesa ha messo a disposizione, per i propri clienti, un servizio di Help Desk. Telefonando al numero verde è possibile aprire una chiamata di supporto e ottenere l'assistenza tramite un operatore.

A.4. Riferimenti normativi e tecnici, definizioni e acronimi (specificatamente riferiti al Manuale Operativo)

A.4.1. Riferimenti normativi

Legge 59/97 Art.15 comma 2	Legge n.59 del 15 marzo 1997: "Delega al Governo per il conferimento di funzioni e compiti alle regioni e enti locali, per la riforma della Pubblica Amministrazione e per la semplificazione amministrativa" pubblicata sulla Gazzetta Ufficiale n.63 del 17 marzo 1997. Art.15 comma 2: "Gli atti, dati e documenti formati dalla pubblica amministrazione e dai privati con strumenti informatici o telematici, i contratti stipulati nelle medesime forme, nonché la loro archiviazione e trasmissione con strumenti informatici, sono validi e rilevanti a tutti gli effetti di legge. I criteri e le modalità di applicazione del presente comma sono stabiliti, per la pubblica amministrazione e per i privati, con specifici regolamenti da emanare entro centottanta giorni dalla data di entrata in vigore della presente legge ai sensi dell'Articolo 17, comma 2, della legge 23 agosto 1988, n.400. Gli schemi dei regolamenti sono trasmessi alla Camera dei deputati e al Senato della Repubblica per l'acquisizione del parere delle competenti Commissioni".
DPR 445/00	Decreto del Presidente della Repubblica del 28 dicembre 2000, n.445. "Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa", pubblicato sulla Gazzetta Ufficiale n.42 del 20 febbraio 2001.
DL 10 23/01/02	Recepimento della Direttiva 1999/93/CE sulla firma elettronica. (G.U. n.39 del 15 Febbraio 2002)
L 16/01/03	Legge 16 gennaio 2003, n. 3 Disposizioni ordinamentali in materia di pubblica amministrazione (G.U. n. 15 del 20 Gennaio 2003 - Supplemento Ordinario n. 5)
DPR 137 07/04/03	Regolamento recante disposizioni di coordinamento in materia di firme elettroniche a norma dell'Articolo 13 del decreto legislativo 23 gennaio 2002, n. 10. (G.U. n.138 del 17 Giugno 2003)
D.Lgs. 196 30/06/03	Codice in materia di protezione dei dati personali. (G.U. n.174 del 29 Luglio 2003, suppl. ord.)
DPCM 13/01/04	Regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici. (G.U. n.98 del 27 Aprile 2004)
CAD 07/03/05	Codice dell'Amministrazione digitale (Decreto Legislativo7 Marzo 2005 n.82)
DPR 68/05	Regolamento recante disposizioni per l'utilizzo della Posta Elettronica Certificata, a norma dell'articolo 27 della legge del 16 gennaio 2003, n. 3 (G.U. n. 97 del 28 Marzo 2005,)
DM 02/11/05	Regole tecniche per la formazione, la trasmissione e la validazione, anche temporale, della Posta Elettronica Certificata (G.U. n. 266 del 15 Novembre 2005)

Circolare CNIPA 14/11/05	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 (G.U. n. 283 del 5 Dicembre 2005)
Racc. per iscrizione IGPEC 13/2/2006	Raccomandazioni sul metodo e sulle procedure di iscrizione nell'elenco pubblico dei Gestori di Posta Elettronica Certificata. (CNIPA, 13 Febbraio 2006)
Circolare CNIPA di vigilanza sui Gestori 7/12/2006	Espletamento della vigilanza e del controllo sulle attività esercitate dagli iscritti nell'elenco dei Gestori di Posta Elettronica Certificata (PEC), di cui all'articolo 14 del decreto del Presidente della Repubblica 11 febbraio 2005, n. 68, «Regolamento recante disposizioni per l'utilizzo della Posta Elettronica Certificata, a norma dell'articolo 27 della legge 16 gennaio 2003, n. 3 ». (G.U. n. 296 del 21 dicembre 2006)
Dlgs 30 dicembre 2010, n. 235	Modifiche ed integrazioni al decreto legislativo 7 marzo 2005, n. 82, recante Codice dell'amministrazione digitale, a norma dell'articolo 33 della legge 18 giugno 2009, n. 69. (suppl. n. 8 alla G.U. n. 6 del 10 gennaio 2010)

A.4.2. Riferimenti tecnici

RFC 1305	Network Time Protocol (Version 3) Specification, Implementation
RFC 1847	Security Multiparts for MIME: Multipart/Signe and Multipart/Encrypted
RFC 1891	SMTP Service Extension for Delivery Status Notifications
RFC 1912	Common DNS Operational and Configuration Errors
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	RFC 3280 (2002): "Internet X.509 Public Key Infrastructure Certificate and CRL Profile
RFC 3161	RFC 3161 (2001): " Internet X.509 Public Key Infrastructure Time Stamp Protocol (TSP)"

A.4.3. Definizioni e acronimi

Sono qui riportati i significati di acronimi e di termini specifici aggiuntivi rispetto a quanto indicato all'Art.1 del DPR 445/00 e del DPCM 13/01/04, ai quali si fa espresso riferimento.

Non sono riportati i significati di alcuni acronimi e termini specifici di uso comune.

Termine o acronimo	*Significato*	*Riferimento*
Destinatario	L'utente che si avvale del servizio di Posta Elettronica Certificata per la ricezione di documenti prodotti mediante strumenti informatici	
Gestore	L'azienda che eroga il servizio di Posta Elettronica Certificata e che gestisce domini di Posta Elettronica Certificat	
http	HyperText Transfer Protocol Il protocollo HTTP definisce un metodo di interazione client-server ottimizzato per le connessioni brevi e veloci necessarie per le connessione tra client web e server web. Si tratta di un protocollo generico, stateless e leggero.	
HTTPS	Versione sicura del protocollo di trasmissione Http, basato su SSL e TLS	
LDAP	Lightweight Directory Access Protocol.	RFC 1777 RFC 2251 RFC 2252
MIME	Multipurpose Internet Mail Extensions standard generico per il formato dei documenti scambiati sulla rete internet tramite posta elettronica	RFC 1341
Mittente	L'utente che si avvale del servizio di Posta Elettronica Certificata per la trasmissione di documenti prodotti mediante strumenti informatici;	
NIC	Network Information Centre Ente responsabile della gestione dei nomi di dominio	
NTP	Network Time Protocol Protocollo per la sincronizzazione del tempo	RFC 1305
Object Identifier	Sequenza di numeri, registrata secondo la procedura definita dallo standard ISO/IEC 6523, che identifica un determinato oggetto all'interno di una gerarchia.	
OID	Object Identifier (vedi).	
PEC	Posta Elettronica Certificata	
PKCS	Public Key Cryptography Standard.	RSA Laboratories
RFC	An RFC (Request For Comments) is a document describing the standards that make the Internet work	

Termine o acronimo	*Significato*	*Riferimento*
SSL	Secure Socket Layer è un protocollo di sicurezza che fornisce privatezza nelle comunicazioni su Internet. Il protocollo permette alle applicazioni client/server di comunicare in una modalità progettata per evitare l'intercettazione, la modifica o la falsificazione dei messaggi.	
TLS	Transport Layer Security, sicurezza dello strato di trasporto.	
TSR	Time Stamp Request Richiesta di marca temporale	RFC 3161
Time Stamping Authority	Autorità che rilascia marche temporali	ETSI TS 102 023
Titolare	Il soggetto cui é assegnata una casella di Posta Elettronica Certificata	
TSA	Time Stamping Authority (vedi)	ETSI TS 102 023
TU	Testo Unico DPR 445/2000 e sue successive modifiche Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa	
URL	Uniform Resource Locator.	RFC 1738 RFC 1808 RFC 2368
UTC	Coordinated Universal Time	ITU-R Recommendation TF,460-5

A.5. Tabella di Corrispondenza

Si riporta di seguito la Tabella di Corrispondenza secondo quanto richiesto al paragrafo 2.1 della Circolare CNIPA 14/11/05 per un più facile reperimento delle informazioni all'interno del documento.

Punto	*Contenuto circolare CNIPA/CR/49*	*Sezione Manuale Operativo*	*Paragrafo Manuale Operativo*
a	i dati identificativi del gestore;	Sezione I	Par. A.3.1
b	l'indicazione del responsabile del Manuale Operativo;	Sezione I	Par. A.2.6
c	i riferimenti normativi necessari per la verifica dei contenuti;	Sezione I	Par. A.4.1
d	l'indirizzo del sito *web* del gestore ove è pubblicato e scaricabile il MO;	Sezione I	Par. A.2.5
e	l'indicazione delle procedure nonché degli standard tecnologici e di sicurezza utilizzati dal gestore nell'erogazione del servizio;	Sezione III	Par. C.3.1 Par. C.5
f	le definizioni, le abbreviazioni e i termini tecnici che figurano nel MO;	Sezione I	Par. A.4.3
g	una descrizione sintetica del servizio offerto;	Sezione III	Par. C.2
h	la descrizione delle modalità di reperimento e di presentazione delle informazioni presenti nei log dei messaggi;	Sezione III	Par. C.2.2.3
i	l'indicazione del contenuto e delle modalità dell'offerta da parte del gestore;	Sezione III	Par. C.6.2
j	l'indicazione delle modalità di accesso al servizio;	Sezione III	Par. C.2.2.1
k	l'indicazione dei livelli di servizio e dei relativi indicatori di qualità di cui all'articolo 12 del decreto del Ministro per l'innovazione e le tecnologie 2 novembre 2005;	Sezione III	Par. C.4.4
l	l'indicazione delle condizioni di fornitura del servizio;	Sezione III	Par. C.6.4.1
m	l'indicazione delle modalità di protezione dei dati dei titolari;	Sezione III	Par. C.5.4
n	l'indicazione degli obblighi e delle responsabilità che ne discendono, delle esclusioni e delle eventuali limitazioni, in sede di indennizzo, relative ai soggetti previsti all'articolo 2 del D.P.R. 68/2005	Sezione III	Par. C.6.4.2

B. SEZIONE II - Introduzione al servizio di Posta Elettronica Certificata

B.1. Premessa alla Sezione

La presente Sezione fornisce una sintesi generale dei principali elementi normativi, tecnici e organizzativi che sono alla base del servizio di PEC.

Nella Sezione vengono anche date indicazioni relative alle caratteristiche generali che devono avere i Gestori di PEC per la loro iscrizione nell'elenco dei Gestori di PEC tenuto da AgID.

La sezione si conclude con una breve descrizione di alcuni scenari di sviluppo dell'utilizzo della PEC in termini di benefici e ottimizzazioni operative nell'ambito dei processi comunicativi tra operatori economici e istituzionali.

B.2. Descrizione generale

La *PEC - Posta Elettronica Certificata* rappresenta uno dei sistemi di comunicazione elettronica tra i più innovativi attualmente a disposizione; consiste in un sistema di e-mail in grado di rilasciare ai mittenti una ricevuta elettronica, con valenza legale, attestante l'invio e la consegna al destinatario dei documenti informatici spediti via Internet.

In virtù dell'entrata in vigore delle regole tecniche disciplinanti il funzionamento della PEC è possibile utilizzare messaggi e-mail che hanno valore a tutti gli effetti di legge.

Infatti, con la certificazione del messaggio inviato con il sistema di PEC, il mittente riceve dal proprio Gestore una ricevuta che costituisce prova legale dell'avvenuta spedizione del messaggio e dell'eventuale allegata documentazione. Alla consegna del messaggio nella casella PEC del destinatario, il mittente riceverà una ricevuta di Avvenuta Consegna da parte del Gestore del destinatario.

La PEC, come l'e-mail di comune utilizzo, viaggia attraverso Internet e consente di inviare messaggi contenenti file di qualsiasi tipo (testi, immagini, video, ecc.).

Il servizio, considerate le sue peculiarità (consente lo scambio di e-mail con valore legale), è stato istituito e regolato dal DPR (DPR 68/05) e le sue Regole Tecniche sono state disciplinate dal DM 02/11/05, che ha determinato le regole tecniche per la formazione, la trasmissione e la validazione, anche temporale, della Posta Elettronica Certificata (PEC).

Il servizio di PEC viene fornito esclusivamente dai Gestori di Posta Elettronica Certificata. I mittenti e i destinatari (pubblici o privati) che intendono fruire del servizio di Posta Elettronica Certificata devono quindi necessariamente rivolgersi ad uno dei Gestori di PEC iscritti nell'elenco tenuto da AgID, il quale svolge funzioni di vigilanza e controllo nel rispetto delle prescrizioni previste dal DM 02/11/05 e provvede a tenere aggiornato tale elenco.

I Gestori di PEC, mediante l'apposizione della firma digitale, agiscono in qualità di garanti della spedizione del messaggio di Posta Elettronica Certificata (vedi Par. B.3).

B.3. I Gestori di Posta Elettronica Certificata

Come detto, a fare da garante dell'avvenuta consegna dell'e-mail saranno i Gestori di posta iscritti in un apposito elenco tenuto da AgID.

Possono chiedere di essere iscritti nel suddetto Albo sia i Privati che le Pubbliche Amministrazioni, mediante apposita domanda.

Dal punto di vista della natura giuridica, i privati che presentano domanda d'iscrizione nell'elenco dei Gestori di PEC ad AgID devono essere costituiti in forma di società di capitali e avere capitale sociale interamente versato non inferiore ad un milione di Euro.

Le modalità di accreditamento all'elenco pubblico dei Gestori di Posta Elettronica Certificata, sono contenute nella Circolare CNIPA 14/11/05.

Le Pubbliche Amministrazioni possono svolgere autonomamente l'attività di Gestore di Posta Elettronica Certificata, rispettando in ogni caso le stesse regole tecniche e di sicurezza previste dalla normativa.

La domanda di iscrizione all'Albo deve essere corredata dei relativi allegati che attestino che il Gestore del servizio di PEC abbia i requisiti specifici, che sia in grado di attestare la propria affidabilità e che il personale addetto al servizio abbia le competenze tecniche necessarie, al fine di garantire la correttezza e serietà del servizio.

I Gestori devono essere in grado di offrire ai propri clienti determinati livelli di servizio e di qualità, in modo da consentire un'adeguata gestione del sistema di posta e da garantire standard qualitativi affidabili ai mittenti e ai destinatari dei messaggi. Il Gestore, quindi, dovrà:

- adottare adeguate misure per garantire l'integrità e la sicurezza del servizio di Posta Elettronica Certificata;
- prevedere servizi di emergenza che assicurino in ogni caso il completamento della trasmissione;
- garantire idonea riservatezza e protezione dei dati personali;
- garantire l'interoperabilità con gli altri Gestori iscritti all'Albo;

- dotarsi di apposita polizza assicurativa a copertura dei rischi dell'attività e dei danni causati a terzi dalla propria attività di Gestore di PEC.

Ai fini della valutazione della domanda d'iscrizione, particolare attenzione é data al manuale operativo di cui all'Art.23 del DM 02/11/05, che esplicita le regole generali e le procedure informatiche adottate dal Gestore di PEC per la prestazione del servizio. Tale manuale deve essere pubblicato sul sito del Gestore in modo da permetterne la consultazione ai potenziali clienti del servizio, agli utenti e ai loro corrispondenti.

L'istruttoria delle domande d'iscrizione viene condotta da AgID: il compito dell'organo é quello di verificare la regolarità della documentazione prodotta, e, qualora sia necessario, procedere con una integrazione di istruttoria al fine di valutare correttamente le capacità dell'azienda candidata. Quindi, ottenute tutte le informazioni necessarie, autorizzare o negare l'iscrizione nell'elenco dei Gestori di PEC.

B.4. Sintesi delle metodologie di funzionamento del sistema di Posta Elettronica Certificata

Il funzionamento del servizio di PEC si differenzia dal normale funzionamento dell'e-mail, in particolare per la gestione delle ricevute collegate al messaggio originale e ai dati di certificazione. Tali ricevute contengono:

- firma digitale dei Gestori (rif. Codice dell'Amministrazione Digitale e s.m.i.);
- indicazione temporale di riferimento opponibile ai terzi.

Il documento informatico trasmesso per via telematica s'intende spedito dal mittente se inviato al proprio Gestore e s'intende consegnato al destinatario se reso disponibile all'indirizzo elettronico da questi dichiarato, nella casella di posta elettronica del destinatario messa a disposizione dal suo Gestore.

I sistemi di gestione di PEC, durante i passaggi intermedi dal mittente al destinatario finale generano dei messaggi specifici (conformi allo standard internazionale S/MIME) elaborati in base alla tipologia di messaggio e distinti in tre categorie (le ricevute, gli avvisi e le buste - Rif. Figura 1), anche nel caso in cui il mittente e il destinatario appartengano allo stesso dominio di Posta Elettronica Certificata.

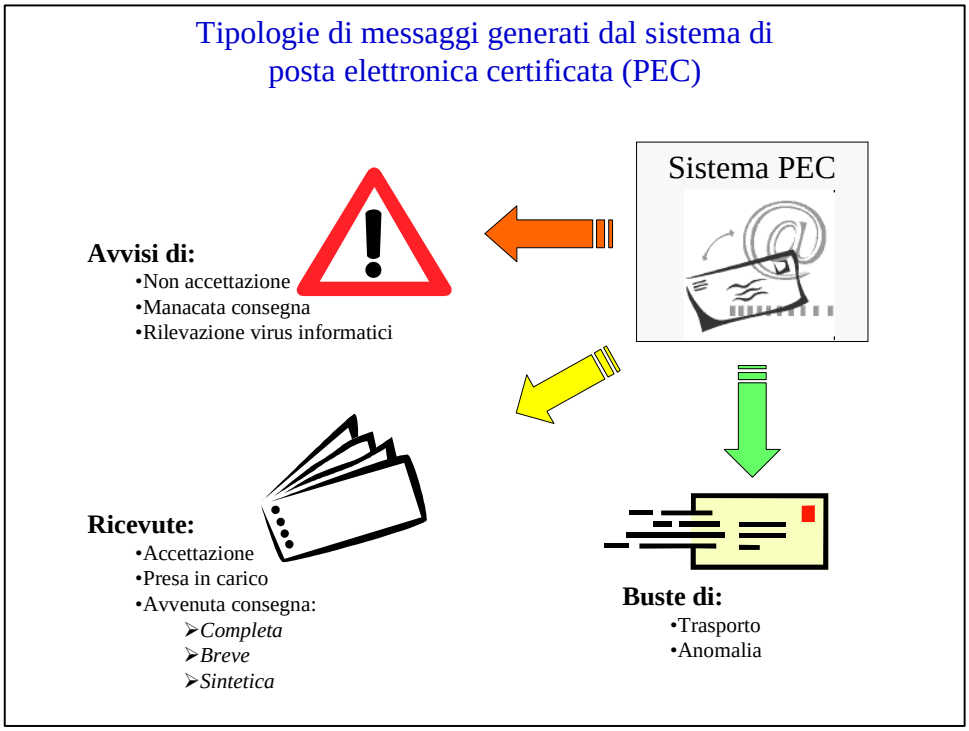

Figura 1: Tipologie di messaggio

Con la certificazione delle fasi del servizio di PEC, il mittente riceve dal proprio Gestore di PEC una ricevuta, che costituisce prova legale dell'avvenuta spedizione del messaggio (e dell'eventuale documentazione allegata) e una successiva ricevuta dal Gestore del destinatario, che costituisce prova legale che il messaggio è stato consegnato nella casella PEC del Destinatario.

Ai fini della validità della trasmissione e della ricezione del messaggio di Posta Elettronica Certificata vengono rilasciate, rispettivamente:

a) ricevuta di accettazione, proveniente dal proprio Gestore di posta, che attesta l'avvenuto invio della mail;
b) ricevuta di presa in carico che attesta il passaggio di responsabilità dal Gestore mittente al Gestore destinatario;
c) ricevuta di avvenuta consegna *completa*, *breve* oppure *sintetica*, proveniente dal Gestore PEC del destinatario, che certifica che quest'ultimo abbia ricevuto la comunicazione. Tale certificazione sarà resa nel momento in cui il destinatario avrà disponibilità del messaggio (ossia al momento del ricevimento), indipendentemente dal fatto che egli lo abbia letto o meno.

Gli avvisi generati dal sistema di Posta Elettronica Certificata possono essere:

a) avviso di non accettazione (per eccezioni formali o virus informatici);

b) avviso di mancata consegna (per il superamento dei tempi massimi previsti o per virus informatici); in caso di un'eventuale mancata ricezione da parte del destinatario, il Gestore di posta del destinatario informerà il mittente qualora entro 24 ore non sarà riuscito ad effettuare la consegna del messaggio;
c) avviso di rilevazione di virus informatici.

Le tipologie di buste create dal sistema possono essere:

a) busta di trasporto (contenente il messaggio originario, i dati di certificazione e la firma del Gestore);
b) busta di anomalia (contenente il messaggio errato e la firma del Gestore).

Tutte le tipologie di messaggi generati dal sistema PEC sono sottoscritti dai Gestori di Posta Elettronica Certificata mediante la firma elettronica avanzata.

I certificati di firma di cui il Gestore deve disporre ai fini della validità della certificazione del messaggio sono rilasciati da AgID al momento dell'iscrizione nell'elenco pubblico dei Gestori di Posta Elettronica Certificata e possono essere sino ad un numero massimo di dieci per ciascun Gestore (ai sensi dell'Art.7, comma 3, del DM 02/11/05 é comunque prevista la possibilità di richiedere un numero di certificati di firma superiore a 10 da parte dei Gestori).

Il percorso dal mittente al destinatario finale del messaggio di PEC é di seguito schematizzato attraverso una sequenza che illustra le fasi del passaggio dal mittente al rispettivo Gestore e dal Gestore del destinatario al destinatario (Rif. Figura 2) stesso e inoltre evidenzia i momenti in cui il servizio di PEC genera le tre tipologie di ricevute descritte in precedenza (Rif. Figura 1).

In caso di un'eventuale mancata ricezione da parte del destinatario, il Gestore di posta del destinatario informerà il mittente qualora entro 24 ore non sia riuscito ad effettuare la consegna del messaggio.

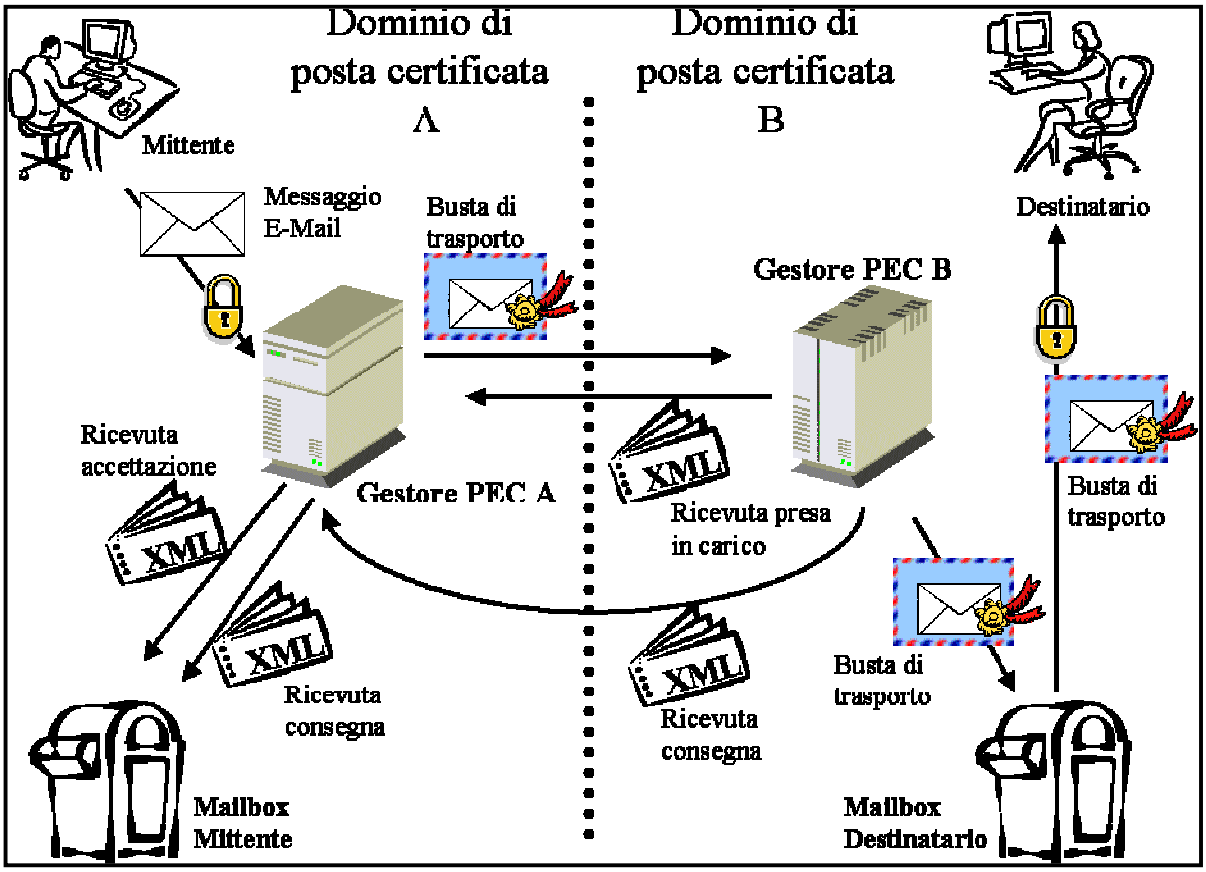

Figura 2: Flusso logico di funzionamento della PEC

Il DPR 68/05 stabilisce, inoltre, la soluzione per l'eventuale smarrimento delle ricevute; infatti, un apposito archivio informatico custodito dai Gestori di Posta Elettronica Certificata ha il compito di conservare, per un periodo di trenta mesi, le tracce informatiche caratterizzate dallo stesso valore giuridico.

Nel caso in cui ci siano problemi nella consultazione dei messaggi notificati, il Gestore potrà fornire, su richiesta, i dati presenti nei propri file di log del sistema di PEC in cui viene tenuta traccia di tutte le operazioni svolte.

Inoltre, i Gestori sono tenuti a verificare che il messaggio di posta elettronica non sia affetto da virus e ad adottare i comportamenti disciplinati all'Art.12 del DPR 68/05 (Rif. Figura 3).

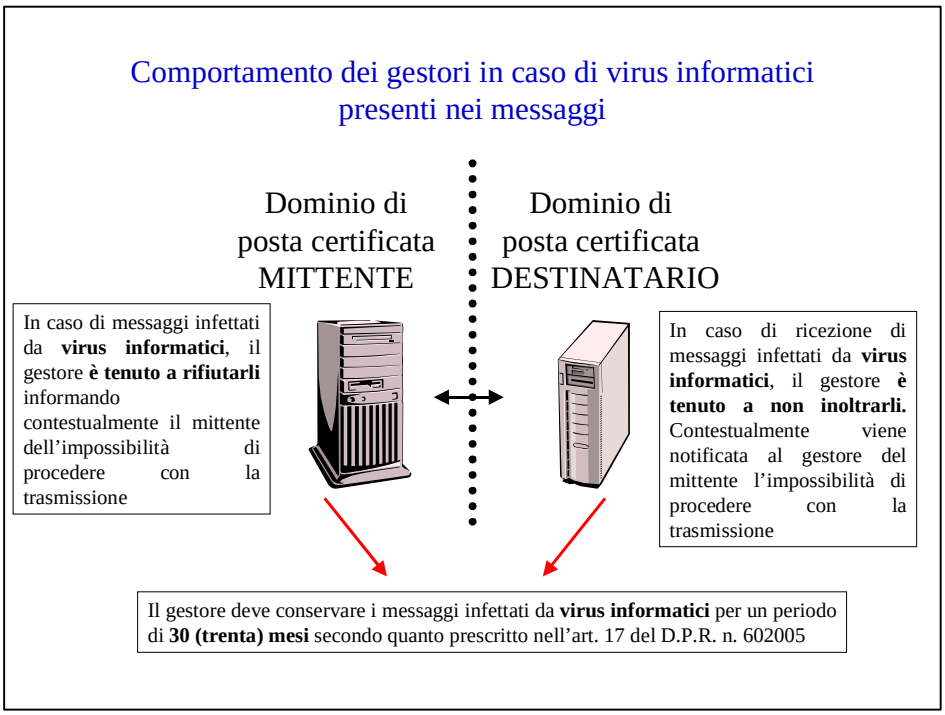

Figura 3: Comportamento in caso di messaggi infettati da virus

B.5. Sintesi degli obblighi e delle responsabilità del Gestore e dei Titolari

Sia il Gestore che il Titolare hanno degli obblighi e delle responsabilità di seguito riportate a titolo indicativo e non esaustivo (il dettaglio sarà fornito nei documenti specifici di ciascun gestore Gestore, nel rispetto delle normative di riferimento).

Il Gestore dovrà fornire il servizio conformemente a quanto stabilito dalla normativa vigente in materia, con le modalità indicate nel Manuale Operativo, assumendosi l'obbligo di:

- assicurare l'erogazione del servizio secondo i livelli minimi di servizio previsti dalla normativa vigente;
- assicurare l'interoperabilità del servizio con gli altri operatori iscritti nell'elenco pubblico dei Gestori di PEC;
- rendere disponibili, nei casi previsti dalla legge, i log inerenti le trasmissioni tra caselle di Posta Elettronica Certificata e il cui accesso, in ogni caso, può avvenire previa richiesta dell'autorità giudiziaria.

Il Gestore ha il diritto/dovere di modificare, opportunamente e in tempi congrui, le specifiche tecniche di erogazione del servizio, in base all'evoluzione tecnologica e/o normativa, aggiornando il Manuale Operativo.

Il Titolare si dovrà assumere, in prima persona e impegnandosi ad estenderli agli Utenti del servizio, l'obbligo di:

- fornire tutte le informazioni e la documentazione, richiesta dal Gestore, necessarie ad una corretta identificazione garantendone, sotto la propria responsabilità, l'attendibilità ai sensi del DPR 68/05;
- prestare il consenso al trattamento dei dati personali ai sensi del D.Lgs. n. 196 del 2003 (ove richiesto);
- informare immediatamente il Gestore in caso risulti compromessa la riservatezza dei codici di accesso per l'utilizzo del servizio;
- consultare in maniera preventiva il Manuale Operativo per conoscerne contenuti;
- conservare con la massima riservatezza e diligenza i codici di accesso al servizio con l'obbligo di non cederli a terzi a nessun titolo;
- non utilizzare il servizio con lo scopo di depositare, inviare, pubblicare, trasmettere e/o condividere applicazioni o documenti informatici che siano in contrasto o violino diritti di proprietà intellettuale, segreti commerciali, marchi, brevetti o altri diritti di proprietà di terzi.

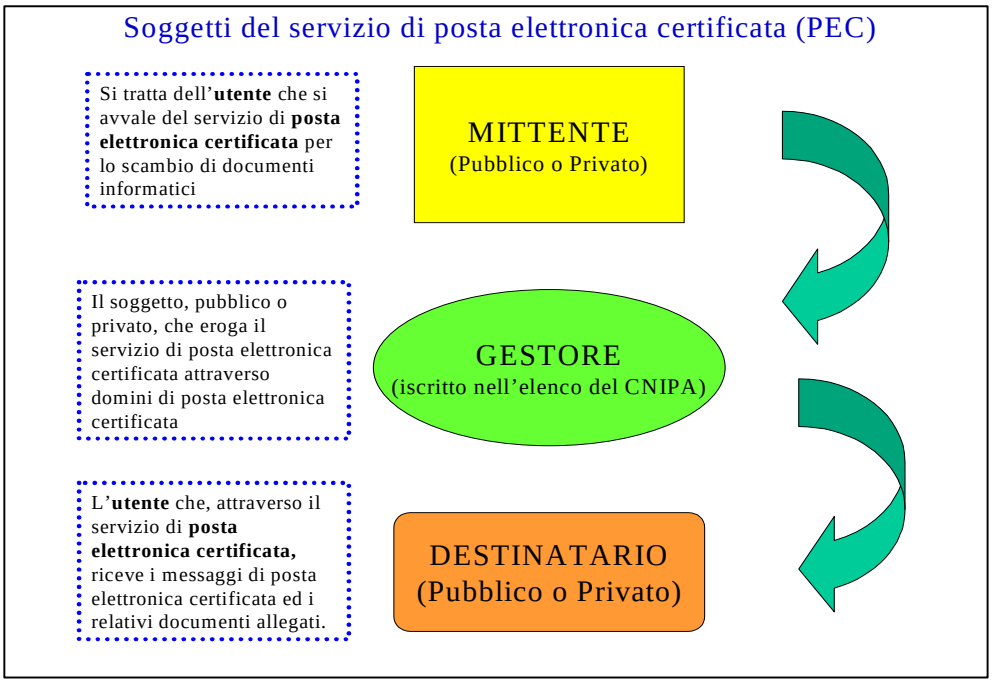

Figura 4: Soggetti del servizio di Posta Elettronica Certificata

B.6. Scenari di utilizzo della PEC

L'avvento della Posta Elettronica Certificata rivoluzionerà il sistema di comunicazioni tra i privati (aziende, professionisti, cittadini), tra i privati e la Pubblica Amministrazione come anche tra le sole Pubbliche Amministrazioni. L'utilizzo del servizio potrà portare inoltre cambiamenti che arriveranno a toccare la gestione delle comunicazioni "da e per" i singoli cittadini.

L'impiego della Posta Elettronica Certificata facilita l'attuazione del cambiamento culturale e organizzativo della Pubblica Amministrazione e risponde alle esigenze di competitività del Paese che si presentano a livello nazionale e internazionale.

L'impiego della Posta Elettronica Certificata apporterà notevoli risparmi, non solo in termini di tempo, ma anche e soprattutto, in termini economici.

La PEC, infatti, può essere utilizzata per lo scambio di messaggi e-mail che hanno valore legale a tutti gli effetti e, pertanto, possono essere assimilati alla *Raccomandata con Avviso di Ricevimento* (*Raccomandata A.R.*). Fino ad oggi, proprio la Raccomandata A.R. rappresentava il mezzo maggiormente utilizzato per avere certezza, da parte del mittente, della ricezione della comunicazione inviata al destinatario.

Il Governo ha già finanziato diversi progetti di sperimentazione finalizzati alla diffusione della Posta Elettronica Certificata quale mezzo di comunicazione in grado di favorire e rendere più rapido e sicuro il dialogo tra le amministrazioni e tra queste e i cittadini. Si cita, a titolo d'esempio, il programma P@P, approvato dal *Comitato dei Ministri per la Società dell'Informazione* a marzo 2003 e avente come obiettivo generale quello di massimizzare i benefici derivanti dall'utilizzo delle comunicazioni elettroniche nella Pubblica Amministrazione.

La PEC potrà quindi, nelle more di quanto comunque sancito dall'Art.16 comma 4 del DPR 68/05, anche essere utilizzata in ambito processuale. L'uso della firma elettronica avanzata e l'invio attraverso la PEC conferisce al messaggio valore ufficiale di notificazione: la casella di Posta Elettronica Certificata consente la trasmissione di documenti sottoscritti aventi piena validità giuridica ai sensi del D.P.R. 28 dicembre 2000, n. 445.

Aziende e professionisti, oltre ad avere un vantaggio nelle gestione delle comunicazioni ufficiali con le Pubbliche Amministrazioni e con il Fisco, potranno spedire e ricevere con il servizio di PEC le fatture elettroniche, per le quali é necessario dimostrare che il documento sia stato effettivamente spedito, riducendo i tempi e migliorando i rapporti con i clienti.

L'Agenzia delle Entrate ha emanato il provvedimento 22 dicembre 2005 (in G.U. 10 gennaio 2006 n. 7), in attuazione delle disposizioni in tema di accertamento tributario contenute nell'Art.32, terzo comma, D.P.R. n. 600/1973 e nell'Art.51, quarto comma, D.P.R. n. 633/1973.

Il provvedimento contiene le modalità di trasmissione telematica delle richieste e delle risposte, nonché di dati, notizie e documenti in esse contenuti, con riferimento all'utilizzo del sistema di Posta Elettronica Certificata nello scambio di informazioni tra enti accentratori e intermediari finanziari.

A decorrere dal 1º marzo 2006, le richieste per esigenze di accertamento o di indagine inoltrate ai sensi dei suddetti articoli da parte di Enti quali l'Agenzia delle Entrate, il Corpo della guardia di Finanza o altri, e le risposte da parte degli operatori finanziari (quali Banche, società Poste italiane S.p.a., intermediari finanziari, ecc.), relative alle informazioni e ai servizi prestati ai propri clienti, devono essere trasmesse con il sistema di Posta Elettronica Certificata.

C. SEZIONE III – Elementi generali e particolari del servizio offerto dal Gestore Intesa

C.1. Premessa alla Sezione

In questa sezione sono presentate le funzionalità e le caratteristiche tecniche del servizio Trusted Mail del Gestore Intesa e ne vengono descritte le relative modalità di offerta.

La sezione é strutturata come segue:

- descrizione dell'*Architettura Funzionale*, in termini di Schema Generale e dettaglio delle funzioni disponibili per l'utente;
- descrizione della *Piattaforma Tecnologica*, con sintesi delle principali componenti infrastrutturali hardware e software utilizzati;
- descrizione del *Processo di Gestione e Erogazione*, del servizio;
- riepilogo delle *Procedure e Misure di Sicurezza*, adottate con riferimento agli standard di qualità e tecnici internazionali e nazionali;
- caratteristiche dell'*Offerta Intesa*, in termini di componenti, modalità di utilizzo e condizioni generali di fornitura.

C.2. Architettura funzionale Trusted Mail

I requisiti guida seguiti nella progettazione e realizzazione del servizio di Posta Elettronica Certificata di Intesa derivano dalle specifiche dettate dalle Normative di Legge combinate con la decennale esperienza di Intesa nel campo dei servizi di Network Broker a supporto dell'interoperabilità tra le Imprese.

Il servizio Trusted Mail soddisfa le regole organizzative e tecniche indicate dalla normativa, con particolare riferimento al DM 02/11/05 e al DM 02/11/05, fornendo in particolare:

- possibilità di firmare i messaggi;
- garanzia dell'avvenuta consegna all'indirizzo di posta elettronica del destinatario;
- rilevazione di eventuali virus informatici sui messaggi;
- tracciamento delle attività del sistema nei log conservati a norma;
- trasmissione delle informazioni in modo sicuro;

consentendo quindi:

- opponibilità di fronte a terzi della provenienza e del recapito del messaggio;
- indipendenza rispetto ai contenuti del messaggio;
- possibilità di utilizzo con una qualsiasi applicazione client di posta elettronica e con soluzioni integrabili nei workflow applicativi.

C.2.1. Schema generale del servizio

A scopo esemplificativo, la descrizione dello schema logico di funzionamento è descritto dalla Figura 5, dove è illustrato il tipico ciclo di una spedizione da parte di un utente Mittente attestato su un Dominio PEC a un utente Destinatario attestato su un Dominio PEC di un altro Gestore.

Ovviamente il servizio Trusted Mail é in grado di soddisfare tutte le combinazioni di interscambio possibili, sia quando il Mittente e il Destinatario sono attestati all'interno di un unico Dominio, sia fungendo da punto di Consegna a fronte di documenti acquisiti da un Dominio terzo. Trusted Mail è in grado di scambiare mail con domini non appartenenti alla PEC, funzionando come un normale server di posta, evidenziando che il messaggio viene scambiato con utente di posta non certificata.

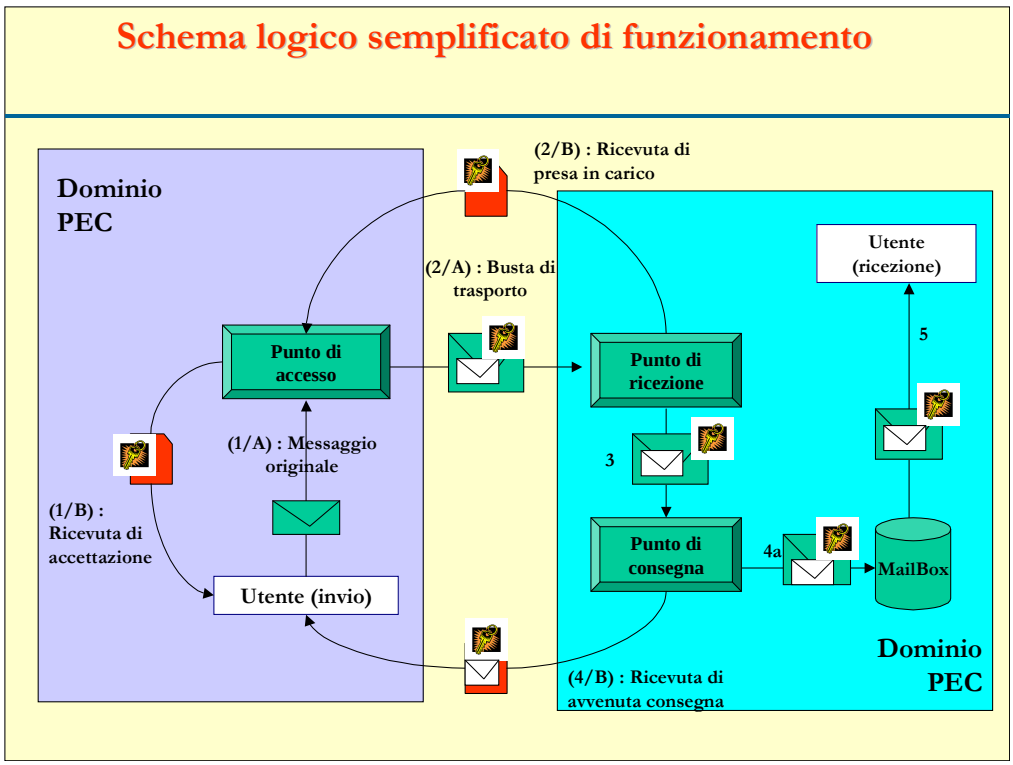

Figura 5: Schema logico del servizio

I principali moduli funzionali sono di seguito descritti più in dettaglio.

C.2.1.1. Modulo Punto di accesso

Un messaggio spedito da un utente attestato direttamente sul servizio di Posta Elettronica Certificata di Intesa viene elaborato dalla componente relativa al Punto di Accesso.

Sul messaggio originale, il Punto di Accesso esegue le seguenti operazioni:

- effettua i controlli formali e di assenza virus informatici (cfr. Par. C.2.1.4);
- in caso di anomalie: viene generato un *Avviso di non accettazione* che informa il mittente dell'esito negativo fornendo la motivazione dello scarto;
- nel caso di esito positivo: viene generata una *Ricevuta di accettazione* e imbustato il messaggio originale in una busta di trasporto, la quale è firmata con il Certificato del Gestore di PEC; viene finalmente inoltrato il plico S/Mime verso la sua destinazione.

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

Il punto di accesso, utilizzando i dati dell'indice locale dei Gestori di PEC, effettua un controllo per ogni destinatario del messaggio originale per verificare se appartiene all'infrastruttura di Posta Elettronica Certificata o se é un utente esterno (posta Internet).

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

Il messaggio originale (completo di header, testo e allegati) è inserito come allegato all'interno di una busta di trasporto, alla quale viene apposta una firma elettronica avanzata che consente di rendere manifesta la provenienza e di assicurare l'integrità e l'autenticità dei messaggi del sistema di Posta Elettronica Certificata. Tale firma, come definito in DM 02/11/05 Art.1.d, viene generata attraverso una procedura informatica che garantisce la connessione univoca al Gestore e la sua univoca identificazione, creata automaticamente con mezzi che garantiscono il controllo esclusivo da parte del Gestore. In particolare il certificato di firma viene consegnato al Gestore direttamente da AgID successivamente all'iscrizione nell'elenco pubblico dei Gestori di PEC.

C.2.1.2. Punto di ricezione

Un messaggio proveniente da un Gestore di Posta Elettronica Certificata remoto viene elaborato dal Punto di Ricezione del Gestore del destinatario, che effettua le seguenti azioni in funzione dell'esito delle operazioni di verifica della correttezza del messaggio in ingresso:

- se il messaggio in ingresso è una busta di trasporto corretta, emette una ricevuta di presa in carico verso il Gestore mittente firmata con il proprio certificato - al fine di permettere il tracciamento del transito del messaggio originale tra i diversi Gestori - e inoltra la busta di trasporto verso il punto di consegna locale;
- se il messaggio in ingresso è una busta di trasporto errata oppure non è una busta di trasporto, imbusta il messaggio in arrivo in una busta di anomalia e la inoltra verso il punto di consegna.

C.2.1.3. Punto di consegna

All'arrivo di un messaggio al Punto di Consegna, il sistema ne verifica la tipologia e stabilisce se deve inviare una ricevuta al mittente. La ricevuta di avvenuta consegna è emessa esclusivamente a fronte della ricezione della corretta busta di trasporto.

La ricevuta di avvenuta consegna indica al mittente che il suo messaggio è stato effettivamente consegnato nella casella del destinatario specificato e certifica la data e l'ora dell'evento tramite un testo leggibile dall'utente e tramite un allegato XML, che contiene i dati di certificazione in formato elaborabile.

A fronte di un errore di consegna nella casella di destinazione (casella piena, messaggio troppo grande, ecc), il punto di consegna emette un avviso di mancata consegna verso il mittente.

C.2.1.4. Gestione virus informatici

Il sistema di Posta Elettronica Certificata del Gestore Intesa è conforme a quanto stabilito dal DPR 11/02/05 (Artt.11 e 12):

- trattare il messaggio contenente virus secondo le regole tecniche indicate nell'allegato;
- informare il mittente che il messaggio inviato contiene virus;
- conservare il messaggio contenente virus per un periodo non inferiore ai trenta mesi secondo le modalità indicate nelle deliberazioni di AgID in materia di riproduzione e conservazione sostitutiva.

- qualora il Gestore del mittente riceva messaggi con virus informatici è tenuto a non inoltrarli, informando tempestivamente il mittente dell'impossibilità di dar corso alla trasmissione; in tale caso il Gestore conserva i messaggi ricevuti per trenta mesi secondo le modalità definite dalle regole tecniche di cui all'Art.17 del DPR 11/02/05.
- qualora il Gestore del destinatario riceva messaggi con virus informatici è tenuto a non consegnarli al destinatario, informando tempestivamente il Gestore del mittente, affinché comunichi al mittente medesimo l'impossibilità di dar corso alla trasmissione; in tale caso il Gestore del destinatario conserva i messaggi ricevuti per trenta mesi secondo le modalità definite dalle regole tecniche di cui all' Art.17 del DPR 11/02/05.

In caso di presenza di messaggi con virus informatici, il sistema di Posta Elettronica Certificata del Gestore Intesa è in grado di rilevarli e di notificare tempestivamente alle seguenti entità l'impossibilità di dar corso alla trasmissione:

- il Mittente, nel caso in cui il messaggio sia pervenuto al punto di accesso;
- il Gestore del mittente, nel caso in cui il messaggio sia pervenuto al punto di ricezione.

La rilevazione dei virus informatici sui messaggi avviene mediante l'utilizzo di un sistema antivirus collegato ai server di erogazione del servizio di Posta Elettronica Certificata.

La notifica da parte del Gestore Intesa è data mediante l'invio di un avviso di rilevazione di virus informatici, come definito in DM 02/11/05 Art.6.8.

I messaggi affetti da virus informatici sono conservati per trenta mesi secondo le modalità indicate nelle deliberazioni di AgID in materia di riproduzione e conservazione dei documenti su supporto ottico (DM 02/11/05 Art.11.3).

C.2.1.5. Formato dei messaggi

I messaggi generati dal sistema (ricevute, avvisi e buste) sono tutti in formato S/MIME in conformità all'Art.6.1 del DM 02/11/05.

I messaggi generati sono composti da una parte di testo descrittivo e da una serie di allegati. Ogni messaggio viene inserito in una struttura S/MIME, a sua volta firmata con la chiave privata del Gestore di posta certificata, generando in tal modo una struttura PKCS#7.

Il certificato associato alla chiave usata per la firma viene incluso in tale struttura.

Il formato PKCS#7 usato per la firma dei messaggi generati dal sistema è il *multipart/signed* (.p7s) così come descritto nello standard tecnologico RFC 2633.

C.2.1.6. Tracciatura

Il sistema Trusted Mail mantiene traccia di tutte le operazioni svolte registrando su di un apposito Log il message-ID del messaggio originale, i tipi di evento cui il messaggio è stato sottoposto, corredati di data, ora, mittente, destinatari, e oggetto del messaggio.

Tali dati sono conservati secondo quanto dettato dalle normative e archiviati a norma. Vengono resi disponibili su richiesta tramite apposita procedura (vedi Par. C.2.2.2.2).

I dati memorizzati costituiscono inoltre la base per le elaborazioni statistiche e la misurazioni del livello di servizio.

C.2.1.7. Avvisi e segnalazioni

Il sistema di Posta Elettronica Certificata Intesa prevede, come da normativa, la generazione di avvisi in caso rilevazione di anomalie.

Nel dettaglio, gli avvisi gestiti dal sistema di Posta Elettronica Certificata del Gestore Intesa sono i seguenti:

- avviso di non accettazione per eccezioni formali;
- avviso di rilevazione di virus informatici;
- avviso di mancata consegna per superamento dei tempi previsti per l'attesa (timeout);
- avviso di mancata consegna (causali: dimensioni eccessive, casella destinatario piena, destinatario inesistente, presenza di visrus).

Tali segnalazioni sono principalmente rivolte al mittente del messaggio affinché sia a conoscenza che il suo messaggio non è stato consegnato e possa, eventualmente, intraprendere azioni per risolvere il problema.

C.2.2. Funzionalità Utenti

Per poter utilizzare il servizio Trusted Mail occorre anzitutto effettuare la registrazione del Titolare come più dettagliatamente descritto nel paragrafo C.6.4.1.

Tale processo permette di riservare una casella di Posta Elettronica Certificata e abbinare ad essa un'Utenza e una Password per l'accesso al sistema. Per l'espletamento di tale operazione, il Gestore deve disporre dei dati anagrafici del Titolare; la richiesta di registrazione deve essere corredata di un documento di riconoscimento. Il processo è analogo anche laddove il Titolare sia una persona giuridica.

Le caselle di Posta Elettronica Certificata possono essere attivate con tre modalità, a seconda dei soggetti:

- Soggetti individuali (Persona Fisica), dove é il Titolare che stipula direttamente il contratto con il Gestore e sottoscrive i documenti necessari;

- Pubbliche Amministrazioni, Enti e Aziende (Persone Giuridiche), in cui è il Cliente del Gestore il soggetto dotato di tale natura giuridica che richiede il servizio per i propri dipendenti. In questo caso il Cliente fornisce al Gestore il nominativo di una propria persona di riferimento, la quale potrà inviare al personale del Gestore addetto alla Registrazione i dati dei Titolari per i quali dovrà essere riservata un casella;
- Persone giuridiche per le quali l'Ente richiedente (sia esso l'ente richiedente stesso o un'entità esterna motivata da esigenze di progetto nel quale viene coinvolta l'organizzazione cui sarà intestata la casella) esibirà documentazione tale da identificare il richiedente. Sarà pertanto quest'ultima entità, attraverso le persone dei legali rappresentanti, l'intestataria della casella PEC.

I dati di Registrazione dei Titolari sono memorizzati su di un apposito database e viene creata la casella sul sistema di Posta Elettronica Certificata. Tale casella risulta quindi associata alla username e alla password comunicate dal Titolare in fase di richiesta. La password assegnata potrà essere modificata in qualunque momento dal Titolare stesso, mediante l'accesso all'opportuna applicazione resa disponibile dal Gestore. Come prassi di sicurezza, è richiesto che la password sia sostituita primo accesso.

Per ogni Utente registrato il servizio Trusted Mail fornisce le funzionalità descritte nei paragrafi seguenti eventualmente erogate con interfacce utente differenti in funzione di specifici progetti:

C.2.2.1. Accesso al servizio

L'accesso al servizio Trusted Mail di Intesa è possibile nelle due diverse modalità:

- client di posta elettronica
- webmail

Per la prima modalità è sufficiente disporre di un'applicazione client di posta elettronica che supporti i protocolli IMAP (RFC 3501) o POP3 (RFC 1939) e SMTP (RFC 3207) su canale di comunicazione sicuro SSL.

La seconda modalità di accesso consiste nell'utilizzo di un browser internet collegato all'URL https://*pec.trustedmail.intesa.it* oppure, se richiesto, al dominio dedicato al Cliente (Vedi Par. C6 - *Offerta del Gestore*).

Le istruzioni per l'utilizzo di questa applicazione web sono contenute nel *Manuale Utente* del servizio che sarà consegnato al cliente al momento della sottoscrizione del contratto.

C.2.2.1.1. Funzioni di accesso alla casella di Posta tramite client di posta

L'utilizzo da parte di un utente del servizio di PEC può avvenire mediante un'applicazione client di posta elettronica che consente di gestire la composizione, la trasmissione, la ricezione e l'organizzazione messaggi di posta elettronica da e verso un server di posta.

A seconda del programma utilizzato, si potrà usufruire di servizi aggiuntivi, quali la gestione degli indirizzi all'interno di una rubrica, la gestione di più di una casella di posta elettronica, la possibilità di applicare dei filtri alla posta in arrivo, di riconoscere, filtrare o rifiutare messaggi di posta indesiderata o l'integrazione con sistemi crittografici a chiave pubblica.

In generale le funzionalità di base offerte da ogni applicazione client di posta elettronica sono le seguenti:

- Ricezione messaggi: all'arrivo di un messaggio sul server, questo provvede all'inserimento dello stesso nella mailbox dell'utente. A seconda delle impostazioni dell'applicazione client, al momento del collegamento con il server, i messaggi vengono scaricati sul computer locale dell'utente (se il protocollo di ricezione messaggi in ingresso è POP3) oppure rimangono sul server (se il protocollo per i messaggi in ingresso è IMAP).
- Consultazione messaggi: l'applicazione client provvede alla visualizzazione dell'elenco dei messaggi divisi in apposite cartelle, alcune delle quali sono già predefinite (Posta in uscita, Posta in arrivo, Bozze). Per ogni cartella, l'applicazione visualizza l'elenco dei messaggi correntemente presenti, visualizzando per ognuno le informazioni principali quali
  - Indirizzo del mittente
  - Oggetto del messaggio
  - Data di ricezione
  - Dimensioni del messaggio
  - Presenza di eventuali allegati.

  L'utente può scegliere l'ordinamento dei messaggi e visualizzarne il contenuto mediante la selezione sulla singola riga dell'elenco. Eventuali file allegati possono essere visualizzati con la corrispondente applicazione oppure essere salvati sulla postazione locale. I messaggi relativi alle ricevute (accettazione e consegna) e agli avvisi sono inseriti nella cartella della posta in arrivo e sono individuabili in base al contenuto del campo *Oggetto*.
- Composizione di nuovi messaggi: è possibile creare nuovi messaggi specificando gli indirizzi dei destinatari, l'oggetto, il corpo del messaggio e eventuali file allegati. Le applicazioni client offrono anche la possibilità di rispondere ad un messaggio ricevuto e di inoltrare un messaggio ad altri destinatari.

C.2.2.2. Funzioni di richiesta delle informazioni presenti nei log dei messaggi

Come accennato in precedenza il sistema di Posta Elettronica Certificata di Intesa mantiene traccia delle operazioni svolte su un apposito registro (*Log dei messaggi*) e i dati contenuti in tale registro sono conservati per trenta mesi (Art.11.2 DPR 11/02/2005).

Al fine di ottemperare a quanto previsto dall'Art.10 del DM 20/11/05, il Gestore adotta specifiche procedure interne per la conservazione dei log emessi dal sistema di Posta Elettronica Certificata.

In particolare:

- vengono applicate tutte le metodologie operative previste dalla normativa vigente in materia di riproduzione e conservazione dei documenti su supporto ottico;
- viene eseguito senza soluzioni di continuità il salvataggio dei log dei messaggi generati in ciascun intervallo temporale non superiore alle ventiquattro ore (Art.10.1 DM 02/11/05);
- ai file generati da ciascuna operazione di salvataggio viene associata la relativa marca temporale emessa dal sistema di validazione temporale della stessa Intesa (Art.10.2 DM 02/11/05).

C.2.2.2.1. Formato dei Log

I dati riportati sul log per ogni operazione eseguita sono i seguenti:

- il codice identificativo univoco assegnato al messaggio originale (Message-ID);
- 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 (accettazione, ricezione, consegna, emissione ricevute, errore, ecc.);
- il codice identificativo (Message-ID) dei messaggi correlati generati (ricevute, errori, ecc.);
- il Gestore mittente.

C.2.2.2.2. Modalità di richiesta dei log

Come previsto dall'Art.6.7 del DPR 11/02/05, nel caso in cui il mittente non abbia più la disponibilità delle ricevute dei messaggi di Posta Elettronica Certificata inviati, le informazioni contenute nel registro informatico del Gestore Intesa possono essere richieste al Gestore stesso e sono, esse stesse, opponibili a terzi.

A tale proposito il Gestore Intesa prevede la seguente procedura per la richiesta di copia dei log dei messaggi:

1. il Titolare compila l'apposito modulo, fornito su richiesta dal Gestore utilizzando i canali definiti nel paragrafo C.2.2.4, indicando i seguenti dati:
    - dati anagrafici del Titolare;
    - periodo temporale del quale si richiedono i log;

- ulteriori dettagli quali Message-ID, oggetto del messaggio, tipo di messaggio;
- motivazione della richiesta;
- autorizzazione relativa alla normativa sulla privacy;
- modalità di invio dei dati di log (raccomandata postale ovvero Posta Elettronica Certificata);
- recapito del Titolare da utilizzare nell'invio;

2. il modulo compilato deve essere inviato al Gestore in una delle seguenti modalità:
   - tramite posta elettronica all'indirizzo ***uff_pec@intesa.it***;
   - tramite raccomandata postale;
3. il personale del Gestore, dopo aver verificato la correttezza della richiesta, recupera le informazioni dal registro mediante l'accesso ai server o agli archivi presso i quali si reperiscono i file di log;
4. il personale del Gestore invia i dati al Titolare entro 3 giorni lavorativi dalla ricezione della richiesta. I dati sono inviati nella modalità indicata nella richiesta. Il log è prodotto in formato testo, firmato digitalmente (.p7m), con i dati minimi di riferimento previsti dalla normativa. Per l'apertura di tale file, il titolare dovrà utilizzare un'applicazione di verifica di firma qualificata, tra cui EasyVerify, che è disponibile sul sito del Gestore Intesa all'indirizzo: *http://e-trustcom.intesa.it/verify/verifica.htm*.

C.2.2.3. Statistiche

Il sistema di PEC del Gestore permette la rilevazione di dati statistici periodici relativi a:

- Numero di domini definiti nel sistema;
- Numero di utenti definiti per ogni dominio;
- Occupazione delle singole mailbox;
- Numero di messaggi inviati/ricevuti;
- Numero di fallimenti;
- Numero di Virus rilevati in ingresso e uscita.

C.2.2.4. Richieste di supporto

Intesa mette a disposizione dei propri clienti un servizio di help-desk.

Il supporto ai Servizi indicati risponde al numero verde 800-80.50.93.

Per chiamate dall'estero il numero è +39 011.5241.999.

Il servizio di Help Desk presidiato tramite operatore sarà attivo tutti i giorni lavorativi con orario dalle 8.30 alle 19.00 (UTC+1).

All'apertura della chiamata il cliente deve citare come riferimento il tipo di servizio (in questo caso Trusted Mail) in modo da indirizzare la richiesta agli operatori esperti della problematica e di classificare le richieste per tipologia omogenea consentendo così di seguire l'evolversi del problema (vedi Par.C.4 - *Gestione ed erogazione del servizio*).

È altresì sempre disponibile un servizio on-line di apertura chiamate, accessibile all'indirizzo *http://www.hda.intesa.it* mediante il quale è possibile segnalare inconvenienti nell'uso del servizio in oggetto anche al di fuori dell'orario presidiato. Al primo accesso al servizio on-line, verrà richiesto all'utente di registrarsi; tale operazione potrà essere effettuata seguendo le istruzioni riportate direttamente sul sito.

C.3. Piattaforma tecnologica

L'architettura realizzata è stata progettata in modo da riflettere le caratteristiche di alta affidabilità richieste per il servizio di Posta Elettronica Certificata.

I server utilizzati sono configurati in modo tale da fornire continuità di servizio in caso di malfunzionamento di uno dei sistemi. La sicurezza del servizio è garantita dalla presenza di firewall ridondati per il controllo degli accessi e da software antivirus e antispam che garantiscono la protezione di tutto il sistema nel caso di attacchi informatici.

Nel contesto dell'infrastruttura sono utilizzati dispositivi di tipo Hardware Security Module (HSM) per lo storage delle chiavi private di firma conformi alle normative di sicurezza indicate da AgID per il servizio di PEC.

Intesa fornisce la connettività Internet per l'erogazione del servizio di Posta Elettronica Certificata: l'infrastruttura realizzata in Intesa consente un collegamento permanente alla rete Internet caratterizzato da un livello di affidabilità e performance come descritto dalle caratteristiche riportate nella sezione C.3.5 dedicata alla connettività.

La piattaforma utilizzata per il servizio é installata nella Server Farm Intesa ospitata nel comprensorio IBM di Via del Carroccio n. 6 a Pero (MI).

C.3.1. Standard tecnologici adottati

Il Gestore Intesa ha basato i propri sforzi progettuali e realizzativi nel rispetto degli standard tecnologici elencati nel DM 02/11/05 e su riconosciuti standard tecnologici di livello nazionale e internazionale:

- RFC 1305 - Network Time Protocol (Version 3) Specification, Implementation
- RFC 1847 - Security Multiparts for MIME: Multipart/Signe and Multipart/Encrypted
- RFC 1891 - SMTP Service Extension for Delivery Status Notifications
- RFC 1912 - Common DNS Operational and Configuration Errors

- 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 - RFC 3280 (2002): "Internet X.509 Public Key Infrastructure Certificate and CRL Profile
- RFC 3161 - RFC 3161 (2001): " Internet X.509 Public Key Infrastructure Time Stamp Protocol (TSP)"

L'infrastruttura tecnologica del servizio Trusted Mail è stata quindi progettata e realizzata in base a criteri di:

- *Scalabilità*, per permetterere un'agevole espansione nel tempo nel caso dovessero aumentare/mutare le esigenze del servizio anche in conseguenza di adeguamenti normativi;
- *Alta affidabiltà*, per avere un sistema in grado di funzionare al meglio non solo in condizioni ottimali, ma anche in caso di fault di qualche componente;
- *Facilità di gestione*, per garantire efficienza operativa e sicurezza globale.

Per i sistemi utilizzati per l'erogazione del servizio sono state adottate le seguenti tecnologie:

- i sistemi sono basati su piattaforma VMWARE multiprocessore, con sistemi operativi Red Hat Enterprise Linux Server release 5.11 e 6.7 ;
- la gestione della registrazione degli utenti è gestita dal software di directory X509 della Synchronoss Messaging (ex Critical Path);
- la gestione delle informazioni degli utenti necessarie al sistema di Posta Elettronica Certificata è basata sul protocollo LDAP.

Ovunque si è ritenuto necessario, si è provveduto ad eliminare single point of failure con l'utilizzo di sistemi ridondati, o configurazioni Master/Slave con replica.

C.3.2. Schema generale

La figura seguente illustra l'architettura del sistema PEC realizzata presso la Server Farm di Intesa.

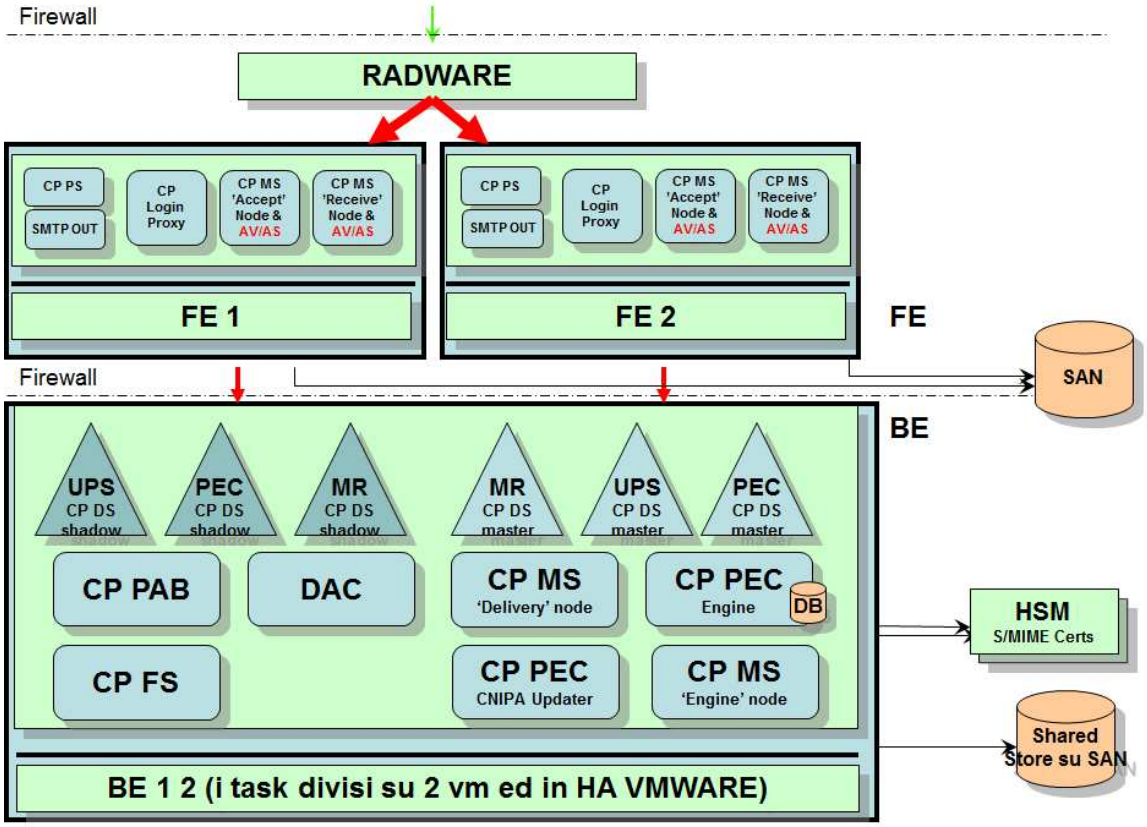

Figura 6: Architettura del sistema PEC

L'infrastruttura del sistema di PEC è sviluppata su quattro server virtuali sui quali sono installate tutte le componenti applicative di *Front End* (FE1 e FE2) e di *Back End* (BE1 e BE2) in comunicazione fra loro.

Le componenti di Front End gestiscono l'interazione con il mondo esterno, da e verso Internet. Le componenti di Back End sovraintendono la gestione dei repository (LDAP) dei dati di configurazione, delle mailbox degli utenti residenti sui dischi condivisi (Share Store) e dell'elaborazione dei messaggi che transitano sul sistema.

Le componenti applicative indicate nella figura sono le seguenti:

- PS - Presentation Server, per la definizione della grafica della Web Mail

- Login Proxy, per l'autenticazione degli utenti
- MS - Messaging Server: è il core del sistema di posta; è suddiviso in quattro componenti applicative:
    - MS *Accept Node*, corrispondente al Punto di accesso
    - MS *Receive Node*, corrispondente al Punto di ricezione
    - MS *SMTP OUT*, corrispondente al punto di spedizione verso l'esterno
    - MS *Delivery Node*, corrispondente al Punto di consegna
- PAB - Personal Address Book: gestisce le rubriche degli utenti
- FS - Fulfillment Server - DAC sono le applicazioni che permettono la definizione di nuovi domini e di nuovi utenti
- PEC Engine – DB – MS Engine: sono le componenti specifiche per le funzionalità di PEC
- PEC CNIPA Updater: è la componente applicativa che si occupa degli aggiornamenti delle informazioni da/verso AgID relative a:
    - dati dell'indice nazionale dei Gestori che devono essere memorizzati localmente
    - dati relativi al Gestore Intesa che devono essere riportati ad AgID

Il sistema di PEC di Intesa utilizza al suo interno un server LDAP come repository delle informazioni relative a:

- Domini locali
- Utenti locali
- Gestori remoti.

I server sono collegati alle seguenti componenti accessorie al servizio di PEC:

- *Tre dispositivi HSM utilizzati per la generazione delle firme elettroniche da parte del Gestore*
- *Due dispositivi Anti-Abuse per la gestione del servizio antivirus.*

C.3.3. Configurazione HW

L'infrastruttura hardware è costituita da 8 host IBM System X3850 sui cui sono definiti i 4 server virtuali che compongono la piattaforma PEC: due di front-end e due di back-end. Le schede di rete installate sono dedicate alla connettività e alle attività di data backup.

I servizi presenti nei server di front end sono bilanciati da un apparato radware. In caso di crash di uno dei due server virtuali o degli host su cui sono attestati o di failure di uno servizi attestati su tali server, il radware smista le richieste verso il server virtuale funzionante.

L’alta affidabilità dei server virtuali di backend è garantita dal sistema VM-WARE **HA** che consente, in seguito al crash dell’host fisico su cui risiedono, il restart immediato dei server virtuali sugli host rimanenti.

La configurazione e il dimensionamento dei dispositivi che compongono l’ambiente attraverso cui viene erogato il servizio sono stati oggetto di studio con il produttore della piattaforma software PEC. Tutte le componenti del servizio sono quindi state selezionate al fine di ottenere una soluzione performante e altamente affidabile.

C.3.4. Modalità per l’apposizione e la definizione del riferimento temporale

Tutte le apparecchiature hardware del sistema di Posta Elettronica Certificata del Gestore sono sincronizzate, per la rilevazione sicura dell’ora, con l’***I.N.RI.M. - Istituto Nazionale di Ricerca Metrologica*** di Torino (già *Istituto Elettrotecnico Nazionale Galileo Ferraris*). Questa funzionalità è realizzata da un software specifico installato su ogni server che, mediante il protocollo NTP (*Network Time Protocol*), si collega al server remoto configurato.

Il Network Time Protocol è uno dei metodi più accurati e flessibili per passare l'informazione di tempo e di data sulla rete Internet. Esso permette di mantenere sincronizzati tra loro computer collegati tramite reti locali, metropolitane o addirittura mondiali (Internet) utilizzando una struttura di tipo gerarchico a piramide.

L'I.N.RI.M fornisce un servizio di sincronizzazione per sistemi informatici collegati alla rete Internet, basato su due server NTP primari installati nel Laboratorio di Tempo e Frequenza Campione. Essi sono sincronizzati, attraverso un generatore di codice di data, dai campioni atomici a fascio di cesio utilizzati per generare la scala di tempo nazionale italiana UTC(IT). Lo scarto di tempo tra i server NTP dell'I.N.RI.M e la scala di tempo nazionale italiana viene tenuto sotto controllo ed è normalmente inferiore ad alcuni millisecondi. La precisione di sincronizzazione ottenibile dipende dalla tipologia della rete e dalla distanza interposta tra il server NTP ed il calcolatore che si vuole sincronizzare; i valori di scarto tipici sono inferiori al millisecondo per sistemi appartenenti alla stessa rete e possono arrivare a qualche centinaio di millisecondi per reti remote.

Il software installato presso il Gestore Intesa si collega al server remoto ad intervalli regolari di tempo e, dopo aver ottenuto l’ora corrente, provvede a correggere il clock della macchina locale mediante sofisticati algoritmi.

I riferimenti temporali apposti dalle applicazioni sono stringhe in formato data (GG/MM/YYYY HH:MM:SS), con la precisione del secondo, che rappresentano l’ora locale, in base alla configurazione della macchina. Tali riferimenti sono conformi al DM 02/11/05 Art.9.2.

C.3.5. Connettività

Il collegamento ad Internet della Posta Certificata può contare su un link primario dedicato in tecnologia SDH (fibra ottica) per l'erogazione di una velocità di banda pari a 100 MBps. Tale link é connesso alla rete internet del provider che eroga la connettività ad Intesa ed è attestato sul backbone del provider sul POP di Milano.

L'infrastruttura del collegamento Internet di Intesa a cui la Posta Certificata è connessa, conta su una coda di accesso in tecnologia SDH(fibra ottica) alla rete Internet del provider, attraverso un link alternativo di accesso con velocità 34 MBps attestato sul POP Internet di Torino del provider, che viene attivato in caso di fault del link o del router primario.

Il collegamento ad Internet è effettuato tramite il doppio link collegato su 2 Router della Cisco Systems connessi tra loro con protocollo HSRP.

L'infrastruttura così realizzata quindi é in grado di garantire l'erogazione del servizio anche in caso di guasto di componenti relative alla connettività e quindi esterne al servizio di PEC vero e proprio.

C.3.6. Gestione delle copie di sicurezza dei dati

I Gestori dei sistemi di PEC eseguono il salvataggio dei dati del sistema di PEC con periodicità fissa prestabilita. Gli archivi informatici che sono oggetto di copie di sicurezza sono i seguenti:

- REPOSITORY LDAP, archivio digitale contenente:
  - le informazioni relative ai domini gestiti dalla PEC;
  - le utenze definite sul servizio;
  - le rubriche dei singoli utenti;
  - le informazioni relative ai sistemi di posta remoti.
- DATA BASE del Mail Server contenente dati relativi a:
  - profili utente;
  - domini.
- INFORMAZIONI OPERATIVE, archivio digitale in cui sono memorizzate tutte le informazioni ricevute dal Titolare al momento della registrazione.
- MAILBOX DEGLI UTENTI, archivio costituito dall'insieme delle caselle di PEC definite sul sistema.

C.3.7. L'interoperabilità del Gestore Intesa con gli altri Gestori di PEC

Per assicurare la trasmissione del messaggio di Posta Elettronica Certificata da e verso altri gestori, il Gestore Intesa assicura l'interoperabilità dei servizi offerti, secondo quanto previsto dalle regole tecniche di cui all'articolo 17.

In particolare, l'interoperabilità é garantita dall'applicazione PEC della Synchronoss Messaging (ex Critical Path Inc.), su cui poggia il servizio Trusted Mail.

In questo ambito il Gestore Intesa si impegna a svolgere le opportune verifiche di interoperabilità con gli altri gestori iscritti nell'elenco di AgID.

C.4. Gestione ed erogazione del servizio

La gestione del servizio Trusted Mail é regolamentata dal Sistema Qualità Intesa che definisce gli standard procedurali validi per tutti i processi aziendali e definisce i controlli periodici cui questi devono essere assoggettati per il mantenimento della Certificazione ISO 9001.

A garanzia del livello di servizio che prevede la disponibilità della piattaforma 24 ore al giorno per 7 giorni alla settimana, in aggiunta alle procedure organizzative, sono predisposti appositi automatismi di monitoraggio e controllo del sistema, che consentono di sfruttare al meglio le caratteristiche di affidabilità e ridondanza della piattaforma.

In linea generale, l'intero ciclo di gestione e erogazione si sviluppa sui seguenti livelli:

1. gestione operativa della piattaforma e presidio sistemistico di 1° livello
2. gestione problemi: supporti specialistici di 2° livello e manutenzione evolutiva
3. monitoraggio del servizio attraverso appositi indicatori che misurano nel tempo le prestazioni a regime.

C.4.1. Gestione operativa e presidio sistemistico

Le attività di gestione operativa e il presidio sistemistico sono affidate al personale che controlla e monitorizza la Server Farm Intesa.

A grandi linee le attività ricorrenti sono:

- Gestione Operativa e monitoring di base finalizzato a verificare lo stato dei server e attivare i processi di problem determination e problem solving di primo livello. Le attività sono supportate da strumenti di gestione e controllo centralizzato che permettono di monitorare in maniera proattiva la disponibilità e continuità del servizio.Le attività a carico della Gestione Operativa prevedono:
    - monitoring dei server (su cui sono installati gli opportuni sw di monitoraggio) in termini di verifica raggiungibilità in tempo reale, controllo singole componenti di sistema (CPU, dischi, memoria, etc.), controllo funzionalità delle applicazioni con appositi tool;
    - notifica degli allarmi causati da anomalie e supporto al problem solving;
    - reboot dei server o restore dei dati quando richiesto.

- Gestione Sistemistica come supporto di 1° livello a fronte di problematiche complesse, cambi di release, installazione patch di aggiornamento e di sicurezza del sistema, gestione e monitoraggio delle prestazioni del DB e conseguente gestione delle risorse fisiche.
- Monitoraggio URL per verificare la disponibilità dei protocolli di servizio (HTTPS, POP3S, IMAPS, LDAP, tcp Port service, ecc.).
- Data Management per backup e restore dei dati in base alle policy dei salvataggi e attraverso una corretta pianificazione e esecuzione di tutte le attività di copia e eventuale ripristino.
- Servizi di rete Internet e LAN interne comprensivi di manutenzione hw e sw dell'infrastruttura firewall, monitoraggio dei servizi, manutenzione delle policy di sicurezza.

Il personale addetto è in grado di effettuare una prima analisi delle segnalazioni di errore e di attivare eventuali contromisure. Esso è pertanto capace d'intervenire rapidamente per avviare le idonee azioni correttive.

Nel caso non sia possibile il ripristino del corretto funzionamento, e quindi si prefiguri un possibile impatto sul servizio all'utenza, gli eventi anomali rilevati vengono segnalati mediante l'apertura di un "ticket" che, in base alla classificazione di criticità, attiva la procedura Gestione Problemi e Assistenza Clienti.

C.4.2. Gestione Problemi

La gestione dei malfunzionamenti può essere attivata dalla Gestione Operativa, come sopra descritto, oppure da un'apertura ticket a fronte di una chiamata pervenuta all'Help Desk (vedi Par. C.2.2.5.*Richieste di Supporto*).

L'iter della gestione é definito da un'apposita procedura del Sistema Qualità Intesa che provvede a:

- Descrivere le modalità con cui vengono segnalati, registrati e risolti i problemi. Viene seguito l'intero ciclo: Segnalazione/Apertura, Problem Determination, Assegnazione ad altro gruppo, Presa in carico, Monitoraggio, Risoluzione, Follow-on, Escalation, Chiusura.
- Assicurare che il processo venga gestito in modo controllato.
- Rendere possibile una risoluzione tempestiva e soddisfacente per il cliente segnalatore.

Le seguenti definizioni sono utilizzate in questa procedura:

- PROBLEMA: un anomalo comportamento o deviazione di un servizio o prodotto Intesa, che influisca negativamente sulla sua utilizzabilità da parte di un Cliente od utilizzatore interno. Ad ogni problema, al momento della sua registrazione, viene assegnato un numero progressivo univoco che ne consente l'identificazione durante tutta la fase della sua Gestione.
- MALFUNZIONAMENTO**:** comportamento non corretto di un servizio/prodotto SW/HW o di un'Applicazione Cliente.
- ANOMALIA**:** comportamento non corretto di un servizio/prodotto SW/HW o di un'Applicazione Cliente. Sinonimo di malfunzionamento.
- ERRORE**:** causa di una anomalia. Richiede un intervento correttivo. Se relativo a Prodotti o Applicazioni SW, la correzione può interessare riguarda uno o più oggetti SW.
- RISOLUZIONE DI UN PROBLEMA: individuazione, implementazione e test della soluzione del problema, che può essere temporanea (bypass) o definitiva.
- CHIUSURA DI UN PROBLEMA**:** verifica della risoluzione, sua applicazione e comunicazione al Cliente che il problema é risolto.
- PROPRIETÀ del PROBLEMA**:** ogni problema viene attribuito, all'atto dell'apertura, automaticamente ad un Proprietario. Esso diviene l'interfaccia ufficiale nei confronti del Cliente per la Gestione dei Problemi sino alla loro chiusura. In casi eccezionali un problema può essere aperto per conto dell'HD da un altro Gruppo che lo assegna loro immediatamente per la soluzione.
- SEVERITY CODE**:** è un codice, attribuito ad ogni problema, che ne indica la gravità e i target di risoluzione secondo 4 livelli (da 1 a 4) di criticità, così come nel seguito descritti.

Ogni problema è registrato all'interno di un'applicazione di Trouble Ticket Management di Intesa (denominata *HDA – HelpDesk Advanced*) che ne traccia l'intero iter fino alla soluzione definitiva tenendo traccia dei singoli casi per alimentare gli Indicatori Aziendali.

Le funzioni coinvolte nella gestione dei problemi sono:

- Call Dispatching: centralino telefonico che risponde alle chiamate al Numero Verde Intesa.
- Help Desk (HD). struttura organizzativa della Direzione Customer Care che:
  - riceve le segnalazioni;
  - fornisce il Primo Livello di Supporto per le problematiche;
  - coinvolge eventualmente i servizi di Supporto di Secondo Livello.
- Gruppi di Supporto di Secondo Livello - Specialisti Intesa che:
  - hanno competenza in specifiche aree Tecnologiche o Applicative;

- possono venire coinvolti dall'HD per la risoluzione di problemi non risolti al Primo livello;
- possono eccezionalmente ricevere direttamente le chiamate da taluni Clienti, individuati dalla Dir. Delivery per la loro criticità, con cui siano in vigore particolari accordi che prevedano figure di Focal Point per gli aspetti tecnici e di assistenza.

Un apposito Gruppo di supporto di Secondo Livello é predisposto per il servizio Trusted Mail, con coordinamento funzionale del Responsabile del Servizio di PEC Trusted Mail.

I criteri di assegnazione della gravità del problema (livelli di severity) sono:

- **SEVERITY 1** - Situazione critica. Il Sistema o l'ambiente sono inutilizzabili. Un prodotto / servizio non é disponibile. L'Utente non può svolgere alcun lavoro produttivo.
- **SEVERITY 2** - L'Utente può collegarsi alla rete, ma alcune funzioni principali di rete o di un prodotto / servizio non sono disponibili. L'Utente può svolgere alcune funzioni, ma la sua produttività é ridotta.
- **SEVERITY 3** - L'Utente ha un problema che non impatta seriamente l'utilizzo della rete o di un prodotto / servizio. Ad esempio: applicazione non utilizzabile, password da riattivare, etc.
- **SEVERITY 4** - L'Utente non ha particolari problemi. Può trattarsi di una domanda di chiarimento o di un suggerimento.

La gravità è rapportata alla criticità che il servizio riveste per il Cliente o la Comunità oppure alla tipologia di malfunzionamento della piattaforma applicativa. Essa é inoltre la base per attivare i diversi livelli di escalation Intesa.

Un problema di Severity 1 comporta la necessità di garantire la presenza continua sia di un responsabile Intesa che del Cliente finché il problema non viene risolto. In assenza di tali condizioni il problema può essere declassato a severity inferiore. La severity può essere modificata nel corso della vita del problema solamente se sono emersi elementi nuovi che ne giustifichino la modifica.

Lo CSIS comunque effettua un tracking (via LOG) delle modifiche di severity, in modo da poterne effettuare un controllo di merito. Lo CSIS permette in ogni momento di conoscere lo stato di un problema, monitorarne l'andamento e i tempi di risoluzione.

Ad ogni livello di severità viene associato un Target di tempo di risoluzione in funzione del livello di servizio dell'applicazione. Il rispetto di tale target viene controllato mensilmente sulla base degli Indicatori Aziendali strutturati per gruppo di servizi.

Il servizio Trusted Mail dispone di uno specifico indicatore a supporto del Responsabile del Servizio di PEC.

C.4.3. Servizi di emergenza

Seppure in presenza di un'architettura HW in alta affidabilità, data la peculiarità dell'applicazione definibile di tipo "Mission Critical", Intesa ha predisposto le procedure necessarie per garantire la riattivazione del servizio anche in situazioni di elevata emergenza.

A questo scopo è previsto un servizio di ripristino dell'intero sistema nel minor tempo possibile. Le peculiarità del servizio sono:

- Utilizzo di un sistema di backup completo dei dati e degli ambienti operativi
- Attuazione del piano di emergenza nel caso in cui si reputi irrecuperabile l'ambiente di produzione.
- Recupero dei dati dai salvataggi ottenuti attraverso le politiche di backup che Intesa ha predisposto. Tali salvataggi, costituiranno la base di partenza per la riattivazione dell'ambiente di produzione.

C.4.4. Monitoraggio del servizio

Il Gestore Intesa garantisce agli utenti del servizio la possibilità di invio di un messaggio di Posta Elettronica Certificata in conformità con quanto previsto dall'Art.12.2 del DM 02/11/05 e successiva modifica proposta nella riunione del GdL di martedì 3 novembre 2015:

- ad un numero di destinatari almeno pari a cinquanta;
- per dimensioni fino a 100 megabytes.

Il servizio è disponibile 7 giorni su 7, dalle ore 0:00 alle ore 24:00.

La disponibilità del servizio di Posta Elettronica Certificata erogato dal Gestore Intesa è maggiore o uguale al 99,8% del periodo temporale di riferimento,così come indicato nel DM 02/11/05.

Il periodo temporale di riferimento per la misurazione della disponibilità del servizio di Posta Elettronica Certificata è il quadrimestre.

La durata massima di ogni singolo evento di non disponibilità del servizio non supera il 50% del totale previsto nel quadrimestre.

Le ricevute previste dal sistema e destinate agli utenti del servizio, durante il periodo di disponibilità del servizio, pervengono al mittente nei tempi previsti dalla normativa vigente.

Gli indicatori utilizzati per la misurazione dei livelli di servizio sono riportati nella seguente tabella.

NOME INDICATORE	***PARAMETRI DI MISURAZIONE***	***VALORI DI SOGLIA***
Disponibilità del servizio	Rapporto tra il tempo di disponibilità e il tempo totale nel periodo di riferimento	7 giorni su 7 24 ore su 24 disponibilità ≥ 99,8%
Invio dati di log	Tempo di invio, a partire dalla richiesta acquisita nel seguente orario: Da lunedì a venerdì Dalle ore 8.30 alle 17.30	3 giorni lavorativi
Livello di Servizio Gestione problemi	Numero e tempi di evasione delle chiamate pervenute all'HD, classificate secondo la loro gravità	Tempi di chiusura chiamata: 98% entro i tempi dichiarati

C.5. Misure di sicurezza e protezione

C.5.1. Le misure di sicurezza adottate nell'erogazione del servizio

Gli *standard di sicurezza* (fisica, logica e organizzativa) in uso presso il Gestore Intesa sono regolamentati da stringenti normative (policy) appositamente predisposte secondo le linee guida ISO 17799. Tali policy sono in vigore presso tutte le società facenti capo al gruppo di appartenenza d'Intesa.

É stato definito quindi uno specifico Piano della Sicurezza predisposto in ottemperanza alle disposizione contenute nelle normative di riferimento e depositato ad AgID nell'ambito della documentazione presentata in sede di istanza di iscrizione all'albo dei Gestori di PEC.

In coerenza con quanto sopra, è in essere un piano di gestione della sicurezza che, sulla base di security policy strategiche, di sistema e specifiche, prevede norme di comportamento in condizioni normali e in occasione di incidenti di sicurezza, anche in caso di emergenza e di disastro, siano essi dovuti a cause umane, tecniche o naturali.

Al personale interno le cui attività riguardano anche il sistema di Posta Elettronica Certificata si applica il programma di sensibilizzazione alla sicurezza, già da tempo operativo, che prevede, oltre ad un addestramento base sulla sicurezza per i nuovi addetti, periodiche sessioni di aggiornamento.

Le problematiche inerenti la sicurezza nell'ambito dell'erogazione del servizio di PEC del Gestore Intesa sono state valutate in funzione delle specifiche peculiarità derivanti dalla natura del servizio.

Conformemente all'ISO 17799 vengono quindi definite una serie di misure non solo tecniche, ma anche di tipo organizzativo e procedurali, al fine di garantire il rispetto dei tre seguenti concetti base:

- Riservatezza: a garanzia che l'informazione sia accessibile solamente alle figure autorizzate.
- Integrità: a garanzia dell'accuratezza e completezza dell'informazione e dei metodi di elaborazione.
- Disponibilità: a garanzia che gli utenti autorizzati possono accedere all'informazione quando vi è necessità.

L'implementazione e il controllo della sicurezza degli asset Intesa e delle procedure e politiche di sicurezza è assegnato a una struttura organizzativa dedicata che provvede in particolare a:

- Identificare e valutare gli asset aziendali.
- Definire le modalità di valutazione del rischio.
- Scegliere le contromisure necessarie.
- Implementare le policy e le procedure di sicurezza.

La verifica dell'aderenza agli standard di queste procedure e il loro rispetto sono garantite da periodici audit della capogruppo IBM. Ogni eventuale eccezione deve essere esplicitamente documentata con una *Risk Acceptance* redatta e approvata secondo una specifica procedura.

C.5.1.1. La Sicurezza a livello fisico e organizzativo

Tali aspetti riguardano in particolare i rischi e le problematiche inerenti il furto o danno alle risorse del sistema informativo, rivelazioni non autorizzate, perdita di informazioni e interruzioni del supporto ai processi aziendali.

Poiché l'accesso fisico alle risorse di gestione delle informazioni espone l'infrastruttura di erogazione del servizio a tutti questi rischi, sono stati istituiti opportuni controlli principalmente per impedire l'accesso alle persone non autorizzate. In tale ambito è quindi regolamentato l'accesso fisico ai locali che ospitano le apparecchiature preposte all'erogazione dei servizi Intesa situate nei locali della Server Farm. In particolare gli accessi al Data Center sono controllati tramite lettore di badge e consentiti solo al personale Intesa esplicitamente autorizzato. I visitatori e quanti non espressamente autorizzati devono essere accompagnati, temporaneamente autorizzati e dotati di badge temporaneo dopo la procedura d'identificazione al fine di superare i controlli.

In sintesi le principali caratteristiche della Server Farm Intesa sono:

- Guardiania 24 ore
- Sistemi anti-intrusione
- Controllo accessi automatizzato
- Sistemi anti-incendio (rilevazione automatica e spegnimento)
- Gruppi di continuità elettrica
- Gruppi elettrogeni
- Impianto di condizionamento autonomo
- Sistema di supervisione e controllo impianti computerizzato.

Il controllo e la gestione di tali sistemi sono affidati ai Responsabili delle Aree ad Accesso Controllato. In presenza di un eventuale anomalia nel sistema di controllo accessi, la verifica all'ingresso potrà essere comunque effettuata grazie alla presenza continuativa del personale di guardiania.

C.5.1.2. La Sicurezza a livello logico

Anche a livello logico l'accesso agli asset informatici è gestito e controllato sulla base di specifiche norme e procedure interne.

In particolare sono definiti e implementati una serie di controlli per gli accessi ai sistemi suddivisi nelle seguenti aree:

- *identificazione e autenticazione degli utenti*: ogni utente è definito secondo uno speciale codice identificativo e un suo profilo. Quando l'utente tenta di accedere al sistema, questo verifica che l'utente sia effettivamente chi dichiara di essere. Tale procedura è supportata da appositi strumenti software e/o hardware;
- *definizione e protezione delle risorse*: le Risorse del Sistema sono chiaramente individuabili e l'accesso ad esse da parte degli utenti é regolato con livelli appropriati di autorizzazione;
- *amministrazione di sistema e di sicurezza*: solo gli utenti autorizzati possono impostare, modificare o disabilitare funzioni riguardanti la gestione della sicurezza;
- *registrazione dei tentativi di accesso*: un sistema di monitoraggio registra ogni tentativo di accesso riuscito o fallito al sistema;
- *report sulle violazioni di accesso*: ogni tentativo di accesso non autorizzato al sistema viene riconosciuto come una violazione e rimandato ad un'analisi successiva per la sua classificazione.

C.5.2. Security Health Checking

É prevista una procedura Security Health Checking, che deve essere eseguita con frequenza semestrale per tutti i servizi esposti in rete come la PEC.

Tale procedura deve verificare in particolare che:

- tutti i parametri obbligatori di configurazione dei sistemi di controllo degli accessi siano impostati in accordo con le best practices relative alla sicurezza;
- solamente gli utenti autorizzati siano dotati delle credenziali di accesso al sistema;
- tutti i controlli sulle risorse di sistema operativo siano impostati coerentemente con le normative interne;
- solamente gli utenti autorizzati siano inclusi nelle liste di accesso delle risorse di sistema operativo;
- i programmi antivirus siano installati e operativi;
- i files di log degli accessi e delle attività devono essere presenti.

Il management Intesa e il Responsabile della Sicurezza devono essere avvisati di ogni deviazione dalla lista sopra indicata.

C.5.3. Security Review

C.5.3.1. Revisioni Tecniche di Sicurezza

I sistemi e i servizi devono essere sottoposti a periodiche Revisioni Tecniche di Sicurezza con l'obiettivo di individuare il maggior numero possibile di punti di debolezza (exposure) e quindi consentire di migliorare il livello di sicurezza.

Il servizio di PEC viene sottoposto ad una procedura di Revisione Tecnica di Sicurezza almeno due volte all'anno.

C.5.3.2. Reporting e Gestione dei punti di debolezza

Il Responsabile del Servizio dovrà, nel caso siano rilevate intrinseche debolezze del sistema, assicurare che siano intraprese le opportune azioni correttive, a fronte delle deviazioni riscontrate, a cui siano stati assegnati gli appropriati livelli di rischio secondo tempi e modalità appropriate e diversificate per il livello di rischio riscontrato.

C.5.3.3. Gestione degli Incidenti di Sicurezza

Pur in presenza delle più stringenti norme, un incidente di sicurezza non può mai essere escluso totalmente. Anche in questi casi, proprio perché più rari, ma di non facile gestione, è importante che la si sia in grado di operare secondo norme e procedure codificate di cui tutto il personale sia conoscenza.

É stata definita una procedura apposita, emanata proprio con l'obiettivo di salvaguardare gli interessi dei Clienti e dell'azienda Intesa, che fa esplicito divieto agli operatori Intesa di:

- procedere ad investigazioni di propria iniziativa, con il rischio di contaminare le prove;
- contattare persone o unità organizzative sospettate di essere la causa dell'incidente senza l'autorizzazione del management;
- provare a penetrare in modo inverso nei sistemi da cui si ritiene sia partito l'attacco, commettendo un'azione illegale;
- fare il *clean up* del sistema senza l'autorizzazione del management, rischiando di cancellare prove fondamentali per le successive indagini.

I risultati delle investigazioni sono comunque strettamente riservati e non devono essere date informazioni ad alcuno all'interno dell'azienda, al di fuori di quanto previsto dalla specifica normativa sugli incidenti di sicurezza.

C.5.4. Modalità di protezione dei dati riservati dei Titolari

Le misure di sicurezza per la protezione dei dati personali sono conformi alle misure minime previste dal D.Lgs. 196/03 - *Codice in materia di protezione dei dati personali*.

In relazione al servizio erogato, il Gestore non tratta dati particolari ovverosia dati sensibili ai sensi dell'Art.4.1.d ovvero giudiziari ai sensi dell'Art.4.1.e del suddetto decreto.

Il D.Lgs. 196/03 prevede la tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali. Secondo quanto previsto dalla normativa, tale trattamento sarà improntato ai principi di correttezza, liceità e trasparenza.

Ai sensi dell'Art.13 del D.Lgs. 196/03, il Richiedente viene previamente informato su quanto espresso nei seguenti punti:

1. i dati forniti dal Titolare verranno trattati per la tenuta dell'elenco dei soggetti assegnatari di casella di Posta Elettronica Certificata rilasciata da Intesa;
2. il trattamento sarà effettuato mediante strumenti idonei a garantire la sicurezza e la riservatezza e attraverso strumenti automatizzati atti ad elaborare, gestire, trasmettere i dati stessi, nonché anche attraverso strumenti cartacei;
3. il conferimento dei dati è obbligatorio e l'eventuale rifiuto di fornire tali dati comporta la non assegnazione della casella di Posta Elettronica Certificata;
4. i dati non saranno oggetto di diffusione.

Il titolare, all'atto della sottoscrizione del contratto, viene invitato a prendere visione dell'*Informativa* relativa al Trattamento dei dati personali e a dare consenso al trattamento per gli scopi indicati.

C.5.5. Standard procedurali

Le procedure operative e di gestione del servizio Trusted Mail seguono i criteri generali definiti dal Sistema Qualità Intesa e riepilogati dal *Manuale della Qualità*. Tale documento costituisce:

- la descrizione del sistema qualità Intesa;
- una base di riferimento per lo svolgimento delle attività nelle varie funzioni;
- uno strumento didattico per l'addestramento del personale;
- la garanzia di coerenza e continuità operative anche a seguito di avvicendamenti di personale;
- il documento di riferimento per verifiche ispettive volte ad assicurare l'adeguatezza e efficacia del sistema qualità e della corretta applicazione delle norme e procedure;
- la dimostrazione verso l'esterno della corrispondenza del sistema qualità al modello di riferimento delle norme UNI EN ISO 9001;
- la dimostrazione della conformità del sistema qualità con gli standard di qualità richiesti da clausole contrattuali.

Il Sistema Qualità Intesa è impostato per Processi e si applica a tutta l'azienda. Per ogni processo è identificato un proprietario, che ha la responsabilità di definirne le finalità, di strutturarne i contenuti e le attività e di approvare le relative Procedure.

C.5.5.1. Misuratori di qualità

Nell'ambito dei processi aziendali, particolare attenzione viene data ai misuratori di qualità, che indicano l'indice quantitativo con cui si misura il raggiungimento (periodico o finale) di un obiettivo di Qualità. Ciascuno di questi misuratori consente di valutare la qualità erogata del servizio in base a specifici obiettivi che il Sistema Qualità Aziendale mira a raggiungere. A tale proposito è stato definito un documento, accessibile a tutto il personale dell'azienda, in cui sono riportati i misuratori periodici dei Progetti di Qualità Aziendale e delle Direzioni Funzionali.

Avendo definito un Piano di Qualità Settoriale per il raggiungimento di precisi obiettivi, con una periodicità stabilita vengono effettuate le seguenti operazioni:

- i misuratori dei Progetti Qualità relativi al periodo in esame vengono raccolti e formalizzati in un apposito documento;
- tali dati sono esaminati e valutati con le modalità previste dal Piano Qualità Settoriale;
- in caso di *Non Conformità*, viene effettuata l'analisi causale, sono identificate le opportune azioni correttive e assegnate la responsabilità;
- vengono individuate le Non Conformità critiche, da portare all'attenzione del Rappresentante della Direzione per la Qualità;

- sono valutate eventuali esposizioni o rischi per il raggiungimento degli obiettivi definiti;
- sono intraprese le necessarie azioni preventive per il contenimento dei rischi.

C.6. L'offerta del Gestore

Intesa, nell'ambito della propria offerta di servizi del brand *e-Trustcom*, propone il servizio Trusted Mail di Posta Elettronica Certificata (PEC) conforme alle normative AgID.

In particolare, Trusted Mail è il naturale completamento dei servizi erogati da Intesa poiché abbina al normale messaggio di posta elettronica le caratteristiche di una comunicazione formale assimilabile alla Raccomandata con Avviso di Ricevimento.

C.6.1. Target di mercato

Trusted Mail interessa potenzialmente tutte le comunicazioni fra gli enti pubblici, le aziende private e i cittadini, che possono così usufruire di un servizio d'invio di documenti informatici in sostituzione dell'attuale servizio di Raccomandata A.R.

Singole Entità interessate:

- Pubblica Amministrazione (Locale e Centrale): in forte legame con l'applicazione di gestione del protocollo informatico e, più in generale, con tutte le applicazioni di dematerializzazione dei documenti cartacei
- Aziende, per l'invio di comunicazioni formali (es. Azienda verso rete Dealers, Assicurazioni verso Agenzie, Aziende/Banche verso Clienti, Aziende verso Agenti, Filiali e rete commerciale, etc.)
- Enti identificati come persona giuridica, che intendono operare in tale veste nello scambio di documenti e informazioni sensibili, anche all'interno di specifici progetti, con altre entità similari o verso la pubblica amministrazione

Aggregatori interessati:

- Ordini professionali (comunicazioni formali)
- Associazioni di categoria
- Banche per Aziende clienti.

La vendita del servizio Trusted Mail può essere indirizzata nell'ambito di soluzioni che siano caratterizzate dall'uso in parallelo di altre componenti di servizio Intesa. In questo caso la PEC è un componente di soluzioni più complesse.

Si segnalano fra i possibili servizi/offerte che possono essere proposti in forma complementare:

- I servizi B2B Trusted Hub/BCHub per l'interconnessione fra la piattaforma Trusted Mail e l'ambiente applicativo e gestionale del cliente, laddove i documenti inviati/ricevuti attraverso il servizio PEC devono essere integrati in forma controllata con le applicazioni e i processi aziendali.
- I servizi Trusted Invoice e Trusted Doc per la gestione elettronica delle fatture e la conservazione a norma dei documenti informatici; il servizio di PEC può essere utilizzato come canale di comunicazione sicuro e "auditabile" per lo scambio dei documenti fra le aziende utenti del servizio.
- La Infrastruttura a chiave pubblica (PKI) di Intesa per il rilascio dei certificati digitali da attribuire ai domini di posta. La firma digitale per garantire l'integrità e la paternità dei documenti spediti (PKI Smart Kit). I servizi di Timestamping della PKI Intesa per un'attribuzione certa degli eventi temporali connessi al servizio.

C.6.2. Componenti dell'offerta

Tenendo quindi conto del target di mercato che Intesa intende approcciare, sono state individuate le componenti ritenute di maggior interesse per una clientela business.

Intesa è in grado di fornire progetti e soluzioni create su misura per la propria clientela all'interno dei quali trovano collocazione i seguenti elementi:

- caselle di Posta Elettronica Certificata;
- dominio condiviso *pec.trustedmail.intesa.it*;
- domini dedicati;
- personalizzazione webmail;
- sviluppo applicazioni.

Ciascuna componente ha caratteristiche peculiari che saranno sinteticamente esposte nel proseguo del documento.

C.6.2.1. Caselle di Posta Elettronica Certificata

Le caselle PEC del servizio Trusted Mail sono proposte con una dimensione iniziale di 50 Megabyte, incrementabile a passi da 50 Megabyte. L'accesso al servizio viene reso disponibile in modalità sicura mediante l'utilizzo di protocolli di tipo IMAP/S POP3/S SMTP/S. L'accesso al servizio è protetto da crittografia SSL per garantire un elevato livello di sicurezza e la relativa riservatezza delle transazioni.

Inoltre, le caselle Trusted Mail sono protette da antivirus e antispam , aggiornati con frequenza oraria, che analizzano il traffico da e verso il sistema di Posta Elettronica Certificata.

Le caselle possono adeguarsi agli standard di denominazione forniti dal cliente allo scopo di renderle omogenee ad altri sistemi di posta elettronica ordinaria già presenti presso il cliente. La password iniziale può essere impostata secondo le richieste del cliente in accordo con le policy proprie del dominio: in ogni caso la lunghezza minima della password non può essere inferiore ad 8 caratteri.

C.6.2.2. Dominio condiviso "pec.trustedmail.intesa.it"

Il dominio *pec.trustedmail.intesa.it* è condiviso tra tutti gli utenti che non intendono personalizzare il dominio di Posta Elettronica Certificata. Si tratta quindi di una modalità semplice e rapida per usufruire del servizio. È particolarmente indicata per piccole organizzazioni o singole entità che non desiderano personalizzare la propria PEC.

Le caselle di posta attivate saranno pertanto del tipo *user@pec.trustedmail.intesa.it*. La creazione, la gestione e la manutenzione sono già incluse nel canone annuale.

Le password delle utenze PEC appartenenti a tale dominio dovranno essere lunghe almeno 8 caratteri, contenere almeno: un carattere maiuscolo, un carattere minuscolo, un numero e un carattere speciale.

C.6.2.3. Domini dedicati

Per tutte le Aziende o Enti che intendono mantenere la visibilità del loro nome e fornire quindi un'immagine di livello, Intesa propone l'attestazione sul proprio servizio PEC di un dominio dedicato.

Il cliente può quindi richiedere ad Intesa la configurazione di un proprio dominio o sottodominio da utilizzarsi all'interno del servizio di Posta Elettronica Certificata Trusted Mail, in conformità con la definizione data nel DPR 11/02/05. Pertanto tutti gli scambi di messaggi effettuati sulle caselle di PEC del cliente configurate all'interno di tale dominio, saranno trattati come messaggi di Posta Elettronica Certificata. Il dominio attestato su Trusted Mail sarà quindi esclusivamente dedicato al servizio PEC.

Il dominio su cui attestare le caselle di Posta Elettronica Certificata, richiesto ad Intesa o fornito direttamente dal cliente, può essere ospitato sul servizio Trusted Mail: tutte le attività di configurazione e set-up saranno quindi trattate come una-tantum alla sottoscrizione del contratto. Intesa offre il servizio di gestione della registrazione del dominio cliente ponendosi come unica interfaccia per quanto concerne la Posta Elettronica Certificata.

Le caselle di posta certificata saranno del tipo *user@dominio_cliente*. Le caselle PEC così create saranno soggette alla tariffazione standard alla stessa stregua delle caselle attestate sul dominio condiviso.

C.6.2.3.1. Gestione delle caselle per domini dedicati

Nell'ottica di offrire un servizio più rispondente alle aspettative di un ente o azienda che intende utilizzare un certo numero di caselle PEC, è possibile richiedere una gestione personalizzata.

Questa tipologia di erogazione del servizio consente di demandare al personale del cliente attività normalmente in carico al personale Intesa addetto alla registrazione degli utenti della Posta Elettronica Certificata.

Ci troviamo pertanto di fronte ad un'emanazione dell'infrastruttura Intesa, demandata ad operare nell'ambito ristretto del proprio dominio di Posta Elettronica Certificata per le operazioni proprie del ciclo di vita del prodotto. A puro titolo d'esempio possiamo citare:

- Istruzione della pratica di registrazione
- Raccolta dei documenti afferenti la pratica
- Operazioni sul sulle caselle di posta (apertura, blocco e revoca)
- Consegna delle credenziali di accesso

La delega ad effettuare attività sul servizio di Posta Elettronica Certificata verrà ratificata da uno specifico contratto di mandato, nel quale verranno esplicitate eventuali limitazioni. Uno degli allegati contrattuali conterrà l'elenco delle persone che il cliente investirà delle responsabilità legate al servizio.

Trattandosi di un servizio sottoposto a normativa in merito, Intesa si farà carico dell'addestramento del personale selezionato, di mantenerlo aggiornato e si occuperà di verificarne periodicamente l'operato.

Intesa verificherà la rispondenza ai requisiti minimi di sicurezza, di riservatezza e tecnici delle apparecchiature e dei locali messi a disposizione. Ovviamente Intesa guiderà il cliente verso la soluzione più appropriata e consona in funzione del livello di delega che verrà ritenuto più opportuno.

Intesa renderà quindi disponibile l'accesso e l'operatività sul servizio di posta elettronica certificata secondo le modalità più opportune e con gli accorgimenti tecnici più indicati.

C.6.2.4. Personalizzazione webmail

Nel caso in cui il cliente richieda la gestione di un dominio dedicato, Intesa offre anche la possibilità di richiedere la personalizzazione della pagina di accesso alla webmail. Quest'attività consente una maggiore enfatizzazione dell'identità dell'azienda cliente al fine di rendere completamente trasparente al fruitore l'ubicazione e la gestione del servizio. Saranno riviste le pagine WEB che l'utente incontra nel corso dell'accesso del servizio con particolare riguardo all'immagine grafica e coerentemente al "look and feel" che il cliente ha scelto per la propria immagine.

Il branding permetterà quindi la fruizione del servizio come se fosse erogato direttamente dall'ICT del cliente, con un ritorno d'immagine paragonabile almeno a quello della posta elettronica ordinaria.

Le attività di sviluppo e personalizzazione sono svolte e verificate da personale Intesa specializzato nell'immagine aziendale ad ulteriore garanzia di qualità e sicurezza.

C.6.2.5. Sviluppo applicazioni

Il servizio Trusted Mail è, come altri servizi Intesa, teso ad andare incontro alle esigenze del cliente durante il processo d'inserimento all'interno del sistema informativo aziendale.

Con quest'intento, Intesa è disponibile a supportare il cliente nell'integrazione del servizio di Posta Elettronica Certificata con il workflow e i sistemi informativi gestiti dal cliente stesso. Il personale e i tecnici sono in grado di supportare il cliente durante tutta l'attività, sviluppando applicazioni e interfacce personalizzate per l'ambiente finale.

Per normalizzare questo tipo d'utilizzo, Intesa può rendere disponibile un'interfaccia standard che permetterà, in maniera molto semplice, di spedire e monitorare mail sul sistema di Posta Elettronica Certificata senza particolari sviluppi specifici. Anche in questo caso i nostri tecnici sono a disposizione per tutta l'attività di consulenza che il cliente riterrà necessaria.

I nostri esperti sono comunque in grado di supportare il cliente anche nella fase di progettazione, in modo da evidenziare e risolvere problematiche sia di natura tecnica che relative agli ambiti di validità del servizio stesso.

C.6.3. Utilizzo del servizio

Trusted Mail è un servizio flessibile che permette la fruizione del servizio sia tramite Webmail che attraverso un client di posta elettronica POP3/SMTP/IMAP in grado di gestire il colloquio criptato SSL.

Come anticipato in precedenza, per poter utilizzare il servizio Trusted Mail, occorre innanzitutto effettuare la Registrazione del Titolare, che permette di riservare una casella di Posta Elettronica Certificata ad una utenza. Per l'espletamento di tale operazione, il Gestore deve disporre dei dati anagrafici del Titolare, corredati di un documento di riconoscimento.

Il Gestore Intesa fornisce :

- L'URL di accesso al servizio Webmail
- L'utenza e la password necessari al logon sia per la modalità Webmail che tramite il client di posta elettronica
- Il supporto e la documentazione necessaria alla configurazione e all'accesso al servizio

Intesa ha posto in essere regole di sicurezza che riguardano l'utenza d'accesso al servizio. Pertanto la password è sottoposta a regole che possono essere concertate con il cliente riguardo la composizione e la durata della password dell'utenza. In ogni caso, anche gli standard eventualmente concordati devono sottostare a requisiti minimi che garantiscano il livello di sicurezza necessario per il servizio.

C.6.3.1. Webmail

La modalità Webmail è quella che permette un più rapido e flessibile utilizzo della Posta Elettronica Certificata.

Collegandosi all'URL di accesso fornito (condiviso o dedicato), l'utente accederà ad un pannello nel quale saranno richieste le sue credenziali.

Completato il processo d'accreditamento, l'utente potrà:

- Verificare la posta in ingresso
- Comporre nuovi messaggi
- Personalizzare l'archiviazione della propria posta
- Ricercare specifici messaggi
- Gestire il proprio profilo utente (es: cambio password)
- Creare e gestire una propria rubrica

C.6.3.2. Client di posta

La documentazione fornita da Intesa contiene tutte le informazioni atte a configurare un client di posta elettronica.

I parametri essenziali da inserire nella configurazione del client sono:

- User e Password
- Indirizzo del server POP3
- Indirizzo del server SMTP
- Indirizzo del server IMAP

Il cliente può in seguito decidere altri parametri che sono diretti alla gestione dei messaggi. Citiamo, a titolo d'esempio, le opzioni relative a:

- archiviazione
- tempi di polling per la verifica di nuovi messaggi e la replica della casella

C.6.4. Le condizioni di fornitura

Nel seguito vengono illustrate le modalità e le condizioni attraverso cui il servizio viene erogato al cliente.

C.6.4.1. Condizioni di fornitura del servizio

Il servizio Trusted Mail prevede diverse modalità di fruizione a seconda della tipologia di utenza.

Caselle per persone fisiche singole: in questo caso il Cliente sottoscrive il contratto di servizio con Intesa e comunica i dati necessari per la registrazione del/i Titolare/i. Tali caselle vengono normalmente attivate sul dominio standard condiviso *pec.trustedmail.intesa.it.*

In particolare il Titolare deve sottoscrivere i seguenti documenti:

- Il contratto di servizio, in duplice copia, in cui sono riportati gli obblighi di ambo le parti.
- Il documento *Modulo Richiesta Casella di Posta Elettronica Certificata*, in duplice copia, in cui riporta i propri dati, sotto indicati:
    - Eventuale Azienda/Ente richiedente
    - Cognome e Nome.
    - Data e luogo di nascita.
    - Codice fiscale (o analogo nel caso di cittadini stranieri non in possesso di codice fiscale italiano).
    - Residenza.
    - Numero di telefono (fisso o cellulare).
    - Numero di Fax.
    - Tipo, numero, Ente di rilascio e data di scadenza del documento di identità esibito.
    - Numero di caselle richieste
    - Utenza e dominio delle caselle richieste
- Il documento *Presa visione del Manuale Operativo del servizio di Posta Elettronica Certificata*, in duplice copia, in cui dichiara di aver preso visione del Manuale Operativo del Gestore Intesa.
- Il documento *Dichiarazione di autorizzazione al trattamento dei dati personali*, in cui dichiara di acconsentire all'utilizzo dei propri dati personali ai sensi del D.Lgs.196/03 e successive modifiche.

Caselle appartenenti ad una Organizzazione: l'Organizzazione (Azienda o Ente) sottoscrive il contratto di servizio con Intesa, nel quale sono regolamentate le clausole contrattuali per le caselle richieste. In tale contratto viene individuata la persona del Cliente che sarà il referente verso il Gestore e che, eventualmente, dovrà fornire i dati dei Titolari delle caselle di Posta Elettronica Certificata.

L'Organizzazione può richiedere l'attivazione delle caselle secondo le seguenti modalità:

1. dominio standard pec.trustedmail.intesa.it
2. dominio dedicato - è possibile distinguere ulteriormente i seguenti due casi:
    - il dominio del Cliente è già definito:occorre attestare il dominio sui sistemi PEC del Gestore Intesa;
    - il Cliente richiede al Gestore la completa definizione del dominio.

Le condizioni di fornitura che regoleranno l'erogazione del servizio di PEC, per quanto non espressamente indicato nel presente Manuale Operativo, saranno quelle contenute nei singoli ordini di servizi.

Il servizio standard prevede l'erogazione del servizio a fronte di un canone annuo anticipato per ciascuna casella acquistata.

C.6.4.1.1. Raccolta della documentazione

Per l'erogazione del servizio di Posta Elettronica Certificata nell'interno di progetti specifici, Intesa potrà avvalersi di un *delegato* appartenente alla struttura organizzativa del Cliente che agirà come interfaccia verso Intesa. In particolare, questo *focal point* opererà con deleghe specifiche che Intesa gli accorderà nell'ambito di un contratto specifico di mandato.

Intesa potrà quindi delegare a questa persona una serie di attività quali:

- inoltro della documentazione di registrazione da e verso i titolari;
- richieste di apertura caselle di posta ;
- distribuzione delle credenziali di accesso ai titolari.

Intesa si farà quindi carico di addestrare il personale selezionato per questo tipo d'incarico sulle procedure, sugli obblighi e sulle responsabilità connesse. Questa figura sarà assimilata alle figure del Gestore abilitate ad operare all'interno del servizio di PEC e quindi soggetta, da parte di Intesa, a verifiche similari a quelle eseguite sul proprio personale.

C.6.4.2. Obblighi e responsabilità

C.6.4.2.1. Obblighi del Gestore

Nello svolgimento della sua attività il Gestore Intesa di Posta Elettronica Certificata opera in conformità con quanto disposto da:

- DPR 68/05;
- DM 02/11/05.

In particolare si attiene ai seguenti obblighi:

- fornisce al mittente di ogni messaggio inviato la ricevuta di accettazione nella quale sono contenuti i dati di certificazione che costituiscono prova dell'avvenuta spedizione di un messaggio di Posta Elettronica Certificata (Art.6.1 DPR 11/02/05);
- per ogni messaggio consegnato ad un titolare, fornisce, all'indirizzo di posta elettronica del mittente, la ricevuta di avvenuta consegna (Art.6.2 DPR 11/02/05);
- rilascia la ricevuta di avvenuta consegna contestualmente alla consegna del messaggio di Posta Elettronica Certificata nella casella di posta elettronica messa a disposizione del destinatario dal Gestore, indipendentemente dall'avvenuta lettura da parte del soggetto destinatario (Art.6.5 DPR 11/02/05);
- emette la ricevuta di avvenuta consegna esclusivamente a fronte della ricezione di una busta di trasporto valida, secondo le modalità previste dal DM 02/11/05 (Art.6.6 DPR 11/02/05);
- quando il messaggio di Posta Elettronica Certificata non risulta consegnabile, comunica al mittente, entro le ventiquattro ore successive all'invio, la mancata consegna mediante l'invio di un avviso di mancata consegna (Art.8.1 DPR 11/02/05);
- sottoscrive le ricevute rilasciate mediante una firma elettronica avanzata, ai sensi dell'articolo 1, comma 1, lettera dd), del TU (Art.9.1 DPR 11/02/05);
- appone un riferimento temporale su ogni messaggio generato e, quotidianamente, una marca temporale sui log dei messaggi (Art.10.2 DPR 11/02/05);
- trasmette il messaggio di Posta Elettronica Certificata dal mittente al destinatario integro in tutte le sue parti, includendolo nella busta di trasporto (Art.11.1 DPR 11/02/05);
- mantiene traccia delle operazioni svolte durante le fasi di trasmissione del messaggio di Posta Elettronica Certificata su un apposito log dei messaggi. (Art.11.2 DPR 11/02/05);
- per la tenuta del registro adotta le opportune soluzioni tecniche e organizzative che garantiscano la riservatezza, la sicurezza, l'integrità e l'inalterabilità nel tempo delle informazioni in esso contenute (Art.11.3 DPR 11/02/05);

- non accetta messaggi con virus informatici e, in caso di loro eventuale ricezione, informa tempestivamente il mittente dell'impossibilità di dar corso alla trasmissione; tali messaggi sono conservati per trenta mesi secondo le modalità definite dal DM 02/11/05 (Artt 12.1 e 12.2 DPR 11/02/05);
- assicura i livelli minimi di servizio previsti dalla normativa vigente (Art.12 DPR 11/02/05) precisati nell'apposito paragrafo C.2.18.
- comunica ad AgID ogni variazione organizzativa o tecnica concernente il servizio di Posta Elettronica Certificata entro il quindicesimo giorno (Art.14.11 DPR 11/02/05);
- assicura l'interoperabilità con gli altri operatori iscritti nell'elenco pubblico dei Gestori di Posta Elettronica Certificata (Art.5.2 DPR 11/02/05). A tale proposito il Gestore si impegna ad effettuare le verifiche sufficienti e necessarie a garantire gli aspetti di correttezza formale necessari per l'interoperabilità.

C.6.4.2.2. Obblighi del Mittente e del Destinatario

Il mittente o il destinatario che intendono fruire del servizio di Posta Elettronica Certificata devono attenersi ai seguenti obblighi:

- avvalersi di uno dei gestori inclusi nell'apposito elenco pubblico (Art.14.1 DPR 11/02/05);
- conservare le ricevute fornite dal Gestore;
- prendere visione del Manuale Operativo e attenersi alle procedure ivi definite.

C.6.4.2.3. Obblighi del Titolare

Gli obblighi a cui deve attenersi ogni Titolare sono i seguenti:

- prendere visione del Manuale Operativo;
- fornire tutte le informazioni richieste dal Gestore per l'identificazione personale;
- conservare con la massima riservatezza i codici di accesso al servizio;
- attenersi alle modalità di utilizzo del servizio indicate dal Gestore;
- comunicare tempestivamente ogni variazione dei propri dati di registrazione.

C.6.4.2.4. Responsabilità del Gestore

Intesa è responsabile, verso i Titolari, per l'adempimento di tutti gli obblighi discendenti dall'espletamento delle attività previste dal TU, dal DPCM 13/01/04, dalla D.Lgs. 196/03 e successive modificazioni e integrazioni, dal DM 02/11/05, dal DPR 11/02/05 (vedi Par. C.6.4.2.1 - *Obblighi del Gestore* e presente paragrafo).

Intesa non assume responsabilità per le conseguenze derivanti da un uso del servizio di Posta Elettronica Certificata diverso da quanto stabilito dalle normative vigenti e dalla violazione agli obblighi indicati alla Sezione III, Parr. C.6.4.2.2 - *Obblighi del Mittente e del Destinatario*, C.6.4.2.3 - *Obblighi del Titolare* e di quanti altri obblighi posti dalla legge a carico di tali soggetti.

Intesa non assume responsabilità, per danni di natura diretta od indiretta, e fatto salvo i casi di dolo e colpa grave, per le conseguenze derivanti da quanto segue:

- mancato rispetto di modalità operative e di procedure e regole specificate in questo Manuale Operativo da parte dell'Utente, dell'Utilizzatore del servizio di PEC, del Terzo Interessato;
- cause ad essa non imputabili, quali, a solo titolo di esempio: calamità naturali, disfunzioni tecniche e logistiche al di fuori del suo controllo, interventi dell'autorità, rivolte o atti di guerra che colpiscano anche o solo i soggetti delle cui attività Intesa si avvale per la prestazione del proprio servizio di PEC;
- erroneo utilizzo di codici identificativi da parte dell'Utente;
- mancato invio o mancata consegna dei messaggi al di fuori dei livelli minimi di servizio previsti dalla normativa vigente (Art.12 del DPCM del 02.11.05), causati da anomalie segnalate al mittente o al destinatario, i quali non abbiano provveduto a riscontrare la comunicazione di anomalia inviata da Intesa;
- uso improprio del servizio di PEC da parte di applicazioni di terze parti;
- impiego del servizio al di fuori delle normative vigenti o dall'utilizzo di servizi di posta elettronica forniti da gestori non inclusi nell'elenco pubblico tenuto da AgID.

Si evidenzia inoltre che Intesa non assume alcuna responsabilità, salvo eventuale dolo o colpa grave, dei ritardi che i messaggi di posta elettronica possono subire nella loro trasmissione via Internet; Intesa è esonerata da ogni potere di controllo, di mediazione o di vigilanza sul contenuto dei messaggi inviati dagli Utenti e non assume nessuna responsabilità riguardo al loro contenuto illecito o contrario alla morale o all'ordine pubblico, non sussistendo alcun obbligo di vigilanza o di cancellazione in capo ad Intesa in riferimento al contenuto dei messaggi e non assume nessun obbligo, garanzia o responsabilità ulteriori rispetto a quelle scaturenti dal contratto di fornitura del servizio per il tramite di Intesa e dalla normativa vigente.

C.6.4.2.5. Assicurazione

Intesa ha stipulato, con decorrenza dalle ore 24 del 03.05.2006, un contratto assicurativo di Responsabilità Civile per la copertura dei rischi derivanti dall'attività di Gestore di PEC e dei danni causati a terzi (DPR 68/05 e DM 02/11/05), il cui contenuto è in linea con quanto necessario per svolgere l'attività professionale di cui trattasi.

Di tale contratto è stato inviata ad AgID apposita dichiarazione di stipula.

L'assicurazione vale per la responsabilità civile che possa derivare ad Intesa per:

a) Perdite patrimoniali derivanti dall'attività di Gestore di Posta Elettronica Certificata ai sensi del DPR 68/05 e successive modificazioni intervenute sino alla stipula della polizza:
   - massimale previsto fino a € 500.000,00 per sinistro;
   - massimale previsto fino a € 2.000.000,00 per anno.

b) Perdite patrimoniali, derivanti dalla diffusione involontaria o per infedeltà dei dipendenti, di dati personali:
   - massimale previsto fino a € 500.000,00 per sinistro;
   - massimale previsto fino a € 500.000,00 per anno (sottolimite al massimale annuo del precedente punto a.).

IN.TE.S.A. S.p.A.