FASTWEB S.p.A.

Manuale Operativo per il Servizio di Posta Elettronica Certificata

Codice FWPEC011

Fasi del Documento	Nominativo	Ruolo	Data	Release
Elaborazione	Ernesto Bellisari Fabrizio Sechi	Responsabile Piattaforme VAS Business Security & Planning Manager	15-6-2007	1.0
Verifica	Guido Roda	Responsabile ICT Services	15-6-2007	1.0
Approvazione	Luca Rizzo	Direttore Sicurezza	18-06-2007	1.0
Elaborazione	Ernesto Bellisari Fabrizio Sechi	Responsabile Piattaforme VAS Business Security & Planning Manager	15-02-2010	1.2
Verifica	Guido Roda	Responsabile ICT Services	20-02-2010	1.2
Approvazione	Luca Rizzo	Direttore Sicurezza	01-03-2010	1.2
Elaborazione	Ernesto Bellisari Fabrizio Sechi	Responsabile Piattaforme VAS Business Security &	04-05-2010	1.3

		Planning Manager		
Verifica	Guido Roda	Responsabile ICT Services	07-05-2010	1.3
Approvazione	Luca Rizzo	Direttore Sicurezza	10-05-2010	1.3
Elaborazione	Ernesto Bellisari	Responsabile Piattaforme VAS	21-01-2013	1.4
Verifica	Andrea Lasagna	Responsabile Network Engineering	24-01-2013	1.4
Approvazione	Luca Rizzo	Direttore Security&Safety	30-01-2013	1.4

Gennaio 2013
Versione 1.4

Sommario

Indice delle Figure

Indice delle Tabelle

1. Introduzione

Scopo del presente documento è illustrare processi, sistemi e modalità operative adottate da FASTWEB S.p.A. (da qui in poi "FASTWEB") nell'erogazione del Servizio di Posta Elettronica Certificata (di seguito "PEC").
La versione in formato elettronico di tale documento ("Codice FWPEC011 - Servizio PEC Manuale Operativo PEC.pdf)" è conservata presso la sede principale di FASTWEB, depositata presso il Centro Nazionale per l'Informatica nella Pubblica Amministrazione, e disponibile liberamente all'indirizzo Internet http://www.fastweb.it/downloads/PDF/PEC/Manuale-Operativo.pdf.

1.1 Assunzioni

Il presente documento viene rivisto ogni qualvolta questo progetto sia coinvolto in significative variazioni della propria organizzazione.

1.2 Riferimenti

Rif. Identificativo	Titolo/Descrizione

1.3 Storia del Documento

Versione	Resp. della Variazione	Data	Descrizione della modifica
1.1	Luca Rizzo	27-08-2007	Certificazioni – Riferimenti Normativi – Variazioni Procedurali
1.2	Luca Rizzo	01-03-2010	Riferimenti Normativi – Variazioni Tecniche
1.3	Luca Rizzo	10-05-2010	Variazioni Organizzative
1.4	Luca Rizzo	30-01-2013	Variazioni Organizzative – Riferimenti Sito WEB

1.4 Copyright

1.5 Tabella di corrispondenza norme - argomenti

Ai fini di una più agevole consultazione del presente manuale e reperimento delle sezioni dello stesso nelle quali sono contenuti i recepimenti dei requisiti normativi, è stata inserita la seguente tabella di corrispondenza.

Tabella di corrispondenza/check list	
Contenuto in relazione alla circolare CNIPA/CR/56	**Manuale Operativo**
Dati identificativi del gestore	§ 1.3
Responsabile del Manuale Operativo	§ 1.3
Riferimenti normativi per la verifica dei contenuti	§ 2.2
Procedure e standard tecnologici e della sicurezza	§ 2.2
Definizioni, abbreviazioni e termini tecnici	§ 2.2
Descrizione sintetica del servizio offerto	§ 3
Contenuto e modalità di offerta	§ 4
Modalità di accesso al servizio	§ 4
Indicazione dei livelli di servizio	§ 2.1
Indicazione delle condizioni di fornitura	§ 7
Indicazione delle modalità di protezione dei dati dei titolari	§ 5, § 6
Obblighi, responsabilità e limitazioni in sede di indennizzo	§ 8

Tabella 1 – Tabella di corrispondenza/checklist.

1.6 Responsabilità documento

Di seguito sono indicati i dati completi dell'organizzazione che svolge la funzione di Gestore del Servizio di Posta Elettronica Certificata:

Denominazione e Ragione sociale	**FASTWEB S.p.A.**
N° Partita IVA	12878470157
N° Iscrizione Registri Imprese	12878470157
Rappresentante legale	Alberto Calcagno
Sede legale	Milano, Via Caracciolo 51
Telefono	02/4545.1

Sede operativa	Milano, Via Caracciolo, 51

Tabella 2 – Dati del Gestore.

Eventuali domande, osservazioni e richieste di chiarimenti relative al presente Manuale Operativo potranno essere rivolte alla persona di seguito indicata:

Dati	
Nome	Ernesto
Cognome	Bellisari
Telefono	02.4545.1
Fax	024545.4411
Indirizzo	Milano Via Caracciolo, 51
Mail	ernesto.bellisari@fastweb.it

Tabella 3 – Responsabile Manuale.

1.7 Validità

Fatto salvo qualunque aggiornamento derivante da requisiti normativi e/o significative evoluzioni del sistema, la conformità dei contenuti del presente Manuale Operativo al servizio di Posta Elettronica Certificata offerto da FASTWEB, sarà verificata con frequenza semestrale.

2. Indicazioni Generali

Il documento ha lo scopo di descrivere le regole e le procedure operative adottate da FASTWEB nella conduzione del servizio di Posta Elettronica Certificata.
Il contenuto si basa sulle regole tecniche allegate al Decreto Ministeriale del 2 novembre 2005 recante "*Regole tecniche per la formazione, la trasmissione, la validazione, anche temporale, della posta elettronica certificata*" e della Circolare CNIPA n. 56 del 21 maggio 2009; sulle modalità per la presentazione delle domande d'iscrizione nell'elenco pubblico dei gestori di Posta Elettronica Certificata.

2.1 Informazioni Generali

2.1.1 Riferimenti Normativi e Tecnici

Riferimento	Documento di Riferimento
1	Decreto del Presidente della Repubblica 7 Aprile 2003, n.137 (G.U. n.138 del 17 Giugno 2003)
2	Decreto legislativo 7 marzo 2005, n. 82 (in G.U. n. 112 del 16 maggio 2005 - S.O. n. 93) - Codice dell'amministrazione digitale (nel seguito referenziato come CAD)
3	Decreto del Presidente della Repubblica 28 Dicembre 2000, n. 445 (G.U. n. 42 del 20/2/2001) e sue modifiche secondo DPR 137/2003 (nel seguito referenziato come TU)
4	Decreto del Presidente del Consiglio dei Ministri 13 gennaio 2004 (G. U. n. 98 del 27/04/2004)
5	Decreto Ministeriale del 2 novembre 2005 recante "Regole tecniche per la formazione, la trasmissione, la validazione, anche temporale, della posta elettronica certificata" (GU n.266 del 15/11/2005)
6	Decreto Legislativo 30 giugno 2003, n. 196 (G.U. n. 174 del 29 luglio 2003) recante "Codice in materia di protezione dei dati personali"
7	CIRCOLARE n. 56 del 21 maggio 2009. Modalità per la presentazione della domanda di iscrizione nell'elenco pubblico dei gestori di posta elettronica certificata (PEC) di cui all'articolo 14 del decreto del Presidente della Repubblica 11 febbraio 2005, n. 68.
8	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.
9	RFC 1847 (Security Multiparts for MIME: Multipart/Signed and Multipart/Encrypted)

10	RFC 1891 (SMTP Service Extension for Delivery Status Notifications)
11	RFC 1912 (Common DNS Operational and Configuration Errors)
12	RFC 2252 (Lightweight Directory Access Protocol (v3): Attribute Syntax Definitions)
13	RFC 2315 (PKCS #7: Cryptographic Message Syntax Version 1.5)
14	RFC 2633 (S/MIME Version 3 Message Specification)
15	RFC 2660 (The Secure HyperText Transfer Protocol)
16	RFC 2821 (Simple Mail Transfer Protocol)
17	RFC 2822 (Internet Message Format)
18	RFC 2849 (The LDAP Data Interchange Format (LDIF) – Technical Specification)
29	RFC 3174 (US Secure Hash Algorithm 1 – SHA1)
20	RFC 3207 (SMTP Service Extension for Secure SMTP over Transport Layer Security)
21	RFC 3280 (Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List - CRL Profile)
22	Information Technology – Open Systems Interconnection – The Directory: Authentication Framework; ITU-T Recommendation X.509 (1997) | ISO/IEC 9594-8
23	ETSI SR 002 176 - Electronic Signatures and Infrastructures (ESI) - Algorithms and Parameters for Secure Electronic Signatures
24	ISO/IEC 9594-8 – INTERNATIONAL STANDARD ISO/IEC 9594-8:2001 – Information technology – Open Systems Interconnection – The Directory: Public key and attribute certificate frameworks
25	RFC 1777 – Lightweight Directory Access Protocol – W. Yeong, T. Howes, S. Kille
26	RFC 2251 – Lightweight Directory Access Protocol (v3) – M. Wahl, T. Howes, S. Kille
27	RFC 2459 - Internet X.509 Public Key Infrastructure Certificate and CRL Profile.- R. Housley, W. Ford, W. Polk, D. Solo
28	RFC 2527 - Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework
29	RFC 2828 – Internet Security Glossary
30	RFC 3161 - Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP). C. Adams, P. Cain, D. Pinkas, R. Zuccherato
31	Roadmap – IETF Secretariat – Internet X.509 Public Key Infrastructure: Roadmap – Sean Turner, Alfred Arsenault

Tabella 4 – Riferimenti Normativi

2.1.2 Definizioni

Vengono di seguito elencate le definizioni utilizzate nella stesura del presente documento.
Non sono stati riportati i significati di termini specifici ritenuti di uso comune.

Termine	Significato
Avviso di mancata consegna	Avviso emesso dal sistema per comunicare al mittente l'impossibilità, da parte del gestore di posta elettronica, di consegnare il messaggio nella casella di posta elettronica certificata del destinatario.
Avviso di non accettazione	Avviso emesso nel caso in cui il gestore del mittente è impossibilitato ad accettare il messaggio in ingresso; tale avviso identifica le motivazioni alla base della non accettazione e viene autenticato con la firma del gestore di posta elettronica certificata del mittente.
Busta di anomalia	Busta utilizzata nel caso in cui un messaggio contenga errori: il messaggio viene inserito in tale busta, che è sottoscritta con la firma del Gestore del destinatario, e comunque al destinatario viene notificata l'anomalia.
Busta di trasporto	Busta utilizzata per tutti i messaggi di posta elettronica certificata, contenente il messaggio originale e i dati di certificazione; la busta è sottoscritta con la firma del Gestore del mittente
Casella di posta elettronica certificata	Casella di posta elettronica inserita all'interno di un dominio di posta elettronica certificata. I messaggi ricevuti tramite tale casella rilasciano delle ricevute di avvenuta consegna al ricevimento di messaggi di posta elettronica certificata.
Dati di certificazione	Insieme di informazioni associato all'invio del messaggio originale e certificato dal Gestore del mittente; i dati di certificazione vengono inseriti nelle ricevute e consegnati al destinatario insieme al messaggio originale, per mezzo di una busta di trasporto.
Destinatario	Utente che utilizza il servizio di Posta Elettronica Certificata per la ricezione di messaggi.
Dominio di posta elettronica certificata	Dominio di posta elettronica certificata contenente esclusivamente caselle di posta elettronica certificata.
Firma del Gestore di Posta Elettronica Certificata	Firma elettronica basata su un sistema di chiavi asimmetriche, che garantisce la provenienza, l'integrità e l'autenticità dei messaggi del sistema di posta elettronica certificata; la firma viene generata tramite una connessione sicura, univocamente attribuibile al Gestore, e questi controlla l'intera procedura
Firma elettronica	Autenticazione informatica basata su un insieme di dati in grado di

Termine	Significato
	identificare un utente del servizio.
Firma elettronica avanzata	Firma elettronica ottenuta attraverso una connessione univocamente attribuibile ad un soggetto firmatario, che mantiene il controllo esclusivo della procedura; la firma permette di rilevare eventuali modifiche successive dei dati ai quali è associata.
Gestore di posta Elettronica certificata	Soggetto che gestisce uno o più domini di posta elettronica certificata, e quindi i punti di accesso, ricezione e consegna dei messaggi; il Gestore, secondo la normativa vigente, è titolare della chiave usata per la firma delle ricevute e delle buste.
Indice dei gestori di Posta elettronica certificata	Sistema, gestito da DigitPA, che contiene l'elenco dei domini e dei gestori di posta elettronica certificata.
Log dei messaggi	Registro contenente tutte le informazioni utili a ricostruire la trasmissione di un messaggio.
Marca Temporale	Evidenza informatica che attribuisce un riferimento temporale ai messaggi inviati e ricevuti tramite posta elettronica certificata; il riferimento è opponibile ai terzi, secondo quanto previsto dal DPR 28 dicembre 200 n. 445 e dal decreto del Presidente del Consiglio dei Ministri 13 gennaio 2004 pubblicato nella Gazzetta Ufficiale n. 98 del 27 aprile 2004.
Messaggio di posta elettronica certificata	Documento informatico che viene trasmesso da un mittente a un destinatario, composto dal testo del messaggio, dai documenti informatici allegati e dai dati di certificazione.
Messaggio Originale	Messaggio inviato dall'utente di posta elettronica certificata, prima della consegna al punto di accesso. Tale messaggio viene consegnato al destinatario utilizzando una busta di trasporto.
Mittente	Utente che si avvale del servizio di Posta Elettronica Certificata per l'invio di messaggi verso dei destinatari.
PEC	Posta Elettronica Certificata
Posta elettronica certificata	Indice di posta elettronica in gradi di fornire agli utenti la documentazione elettronica attestante l'invio e la consegna dei messaggi.
Punto di accesso	Sistema che fornisce i servizi di accesso al servizio di posta elettronica certificata, per l'identificazione degli utenti, per l'invio e la ricezione di messaggi di posta elettronica certificata; il sistema è in grado anche di verificare la presenza di virus informatici all'interno dei messaggi trasmessi ed emette le ricevute di accettazione ed imbustamento.
Punto di consegna	Sistema che verifica la provenienza e la correttezza del messaggio trasmesso e lo consegna nella casella del destinatario; a seconda dell'esito dei controlli, il sistema emette la ricevuta di avvenuta

Termine	Significato
	consegna o l'avviso di mancata consegna.
Punto di ricezione	Sistema che effettua controlli sulla provenienza e sulla correttezza del messaggio da trasmettere, emette la ricevuta di presa in carico, verifica la presenza di virus informatici, imbusta gli eventuali messaggi errati in una busta di anomalia e quindi riceve il messaggio all'interno di un dominio di posta elettronica certificata.
Ricevuta breve di avvenuta consegna	Ricevuta contenente i dati di certificazione ed un estratto del messaggio originale.
Ricevuta completa di Avvenuta consegna	Ricevuta contenente i dati di certificazione ed il messaggio originale in forma completa.
Ricevuta di accettazione	Ricevuta contenente i dati di certificazione rilasciata dal punto di accesso al mittente in seguito all'invio di un messaggio di posta elettronica certificata; la ricevuta viene firmata da Gestore del mittente.
Ricevuta di avvenuta consegna	Ricevuta emessa dal punto di consegna al mittente nel momento in cui il messaggio viene consegnato nella casella destinatario; la ricevuta viene firmata con la firma del gestore di posta elettronica certificata del destinatario.
Ricevuta di presa in carico	Ricevuta emessa dal punto di ricezione, che attesta l'avvenuta presa in carico del messaggio nei confronti del Gestore del mittente; tale ricevuta contiene i dati di certificazione e viene sottoscritta con la firma del Gestore del destinatario.
Ricevuta sintetica di avvenuta consegna	Ricevuta contenente i dati di certificazione relativi al messaggio trasmesso.
Titolare	Soggetto assegnatario di almeno una casella di posta elettronica certificata. Per semplicità, all'interno del presente manuale si identifica come titolare anche il soggetto firmatario del contratto di fornitura.
Titolare del trattamento dei dati	Soggetto che definisce finalità e modalità del trattamento dei dati, secondo quanto definito nel Decreto 196 del 2003.
Utente di posta elettronica certificata	Persona fisica, giuridica, amministrazione pubblica, ente, associazione o organismo, (ivi comprese eventuali unità organizzative interne) che sia mittente o destinatario di un messaggio di Posta Elettronica Certificata.
Virus Informatico	Programma informatico implementato in modo che l' esecuzione determini il danneggiamento di un sistema informatico, con alterazione dei dati e dei programmi in esso contenuti o ad esso pertinenti.

Tabella 5 – Definizioni

2.1.3 Acronimi

Di seguito sono riportate le abbreviazioni e gli acronimi utilizzati.

Acronimo	Significato
CAD	Codice dell'Amministrazione digitale (Decreto Legislativo 7 Marzo 2005 n.82)
CMS	Cryptographic Message Syntax
DigitPA	Centro Nazionale per l'Informatica nella Pubblica Amministrazione
CRL	Certificate Revocation List
CRL DP	Certificate Revocation List Distribution Point
DNS	Domain Name Service
DPR	Decreto del Presidente della Repubblica
FQDN	Fully Qualified Domain Name
LDAP	Lightweight Directory Access Protocol
LDIF	LDAP Data Interchange Format
MIME	Multipurpose Internet Mail Extensions
PEC	Posta Elettronica Certificata
S/MIME	Secure/MIME
SMTP	Simple Mail Transfer Protocol
TLS	Transport Layer Security
XML	eXtensible Markup Language

Tabella 6 – Acronimi

2.1.4 Certificazioni di Qualità e Sicurezza

FASTWEB garantisce l'adeguatezza dei propri principali processi operativi in conformità alla norma UNI EN ISO ISO 9001:2000, per la quale ha ottenuto la certificazione di qualità dal BVQI, un ente di certificazione accreditato dal Sincert.

Il 26 maggio 2006 FASTWEB ha ottenuto il rinnovo della certificazione, per i settori di attività EA 33, 31.b e 28, relativamente a:

- Progettazione di reti di telecomunicazione, implementazione ed esercizio di reti a banda larga.
- Progettazione, erogazione e gestione di prodotti e servizi informatici integrati destinati a clienti aziende.
- Progettazione, installazione ed esercizio di impianti di telecomunicazione e trasmissione dati.

Per la gestione della sicurezza del sistema informativo aziendale il riferimento è negli standard "ISO/IEC 27001:2005 – Information security management systems - Requirements" e "ISO/IEC 17799:2005 – Code of practice for information security management", derivati dallo standard inglese BS 7799.

Il 13 luglio 2007 FASTWEB ha superato con esito positivo la verifica ispettiva per la certificazione ISO 27001, condotta dal Bureau Veritas, ed è in attesa di ricevere il Certificato di Conformità relativo al seguente scopo:

"Progettazione, sviluppo, fornitura, esercizio e manutenzione di prodotti e servizi integrati di telecomunicazione e informatica (ICT) destinati ai clienti Large Account e dei servizi e sistemi gestionali a supporto"

2.2 SLA e Disponibilità del servizio

Num. max. destinatari di ciascun invio	Valore
Numero massimo di destinatari per messaggi originati da caselle di PEC	50
Dimensione dei messaggi	**Valore**
Dimensione massima per il singolo messaggio accettabile da caselle di PEC	30MB
Disponibilità	**Valore**
Disponibilità del servizio nel periodo di riferimento (*)	99,8%

Durata massima di indisponibilità del servizio nel periodo (*)	345,6 minuti
Durata massima per singola indisponibilità del servizio (*)	172,8 minuti

Tabella 7 – SLA del servizio

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

3. Caratteristiche del Servizio

3.1 Introduzione al servizio di posta elettronica certificata

In Figura 1 viene descritto il modello di funzionamento del servizio PEC proposto da FASTWEB. Analizzando lo schema, è possibile individuare le principali caratteristiche del servizio di posta elettronica certificata, la figura è da considerarsi un modello semplificato, non una dettagliata descrizione delle specifiche tecniche del servizio. Secondo quanto richiesto dalla norma del DM [5], in questo documento vengono discussi tutti i punti del servizio erogato.

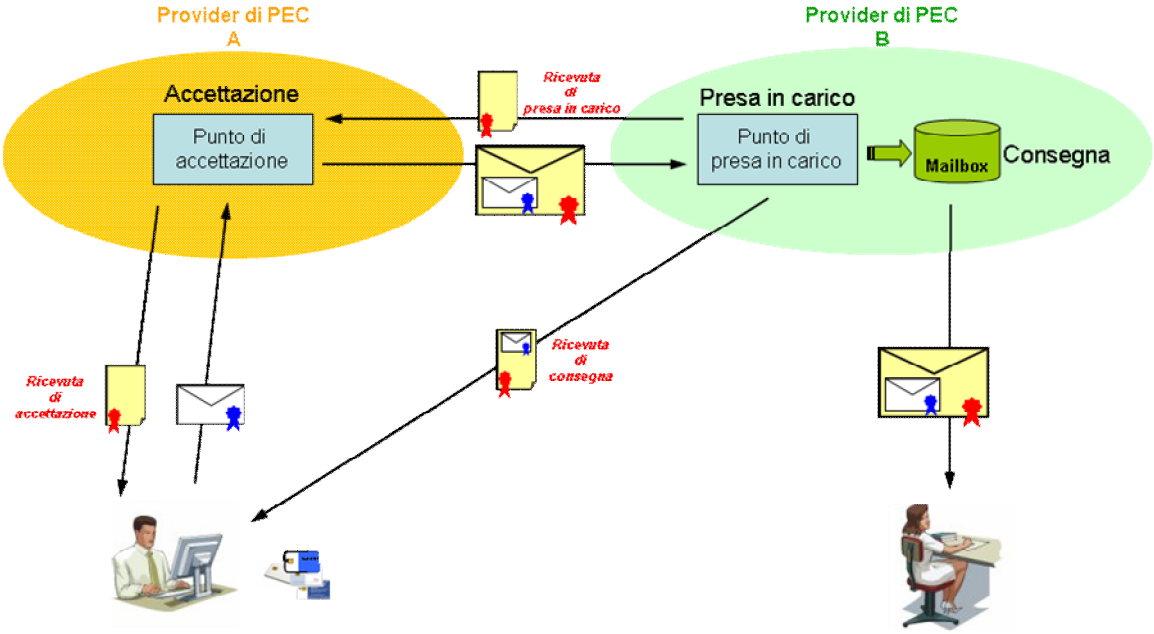

Figura 1 – Schema PEC

Per poter accedere al servizio PEC, l'utente deve procedere alla propria identificazione: tramite apposite procedure di autenticazione, il sistema controlla e convalida le credenziali di accesso, permettendo all'utente di accedere alla propria casella di posta elettronica sulla quale è autorizzato ad operare.

Il sistema PEC accetta la ricezione di messaggi di posta e/o allegati sia firmati, sia privi di firma, ed eventualmente secretati con tecnologie di crittografia. Per inserire la firma sui messaggi, l'utente ha la possibilità di utilizzare una chiave privata, memorizzata sul proprio dispositivo di firma.
Secondo quanto descritto dalla figura, per i messaggi in uscita, il sistema:

- verifica la conformità del messaggio alle regole di posta elettronica certificata;

- se il messaggio è conforme, lo valida ed invia all'utente la "ricevuta di accettazione" firmata dal Gestore, come prova della corretta acquisizione del messaggio;
- se il messaggio non è conforme, il messaggio non viene validato e il mittente riceve un "avviso di non accettazione", recante la motivazione della mancata accettazione;
- imbusta il messaggio originale in un altro messaggio, che viene firmato dal Gestore di posta;
- inoltra il messaggio alla destinazione desiderata.

La figura descrive il caso generale, in cui mittente e destinatario del messaggio appartengano a domini gestiti da provider diversi: in tale situazione, il messaggio inviato tramite PEC deve transitare dal dominio A al dominio B:

- Il provider del destinatario (dominio B) notifica, tramite la "ricevuta di presa in carico", al gestore del mittente (dominio A), di aver preso in carico il messaggio. Il meccanismo di notifica permette di tracciare le tappe di transito del messaggio, permettendo di dare precise informazioni sul *tracking* del messaggio al mittente.
- Il provider del dominio B deposita il messaggio nella casella di posta del destinatario
- Ad operazione avvenuta con successo, il provider B notifica al mittente l'avvenuta consegna del messaggio, inviando la "ricevuta di consegna", contenente in allegato il messaggio originale.

Qualora il mittente intenda inviare il messaggio a più destinatari contestualmente, riceverà un'unica ricevuta di accettazione e una ricevuta di consegna per ciascun destinatario di PEC.

3.2 Servizio PEC di FASTWEB

Il Servizio PEC erogato da FASTWEB utilizza l'infrastruttura di Critical Path "Posta Certificata", che permette al Gestore di mettere a disposizione degli utenti una casella di posta elettronica certificata, in grado di comunicare con tutte le altre caselle di stessa tipologia, indipendentemente dal Gestore prescelto.
L'accesso sicuro alla casella di posta elettronica certificata è ottenibile attraverso due modalità:

- Attraverso un client di posta (es. Outlook Express),
- Utilizzando il servizio Webmail, ossia accedendo direttamente da Internet tramite browser (es. Internet Explorer).

Secondo il Decreto legislativo 7 marzo 2005, n. 82 pubblicato in G.U. del 16 maggio 2005, n. 112 - S.O. n. 93 "Codice dell'amministrazione digitale" aggiornato dal D.Lgs. n. 159 del 4 aprile 2006 pubblicato in G.U. del 29 aprile 2006, n. 99 – S.O. n. 105 "Disposizioni integrative e correttive al decreto legislativo 7 marzo 2005, n. 82 recante codice dell'amministrazione digitale", le caselle di PEC, a differenza delle normali caselle di posta elettronica, consentono l'invio di messaggi di posta elettronica che hanno valore legale. Infatti, dopo aver dichiarato la disponibilità all'utilizzo della posta elettronica certificata, in caso di comunicazioni legali la posta certificata può essere utilizzata in sostituzione della posta cartacea e, grazie al sistema di ricevute descritto nel paragrafo precedente, i messaggi ricevuti nella casella di posta certificata si intendono pervenuti al titolare della casella.

Il servizio di posta elettronica certificata FASTWEB è conforme alle regole tecniche e organizzative indicate dalla normativa in riferimento, ed esattamente:

- DPR 11 febbraio 2005, n. 68, "Regolamento recante disposizioni per l'utilizzo della posta elettronica certificata";
- DM 2/11/2005 recante "Regole tecniche per la formazione, la trasmissione e la validazione, anche temporale, della posta elettronica certificata";
- Allegato tecnico al DM indicato al punto precedente "Regole tecniche del servizio di trasmissione di documenti informatici mediante posta elettronica certificata".

FASTWEB si impegna inoltre ad adeguare tempestivamente il servizio alle eventuali variazioni normative.

L'infrastruttura tecnologica utilizzata per erogare il Servizio PEC di FASTWEB risulta essere pienamente conforme alle regole tecniche richiamate dal DM [5] e pubblicate da DigitPA sul sito (www.cnipa.gov.it); le caratteristiche di queste

caselle sono pertanto tali da permettere l'interoperabilità con le caselle di posta elettronica certificata distribuite da altri gestori di PEC accreditati da DigitPA.

3.3 Funzionalità standard

Il servizio PEC erogato da FASTWEB è dotato non solo delle funzionalità minime richieste dalla normativa ufficiale, ma anche di ulteriori funzionalità che ne aumentano la facilità d'uso e la sicurezza.
Le funzionalità principali del servizio PEC, in conformità alla normativa ufficiale sono:

Ambito	Funzionalità
Sistema di ricevute	Ricevuta di accettazione al mittente per ogni messaggio in uscita che sia conforme ai requisiti normativi.
	Ricevuta di consegna per ogni destinatario a cui risulta consegnato un messaggio inviato ad una casella PEC
	Invio, in allegato alla ricevuta di consegna al mittente, del messaggio originario per ogni destinatario in "To (A)" (a meno di richiesta diversa da parte del mittente)
	Ricevuta di presa in carico tra diversi provider di posta del circuito (necessario per il tracking, ma comunque non visibile agli utenti)
Sicurezza del canale	Utilizzo di una "busta di trasporto" contenente i messaggi in uscita dalla casella del mittente, che viene consegnata, senza alcuna modifica, nella casella di posta di destinazione.
	Inserimento dei messaggi in ingresso, non provenienti da caselle di posta elettronica certificata, in una "busta di anomalia", che viene notificata al destinatario con un messaggio di anomalia di trasporto firmato con la chiave del relativo Gestore
	Firma elettronica del Gestore sulle ricevute e sulla busta di trasporto, contenenti informazioni relative al messaggio quali Time (Ora), From (Da), To (A), sia in formato testo leggibile sia in formato XML
	Conservazione di un log degli eventi principali; con tracciamento delle operazioni svolte. In particolare viene tracciato: • il codice identificativo univoco del messaggio (Message-ID) • la data e l'ora dell'evento • il mittente del messaggio originale • l'oggetto del messaggio In ogni caso, il servizio si limita a memorizzare dati relativi al processo di trasmissione del messaggio, non trattenendo alcuna informazione che permetta di risalire al contenuto del messaggio, a meno di esplicita richiesta da parte del cliente o di eventuali provvedimenti dell'Autorità Giudiziaria (es. intercettazioni richieste sulla base di indagini in corso), richieste con le modalità prescritte dalla normativa in vigore
	Divieto di utilizzo dei destinatari nascosti (BCC o CCN)

	Obbligo di almeno un destinatario in "To (A)".
Livello di servizio	Rispetto del tempo ufficiale coordinato (UTC) dell'ora riportata nelle ricevute e nel messaggio di trasporto, con una tolleranza pari a meno di un secondo.

Le funzionalità descritte in tabella verranno adeguate da FASTWEB in caso di evoluzione della normativa e delle disposizioni da parte di DigitPA.
FASTWEB non assume comunque alcuna responsabilità della corretta gestione dei messaggi da parte degli altri fornitori di posta elettronica.

Ove non espressamente indicato in modo diverso il servizio PEC di FASTWEB garantisce i seguenti limiti:

- la dimensione della casella di posta elettronica certificata è non inferiore a 100 MB;
- la dimensione massima prevista per ogni messaggio è di 30 MB.

Il servizio erogato da FASTWEB permette all'utente di usufruire di una serie di specifiche funzionalità, quali:

- rilascio di una user id specifica per l'accesso alla casella PEC;
- assegnazione di una password per l'accesso in modalità sicura, con eventuale modifica e riassegnazione su richiesta dell'utente;
- accesso alla casella e spedizione dei messaggi tramite client di posta;
- accesso alla casella e spedizione di messaggi tramite Webmail;
- presenza di un Call Center per il supporto informativo;
- presenza di un sistema AntiAbuse sofisticato e costantemente aggiornato, per la verifica della presenza di Virus nei documenti e nei messaggi in transito da e per il sistema (email in ingresso ed in uscita), al fine di procedere al corretto trattamento dei messaggi infetti secondo le regole tecniche previste dalla normativa PEC. La Soluzione adottata, Memova Anti-Abuse di Critical Path (MAA C-2000) utilizza HW Hewlett-Packard (HP) ProLiant DL385 bi-processore AMD Opteron dual core e sistema operativo Linux ed eroga il servizio di Anti-Virus con uno dei migliori prodotti disponibili sul mercato in termini di qualità delle euristiche di rilevamento, di reattività alla scoperta di nuovi vettori virali e frequenza degli aggiornamenti dei pattern virali, attraverso il prodotto Kaspersky AntiVirus.

3.3.1 Elaborazione dei messaggi

Il sistema garantisce il rispetto di tutte le regole previste dalla normativa per la posta elettronica certificata:

- **Ricevuta di accettazione e Busta di trasporto per l'invio:**

Funzionalità che permette al sistema PEC di notificare all'utente proprietario l'avvenuto invio di un messaggio attraverso la ricevuta di accettazione; l'invio della ricevuta di accettazione garantisce che tutti i controlli di conformità del messaggio siano stati superati e sia avvenuto il corretto "imbustamento" del messaggio nella busta di trasporto.

La normativa prevede che il tempo di rilascio della ricevuta di accettazione sia concordato tra Gestore e Titolare; in mancanza di accordo specifico tra Gestore ed utente, la ricevuta di accettazione viene rilascia entro un tempo di 30 minuti nel 99% dei casi (ai fini degli SLA, il dato viene calcolato su base quadrimestrale).

- **Avvisi di non accettazione per eccezioni formali e per virus informatico:**

Funzionalità che permette al sistema PEC di notificare all'utente proprietario la non accettazione del messaggio e la motivazione per cui è stato respinto.

La non accettazione del messaggio scaturisce ogniqualvolta fallisce uno dei controlli di conformità (es. se non si inserisce almeno un destinatario in "To (A)", se si cerca di inserire dei destinatari nascosti, oppure se non vengono rispettate le congruenze attese tra il campo "From (Da)"e la casella utilizzata).

- **Ricevute di preso in carico:**

Funzionalità che garantisce che, in caso di comunicazione tra mittente e destinatario con Gestori differenti, i due sistemi PEC si scambino l'informazione di presa in carico del messaggio, in modo da permettere la tracciabilità del percorso seguito dal messaggio. Questi messaggi non coinvolgono gli utenti, ma sono scambiati e conservati esclusivamente dai gestori del servizio con messaggi di posta in formato RFC 2822. Tali messaggi, sono conservati per almeno 30 mesi e sono consultabili anche attraverso una apposita interfaccia web, nel rispetto della normativa vigente.

- **Ricevuta completa di avvenuta consegna:**

Funzionalità che garantisce che l'utente riceva dal sistema di posta elettronica certificata un messaggio di notifica dell'avvenuto inserimento del messaggio inviato nella casella PEC del destinatario.

A meno di una differente richiesta da parte degli utenti, il sistema invia una ricevuta contenente, in allegato, i dati di certificazione e il messaggio originale per ciascun destinatario in "To (A)".

- **Ricevuta breve di avvenuta consegna:**

Funzionalità che permette all'utente di ricevere, in sostituzione della ricevuta completa, una ricevuta contenente i dati di certificazione e solo un estratto del messaggio originale. L'estratto del messaggio non può essere letto autonomamente, ma deve essere associato al messaggio che lo ha generato tramite opportune tecniche (*hashing*). In questa situazione, qualora il messaggio

originale non sia disponibile o sia stato alterato l'utente non sarà in grado di dimostrare l'avvenuta consegna del messaggio.

- **Ricevuta sintetica di avvenuta consegna:**

Funzionalità che garantisce al mittente l'ottenimento, per destinatari in copia "CC (Carbon Copy o Copia per Conoscenza)", la notifica di consegna tramite una ricevuta completa. La ricevuta sintetica può essere richiesta anche per i destinatari in "TO (A)": in questo caso, tuttavia, non è possibile ottenere la certificazione sul contenuto del messaggio ma esclusivamente sull'intestazione.

- **Busta di anomalia per i messaggi provenienti da caselle di posta non certificata:**

Funzionalità che permette al sistema PEC di identificare i messaggi, non di posta elettronica certificata recapitati ad una casella PEC: in questa situazione il messaggio viene inserito in una "busta di anomalia" per comunicare all'utente quali siano i messaggi ricevuti dotati di certificazione e quali no.

- **Avviso di rilevazione virus informatico:**

Funzionalità che garantisce il mantenimento di un adeguato livello di sicurezza degli utenti dalla ricezione e propagazione di virus informatici: il modulo di accettazione individua i messaggi PEC in uscita affetti da virus, mentre i messaggi in ricezione vengono bloccati, generando un avviso di rilevazione virus che il Gestore del destinatario restituisce al mittente (Il messaggio di notifica virus è comunque archiviato dal gestore destinatario).

- **Avvisi di mancata consegna:**

Funzionalità che si applica nei casi in cui un messaggio spedito da una casella di posta elettronica certificata non possa essere recapitato: in questo caso il mittente riceve un avviso di mancata consegna contenente il motivo per cui il sistema non ha potuto depositare il messaggio nella casella di destinazione, eventualmente fornendo all'utente indicazioni utili sulle azioni da intraprendere per poter inviare correttamente il messaggio.

- **Generazione dei file xml previsti dalla normativa:**

Funzionalità che permette di creare dei file contenenti i dati identificativi del messaggio (data e ora di invio, mittente, destinatario, oggetto, etc…) e utilizzati dai sistemi di posta elettronica certificata per eventuali elaborazioni automatiche.

- **Inserimento del riferimento temporale in tutti i messaggi/log previsti:**

Rispetto al Tempo Universale Coordinato (UTC), il sistema PEC di FASTWEB garantisce un errore inferiore al secondo.

- **Conservazione per 30 mesi dei log con gli eventi principali riguardanti i messaggi in transito:**

Le procedure di logging del sistema PEC di FASTWEB registrano una serie di informazioni relativamente ai messaggi trasmessi:

- codice identificativo univoco assegnato al messaggio originale;
- indirizzo del mittente del messaggio originale;
- indirizzo dei destinatari del messaggio originale;
- oggetto del messaggio originale;
- data e ora dell'evento;
- tipo di evento (accettazione, ricezione, consegna, ricevute, errore, ecc.)
- codice identificativo dei messaggi correlati generati (ricevute, errori, ecc.);
- nome del Gestore del mittente.

Secondo la normativa vigente, tutti i gestori di posta elettronica certificata dovranno conservare i log delle informazioni elencate, in modo che l'utente abbia la garanzia di poter ottenere tutti i dettagli relativi all'invio effettuato, facendone richiesta entro un periodo di 30 mesi dall'invio.

3.3.2 Funzionalità del servizio

Il servizio di PEC di FASTWEB è dotato di funzionalità, implementate con l'obiettivo di migliorare la facilità d'uso dello strumento:

- Per facilitare la comprensione del meccanismo di invio, il sistema inserisce del testo esplicativo (in aggiunta a quanto previsto dalla normativa) in tutte le buste e le ricevute, in modo da guidare l'utente ad un corretto utilizzo del servizio.
- Per permettere una maggior tracciabilità delle informazioni, le ricevute di accettazione contengono il numero identificativo originario del messaggio inviato dal mittente.
- Per garantire l'univocità dell'identificativo dei messaggi accettati, il server di PEC assegna un numero di ID a tutti i messaggi accettati, sovrascrivendo l'identificativo originario.

3.3.3 Gestione domini certificati

Tra le funzionalità offerte dal servizio PEC erogato da FASTWEB, l'utente ha la possibilità di personalizzare le proprie caselle PEC, definendo l'appartenenza ad altri domini o sottodomini, in alternativa a quello fornito di default.
I sottodomini possono essere definiti sia all'interno della disponibilità di FASTWEB sia come personalizzazione di un sottodominio proprio dell'utente. Qualora si voglia definire un sottodominio PEC all'interno di un dominio non PEC esistente, il nuovo sottodominio certificato dovrà essere gestito direttamente dal Gestore.
E' previsto che il sottodominio interno a FASTWEB sia configurato come un dominio di terzo livello del tipo *nomeimpresa*.fastweb-pec.it. Il nome del dominio è quindi proposto dal Cliente a FASTWEB, che si riserva la facoltà di rifiutare le proposte di variazione avanzate dai clienti.

Si fa presente che i domini/sottodomini utilizzati, in base alle regole di posta elettronica certificata, non possono essere utilizzati anche per caselle di posta non certificata.

Per poter attivare un dominio di posta certificata è necessario che FASTWEB sia il gestore del domino del cliente.
Nel caso di tale richiesta, FASTWEB provvede all'inserimento dei domini identificati nell'indice dei gestori di posta elettronica certificata. Questo indice contiene la lista di tutti i domini di posta elettronica certificata gestiti da ciascun operatore. Il servizio PEC FASTWEB prevede alcune ulteriori funzionalità, offerte separatamente, che consentono la personalizzazione delle caselle, dei domini e dell'interfaccia grafica per gli utilizzatori che accedono al servizio PEC attraverso l'interfaccia browser Webmail. In particolare, FASTWEB offre la possibilità di personalizzare i banner presenti sulle pagine e la combinazione di colori dell'interfaccia (tramite elementi forniti dal cliente), mantenendone comunque inalterata la struttura
FASTWEB si riserva la facoltà di non inserire materiali che possano costituite violazioni alla normativa in vigore e/o potenzialmente in grado di disturbare la fruizione del servizio. In ogni caso, FASTWEB non si assume, salvo il caso di dolo o colpa grave, responsabilità in merito al controllo dei materiali forniti dal Cliente.

3.3.4 Autogestione delle caselle

Il servizio PEC di FASTWEB conferisce al cliente la possibilità di autogestire le caselle di cui è proprietario, qualora abbia definito un dominio personalizzato.
Come per gli altri servizi aggiuntivi, FASTWEB si riserva la possibilità di non attivare il servizio nei casi in cui si registri una potenziale violazione della normativa in vigore e/o delle politiche di sicurezza aziendali.

3.4 Funzionalità specifiche

Il presente paragrafo descrive le principali funzionalità che caratterizzano il servizio di Posta Elettronica Certificata di FASTWEB.

3.4.1 Sincronizzazione del tempo

La sincronizzazione del tempo è garantita dall'accesso a diversi riferimenti temporali esterni secondo protocolli standard. Il modulo Critical Path "PEC Engine" (che si occupa di firmare i messaggi e le ricevute prodotti dal sistema) è in grado di utilizzare il tempo macchina la cui precisione è garantita dalla sua sincronizzazione via NTP (Network Time Protocol) con l'IEN (Istituto Elettrotecnico Nazionale) Galileo Ferraris di Torino.

3.4.2 Archiviazione

Il servizio PEC di FASTWEB mette a disposizione un sistema di archiviazione che comprende:

- integrazione con servizi di marca temporale; il servizio effettua quindi la marcatura temporale del documento oggetto di archiviazione (del file giornaliero di registro);
- archiviazione dei registri;
- interfaccia per amministratori di sistema, che permette di ricercare le righe del file di registro, e di visualizzare le ricevute corrispondenti.

4. Modalità di erogazione

La figura sottostante rappresenta uno schema dell'architettura e dei flussi del sistema PEC di FASTWEB.

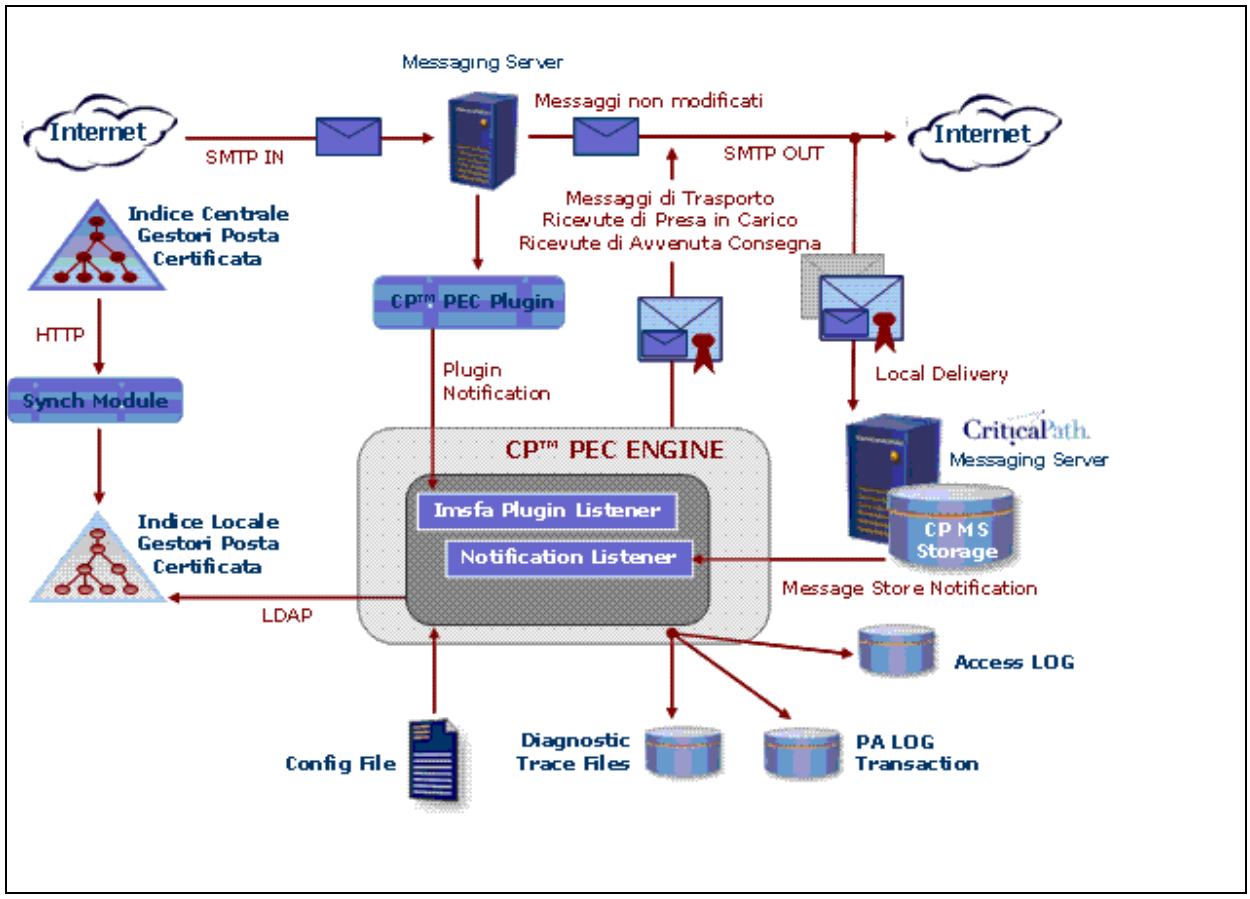

Figura 2 – Schema Architettura PEC

Il servizio PEC di FASTWEB mette a disposizione degli utenti registrati diverse modalità per effettuare le richieste di:

- attivazione nuove caselle
- rinnovo caselle
- attivazione servizi aggiuntivi
- revoca caselle.

Il servizio PEC di FASTWEB è acquistabile sia attraverso il canale di vendita diretto sia tramite il canale di vendita indiretto (dealer); le condizioni di acquisto sono diverse a seconda del numero di caselle richieste e della tipologia del cliente.

4.1 Richiesta attivazione raccolta tramite canale diretto e indiretto

Le risorse commerciali di FASTWEB raccolgono gli ordini relativi alle caselle PEC da attivare; per procedere all'accettazione dell'ordine e alla chiusura del contratto, le procedure di back-end prevedono di:

- identificare univocamente il richiedente;
- negoziare l'accordo;
- firmare il contratto di fornitura del servizio con il titolare, verificandone la correttezza e la completezza;
- attivare caselle e servizi aggiuntivi richiesti, tramite personale tecnico di FASTWEB, o comunque autorizzato dal Gestore.

4.2 Modalità alternative per l'attivazione del servizio

Sulla base delle proprie strategie aziendali, FASTWEB si riserva la possibilità di identificare nuovi canali di commercializzazione del servizio, in sostituzione o in aggiunta a quelli esistenti.
Il processo di raccolta delle richieste e attivazione del servizio sarà implementato nel rispetto dei principi di efficienza aziendale, soddisfazione del cliente e rispetto delle normative vigenti sul trattamento delle informazioni.

4.3 Attivazione del servizio

Una volta sottoscritto il contratto attraverso la rete commerciale di FASTWEB, il servizio PEC è attivato attraverso l'erogazione di una casella di posta. In particolare si sottolinea che:

- la casella di posta avrà dominio certificato del Gestore;
- il nome della casella verrà proposto dal cliente, e FASTWEB si riserva la possibilità di valutarne la fruibilità ed eventualmente richiedere al cliente di modificare la propria proposta;
- una volta siglato il contratto, il cliente avrà a disposizione 15 giorni per effettuare il pagamento;
- dopo aver ricevuto la notifica del pagamento, FASTWEB provvederà all'attivazione della casella;
- l'attivazione della casella verrà comunicata al cliente tramite l'invio di una e-mail all'indirizzo comunicato al momento della richiesta;
- le informazioni comunicate nella conferma di attivazione conterranno i riferimenti per accedere e configurare la casella.

4.4 Accesso al servizio

L'accesso al servizio PEC di FASTWEB può avvenire in 2 modalità:

- accesso tramite Internet via WebMail;

- accesso tramite client di Posta.

Nel primo caso l'utente, attraverso un browser (FASTWEB certifica Internet Explorer 5.5/6.0 e Firefox v. 1.0 o superiore) accede tramite la propria User-ID e Password, al servizio attraverso una URL comunicata da FASTWEB all'atto dell'attivazione. Per l'accesso è necessaria una semplice connessione ad Internet.
L'applicazione WebMail permette di spedire messaggi di posta elettronica e consultare la posta in arrivo. La sessione di lavoro con Webmail ha una durata di tempo limitata, e trascorsi 30 minuti di inattività, l'utente verrà disconnesso automaticamente dalla casella; per riaccedere alla casella, sarà sufficientemente inserire nuovamente User-ID e Password.
Nel secondo caso, l'utente utilizza un client di posta elettronica (FASTWEB certifica Outlook Express 5.5 o superiore) per collegarsi alla casella postale con protocollo di accesso POP3S o IMAPS. Per rispettare le policy di sicurezza di FASTWEB, il server di posta in arrivo deve avere una connessione protetta, ed utilizzare la porta POP3S (in alternativa IMAPS).

L'accesso alla casella di posta certificata, con client o Webmail, e lo scambio di messaggi avviene sempre tramite protocollo sicuro SSL (il livello utilizzato è SSL3). Se l'utente utilizza la posta elettronica certificata via client, deve attivare sul proprio client una connessione protetta SSL per il server di posta in arrivo, mentre se l'utente accede alla posta elettronica certificata via browser (Webmail) non è necessaria alcuna configurazione.

Si ricorda inoltre che la velocità di trasferimento dei dati dalle linee Internet alla propria stazione di lavoro ha un'influenza determinante sulle prestazioni del servizio percepite dall'utente. Pertanto, un collegamento ad elevata velocità assicura un migliore accesso al servizio e FASTWEB non è dotata di strumenti per velocizzare il servizio qualora la lentezza sia legata ad un problema di accesso dalla rete esterna.

4.5 Raccomandazioni generali per l'utenza

Di seguito si riportano una serie di raccomandazioni generali al fine di permettere un corretto utilizzo del Servizio PEC:

- la tipologia di accesso al Servizio PEC (Client o WebMail) determina la modalità di utilizzo del servizio stesso;
- è buona norma verificare sempre l'identità del mittente e dei destinatari dei messaggi ricevuti;
- è buona norma consultare frequentemente la casella, non solo poiché i messaggi PEC ricevuti hanno valore legale (cfr. DPR 68/2005 [8]), ma anche per motivazioni tecniche dovute alla dimensione dello storage della casella (di norma 100 MB complessivi, a meno di accordi specifici tra

Gestore e cliente), eventualmente eliminando dal server di posta i messaggi per evitare che i messaggi successivi vengano rifiutati per mancanza dello spazio necessario al salvataggio;

- per garantire un sufficiente livello di sicurezza, l'utente dovrebbe cambiare la password di accesso assegnata di default, scegliendone una sicura ed in possesso solo degli autorizzati alla gestione della casella;
- tutti i punti di accesso alla casella PEC dovrebbero essere dotati di un sistema antivirus costantemente aggiornato. FASTWEB garantisce un antivirus attivo sul Servizio PEC in grado di proteggere l'utente dai principali pericoli di infezione, ma il sistema non è in grado di controllare automaticamente tutti i contenuti potenzialmente dannosi (es. in caso di messaggi o file crittografati).

4.6 Cessazione del servizio

Qualora FASTWEB dovesse decidere di cessare la fornitura del servizio PEC, comunicherà la propria intenzione con 60 giorni di anticipo a tutti i possessori di caselle PEC gestite e a DigitPA, eventualmente indicando il Gestore individuato come sostitutivo.
In assenza di un gestore sostitutivo, FASTWEB si impegna a segnalare tutte le caselle che non saranno più accessibili dal momento della cessazione dell'attività.
In ogni caso, le caselle PEC oggetto di cessazione resteranno attive in sola lettura per un periodo non inferiore a 30 giorni.

5. Misure di Sicurezza

Al fine di assicurare un livello di sicurezza del servizio PEC adeguato ai massimi standard di servizio, FASTWEB ha avviato, in fase di progettazione e di analisi dei requisiti, un idoneo processo di valutazione dei rischi.
Tale processo, mirante all'identificazione di minacce e vulnerabilità e, quindi, all'identificazione delle adeguate contromisure preventive atte alla minimizzazione del rischio, viene ripetuto a cadenza regolare o nel caso in cui significativi cambiamenti normativi od infrastrutturali lo rendano necessario.

La fase di valutazione del rischio ha posto l'attenzione su tutte e tre le principali dimensioni della sicurezza di un servizio e/o di un dato: *Riservatezza, Integrità, Disponibilità*. I risultati della fase di valutazione del rischio sono stati declinati nelle specifiche di sistema e di processo ed hanno avuto ricadute su tutti gli ambiti principali di sicurezza (fisica, delle infrastrutture, logica, tecnologica).

Il Cliente, nel caso necessiti di ulteriori informazioni o si trovi nella necessità di segnalare potenziali problemi inerenti l'ambito sicurezza, potrà rivolgersi ai normali canali di Customer Care i cui recapiti verranno comunicati durante la fase di acquisizione del servizio oppure scrivere a: **sicurezza-pec@pec.fastweb.it**

Nel prosieguo del presente capitolo sono descritte, sinteticamente per evidenti motivi di sicurezza, le linee guida ed i principali aspetti in chiave di sicurezza della soluzione adottata.

5.1 Standard di Sicurezza

Il 13 luglio 2007 FASTWEB ha superato con esito positivo la verifica ispettiva per la certificazione ISO 27001, condotta dal Bureau Veritas, ed è in attesa di ricevere il Certificato di Conformità relativo al seguente scopo:

"Progettazione, sviluppo, fornitura, esercizio e manutenzione di prodotti e servizi integrati di telecomunicazione e informatica (ICT) destinati ai clienti Large Account e dei servizi e sistemi gestionali a supporto"

FASTWEB si è dunque dotata di un'adeguata struttura organizzativa e procedurale del SGSI conforme alla norma con particolare attenzione ai temi della formazione degli utenti e delle risorse, delle verifiche ispettive e della suddivisione dei ruoli e delle responsabilità.

5.2 Sicurezza sale dati

Tutte le infrastrutture atte ad erogare il servizio PEC sono collocate all'interno delle Server Farm FASTWEB.

Le Server Farm sono state classificate come Aree ad elevato livello di Sicurezza e sono collocate nel cuore delle sedi FASTWEB.

Tali aree sono:

- prive di accessi diretti sulle strade perimetrali;
- dotate di presidio di vigilanza 24h;
- dotate di moderni ed efficaci impianti anti intrusione e di videosorveglianza con registrazione delle immagini;
- dotate di eventuali porzioni in finestrato composte da vetri antisfondamento e protetti da lamiera rinforzata.

A tali aree si accede esclusivamente attraverso un unico ingresso controllato da un sistema di controllo accessi.

5.2.1 Controllo accessi

L'accesso è reso possibile esclusivamente mediante un unico ingresso controllato da un sistema di controllo accessi dotato di lettori automatici di accrediti, che effettua, contestualmente, la registrazione automatica di ogni transito.
Gli accessi sono dotati di bussola a tutta altezza per impedire "l'accodamento" e l'accesso multiplo contemporaneo, il sistema è dotato di anti pass back.
L'accesso ai locali è presidiato da un servizio di vigilanza e controllo attivo H24.

5.2.2 Sistema antincendio

Le aree CED sono dotate di porte, segnaletica e illuminazione d'emergenza conformi alla normativa ed al numero di addetti contemporaneamente presenti nelle aree. Tutti i locali sono dotati di sistema di rilevazione incendi che riporta automaticamente ed istantaneamente ogni allarme al personale di sicurezza presente H24.

5.2.3 Sistema antintrusione

È installato e funzionante un sistema anti-intrusione in grado di rilevare effrazioni e presenze non autorizzate.
Il sistema genera allarmi autoesplicativi che sono raccolti ed inviati istantaneamente alla centrale di controllo e di sicurezza attiva 24 ore al giorno, 7 giorni su 7.

5.2.4 Impianti elettrici

Le apparecchiature presenti nella sala dati sono mantenute sotto continuità elettrica tramite due livelli di alimentazione di emergenza:

- UPS (interruzioni di continuità di breve durata);
- gruppo Elettrogeno (interruzioni prolungate).

Tutti gli impianti elettrici, gli UPS ed il gruppo elettrogeno sono soggetti a verifiche periodiche di funzionamento e collaudo.

5.2.5 Condizionamento e ventilazione

La sala dati che ospita i sistemi della PEC è dotata di un sistema di condizionamento i cui apparati sono collegati in rete tra loro e ridondati per prevenire eventuali malfunzionamenti.

Le anomalie nella temperatura dei locali sono segnalate dal sistema di building automation. In caso di segnalazione per il superamento della soglia di temperatura impostata, un allarme viene notificato al centro di supervisione FASTWEB.
Il sistema di condizionamento è soggetto a verifiche periodiche di funzionamento e collaudo.

5.3 Sicurezza infrastruttura tecnologica PEC

La piattaforma tecnologica utilizzata per il Servizio di Posta Elettronica Certificata si basa su un'architettura completamente ridondata atta a garantire:

- Affidabilità;
- Disponibilità;
- Sicurezza;
- scalabilità.

5.3.1 Architettura

L'architettura della piattaforma di PEC è stata implementata in modo da realizzare una separazione tra i vari strati (layer) di impiego.
Si distinguono 3 layer principali:

- ***Presentation layer***
  In questo strato vengono inserite le componenti applicative che costituiscono il punto di contatto verso i clienti esterni. Tutto ciò che deve essere raggiungibile dall'esterno (Internet) è inserito all'interno di questo strato.
- ***Logic layer***
  All'interno di questo strato vengono inserite le componenti che integrano le logiche applicative e richiedono un dialogo tra le componenti del presentation layer (nei confronti delle quali si comportano da server) e le componenti del data layer (nei confronti delle quali si comportano da client).
- ***Data layer***
  È lo strato che comprende le componenti sulle quali risiedono i dati applicativi, i database e lo storage delle mailbox.

Tale articolazione viene effettuata sia per separare logicamente classi di dati e di informazioni che hanno livelli di criticità e di riservatezza differenti, sia per poter modulare al meglio le differenti soluzioni di sicurezza logica sulla base del tipo di accesso e di dato trattato.

5.3.2 Reti

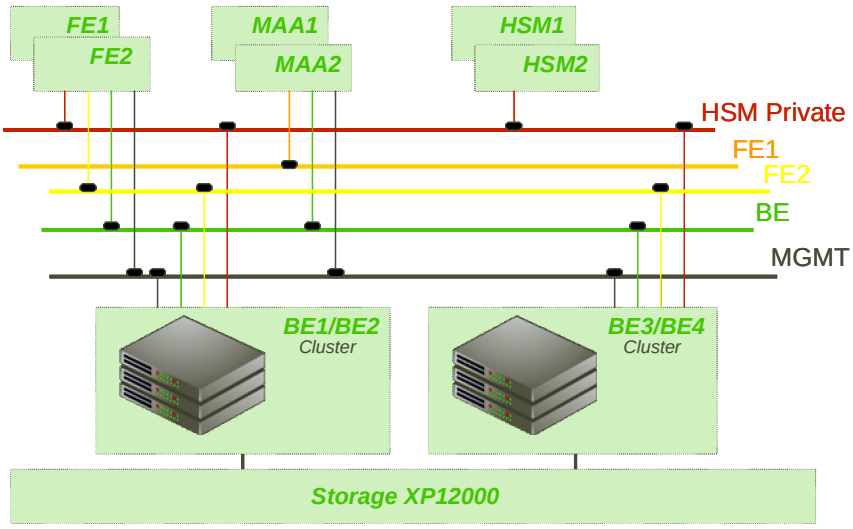

Figura 3 – Dettaglio reti PEC

Nel dettaglio si distinguono 4 differenti reti:

- ***rete pubblica***, per le componenti di front end:
  rete atta all'erogazione del servizio che consente l'accesso agli utenti esterni.
  Per maggiore cautela i server non sono direttamente esposti sulla rete pubblica, bensì vengono protetti attraverso firewall e bilanciatori. Tale accorgimento consente, tra l'altro, il mascheramento dell'IP dei server nei confronti di chi accede dalla rete pubblica;
- ***rete interna*** per le componenti di back end:
  rete impiegata per il dialogo applicativo tra le varie componenti di front end e quelle di back end;
- ***rete privata*** dedicata alle HSM:
  rete separata dalle altre e dedicata al dialogo applicativo tra le varie componenti dell'architettura PEC e i server HSM, impiegati per le operazioni di firma e scambio dei certificati;
- ***rete interna di backup e management***:
  Impiegata per il controllo sistemistico delle varie componenti, il monitoring, l'invio degli allarmi e il backup.

Sulla rete pubblica di front end sono attestati gli apparati di rete in Alta Affidabilità (Cisco Content Switching Module - CSM) che garantiscono un layer di firewalling e di balancing sulle macchine di FE.
Per quanto riguarda il firewalling sono state lasciate aperte esclusivamente le porte strettamente necessarie per erogare il servizio tramite l'impiego dei seguenti protocolli:

- SMTP
- SMTPs
- HTTPs
- IMAP4 su SSL
- POP3 su SSL

5.3.3 Colloquio Sicuro

La sicurezza del colloquio tra mittente e destinatario del servizio PEC viene garantita attraverso l'impiego di canali sicuri per tutte le connessioni previste dall'architettura di Posta Elettronica Certificata (tra Utente e punto di accesso FASTWEB, tra FASTWEB e gli altri gestori, tra punto di consegna Gestore ed Utente). Integrità e riservatezza delle comunicazioni tra FASTWEB e l'Utente sono quindi garantite mediante l'uso di protocolli sicuri (protocollo SMTP su trasporto TLS, come descritto nella RFC 3207).

5.3.4 Backup full (dati, sistema informativo e configurazioni)

Tutti i dati e le configurazioni del sistema PEC (inclusi dettagli su directory server e mail server) sono soggetti a regolare backup su una libreria a nastro posta all'interno della Tape Area Network e utilizzati in modo condiviso dalle diverse piattaforme presenti all'interno della Web Farm.
FASTWEB è dotata delle più moderne infrastrutture per il salvataggio su nastro dei contenuti dei dischi. Il prodotto utilizzato controlla e gestisce l'esecuzione dei salvataggi e la loro archiviazione. Le politiche di backup prevedono:

- un backup incrementale con cadenza giornaliera;
- un backup di tipo Fulled con cadenza settimanale;
- una retention dei salvataggi effettuati pari ad 1 (uno) mese.

La libreria contenente i nastri si trova in un locale separato rispetto ai server sottoposti a backup.
In caso di guasto hardware dei dischi è quindi possibile "ripristinare" il sistema nello stesso stato in cui si trovava nel momento dell'ultimo backup. Le procedure di backup sono organizzate in maniera tale da poter disporre di uno storico e poter così recuperare lo stesso dato in più stadi. I nastri di back up sono riposti all'interno di librerie robotizzate posizionate in locali diversi da quelli che ospitano i sistemi con i dati.
L'accesso fisico e logico alle copie di backup e il recupero dei dati è consentito esclusivamente a personale autorizzato.

5.4 Sicurezza logica

5.4.1 Gestione degli accessi

Ogni accesso alle macchine FASTWEB è controllato mediante idonei processi di profilazione e di controllo degli accessi in conformità alle norme sulla Privacy ed alle politiche e procedure aziendali di sicurezza.
Nel caso di specie l'accesso ai server è consentito solamente al personale accreditato e solamente secondo il proprio profilo di accesso i cui privilegi sono definiti in funzione del tipo di supporto (applicativo, sistemistico, database, infrastrutturale, ecc…).
L'accesso viene reso possibile mediante account personali il cui processo di generazione, gestione e aggiornamento è pienamente rispondente ai requisiti di legge.

5.4.2 Autenticazione al servizio

Il sistema di Posta Elettronica Certificata FASTWEB prevede che tutti gli utenti debbano essere autenticati con username e password personali sia per l'invio di mail che per la ricezione. L'autenticazione permette di garantire che ciascun messaggio possa essere inviato esclusivamente da un utente riconosciuto del servizio di Posta Elettronica Certificata, evitando che sulle caselle operino soggetti non autorizzati.

5.4.3 Inalterabilità del messaggio

Al fine di garantire l'inalterabilità del messaggio originale spedito dal mittente, il servizio PEC prevede l'utilizzo dell'imbustamento e la firma dei messaggi in uscita dal punto di accesso e la successiva verifica in ingresso al punto di ricezione.
Il messaggio originale (completo di header, testo ed eventuali allegati) è quindi inserito come allegato all'interno di una busta di trasporto. La busta di trasporto è firmata dal Gestore mittente, ciò permette di verificare che il messaggio originale non sia stato modificato durante il suo percorso dal dominio mittente al dominio destinatario.

5.4.4 Firma

La disponibilità del servizio di firma a chiave privata dei messaggi PEC è massimizzata mediante l'utilizzo di dispositivi hardware totalmente dedicati al servizio e ridondati.

I dispositivi in questione dialogano con le necessarie componenti dell'architettura PEC tramite un apposita rete interna, al fine di garantire un ulteriore livello di protezione.
I dispositivi HSM che erogano tale servizio sono stati progettati e integrati secondo quanto previsto dalle norme vigenti.

5.4.5 AntiVirus

FASTWEB utilizza un sistema Antivirus, composto da 2 unità per garantire la ridondanza, al fine di ottenere protezione da eventuali infezioni.
Le configurazioni adottate sono tali per cui tutti i messaggi con virus rilevati vengono gestiti per analizzare se sia opportuno consegnare un messaggio di non "accettazione/rilevazione/mancata consegna per virus informatico" o respingere/cancellare il messaggio nel rispetto della normativa vigente.
Il sistema effettua automaticamente controlli per verificare la presenza di aggiornamenti del prodotto di antivirus con cadenza ogni 12 ore e, se disponibili, li rende immediatamente ed automaticamente operativi.
In modo complementare ai sistemi Antivirus, FASTWEB individua una serie di misure di sicurezza:

- politiche di prevenzione per impedire l'introduzione dei virus all'interno dell'azienda;
- politiche per la rilevazione della presenza dei virus all'interno di applicazioni, dati o boot record;
- politiche di rimozione di eventuali virus presenti.

5.5 Monitoraggio

Nella progettazione e realizzazione del Servizio PEC, FASTWEB ha sviluppato una soluzione che garantisce la disponibilità del servizio; per questo motivo sono state attivate sonde e strumenti per il controllo dei singoli elementi costitutivi della piattaforma e vengono svolti test dei vari servizi.

Le sonde/controlli agiscono a livello di singolo sistema/servizio in modo da rilevare malfunzionamenti prima che questi causino un'indisponibilità dell'intero servizio.
Al rilevamento di un malfunzionamento il sistema invia un allarme in tempo reale al personale addetto al monitoraggio e all'assistenza affinché vengano attivate le procedure del caso.

A questo punto, e sulla base dell'allarme rilevato, si attivano le preventivamente predisposte procedure di escalation, ossia una serie di attività da compiersi nel caso in cui le anomalie del sistema rendano necessario il passaggio ad un livello di competenza e/o responsabilità superiore rispetto al personale che riceve la segnalazione.

Il servizio è attivo 24 ore su 24.

Il monitoraggio dei sistemi e delle applicazioni viene eseguito utilizzando il prodotto "*HP OpenView Operations*" e, dove necessario, prodotti sviluppati ad hoc che consentano di mantenere sotto controllo le componenti specifiche della soluzione PEC.

Per garantire la disponibilità del servizio e prevenire possibili malfunzionamenti vengono monitorate le seguenti componenti:

- *Sistema operativo*: raggiungibilità dei server attraverso la rete e verifica dell'esecuzione di specifici processi/applicativi del sistema operativo;
- *File System*: disponibilità e livello di riempimento dei vari file system;
- *Cluster*: verifica del corretto funzionamento del software di clustering e di eventuali operazioni di switch degli applicativi su differenti nodi;
- *Database*: verifica dei processi richiesti dai DB e analisi dei log;
- *Applicativi*: esistenza in vita di processi/servizi necessari per la corretta esecuzione del servizio di PEC, analisi dei log generati dai vari processi per individuare la presenza di errori e verifica di raggiungibilità via rete delle porte corrispondenti ai vari servizi.

5.6 Riferimento temporale

Il sistema PEC di FASTWEB fornisce il riferimento temporale sia delle operazioni effettuate durante l'elaborazione dei messaggi (es. ricevute, log) sia degli eventi che costituiscono la transazione di elaborazione del messaggio (es. generazione di ricevute e di buste di trasporto). Combinando le due informazioni, l'indicazione dell'istante di elaborazione del messaggio risulta univocamente definita all'interno dei log, delle ricevute, delle buste e dei messaggi generati dal server.
Tutte le indicazioni temporali che il sistema fornisce in formato testo intelligibile dall'utente contengono il riferimento all'ora legale vigente al momento indicato per l'operazione.

I formati utilizzati per l'identificazione dei riferimenti sono i seguenti:

- Data: gg/mm/aaaa;
- Ora: hh:mm:ss (hh in formato 0-24);
- Zona: [+|-]hhmm (ossia, differenza tra l'ora legale e UTC);

La fonte utilizzata per registrare il riferimento è l'orologio di sistema, che è sincronizzato via NTP (Network Time Protocol) con l'IEN (Istituto Elettrotecnico Nazionale) Galileo Ferraris.
Lo IEN fornisce un servizio di sincronizzazione tramite la tecnologia Internet, che utilizza due server primari installati nel Laboratorio di Tempo e Frequenza Campione. I server 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(IEN). Lo scarto di tempo tra i server NTP dello IEN 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 Network Time Protocol (NTP) è uno dei metodi più accurati e flessibili per distribuire l'informazione di tempo e di data sulla rete Internet. Il NTP permette di sincronizzare e mantenere sincronizzati tra loro computer collegati tramite reti locali, metropolitane o mondiali (Internet) utilizzando una struttura di tipo gerarchico.

6. Trattamento dei dati personali e dei log

FASTWEB opera conformemente a quanto previsto dalle norme sul trattamento dei dati personali così come stabilito dal decreto Legislativo 196/2003 e dai successivi Provvedimenti emessi dall'Autorità Garante della Privacy.
Pertanto FASTWEB rilascia al Cliente, insieme ai documenti contrattuali, l'informativa sulle finalità e sul trattamento dei dati comunicati, così come stabilito dal decreto Legislativo 196/2003 [2], che dovrà essere sottoscritta per accettazione dall'interessato. FASTWEB provvede inoltre ad implementare idonee policy e procedure di gestione dei dati personali nonché di formazione ed informazione del proprio personale interessato.

Di seguito sono illustrate alcune procedure attivate da FASTWEB in materia, per ogni ulteriore dettaglio si rimanda all'informativa ed al contratto, nonché al sito Internet dell'Autorità Garante della Privacy: www.garanteprivacy.it

Si è sensibilizzato tutto il personale preposto dell'importanza di un utilizzo non improprio dei dati di cui vengono a conoscenza per le loro mansioni lavorative.
Di seguito sono definite alcune procedure attivate da FASTWEB per il trattamento dei dati dell'interessato:

6.1 Principi generali

I principali principi generali che regolano il trattamento dei dati sono i seguenti:

- i dati sono raccolti presso l'interessato mediante compilazione di un apposito modulo che comprende l'informativa e l'esplicita richiesta di consenso al trattamento da parte dello stesso;
- il trattamento si riferisce ai soli dati strettamente trattati per l'erogazione del servizio PEC; per tali dati viene periodicamente verificata la pertinenza. I dati non più pertinenti vengono cancellati;
- le operazioni effettuate sui dati sono solo quelle strettamente necessarie;
- i dati trattati sono accessibili esclusivamente da chi necessiti accedervi;
- ogni operatore che acceda ai dati personali viene formalmente *incaricato del trattamento dei dati* e riceve un'adeguata formazione in materia;
- sono impartite precise istruzioni operative su come debbano essere trattati i dati;

6.2 Finalità del trattamento

I dati personali, direttamente forniti direttamente dall'interessato, saranno trattati da FASTWEB unicamente allo scopo di permettere la gestione e l'erogazione del servizio nei limiti stabiliti dalla legge.
Segnatamente tali dati, necessari all'identificazione univoca del mittente di un messaggio di PEC, potranno essere comunicati a chi, avendone un lecito interesse, richieda un accertamento sulla titolarità della casella di posta elettronica di cui risulta assegnatario un utente del servizio.

Ogni informazione relativa al Titolare del trattamento dei dati, ai responsabili ed alle policy potrà essere reperita sul sito www.fastweb.it nella sezione "Privacy e trasparenza"

6.3 Diritti degli interessati

L'interessato potrà in ogni momento esercitare tutti i diritti previsti all'art. 7 del decreto legislativo 196/2003, di seguito riportato integralmente:

Art. 7. Diritto di accesso ai dati personali ed altri diritti
1. L'interessato ha diritto di ottenere la conferma dell'esistenza o meno di dati personali che lo riguardano, anche se non ancora registrati, e la loro comunicazione in forma intelligibile.

2. L'interessato ha diritto di ottenere l'indicazione:

a) dell'origine dei dati personali;

b) delle finalità e modalità del trattamento;

c) della logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici;

d) degli estremi identificativi del titolare, dei responsabili e del rappresentante designato ai sensi dell'articolo 5, comma 2;

e) dei soggetti o delle categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di rappresentante designato nel territorio dello Stato, di responsabili o incaricati.

3. L'interessato ha diritto di ottenere:

a) l'aggiornamento, la rettificazione ovvero, quando vi ha interesse, l'integrazione dei dati;

b) la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati;

c) l'attestazione che le operazioni di cui alle lettere a) e b) sono state portate a conoscenza, anche per quanto riguarda il loro contenuto, di coloro ai quali i dati sono stati comunicati o diffusi, eccettuato il caso in cui tale adempimento si rivela impossibile o comporta un impiego di mezzi manifestamente sproporzionato rispetto al diritto tutelato.

4. L'interessato ha diritto di opporsi, in tutto o in parte:

a) per motivi legittimi al trattamento dei dati personali che lo riguardano, ancorchè pertinenti allo scopo della raccolta;

b) al trattamento di dati personali che lo riguardano a fini di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale.

L'esercizio dei diritti potrà essere esercitato mediante comunicazione ai recapiti dell'Ufficio Privacy di FASTWEB che possono essere reperiti sul sito www.fastweb.it, nella sezione "Privacy e trasparenza", ove è possibile ANCHE leggere ogni informazione relativa al *Titolare del trattamento* dei dati, ai *Responsabili* ed alle policy FASTWEB in materia.

6.4 Misure di sicurezza per la protezione dei dati personali

Come previsto dalle norme vigenti in materia, FASTWEB, in qualità di Titolare del trattamento, adotta tutte le necessarie misure minime di sicurezza al fine di garantire sempre i seguenti principi relativi ai dati forniti dal Cliente:

- *Disponibilità*: i dati sono sempre fruibili, quando è necessario, e sono ridotti al minimo i rischi di perdita o distruzione, anche accidentale, grazie ad un sistema di backup e di disaster recovery.
- *Integrità*: i dati sono difesi da manomissioni o da modifiche improprie eseguite da soggetti non autorizzati
- *Riservatezza*: i dati sono accessibili solo da persone che abbiano le credenziali per accedervi e mediante idonei sistemi di autenticazione.

A tale fine il servizio PEC FASTWEB dispone di:

- **Antivirus**: sono in uso politiche di prevenzione, rilevazione e rimozione dei virus all'interno di dati, applicazioni e boot record. In particolare, il sistema utilizzato nella piattaforma PEC di FASTWEB, è descritto al paragrafo 5.4.5;
- **Backup dei dati**: sono impiegate procedure di copia periodica dei database e dei log della piattaforma PEC su opportuni dispositivi. Nel caso si verificasse un guasto hardware dei dischi è quindi possibile ripristinare il sistema nel medesimo stato in cui si trovava nel momento in cui è stato effettuato l'ultimo back-up (cfr. paragrafo 5.3.4);
- **Autenticazione al sistema PEC:** Il sistema prevede che tutti gli utenti debbano siano essere autenticati con username e password personali sia per l'invio sia per la ricezione di messaggi di posta elettronica certificata. Le credenziali di accesso sono generate e gestite in conformità con le misure minime di sicurezza previste dal d.lgs 196/03. Tale procedura garantisce che il messaggio sia inviato da un Utente del servizio di Posta Elettronica Certificata i cui dati di identificazione siano congruenti con il mittente specificato al fine di evitare la falsificazione di questo ultimo;
- **Colloquio sicuro**: l'accesso alle caselle di posta elettronica certificata avviene esclusivamente su canale sicuro; il colloquio attraverso l'interfaccia web o il client utilizzato tra l'Utente e il sistema avvengono attraverso protocolli e connessioni sicure (SMTP/S, IMAP/S, POP3/S e HTTPS dettagli presenti nel paragrafo fo **Error! Reference source not found.**).

6.5 Gestione dei Log

Durante le fasi di trattamento del messaggio presso i punti di accesso, ricezione e consegna, il sistema mantiene traccia delle operazioni svolte. Tutte le attività sono memorizzate su un registro riportante i dati significativi dell'operazione:

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

6.5.1 Conservazione

I log generati dai sistemi vengono "ruotati" con cadenza giornaliera generando dei file ai quali, immediatamente dopo la rotazione, viene apposta una marca temporale che ne garantisce l'integrità e l'inalterabilità.
La disponibilità dei log viene garantita mediante i seguenti processi di conservazione:

- registrazione dei log marcati temporalmente su idoneo supporto secondo quanto previsto dalle norme vigenti, con scadenza massima giornaliera;
- invio settimanale di una copia dei log e memorizzazione presso una sede diversa da quella in cui viene erogato il servizio log dei messaggi. Tali file di log sono conservati per 30 mesi a cura di FASTWEB all'interno di una cassaforte ignifuga.

6.5.2 Reperimento e presentazione informazioni presenti nei Log

Le richieste di estrazione di informazioni memorizzate nei log possono essere effettuate, a seconda del tipo della richiesta:

- dal titolare della casella PEC;
- da soggetti autorizzati dalla Legge,;

tramite richiesta scritta all'indirizzo **servizio-pec@pec.fastweb.it**

La richiesta, per essere evadibile, deve contenere alcuni dati identificativi:

- data della trasmissione (invio/ricezione);
- indicazione del mittente (FROM/da) e del destinatario (TO/a);

- codice identificativo della trasmissione (facoltativo);
- parte dell'oggetto (facoltativo).

L'estrazione dei log viene effettuata mediante accesso ai server o agli archivi ottici da parte del personale tecnico autorizzato.
La consegna delle informazioni presenti nei log richieste avviene tramite invio all'indirizzo di Posta Elettronica Certificata del richiedente. Le informazioni rilasciate potranno essere utilizzate per gli usi consentiti dalla legge.

Secondo la normativa vigente (cfr. allegato tecnico al DM 2/11/2005 [5]), le informazioni che FASTWEB renderà disponibili sono:

- il codice identificativo univoco assegnato al messaggio originale;
- la data e l'ora dell'evento;
- il mittente del messaggio originale;
- i destinatari del messaggio originale;
- l'oggetto del messaggio originale;
- il tipo di evento oggetto del log;
- il codice identificativo dei messaggi correlati generati.

Nel caso di indisponibilità o di irraggiungibilità della casella di posta elettronica certificata **servizio-pec@fastweb-pec.it** (anche per malfunzionamento della casella di PEC del titolare/utilizzatore), è possibile indirizzare la presente richiesta anche via fax al numero 02/89699132.

Tale domanda, oltre a tutte le informazioni elencate per il normale invio tramite PEC, dovrà recare in allegato anche copia del documento di identità del titolare/utilizzatore della casella di PEC per la quale si sta trasmettendo la richiesta.

7. Condizioni di Fornitura

7.1 Proposta e documentazione del servizio

Il servizio di Posta Elettronica Certificata è commercializzato da FASTWEB tramite la propria rete commerciale.
Il servizio è disciplinato e fornito in conformità con la normativa vigente e con quanto previsto dalla documentazione, di seguito elencata, che FASTWEB fornirà al Cliente:

- condizioni generali di contratto;
- proposta di contratto contenente gli elementi del servizio, i valori economici e la richiesta di attivazione del servizio;
- informativa sulla privacy.

7.2 Modalità alternative per l'attivazione del servizio

FASTWEB si riserva la facoltà di fornire nuove modalità e flussi per la richiesta di nuove attivazioni (ad esempio introducendo la modalità online via web). Le modalità oggi disponibili e quelle future garantiscono e garantiranno il rispetto delle norme relative alla privacy e alla normativa vigente relativa al servizio di Posta Elettronica Certificata.

7.3 Attivazione del Servizio

Per dettagli sulle modalità di attivazione del servizio si rimanda al capitolo 4.

7.4 Corrispettivo economico

Il corrispettivo economico è legato alle necessità puntuali della richiesta del Cliente.

7.5 Descrizione generale degli elementi del contratto

FASTWEB si riserva la possibilità di sospendere temporaneamente il servizio per procedere alla manutenzione ordinaria e straordinaria dell'infrastruttura necessaria all'erogazione del servizio: tali sospensioni saranno comunicate ai clienti tramite e-mail e con un preavviso minimo di 24 ore.

In caso di guasti alla rete o comunque di modifiche e/o manutenzioni straordinarie non programmabili e tecnicamente indispensabili, FASTWEB potrà sospendere in ogni momento il Servizio, in tutto o in parte, anche senza preavviso. Rientrano in questa tipologia, tra gli altri, gli eventi di forza maggiore e al di fuori del ragionevole controllo di FASTWEB (es. atti dell'Autorità Militare, catastrofi naturali, ecc…).

7.6 Risoluzione del contratto

FASTWEB potrà procedere alla risoluzione del contratto:

- nel caso in cui il servizio venga utilizzato per finalità contrarie a leggi, regolamenti, disposizioni normative;
- in caso di mancato pagamento, secondo quanto indicato nel contratto di fornitura del servizio;
- altre motivazioni, secondo quanto indicato nel contratto di fornitura del servizio.

La comunicazione della risoluzione verrà comunicata al Cliente a mezzo di raccomandata a/r, fermo restando l'obbligo da parte del Cliente al pagamento degli eventuali corrispettivi non pagati.

8. Obblighi e responsabilità di FASTWEB

8.1 Obblighi del gestore – FASTWEB

FASTWEB si impegna a fornire il servizio di Posta elettronica Certificata in ottemperanza alla normativa vigente e nel rispetto di quanto riportato nel presente documento.
FASTWEB si fa inoltre carico di:

- dare disponibilità a fornire, nei casi previsti dalla legge, tutti i log concernenti le trasmissioni tra differenti caselle di posta elettronica certificata;
- fornire all'autorità giudiziaria il dovuto supporto alle attività investigative, secondo quanto previsto dalla normativa vigente.

FASTWEB si impegna ad apportare tutte le modifiche tecniche ritenute necessarie in base all'evoluzione tecnica e normativa.

8.2 Obblighi del Titolare del Servizio PEC

All'atto della sottoscrizione del contratto, il Titolare:

- si impegna a rendere disponibile a FASTWEB la documentazione e tutte le informazioni che il Gestore riterrà necessarie per procedere ad una corretta identificazione del Titolare; questi garantirà, sotto la propria responsabilità, la veridicità della documentazione fornita ai sensi del DPR n. 68/2005 e successive modifiche ed integrazioni;
- fornisce il consenso al trattamento dei propri dati personali ai sensi del D.Lgs. n. 196 del 2003 (di contro, il Gestore si impegna a trattare i dati in proprio possesso secondo quanto prescritto dal medesimo codice);
- si impegna a garantire una tempestiva e corretta informazione a FASTWEB nel momento in cui si prefigurasse un reale o potenziale rischio di violazione della riservatezza dei codici di accesso al Servizio.

Il Titolare, oltre alle responsabilità testè descritte, si assume una serie di obblighi:

- conoscere i contenuti del presente Manuale operativo e consultarlo in caso di necessità di approfondimenti sul funzionamento del sistema;
- proteggere i codici di accesso al Servizio, conservandoli secondo i principi di massima riservatezza e diligenza;
- utilizzare il Servizio rispettando la normativa vigente, e segnatamente in tema di norme sulla riservatezza dei dati e delle informazioni ed in tema di tutela dei diritti d'autore e della proprietà intellettuale, quindi evitando di pubblicare, trasmettere e/o condividere software, documenti o qualsiasi

altro prodotto tutelato da diritti di proprietà intellettuale (es. marchi, brevetti), senza il preventivo consenso da parte del proprietario;
- estendere tali obblighi ad ogni utente che ricada sotto il proprio ambito di responsabilità, curando di informarlo compiutamente

Il rapporto contrattuale è da intendersi stipulato tra FASTWEB e Titolare, pertanto, in caso di risoluzione dello stesso, sarà il Titolare che avrà l'obbligo di comunicare agli utenti l'inaccessibilità del Servizio, sollevando FASTWEB da ogni responsabilità connessa con il mancato utilizzo del Servizio.

8.3 Responsabilità del Titolare del Servizio PEC

Il Titolare malleva FASTWEB da qualsiasi responsabilità diretta o indiretta derivante da eventi:
- connessi con un erroneo o illegale utilizzo del Servizio da parte del Titolare e/o degli Utenti;
- derivanti dalla non veridicità, totale o parziale, o dal mancato aggiornamento dei dati forniti al Gestore dal Titolare.

8.4 Cessione del servizio

Qualora il Titolare intenda cedere a terzi, in tutto o in parte, il Servizio regolato dalle condizioni contrattuali descritte, è da considerarsi condizione necessaria un autorizzazione scritta di FASTWEB.

8.5 Esclusioni e limitazione in sede di indennizzo

FASTWEB non è da ritenersi responsabile per danni diretti e/o indiretti derivanti da:
- atti della Pubblica Autorità, caso fortuito, cause di forza maggiore e comunque qualsiasi evento non dipendente dalla volontà e dalle azioni di FASTWEB (es. anomalie nel funzionamento di apparecchiature tecniche non gestite direttamente da FASTWEB, catastrofi naturali), esclusi i casi di dolo o colpa grave;
- utilizzo non conforme dei codici di accesso al sistema da parte del Titolare e\o degli utenti;
- disservizi nell'invio o nella consegna di messaggi, riscontrati al di fuori dei livelli minimi di servizio previsti dalla normativa vigente, causati da anomalie segnalate al Titolare e da questi non prese in considerazione;
- utilizzo del Servizio con modalità non conformi alle normative vigenti;

- utilizzo del Servizio PEC tramite Gestori non inclusi nell'elenco pubblico tenuto da DigitPA.

FASTWEB, secondo i principi contrattuali definiti, non ha alcuna responsabilità:

- sui ritardi subiti dai messaggi nella trasmissione sulla rete Internet, fatta eccezione per i casi di dolo o colpa grave commessi da FASTWEB stessa;
- sul contenuto dei messaggi inviati dagli utenti, poiché il Gestore non ha alcun obbligo di vigilanza né potere di controllo sulle informazioni scambiate;
- su elementi non normati dal contratto di fornitura e\o dalla normativa vigente.

FASTWEB, in qualità di Gestore PEC e nel rispetto della normativa vigente (DPR 68/05), ha stipulato una polizza assicurativa a copertura dei rischi dell'attività e dei danni causati a terzi, le cui condizioni principali sono riportate nella seguente tabella:

Tipologia di risarcimento	Massimale annuo	Massimale per singolo sinistro
Perdite patrimoniali derivanti dall'attività di FASTWEB di relativamente al servizio di posta elettronica certificata.	1.500.000 €	1.500.000 €
Perdite patrimoniali derivanti dalla diffusione involontaria o per infedeltà dei dipendenti, di dati personali.	500.000 €	500.000 €

Tabella 8 – Tabella dei Risarcimenti

Allegato 1- Modalità di accesso

Come descritto nel documento, è possibile effettuare l'accesso al servizio PEC di FASTWEB secondo due modalità, ossia tramite accesso diretto con l'ausilio di un Web browser, oppure tramite l'utilizzo di programmi e-mail client (es. MS Outlook Express). Il presente allegato descrive nel dettaglio le due procedure di accesso.

Ulteriori informazioni, per le specifiche necessità di configurazione dei sistemi, potranno essere richieste ai canali di Customer Care designati e comunicati in fase di definizione del contratto.

Modalità di accesso via Webmail

L'accesso da Webmail può essere effettuato attraverso un qualsiasi browser, alla URL comunicata nell'e-mail di conferma di attivazione del servizio. A seconda della scelta effettuata si dovranno digitare userid/password oppure il PIN del dispositivo contenente il certificato.

- in caso di logon attraverso credenziali è consigliabile cambiare la password di default assegnata automaticamente dal gestore del servizio con una nuova password lunga almeno otto (8) caratteri e contenente caratteri alfanumerici e, successivamente, cambiarla periodicamente, almeno ogni 3 mesi; una elevata garanzia di sicurezza si raggiunge nel caso la propria password sia cambiata ogni 15 giorni;
- in caso di logon via certificato di autenticazione, è necessario configurare preventivamente il browser e cambiare il PIN di default del dispositivo.

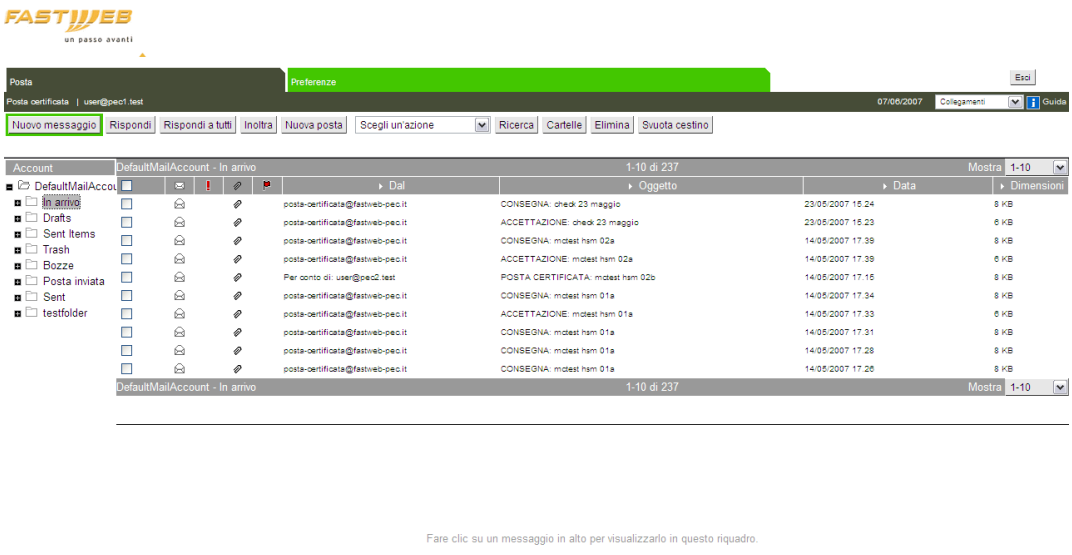

Figura 3 – Accesso via WebMail

Modalità di accesso via Client

Per accedere al servizio tramite Client di Posta Elettronica (es. Outlook, Outlook Express, Edera, ecc…); è necessario configurare lo strumento, secondo la procedura descritta nella sezione "Help" del proprio client.
A titolo esemplificativo, si indica che per il Client MicroSoft Outlook Express 6 (il client certificato da FASTWEB) la funzione è presente sotto la voce "Account" del menu "Strumenti", attraverso la quale si apre il wizard per la configurazione (nel caso specifico denominato "Connessione Guidata Internet")

- per quanto riguarda gli indirizzi dei server di posta di ricezione (POP3) e di invio (SMTP), in entrambi i casi va inserito l'indirizzo **client.nomedominio.it**;
- una volta inserito l'account, è necessario configurare l'accesso con canale sicuro e la spedizione autenticata, assegnando le due caratteristiche alle proprietà dell'account;
- per configurare l'accesso su canale criptato, è necessario indicare in fase di configurazione le porte da utilizzare per la ricezione e la spedizione dei messaggi, nonché specificare se i canali useranno crittografia SSL (Secure Socket Layer) da e verso il server PEC;
- il numero di porta per POP3S per il server PEC è **995** (impostato automaticamente da MicroSoft Outlook Express 6) mentre per la posta in uscita **Il server necessita di una connessione protetta**, e il valore della porta da impostare è **465** per SMTP su SSL.