Manuale Operativo

Posta Elettronica Certificata

ARUBA PEC *S.p.A.*

VERSIONE DEL MANUALE E RESPONSABILITÀ

Versione	1.4
Emesso il	1.0: 04/07/2006 1.1: 06/05/2008 1.2: 10/10/2008 1.3: 07/11/2008 1.4: 20/02/2009
Redatto da	Evita Vignoli; Marco Grassi
Verificato da	Claudio Gremoli
Approvato da	Simone Braccagni
Classe di riservatezza	Documento Pubblico

REVISIONI

Data	Versione	Modifica
04/07/2006	1.0	Prima emissione
06/05/2008	1.1	**Cap. 2**: Modificata Sede Legale, Capitale Sociale e numeri fax **Par. 2.5**: Aggiunte certificazioni ISO **Cap. 5**: Modificata dim. minima delle caselle PEC e procedure per la richiesta del servizio **Par. 5.5**: Modificata procedura di richiesta rigenerazione password in caso di smarrimento **Par. 5.6**: Modificata procedura di richiesta cancellazione caselle PEC **Par. 5.9**: Modificata procedura di richiesta log **Par. 9.7.7**: Aggiunte azioni promosse dal Gestore in caso di malfunzionamento **Tutto**: Correzioni varie
10/10/2008	1.2	**Cap. 2**: Modificato sito di riferimento **Par. 2.2, 2.2.1, 2.2.2**: Modificato sito di riferimento del servizio **Par. 4.3.4:** Aggiunti dettagli sul trattamento dei messaggi di posta elettronica tradizionale (non PEC) **Par. 5.1**: Modificate le tipologie di servizio offerto **Par. 5.3.1**: Aggiunta procedura per attivazioni di caselle su dominio del Gestore **Par. 5.4.1:** Aggiunti dettagli sui client di posta in merito alla compatibilità con gli algoritmi di firma RSA **Par. 6.9:** Aggiornate caratteristiche Webfarm **Par 8.1:** Aggiunti e modificati obblighi per il Gestore **Par 8.2:** Aggiunti e modificati obblighi per il Titolare **Par. 8.4:** Aggiunta clausola di risoluzione del contratto
7/11/2008	1.3	Modificato rappresentante legale di ArubaPEC **Cap. 2, Par. 2.1, 2.2, 2.2.1, 2.2.2:** modificati indirizzi email per contattare il gestore
20/02/2009	1.4	Modificato sito di riferimento del Gestore in *www.pec.it* **Cap. 3** Aggiunto nuovo riferimento normativo **Par. 5.1**: Modificate le tipologie di servizio offerto

INDICE

INDICE DELLE FIGURE

1 – Informazioni di carattere generale

1.1 Scopo

Il Manuale Operativo definisce le regole e descrive le procedure utilizzate dal Gestore Aruba Pec S.p.A. (di seguito per brevità Aruba Pec) per l'erogazione del servizio. Il documento viene pubblicato per garantire la massima trasparenza nei confronti dei clienti del servizio e degli altri Gestori.

1.2 Versione del manuale e responsabilità

ARUBA PEC è responsabile della stesura del presente documento.

La versione del manuale e le singole responsabilità dei redattori e supervisori sono riportate a pagina 2.

1.3 Definizioni ed acronimi

PEC	Posta Elettronica Certificata
CNIPA	Centro Nazionale per l'Informatica nella Pubblica Amministrazione
Gestore di posta elettronica certificata	E' il soggetto che gestisce uno o più domini di posta elettronica certificata con i relativi punti di accesso, di ricezione e di consegna, Titolare della chiave usata per la firma delle ricevute e delle buste e che si interfaccia con altri Gestori di posta elettronica certificata per l'interoperabilità con altri titolari
Titolare	E' il soggetto a cui é assegnata una casella di posta elettronica certificata
Dominio di posta elettronica certificata	E' un dominio, fully qualified domain name (FQDN), di posta elettronica certificata dedicato alle caselle di posta elettronica certificata.
Indice dei Gestori di posta elettronica certificata	E' il sistema, che contiene l'elenco dei domini e dei Gestori di posta elettronica certificata, con i relativi certificati corrispondenti alle chiavi usate per la firma delle ricevute, degli avvisi e delle buste, realizzato per mezzo di un server Lightweight Directory Access Protocol, di seguito denominato LDAP, posizionato in un'area raggiungibile dai vari Gestori di posta elettronica certificata e che costituisce, inoltre, la struttura tecnica relativa all'elenco pubblico dei Gestori di posta elettronica certificata.
Casella di posta elettronica certificata	E' la casella di posta elettronica definita all'interno di un dominio di posta elettronica certificata ed alla quale é associata una funzione che rilascia ricevute di avvenuta consegna al ricevimento di messaggi di posta elettronica certificata;
Marca temporale	evidenza informatica con cui si attribuisce, ad uno o più documenti informatici, un riferimento temporale opponibile ai terzi secondo quanto previsto dal decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 e dal decreto del Presidente del Consiglio dei Ministri 13 gennaio 2004, pubblicato nella Gazzetta Ufficiale n. 98 del 27 aprile 2004.
Riferimento temporale	Informazione contenente la data e l'ora che viene associata ad un messaggio di posta elettronica certificata

PEC	Posta Elettronica Certificata
Tamper evidence	Sistema per segnalare qualsiasi tentativo di manomissione fisica del server che possa aver compromesso l'integrità del sistema e/o dei dati in esso contenuti; tipicamente realizzato tramite l'apposizione sulle macchine di sigilli, lucchetti, etichette autoadesive e/o qualsiasi altro mezzo di protezione il cui stato, in caso di accesso non autorizzato, risulti evidentemente compromesso ad un osservatore esterno.
Tamper proof hardware	Sistema di protezione fisica del server allo scopo di prevenire/impedire l'accesso e la manomissione del sistema dati da parte di soggetti non autorizzati.
HTML	HTML (acronimo per Hyper Text Mark-Up Language) è un linguaggio usato per descrivere i documenti ipertestuali disponibili su Internet. Non è un linguaggio di programmazione, ma un linguaggio di markup, ossia descrive il contenuto, testuale e non, di una pagina web.
MTA	*Mail Transfer Agent*. E' un modulo che ha il compito di effettuare il dispatching dei messaggi di posta elettronica (invio e ricezione)
LDAP	*Lightweight Directory Access Protocol.* E' un protocollo di rete utilizzato per la ricerca e memorizzazione di informazioni su un Directory Server. Una directory server LDAP è un albero di entità costituite da attributi e valori. Un classico utilizzo di un directory server è la memorizzazioni degli account email o degli utenti registrati ad un sito.
SNMP	*Simple Network Management Protocol.* E' un protocollo utilizzato per la gestione ed il monitoring degli apparati di rete
HSM	*Hardware Security Module.* E' un dispositivo hardware per la generazione, la memorizzazione e la protezione sicura di chiavi crittografiche.
NTP	Network Time Protocol
LMTP	Local Mail Transport Protocol
OPT-IN	Consenso preventivo esplicito. Riferimenti normativi: direttiva europea sulle comunicazioni elettroniche (direttiva 2002/58/CE), decreto legislativo 30 giugno 2003, n. 196 - Codice in materia di protezione dei dati personali
Secure Socket Layer (SSL)	Protocollo per realizzare comunicazioni cifrate su Internet. Questo protocollo utilizza la crittografia per fornire sicurezza nelle comunicazioni su Internet e consentire alle applicazioni client/server di comunicare in modo tale da prevenire il 'tampering' (manomissione) dei dati, la falsificazione e l'intercettazione. Scopo primario di SSL è fornire sistemi di crittografia per comunicazioni affidabili e riservate sul Web sfruttabili in applicazioni quali, ad esempio, posta elettronica e sistemi di autenticazione.
HTTPS	Con il termine HTTPS ci si riferisce al protocollo HTTP (Hyper Text Transfer Protocol) utilizzato in combinazione con lo strato SSL (Secure Socket Layer).

1.4 Tabella di corrispondenza

Riportiamo qui di seguito la tabella di corrispondenza tra i paragrafi del presente documento e gli argomenti contenuti nella Circolare 24 novembre 2005 emessa dal CNIPA (CNIPA/CR/49).

Manuale Operativo	Circolare CNIPA
Cap. 2	Circolare 24 novembre 2005, n. CNIPA/CR/49 2.1 Manuale Operativo. **Punto a:** dati identificativi del Gestore
Par. 2.1	Circolare 24 novembre 2005, n. CNIPA/CR/49 2.1 Manuale Operativo. **Punto b:** indicazione del responsabile del manuale
Cap. 3	Circolare 24 novembre 2005, n. CNIPA/CR/49 2.1 Manuale Operativo. **Punto c:** riferimenti normativi necessari per la verifica dei contenuti
Par. 2.4	Circolare 24 novembre 2005, n. CNIPA/CR/49 2.1 Manuale Operativo. **Punto d:** indirizzo del sito web del Gestore ove il manuale è pubblicato e scaricabile – punto d circolare
Cap. 7	Circolare 24 novembre 2005, n. CNIPA/CR/49 2.1 Manuale Operativo. **Punto e:** indicazione delle procedure oltre che degli standard tecnologici e di sicurezza utilizzati dal Gestore nell'erogazione del servizio
Par. 1.3, 4.2	Circolare 24 novembre 2005, n. CNIPA/CR/49 2.1 Manuale Operativo. **Punto f:** definizioni, abbreviazioni e termini tecnici
Cap. 5	Circolare 24 novembre 2005, n. CNIPA/CR/49 2.1 Manuale Operativo. **Punto g:** descrizione sintetica del servizio offerto
Par. 5.9	Circolare 24 novembre 2005, n. CNIPA/CR/49 2.1 Manuale Operativo. **Punto h:** descrizione delle modalità di reperimento e di presentazione delle informazioni presenti nei log dei messaggi

Manuale Operativo	Circolare CNIPA
Par. 5.1	Circolare 24 novembre 2005, n. CNIPA/CR/49 2.1 Manuale Operativo. **Punto i:** indicazione del contenuto e delle modalità dell'offerta da parte del Gestore
Par. 5.4	Circolare 24 novembre 2005, n. CNIPA/CR/49 2.1 Manuale Operativo. **Punto j:** indicazione delle modalità di accesso al servizio
Par. 5.12	Circolare 24 novembre 2005, n. CNIPA/CR/49 2.1 Manuale Operativo. **Punto k:** indicazione del livelli di servizio e dei relativi indicatori di qualità di cui all'art. 12 del decreto del Ministero per l'Innovazione e le Tecnologie 2 novembre 2005
Par. 5.11	Circolare 24 novembre 2005, n. CNIPA/CR/49 2.1 Manuale Operativo. **Punto l:** indicazione delle condizioni di fornitura del servizio
Cap. 9	Circolare 24 novembre 2005, n. CNIPA/CR/49 2.1 Manuale Operativo. **Punto m:** indicazione delle modalità di protezione dei dati dei titolari
Cap. 8	Circolare 24 novembre 2005, n. CNIPA/CR/49 2.1 Manuale Operativo. **Punto n:** indicazione degli obblighi e delle responsabilità che ne discendono, delle esclusioni e delle limitazioni, in sede di indennizzo, relative ai soggetti previsti all'art. 2 del DPR n.68/2005

2 – Dati identificativi del Gestore

Il servizio di Posta Elettronica Certificata verrà erogato da ARUBA PEC della quale riportiamo nel seguito tutte le informazioni identificative.

Dati identificativi del Gestore	
Ragione Sociale:	Aruba PEC S.p.A.
Sede Legale:	Via Sergio Ramelli, 8 52100 - Arezzo (AR) Tel: +39 0575 0500 Fax: +39 0575 862020
Sede di erogazione del servizio:	Via Sergio Ramelli, 6 52100 - Arezzo (AR) Tel: +39 0575 0500 Fax: +39 0575 862020
Partita IVA:	01879020517
Iscrizione registro delle imprese:	Iscritta al registro delle imprese di Arezzo con numero 01879020517
REA:	145843
Capitale sociale:	€ 6.500.000 (interamente versati)
Siti web:	www.pec.it
email:	info@arubapec.it

2.1 Responsabile del Manuale Operativo

Il responsabile del presente manuale operativo è:

Simone Braccagni

Il responsabile può essere contattato ai recapiti

tel: +39-0575-0500

email: info@arubapec.it

indirizzo: Via Sergio Ramelli, 8 - 52100 - AREZZO

2.2 Canali di comunicazione

Oltre al riferimento al precedente paragrafo, il cliente può contattare il Gestore attraverso i canali di seguito specificati.

Call center

tel: +39-0575-0500

email: info@arubapec.it

web: www.pec.it

2.2.1 Assistenza sul servizio

Per assistenza sul funzionamento del sistema e su eventuali malfunzionamenti è possibile mettersi in contatto con il fornitore del servizio con i seguenti mezzi:

tel: +39-0575-050011

fax: +39-0575-862020

email: info@arubapec.it

web: www.pec.it

2.2.2 Informazioni commerciali

Per ricevere informazioni commerciali sul servizio e sulle novità dell'offerta è possibile mettersi in contatto con il fornitore del servizio con i seguenti mezzi:

tel: +39-0575-0500

fax: +39-0575-862020

email: info@arubapec.it

web: www.pec.it

2.2.3 Network Operations Center (NOC)

Emergenze tecniche tra Gestori

tel: +39-0575-050012

fax: +39-0575-862020

email: noc@info.arubapec.it

web: www.pec.it

2.3 Modifiche al manuale

Il presente manuale potrà, nel futuro, subire modifiche dettate dalla necessità di adattare il sistema a nuove normative che verranno emesse da parte degli organi competenti. Il manuale sarà inoltre aggiornato nel caso in cui si rendano necessarie modifiche ed ottimizzazioni al sistema o cambiamenti relativi alle modalità di erogazione del servizio e dell'offerta da parte di ARUBA PEC.

ARUBA PEC garantisce in qualsiasi momento la coerenza del manuale con la versione del sistema

Tutte le future modifiche del Manuale verranno sottoposte a verifica ed approvazione interna, ad opera dei responsabili del servizio, ed esterna, ad opera del CNIPA.

2.4 Indirizzo web del Gestore dal quale scaricare il manuale

All'interno del sito web del Gestore (www.pec.it) è disponibile la copia in formato pdf del presente documento. Il file può essere scaricato all'indirizzo http://www.pec.it/Documentazione.aspx .

ARUBA PEC garantisce che sul sito sia sempre pubblicata l'ultima versione esistente del manuale operativo.

2.5 Certificazioni ISO

ARUBA PEC ha conseguito la certificazione di qualità ISO 9001:2000 in data 05 ottobre 2007. Ha conseguito inoltre la certificazione ISO 27001:2005 in data 28 settembre 2007.

Il dominio di certificazione è:

"Erogazione del servizio di Posta Elettronica Certificata (PEC) e convenzionale, assistenza ai clienti e ai rivenditori"

3 – Riferimenti normativi

[1] Il Decreto Legislativo 30 giugno 2003, n. 196, "Codice in materia di protezione dei dati personali", garantisce che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità degli interessati, con particolare riferimento alla riservatezza, all'identità personale ed al diritto alla protezione dei dati.

[2] Il Decreto del Presidente della Repubblica 28 dicembre 2000 n. 445 stabilisce che, a partire dal 2004, tutte le Pubbliche Amministrazioni (PA) (compresi Enti Locali, Istituti scolastici e universitari, ecc.) debbano adeguare i propri sistemi informativi per gestire lo scambio di documenti informatici tramite questo strumento.

[3] Il Decreto del Presidente della Repubblica del 11 febbraio 2005 n. 68 disciplina le caratteristiche e le modalità per l'erogazione e la fruizione di servizi di trasmissione di documenti informatici mediante posta elettronica certificata.

[4] Il Decreto Legislativo del 7 marzo 2005 n. 82 "Codice dell'Amministrazione Digitale" (CAD) raccoglie e coordina una serie di norme eterogenee che riguardano l'uso delle tecnologie dell'informazione nella pubblica amministrazione.

[5] Con il Decreto Ministeriale del 2 novembre 2005 e le successive note integrative vengono emesse le "Regole Tecniche del servizio di trasmissione dei documenti informatici tramite Posta Elettronica Certificata" che definiscono i requisiti tecnico–funzionali necessari per l'erogazione del servizio.

[6] Il 5 dicembre 2005 viene pubblicato in Gazzetta Ufficiale la Circolare CNIPA recante le modalità di presentazione della domanda di accreditamento nell'elenco pubblico dei Gestori di PEC. A partire da questa data i soggetti pubblici e privati possono richiedere di certificarsi quali fornitori del servizio di PEC.

[7] Il Decreto legge n. 185 del 29/11/2008 convertito nella legge n. 2 del 28/01/2009 rende obbligatorio l'uso della Posta Elettronica Certificata per le Aziende e i Professionisti.

4 – Informazioni generali sulla Posta Elettronica Certificata

4.1 Introduzione

La Posta Elettronica Certificata (PEC) è un sistema di posta elettronica nel quale al mittente viene fornita documentazione elettronica, con valenza legale, attestante l'invio e la consegna di documenti informatici.

La PEC è nata con l'obiettivo di trasferire su mezzi di comunicazione digitale il concetto di Raccomandata con Ricevuta di Ritorno. Come mezzo di trasporto si è scelto di utilizzare l'email che garantisce, oltre alla facilità di utilizzo e alla larga diffusione, una velocità di consegna non paragonabile alla posta tradizionale.

Attraverso la PEC chi invia una email ha la certezza della avvenuta (o mancata) consegna del proprio messaggio e dell'eventuale documentazione allegata.

Per certificare l'avvenuta consegna vengono utilizzate delle ricevute che costituiscono prova legale dell'avvenuta spedizione del messaggio e dell'eventuale documentazione allegata. Le operazioni sono inoltre siglate con riferimenti temporali che "timbrano" in modo inequivocabile gli istanti di invio e ricezione.

Come garanti del servizio vengono costituiti dei **Gestori accreditati** da parte del Centro Nazionale Informatica per la Pubblica Amministrazione (CNIPA). I Gestori possono essere sia Enti Pubblici che soggetti privati.

La traccia informatica delle operazioni svolte durante le trasmissioni viene conservata dai Gestori, per un periodo di tempo previsto dalla normativa ed ha lo stesso valore giuridico delle ricevute consegnate dal sistema. L'utente che avesse smarrito le ricevute, può richiedere al proprio Gestore un estratto della suddetta traccia.

I messaggi possono includere testo, immagini, audio, video o qualsiasi altro tipo di file.

4.2 Definizioni

Punto di accesso: il sistema che fornisce i servizi di accesso per l'invio e la lettura di messaggi di posta elettronica certificata, nonché i servizi di identificazione ed accesso dell'utente, di verifica della presenza di virus informatici all'interno del messaggio, di emissione della ricevuta di accettazione e di imbustamento del messaggio originale nella busta di trasporto.

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

Punto di consegna: il sistema che compie la consegna del messaggio nella casella di posta elettronica certificata del Titolare destinatario, verifica la provenienza e la correttezza del messaggio ed emette, a seconda dei casi, la ricevuta di avvenuta consegna o l'avviso di mancata consegna.

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

Ricevuta di accettazione: la ricevuta, firmata con la chiave del Gestore di posta elettronica certificata del mittente, contenente i dati di certificazione, rilasciata al mittente dal punto di accesso a fronte dell'invio di un messaggio di posta elettronica certificata.

Avviso di non accettazione: l'avviso, firmato con la chiave del Gestore di posta elettronica certificata del mittente, che viene emesso quando il Gestore mittente é impossibilitato ad accettare il messaggio in ingresso, recante la motivazione per cui non é possibile accettare il messaggio e l'esplicitazione che il messaggio non potrà essere consegnato al destinatario.

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

Ricevuta di avvenuta consegna: la ricevuta, firmata con la chiave del Gestore di posta elettronica certificata del destinatario, emessa dal punto di consegna al mittente nel momento in cui il messaggio é inserito nella casella di posta elettronica certificata del destinatario.

Ricevuta completa di avvenuta consegna: la ricevuta nella quale sono contenuti i dati di certificazione ed il messaggio originale.

Ricevuta breve di avvenuta consegna: la ricevuta nella quale sono contenuti i dati di certificazione ed un estratto del messaggio originale.

Ricevuta sintetica di avvenuta consegna: la ricevuta che contiene i dati di certificazione.

Avviso di mancata consegna: l'avviso, emesso dal sistema, per indicare l'anomalia al mittente del messaggio originale nel caso in cui il Gestore di posta elettronica certificata sia impossibilitato a consegnare il messaggio nella casella di posta elettronica certificata del destinatario.

Messaggio originale: il messaggio inviato da un utente di posta elettronica certificata prima del suo arrivo al punto di accesso e consegnato al Titolare destinatario per mezzo di una busta di trasporto che lo contiene.

Busta di trasporto: la busta creata dal punto di accesso e sottoscritta con la firma del Gestore di posta elettronica certificata mittente, all'interno della quale sono inseriti il messaggio originale inviato dall'utente di posta elettronica certificata ed i relativi dati di certificazione.

Busta di anomalia: la busta, sottoscritta con la firma del Gestore di posta elettronica certificata del destinatario, nella quale é inserito un messaggio errato ovvero non di posta elettronica certificata e consegnata ad un Titolare, per evidenziare al destinatario detta anomalia.

Dati di certificazione: i dati, quali ad esempio data ed ora di invio, mittente, destinatario, oggetto, identificativo del messaggio, che descrivono l'invio del messaggio originale e sono certificati dal Gestore di posta elettronica certificata del mittente; tali dati sono inseriti nelle ricevute e sono trasferiti al Titolare destinatario insieme al messaggio originale per mezzo di una busta di trasporto.

Gestore di posta elettronica certificata: il soggetto che gestisce uno o più domini di posta elettronica certificata con i relativi punti di accesso, di ricezione e di consegna, Titolare della chiave usata per la firma delle ricevute e delle buste e che si interfaccia con altri Gestori di posta elettronica certificata per l'interoperabilità con altri titolari.

Titolare: il soggetto a cui é assegnata una casella di posta elettronica certificata.

Dominio di posta elettronica certificata: dedicato alle caselle di posta elettronica dei titolari. All'interno di un dominio di posta elettronica certificata tutte le caselle di posta elettronica certificata devono appartenere a titolari. L'elaborazione dei messaggi di posta elettronica certificata (ricevute, buste di trasporto, ecc.) deve avvenire anche nel caso in cui il mittente ed il destinatario appartengano allo stesso dominio di posta elettronica certificata.

Indice dei Gestori di posta elettronica certificata: il sistema, che contiene l'elenco dei domini e dei Gestori di posta elettronica certificata, con i relativi certificati corrispondenti alle chiavi usate per la firma delle ricevute, degli avvisi e delle buste, realizzato per mezzo di un server Lightweight Directory Access Protocol, di seguito denominato LDAP, posizionato in un'area raggiungibile dai vari Gestori di posta elettronica certificata e che costituisce, inoltre, la struttura tecnica relativa all'elenco pubblico dei Gestori di posta elettronica certificata.

Casella di posta elettronica certificata: la casella di posta elettronica posta all'interno di un dominio di posta elettronica certificata alla quale é associata una funzione che rilascia ricevute di avvenuta consegna al ricevimento di messaggi di posta elettronica certificata.

Marca temporale: un'evidenza informatica con cui si attribuisce, ad uno o più documenti informatici, un riferimento temporale opponibile ai terzi secondo quanto previsto dal decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 e dal decreto del Presidente del Consiglio dei Ministri 13 gennaio 2004, pubblicato nella Gazzetta Ufficiale n. 98 del 27 aprile 2004.

Time Stamping Authority (TSA): Autorità "super partes" che realizza il servizio di marcatura temporale di documenti informatici.

Hardware security module (HSM): un dispositivo hardware per la generazione, la memorizzazione e la protezione sicura di chiavi crittografiche.

4.3 Funzionamento di un sistema di Posta Elettronica Certificata

Il funzionamento di un sistema di Posta Elettronica Certificata può essere descritto sulla base del seguente schema. I messaggi di posta certificata vengono spediti tra 2 caselle, e quindi domini, certificati.

Nel disegno (Fig. 1) sono rappresentati 2 diversi domini di posta certificata e vengono evidenziati in rosso i percorsi del messaggio originale dal mittente al destinatario ed in azzurro i percorsi della ricevuta.

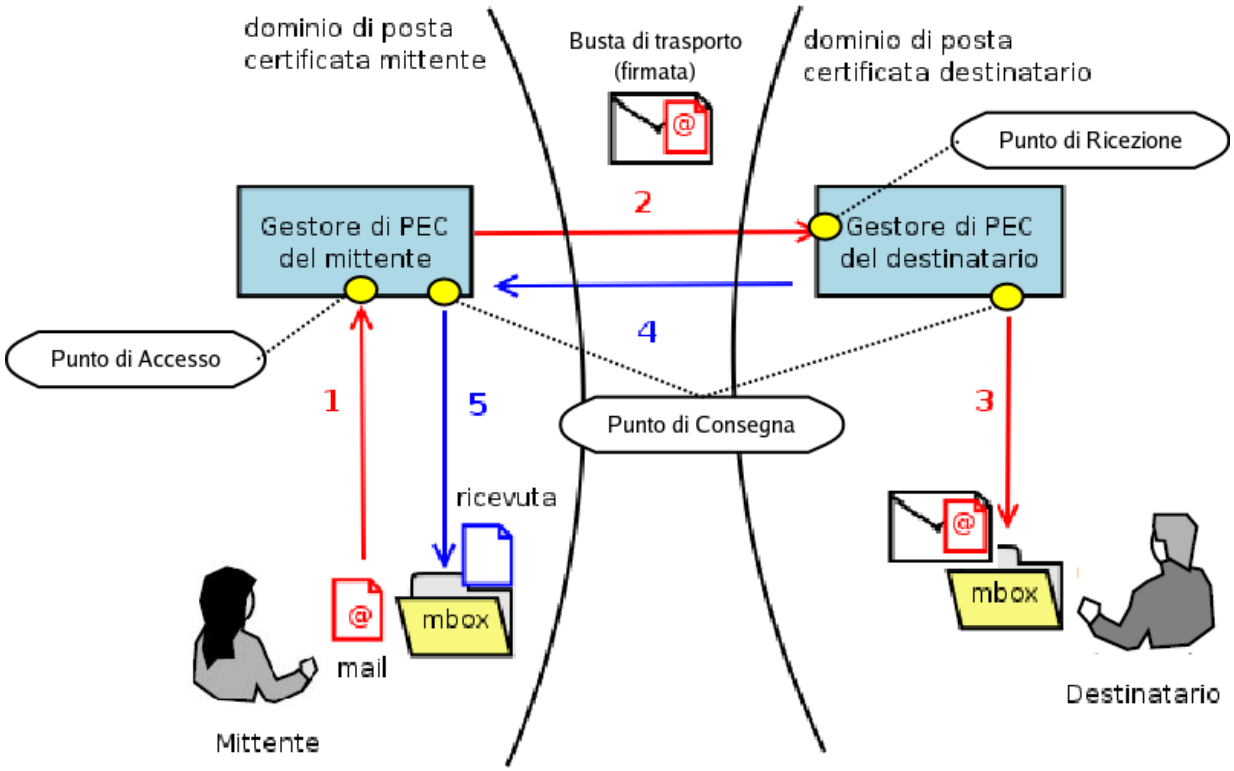


Figura 1 - Funzionamento di un sistema di PEC

Nel dettaglio: quando il mittente possessore di una casella di PEC invia un messaggio ad un altro utente certificato (passo 1), il messaggio viene raccolto dal Gestore del dominio certificato (punto di accesso) che lo racchiude in una busta di trasporto e vi applica una firma elettronica in modo da garantire inalterabilità e provenienza. Fatto questo indirizza il messaggio al Gestore di PEC destinatario (passo 2, punto di ricezione) che verifica la firma e lo consegna al destinatario (passo 3, punto di consegna).

Una volta consegnato il messaggio il Gestore PEC destinatario invia una **ricevuta di avvenuta consegna** all'utente mittente (passi 4 e 5) che può essere quindi certo che il suo messaggio è giunto a destinazione.

Nell'istante in cui invia il proprio messaggio, l'utente ha la possibilità di decidere il tipo di ricevuta di avvenuta consegna che desidera ricevere tra completa, breve e sintetica:

- La **ricevuta completa** contiene, oltre ai dati di certificazione, il messaggio originale in allegato; con questa ricevuta il mittente può verificare che il messaggio consegnato sia effettivamente quello spedito.
- La **ricevuta breve** contiene, oltre ai dati di certificazione, gli hash crittografici (in allegato) del messaggio originale. Questo tipo di ricevuta è stata introdotta per ridurre le dimensioni dei messaggi trasmessi. Il mittente ha la possibilità di verificare che il messaggio consegnato sia effettivamente quello spedito a patto di conservare gli originali *inalterati* degli allegati al messaggio inviato.
- La **ricevuta sintetica** contiene i soli dati di certificazione.

Durante la trasmissione di un messaggio attraverso 2 caselle di PEC vengono emesse altre ricevute che hanno lo scopo di garantire e verificare il corretto funzionamento del sistema e di mantenere sempre la transazione in uno stato consistente.

In particolare:

- Il punto di accesso, dopo aver raccolto il messaggio originale, genera una **ricevuta di accettazione** che viene inviata al mittente; in questo modo chi invia una mail certificata sa che il proprio messaggio ha iniziato il suo percorso.
- Il punto di ricezione, dopo aver raccolto il messaggio di trasporto, genera una **ricevuta di presa in carico** che viene inviata al Gestore mittente; in questo modo il Gestore mittente viene a conoscenza che il messaggio è stato preso in custodia da un altro Gestore.

Quanto sopra riportato descrive il funzionamento di un sistema di PEC nel caso in cui non si verifichino problemi durante la spedizione. Vediamo nel seguito alcuni casi particolari.

4.3.1 Messaggio formalmente non corretto

Nel caso in cui il messaggio inviato dal mittente sia formalmente non corretto, ossia non rispetti i vincoli formali previsti dalla normativa, il Gestore invia al proprio utente (mittente) un **avviso di mancata accettazione per vincoli formali**.

4.3.2 Presenza virus

Nel caso in cui il Gestore del mittente rilevi nel punto di accesso la presenza di un virus nel messaggio, invia al proprio utente un **avviso di mancata accettazione per virus**.

Nel caso in cui sia il Gestore del destinatario a rilevare il virus, il punto di ricezione invia al Gestore del mittente un **avviso di rilevazione virus**. Il Gestore mittente, alla ricezione di un avviso di rilevazione virus invia al mittente del messaggio un **avviso di mancata consegna per virus**.

4.3.3 Ritardi di consegna

Nel caso in cui il Gestore del mittente non riceva alcuna ricevuta di presa in carico nelle 12 ore successive alla spedizione, invia al mittente un **primo avviso di mancata consegna per superamento limiti di tempo**. Con tale avviso il Gestore avverte il proprio utente che il messaggio ***potrebbe non arrivare a destinazione***.

Nel caso in cui dopo ulteriori 12 ore non sia stata ancora recapitata la ricevuta di presa in carico, il Gestore del mittente invia al proprio utente un **secondo avviso di mancata consegna per superamento limiti di tempo**. Con questo secondo avviso il Gestore comunica che la spedizione deve considerarsi ***non andata a buon fine***.

4.3.4 Comunicazioni con indirizzi email non certificati

Messaggi da caselle PEC a caselle tradizionali

Le email inviate da caselle di PEC a caselle di posta tradizionale vengono recapitate normalmente anche se, in questo caso, il destinatario si vedrà recapitare il messaggio originale "imbustato" all'interno di un altro messaggio (in altre parole come allegato).

Nel caso in cui il mail server remoto segnali l'impossibilità di consegnare il messaggio (rimbalzo), il sistema di Aruba Pec invia al mittente certificato un'anomalia di messaggio contenente, in allegato, il motivo della mancata consegna.

Messaggi da caselle tradizionali a caselle PEC

Viceversa, i messaggi provenienti da caselle tradizionali a caselle di PEC possono essere gestiti in due modi a discrezione del Titolare:

- possono essere scartati
- possono essere inoltrati su un indirizzo convenzionale scelto dal cliente

Aruba Pec spa non consente l'ingresso verso caselle PEC di messaggi provenienti da caselle di posta elettronica convenzionale. Il Titolare del servizio, attraverso il servizio di "Inoltro", ha però la possibilità di reindirizzare tali messaggi verso una casella di posta elettronica convenzionale scelta dal cliente tramite accesso all'interfaccia di gestione della casella. Una volta completata l'operazione, tutti i messaggi convenzionali diretti alla casella PEC verranno indirizzati in maniera automatica verso la casella convenzionale indicata.

5 – Il servizio di Posta Elettronica certificata di ARUBA PEC

5.1 Tipologie di servizio offerto

L'offerta di ARUBA PEC è rivolta a persone giuridiche e ad enti pubblici che hanno la possibilità di configurare un dominio di posta elettronica certificata su cui attivare caselle certificate.

Il Gestore si avvale dei propri canali commerciali Partner Aruba Pec (di seguito per brevità Partner Aruba Pec) per fornire caselle singole su dominio del Gestore medesimo.

5.1.1 Vendita caselle PEC tramite Partner Aruba Pec del Gestore

Attraverso il sito www.pec.it è possibile acquistare caselle di pec su uno o più domini di proprietà del Gestore stesso.

Il cliente può scegliere l'indirizzo email; nel caso di account già presente, il Gestore suggerirà uno o più indirizzi alternativi.

ARUBA PEC si riserva il diritto di rifiutare il nominativo scelto nel caso in cui lo ritenga offensivo, irrispettoso o lesivo nei confronti di terzi.

Il cliente ha la possibilità di modificare la password di accesso e di configurare la propria casella attraverso un'interfaccia web di amministrazione.

5.1.2 Dominio personale di posta elettronica certificata (con caselle)

E' possibile richiedere la configurazione di un dominio (FQDN) per privati, enti ed aziende che intendano dotarsi di un proprio dominio di posta elettronica certificata.

Il nome del dominio sarà scelto dal cliente tra quelli non ancora in uso.

ARUBA PEC si riserva il diritto di rifiutare il nominativo scelto nel caso in cui lo ritenga offensivo, irrispettoso o lesivo nei confronti di terzi.

Contestualmente alla richiesta del dominio il cliente ha la possibilità di richiedere un numero di caselle ben definito e estendibile nel futuro.

Il sistema mette a disposizione del cliente un'interfaccia web di amministrazione con la quale è possibile creare nuove caselle, modificarle ed eliminarle.

5.1.3 Titolare delle caselle di PEC

ARUBA PEC richiede al cliente idonea documentazione e registra il Titolare della casella di PEC effettuando le opportune verifiche.

La stessa procedura è applicata anche nel caso di richiesta di attivazione di più caselle nominative da parte di una singola persona; per ogni casella viene nominato il Titolare.

Le informazioni che il Titolare deve inviare all'atto della richiesta di una casella PEC o di un dominio certificato sono le seguenti:

- nome e cognome o ragione sociale
- indirizzo (via, numero civico, città e CAP)
- codice fiscale o partita iva
- indirizzo email di riferimento

- recapito telefonico

Il Titolare deve inoltre inviare al Gestore tutte le informazioni da quest'ultimo richieste allo scopo di procedere con sua identificazione.

5.1.3.1 Cambio di Titolare

ARUBA PEC mette a disposizione dei propri clienti la funzionalità di cambio del Titolare di una casella di PEC. Per ottenere il servizio è necessario che il Titolare richieda esplicitamente il cambio e presenti al Gestore le seguenti informazioni:

1. i dati anagrafici del vecchio Titolare:
   - nome e cognome
   - luogo e data di nascita
   - indirizzo di residenza (via, numero civico, città e CAP)
   - codice fiscale o partita iva
1. una copia del documento di identità del vecchio Titolare
2. i dati anagrafici del nuovo Titolare:
   - nome e cognome
   - luogo e data di nascita
   - indirizzo di residenza (via, numero civico, città e CAP)
   - codice fiscale o partita iva
3. una copia del documento di identità del nuovo Titolare
4. modulo di adesione compilato dal nuovo Titolare
5. visura camerale o dichiarazione sostitutiva compilata dal nuovo Titolare in caso di persona giuridica, liberi professionisti o ditte individuali.

5.2 Servizi opzionali

ARUBA PEC mette a disposizione dei propri clienti una serie di servizi addizionali quali l'upgrade di dimensione delle caselle, la personalizzazione grafica della web mail, ecc. Per queste attività, le modalità di erogazione ed i dettagli dell'offerta con le relative tariffe verranno di volta in volta concordati con il cliente.

5.3 Modalità di erogazione del servizio

5.3.1 Attivazione del servizio su dominio del Gestore

Il cliente ha la possibilità di richiedere l'attivazione di una casella su uno o più domini di proprietà del Gestore. Per richiedere l'attivazione il cliente deve seguire la procedura di seguito descritta:

1. Download moduli e condizioni fornitura

Download dei moduli dal sito http://www.pec.it/Documentazione.aspx

In particolare:

- il modulo di adesione
- la dichiarazione sostitutiva in caso di persona giuridica, liberi professionisti o ditte individuali;

Sempre sullo stesso sito è possibile scaricare il Manuale operativo e le condizioni di fornitura.

2. Pagamento

Il pagamento dovrà avvenire con le modalità indicate alla pagina www.pec.it in base alle diverse tipologie di servizio acquistato.

3. Invio condizioni di fornitura

Il richiedente invia ad ARUBA PEC via fax o attraverso altri canali abilitati e pubblicati sul sito del Gestore la documentazione richiesta:

- documento di adesione firmato dal Titolare
- visura camerale o dichiarazione sostitutiva (nel caso di persona giuridica, liberi professionisti o ditte individuali);
- ricevuta dell'avvenuto pagamento

Il Titolare, al fine di permettere la sua identificazione, è tenuto ad inviare copia di un suo documento di identità in corso di validità oppure ad utilizzare eventuali mezzi alternativi di riconoscimento pubblicati sul sito del Gestore.

4. Attivazione ed invio messaggio di benvenuto

Il Gestore, in collaborazione con il Partner Aruba Pec, porta a termine la richiesta configurando il dominio di posta elettronica certificata con conseguente creazione delle caselle di PEC richieste.

L'attivazione viene effettuata registrando il Titolare della casella con conseguente invio al richiedente di un messaggio di benvenuto con il quale vengono descritti i dettagli del servizio e vengono forniti tutti i parametri di accesso al sistema compresa login e password.

Nello schema di seguito riportato è possibile vedere le interazioni tra il Gestore ed il cliente a seguito di una richiesta di attivazione di una casella PEC su dominio del Gestore.

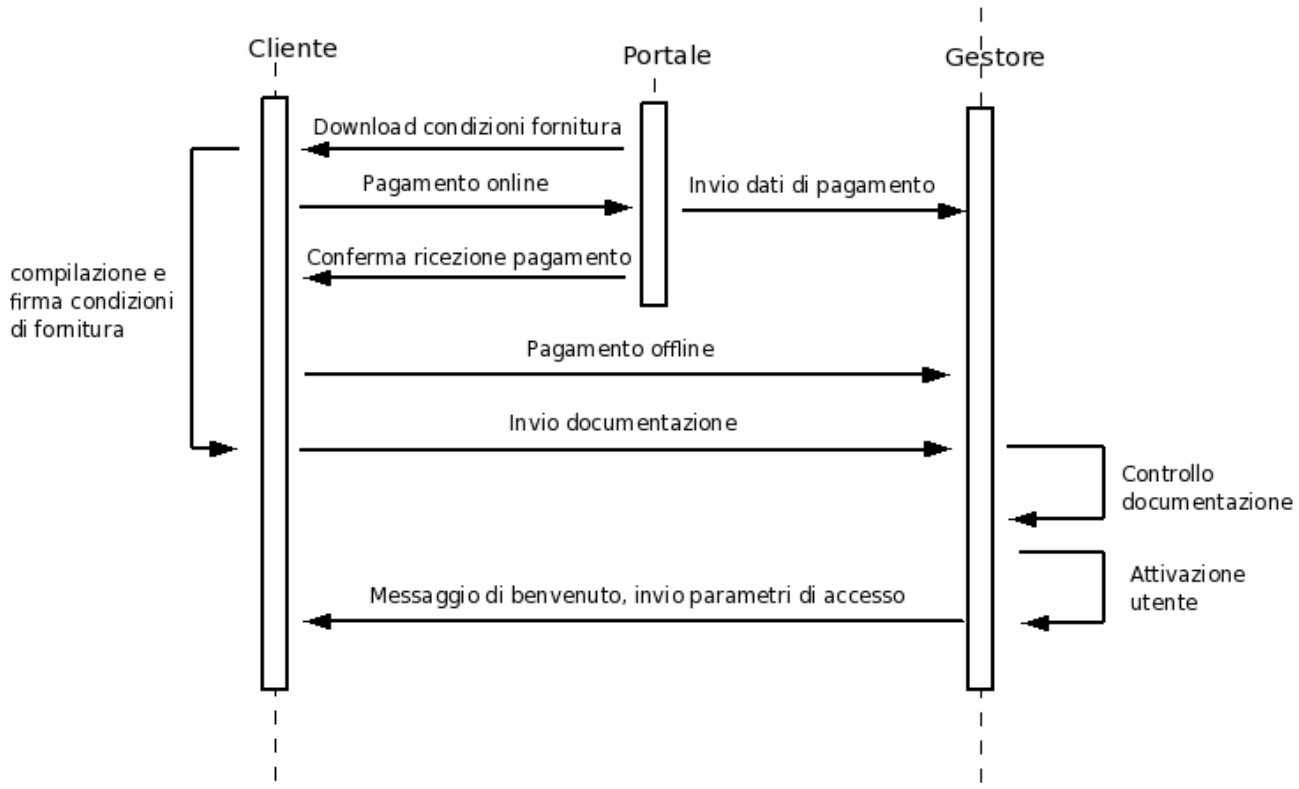


Figura 2 - Attivazione casella PEC su dominio del Gestore

Per i dettagli sulle modalità di richiesta del servizio si rinvia comunque al sito del Gestore.

5.3.2 Attivazione di un dominio personale di posta elettronica certificata attraverso Partner Aruba Pec

Il cliente ha la possibilità di certificare un dominio personale sul quale creare delle caselle PEC. L'attivazione di questo tipo di servizio viene effettuata in collaborazione con la società Aruba S.p.A. o altri Partner Aruba Pec accreditati presso il Gestore.

Modalità di attivazione:

1. Compilazione form online

Il richiedente compila il form presente all'indirizzo web del canale di vendita di ARUBA S.p.A o segue le modalità richieste dal Partner Aruba Pec scelto.

Il Titolare, al fine di permettere la sua identificazione, è tenuto ad inviare copia di un suo documento di identità in corso di validità oppure ad utilizzare eventuali mezzi alternativi di riconoscimento pubblicati sul sito del Gestore.

2. Download condizioni fornitura

Le condizioni generali di fornitura sono disponibili per il download alla pagina http://www.pec.it/Documentazione.aspx.

3. Pagamento

Il pagamento dovrà avvenire con le modalità indicate alla pagina www. pec.it in base alle diverse tipologie di servizio acquistato oppure con le modalità indicate dal Partner Aruba Pec.

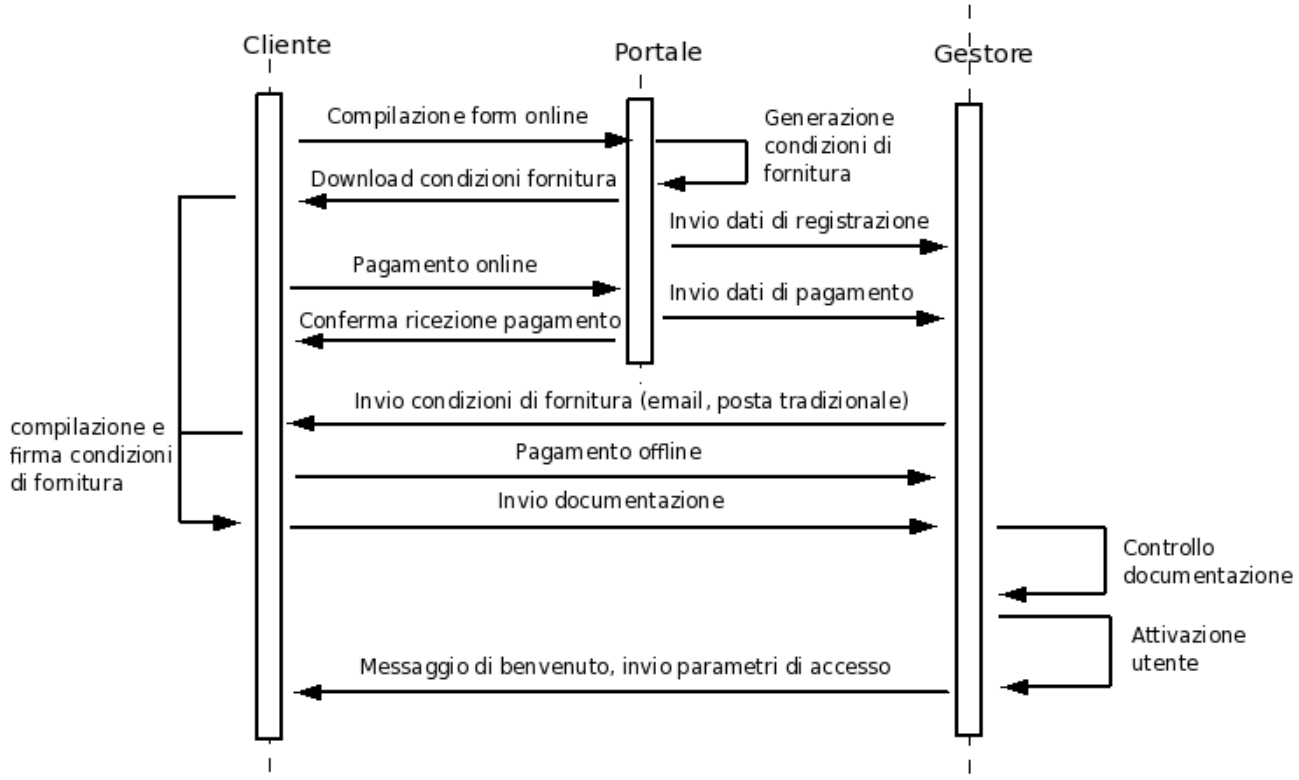
4. Invio della documentazione

Il richiedente invia la documentazione richiesta ed indicata al precedente punto 1 del presente articolo attraverso le modalità indicate dal Partner Aruba Pec scelto.

5. Attivazione ed invio messaggio di benvenuto

Il Gestore, in collaborazione con il Partner Aruba Pec, porta a termine la richiesta configurando il dominio di posta elettronica certificata e creando le caselle di PEC richieste.

L'attivazione viene effettuata registrando il Titolare della casella con conseguente invio al richiedente di un messaggio di benvenuto con il quale vengono descritti i dettagli del servizio e vengono forniti tutti i parametri di accesso al sistema compresa login e password. Nello schema di seguito riportato è possibile vedere le interazioni tra il Gestore ed il cliente a seguito di una richiesta di attivazione di un



dominio personale di posta certificata.

Figura 3 - Attivazione dominio personale PEC

Per i dettagli sulle modalità di richiesta del servizio si rinvia comunque al sito del Gestore.

5.4 Accesso ed utilizzo del servizio

La casella di PEC può essere utilizzata attraverso i più diffusi client di posta ed attraverso un sistema di web mail con le modalità di seguito riportate.

5.4.1 Utilizzo tramite client di posta

Il sistema è compatibile con tutti i principali client di posta che supportano il protocollo S/MIME tra i quali Thunderbird, Eudora, Evolution, Outlook, Outlook Express, ecc.

Per il corretto funzionamento è necessario che il client di posta venga abilitato a connettersi ai server PEC attraverso i protocolli POP3/S, IMAP/S, SMTP/S. Gli indirizzi dei server ed i relativi parametri verranno comunicati dal Gestore nel messaggio di conferma attivazione.

L'utilizzo del sistema attraverso i client di posta è del tutto simile all'utilizzo nel caso di caselle di posta tradizionali. La sola differenza è di tipo funzionale: per ogni messaggio inviato il mittente riceve una ricevuta di accettazione ed una ricevuta di avvenuta consegna; il destinatario, riceve il messaggio originale imbustato in un messaggio di trasporto il cui oggetto ha un prefisso del tipo "**Posta Certificata:**", seguito dal subject originale.

Sul sito del Gestore vengono descritte le modalità di configurazione dei principali client di posta (Thunderbird, Outlook, Eudora, ecc.).

5.4.2 Utilizzo tramite webmail

E' possibile accedere al sistema di posta elettronica certificata inserendo le proprie credenziali (nome utente e password) all'indirizzo web che verrà comunicato dal Gestore nel messaggio di conferma attivazione.

Il nome utente corrisponde all'indirizzo email della casella di PEC mentre la password è rappresentata dalla sequenza di caratteri rilasciata al momento dell'attivazione.

L'accesso alla webmail offre la possibilità di:

- consultare i messaggi arrivati
- inviare nuove mail
- ricercare i messaggi in base all'oggetto
- gestire la propria rubrica
- modificare le impostazioni dell'applicazione.

Per ogni messaggio l'utente ha la possibilità di scegliere il tipo di ricevuta di avvenuta consegna che intende ottenere dal destinatario. La ricevuta, come specificato al par. 4.3 , può essere completa (contiene il messaggio originale), breve (contiene una codifica hash del messaggio originale) o sintetica (contiene i soli dati di certificazione).

5.5 Smarrimento delle credenziali di accesso

Nel caso in cui il cliente smarrisca le credenziali di accesso (login e password), potrà fare richiesta di nuove credenziali al Gestore.

La richiesta può essere effettuata via fax, via email ed attraverso il sistema di trouble ticketing.

In tutti i casi l'avente diritto deve inviare al Gestore le seguenti informazioni:

- il proprio nome e cognome
- codice fiscale

- la fotocopia di un documento di identità valido
- numero telefono
- un indirizzo email valido

Una volta ripristinata la password originale il richiedente viene avvisato via email, oppure mediante ticket nel caso in cui la richiesta sia stata aperta attraverso il sistema di trouble ticketing.

5.6 Eliminazione di una casella PEC da parte del Titolare

Il Titolare di una casella PEC può richiedere al Gestore o al Partner Aruba Pec l'eliminazione della propria casella.

L'eliminazione della casella comporta l'eliminazione, completa e irreversibile, di tutti gli eventuali dati in essa contenuti.

Il Titolare può richiedere la disattivazione a mezzo fax, email o PEC. Per farlo deve comunicare:

- il proprio nome e cognome
- la fotocopia di un documento di identità valido
- l'indirizzo della casella di PEC da eliminare
- numero telefono
- un indirizzo email valido

Il Gestore dopo aver effettuato i dovuti controlli, provvederà all'eliminazione, ed avviserà il richiedente del completamento dell'operazione attraverso un messaggio email, oppure tramite ticket nel caso in cui la richiesta sia stata effettuata attraverso il sistema di trouble ticketing.

5.7 Assistenza

Il servizio di assistenza fornito dal Gestore si sviluppa secondo due modalità che dipendono dalla tipologia e dalla gravità della segnalazione effettuata.

5.7.1 Assistenza su segnalazioni standard

Per segnalazioni standard sulle funzionalità del sistema il servizio è attivo in orario di ufficio (dalle ore 8.30 alle 18.00) dal lunedì al venerdì (esclusi festivi).

Il cliente può chiamare durante i suddetti orari per ottenere supporto sulle problematiche legate al servizio acquistato. Ad esempio:

- generalità sulla posta elettronica certificata (valore legale, funzionamento, interoperabilità con gli altri Gestori, interazioni con la pubblica amministrazione, ecc.)
- configurazione del client di posta
- funzionamento della webmail
- sicurezza ed affidabilità del sistema
- smarrimento delle credenziali di accesso al sistema (login, password)
- richiesta di invio del log messaggi
- problemi durante la connessione al server di PEC
- problemi durante l'invio e la ricezione di messaggi.

La segnalazione viene gestita attraverso il sistema di **trouble ticketing** successivamente descritto.

5.7.2 Trouble ticketing

Il sistema di trouble ticketing è stato pensato e creato per semplificare e velocizzare al massimo tutte le comunicazioni con i clienti in merito alle richieste di supporto tecnico, amministrativo o commerciale.

Oltre all'apertura di un nuovo ticket è anche possibile visualizzare lo stato di tutti i ticket aperti ed effettuare ricerche su tutti i ticket risolti o in attesa di soluzione.

Ad ogni variazione di stato delle richieste, l'utente riceverà notifica via email con la possibilità, in un solo click, di aprire ed aggiornare il ticket in questione, oppure semplicemente di prendere visione della risposta alla richiesta stessa.

Il sistema mette infine a disposizione del cliente una Knowledge Base che contiene le risposte a tutte le domande frequenti ricevute dal servizio assistenza, oltre alle soluzioni ed alle guide per l'utilizzo dei servizi. La Knowledge Base è completamente dinamica e viene costantemente aggiornata ed ampliata in modo da poter fornire supporto in tempo reale a tutte le richieste di informazioni sui nostri servizi e sulle relative modalità di utilizzo.

5.7.3 Assistenza su segnalazioni gravi

Nel caso di problemi tra Gestori, questi hanno la possibilità di contattare il Network Operations Center (NOC) 24 ore su 24, 7 giorni su 7.

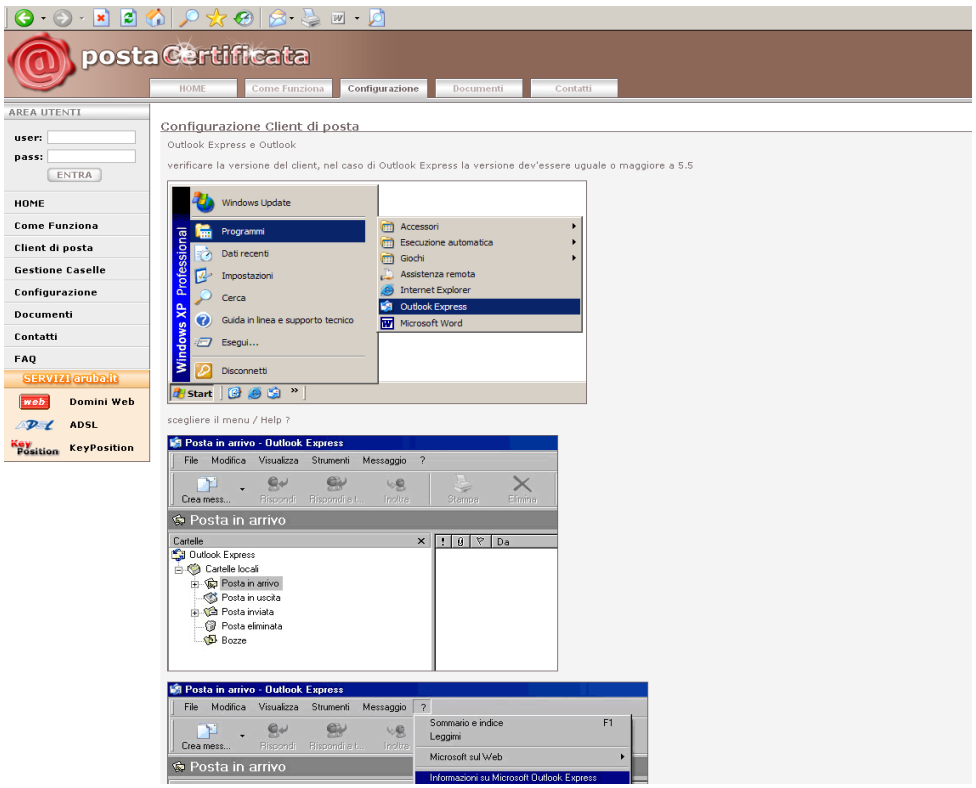


Figura 4 - Trouble ticketing

5.8 Raccomandazioni per gli utenti

Per un corretto e sicuro utilizzo del servizio di posta elettronica certificata è necessario:

- Non utilizzare la casella di PEC per le comunicazioni usuali (come se fosse una normale casella di posta) ma limitarne l'utilizzo alle solo comunicazioni ufficiali e per gli usi consentiti dalla legge.
- Controllare frequentemente la casella di posta: i messaggi di PEC hanno validità legale e si intendono ricevuti dal destinatario nell'istante di deposito nella mailbox dell'utente, non nel momento in cui vengono effettivamente letti.
- Controllare l'occupazione della propria mailbox e procedere, eventualmente, ad una cancellazione dei messaggi più vecchi in modo da evitare che la casella si riempia ed i messaggi non possano essere recapitati.
- Modificare la propria password al primo accesso al servizio e successivamente almeno ogni sei mesi. In caso di trattamento di dati sensibili e dati giudiziari l'utente è tenuto a modificarla almeno ogni tre mesi.
- Utilizzare come password una sequenza di almeno 8 caratteri alfanumerici che non contenga riferimenti agevolmente riconducibili all'incaricato in modo tale da renderne difficile l'individuazione.
- Adottare le necessarie cautele per assicurare la segretezza della componente riservata della credenziale e la diligente custodia dei dispositivi in possesso ed uso esclusivo del Titolare
- Proteggere il proprio computer con firewall e software antivirus.

5.9 Richiesta dei log dei messaggi da parte del Titolare

Come previsto dalla normativa, i Titolari delle caselle di posta elettronica certificata, possono richiedere in qualsiasi momento degli estratti dei contenuti dei file di log relativi alla loro casella di posta elettronica certificata.

La richiesta può essere effettuata via fax, email, PEC o attraverso il sistema di trouble ticketing. Nella richiesta il Titolare deve inviare le seguenti informazioni:

- nome e cognome
- casella PEC
- periodo di interesse
- oggetto della mail (opzionale)
- mittente
- destinatario/i
- copia di un documento di identità valido

Recuperate le informazioni richieste, il Gestore le invia al richiedente attraverso un messaggio PEC oppure mediante ticket se la richiesta è stata aperta attraverso il sistema di trouble ticketing.

5.10 Interoperabilità con gli altri sistemi di PEC

ARUBA PEC si impegna a garantire l'interoperabilità del proprio servizio di PEC con gli altri Gestori secondo quanto stabilito dalle Regole Tecniche di posta elettronica certificata (Decreto Ministeriale 2 novembre 2005 [5]).

ARUBA PEC inoltre verifica periodicamente l'interoperabilità del proprio sistema con gli altri Gestori accreditati attraverso uno scambio concordato di email.

A questo scopo ARUBA PEC renderà pubblico un indirizzo di una casella PEC di test alla quale gli altri Gestori potranno inviare messaggi in modo da controllare il funzionamento e l'interoperabilità del proprio sistema. ARUBA PEC chiederà anche agli altri Gestori di creare una propria casella di test da utilizzare per verifiche periodiche.

5.11 Dettagli offerta, condizioni fornitura e tariffe applicate

I dettagli dell'offerta, le condizioni di fornitura e le tariffe applicate per l'erogazione del servizio sono pubblicate online all'indirizzo web del Gestore.

5.12 Livelli di servizio ed indicatori di qualità

Per l'erogazione del servizio ARUBA PEC garantisce il rispetto dei livelli di servizio previsti dalla normativa.

Livelli di Servizio	
Numero massimo di destinatari contemporanei accettati	50
Dimensione massima di ogni singolo messaggio (intesa come prodotto tra il numero dei destinatari e la dimensione del messaggio)	30 MB (ho tolto >=)
Disponibilità del servizio nel periodo di riferimento previsto (quadrimestre)	Maggiore o uguale al 99,8%
Indisponibilità del servizio per il singolo fermo nel periodo di riferimento previsto (quadrimestre)	Minore o uguale al 50%
Tempo massimo per il rilascio della ricevuta di accettazione nel periodo di disponibilità del servizio (calcolato escludendo i tempi di trasmissione)	30 min

Riportiamo qui di seguito gli indicatori di qualità del servizio (con giorni lavorativi si intendono i giorni dal lunedì al venerdì).

Indicatori di qualità	
Disponibilità del servizio (invio e ricezione email)	7 giorni su 7 - h24
Disponibilità del servizio di richiesta di attivazione	7 giorni su 7 - h24
Tempo massimo per l'attivazione di un nuovo account di PEC su dominio del gestore (dalla ricezione di tutta la documentazione necessaria)	2 giorni lavorativi
Tempo massimo per l'attivazione di un nuovo account di PEC su dominio personale (dalla ricezione di tutta la documentazione necessaria)	3 giorni lavorativi
Tempo massimo per l'esecuzione di interventi di manutenzione che causino il fermo servizio	2 ore

Indicatori di qualità	
Disponibilità del servizio di richiesta da parte del Titolare della traccia delle comunicazioni effettuate (log)	7 giorni su 7, 24 ore su 24
Accesso ai file di log da parte del personale di ARUBA PEC	5 giorni la settimana (lun-ven) dalle ore 8.30 alle 18.00
Tempo massimo per l'invio delle informazioni relative ai file di log dietro richiesta del Titolare	5 giorni lavorativi
Sistema di monitoring con invio di messaggi di alert via email ed sms al presentarsi di malfunzionamenti e situazioni critiche	7 giorni su 7, 24 ore su 24
Assistenza standard tramite call center (trouble ticketing)	5 giorni la settimana (lun-ven) dalle ore 8.30 alle 18.00
Assistenza di emergenza per i Gestori tramite il Network Operations Center (NOC)	7 giorni su 7, 24 ore su 24

6 – Descrizione della soluzione

6.1 Principali caratteristiche

La soluzione di ARUBA PEC presenta le seguenti caratteristiche:

- E' conforme alle specifiche CNIPA ed alla normativa vigente in materia di PEC.
- Rispetta le caratteristiche di interoperabilità ed è conforme, per quanto riguarda la sicurezza, alla normativa vigente.
- È basata su un'infrastruttura Hardware con caratteristiche di scalabilità, modularità e sicurezza nella gestione dei dati sensibili (Chiavi di Firma).
- È compatibile con tutti i client di posta (Thunderbird, Outlook, ecc.) che soddisfano i requisiti minimi stabiliti dalle regole tecniche.
- Le marcature temporali sono generate secondo lo standard internazionale RFC3161 tramite l'utilizzo di un'apposita Time Stamping Authority esterna ed integrata in modalità sicura.
- È interoperabile con qualsiasi Certification Authority che soddisfa gli standard di interoperabilità.
- Si integra semplicemente alle tipologie di rete più diffuse sul mercato, Microsoft, Linux, ecc. Si integra in maniera trasparente a qualsiasi tipologia di rete eterogenea.
- Il certificato e la chiave di firma associati a ciascun dominio di posta elettronica certificata, nonché le procedure che espletano tutte le operazioni crittografiche necessarie durante la firma e/o la verifica dei messaggi risiedono su dispositivi HSM non suscettibili di alterazione (*tamper-proof* , *tamper-evident*).

6.2 Scalabilità e Affidabilità

L'architettura è progettata in modo da garantire una scalabilità praticamente illimitata al fine di soddisfare le esigenze di crescita di comunità di grandi dimensioni mantenendo nel contempo inalterati performance e livelli di fruibilità.

Di seguito evidenziamo alcune delle caratteristiche principali.

- Tutti i server e gli apparati di rete, inclusi gli stessi moduli HSM, sono duplicati e bilanciati per implementare un servizio non soltanto scalabile ma anche di alta affidabilità e disponibilità (*high availability*)
- Il front-end ed il back-end sono fisicamente separati per aumentare la sicurezza e la scalabilità
- Vengono utilizzati dei supporti di memorizzazione esterni, condivisi via NFS (tramite *storage area network*) e residenti su un'architettura in cluster, così da risolvere tutte le possibili problematiche di disponibilità, affidabilità e continuità del servizio.

6.3 Sicurezza dei dati

Il sistema garantisce un elevato grado di sicurezza soprattutto riguardo alla gestione delle chiavi private e dei certificati utilizzati per la generazione delle firme delle ricevute, degli avvisi e delle buste di trasporto e per il processo di verifica delle suddette operazioni.

A tale scopo, la chiave privata del sistema di PEC nonché le operazioni crittografiche necessarie durante la firma e/o la verifica dei messaggi risiedono su un dispositivo HSM **tamper proof** e **tamper evident** certificato **FIPS 140-2 level 3**.

(Vedi http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf)

6.4 Architettura di massima del sistema

Grazie all'installazione dei principali componenti su macchine separate riusciamo ad ottenere una soluzione scalabile ed estendibile in qualsiasi momento. Tutti i componenti critici sono inoltre ridondati e bilanciati in modo da assicurare un alto livello di tolleranza ai guasti ed assicurare alte performance.

Riportiamo qui di seguito un'architettura di massima del sistema che ha il solo scopo di descrivere l'approccio utilizzato e non ha la pretesa di essere dettagliata ed esaustiva in termini di numero di macchine coinvolte e di moduli utilizzati.

Come è possibile dallo schema sotto riportato vedere il sistema è strutturato *logicamente* su 3 livelli.

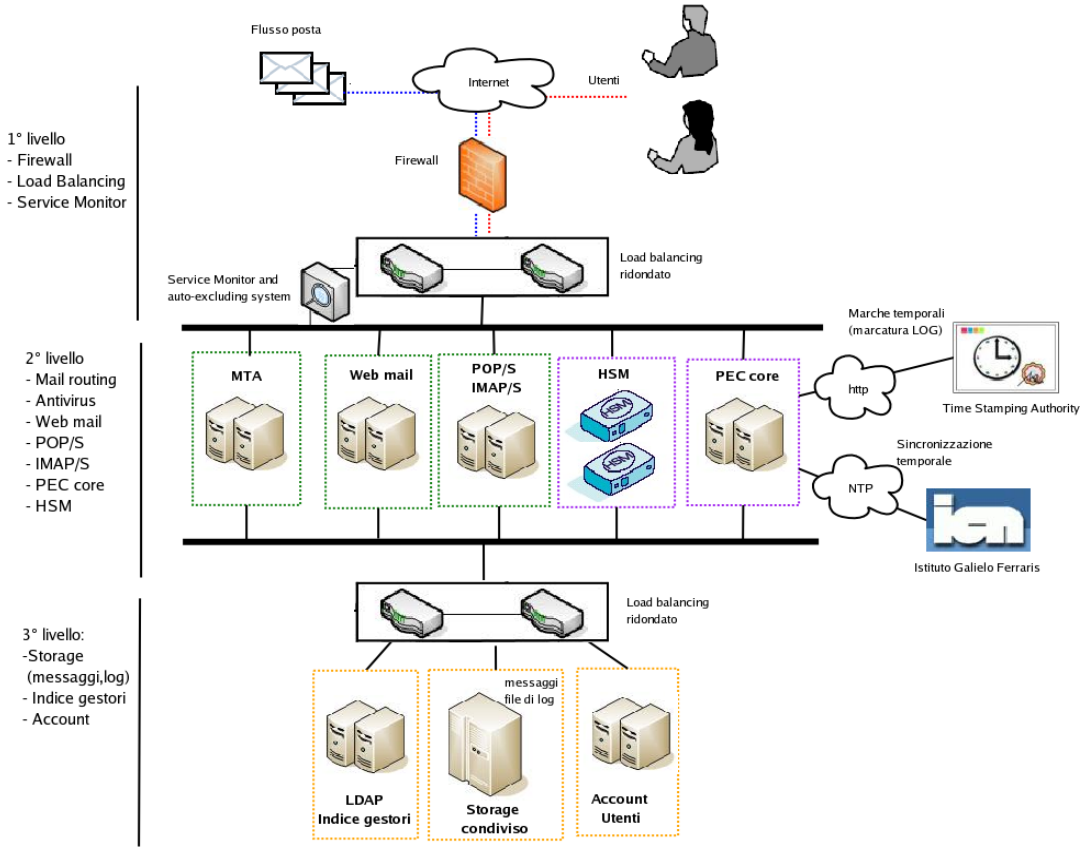


Figura 5 - Architettura di massima del sistema

6.4.1 Primo livello

Il primo livello è costituito dagli apparati di rete (router, switch), dal modulo firewall e dal sistema di monitor che si occupa del controllo di tutti i moduli del sistema e che contiene un meccanismo di esclusione automatica degli apparati non funzionanti.

6.4.2 Secondo livello

Il secondo livello costituisce il centro nevralgico del sistema e rappresenta: l'interfaccia verso il mondo esterno, il principale centro di elaborazione e l'interfaccia verso i dispositivi di memorizzazione.

All'interno del secondo livello sono presenti i moduli che si occupano del mail routing, di rilevare l'eventuale presenza di virus, di mettere a disposizione dell'utente finale la web mail ed i server POP/S e IMAP/S.

Il livello contiene anche il nucleo centrale del sistema (PEC Core). Le macchine si sincronizzano con l'Istituto Galileo Ferraris di Torino mediante protocollo NTP. Inoltre il sistema si interfaccia con una Time Stamping Authority allo scopo di effettuare la marcatura giornaliera dei log.

Il secondo livello si occupa anche di effettuare la firma dei messaggi attraverso appositi device chiamati **Hardware Security Module** (**HSM**). Si tratta di periferiche server ad alta sicurezza per la gestione e la protezione di chiavi crittografiche.

6.4.3 Terzo livello

Il terzo livello rappresenta il data store del sistema e contiene, all'interno di uno storage condiviso, le mailbox degli utenti ed i file di log. Il terzo livello memorizza inoltre su apposite strutture gli account degli utenti ed il mirror dell'indice pubblico dei Gestori (CNIPA).

6.5 Architettura della soluzione

Di seguito riportiamo uno schema che descrive i principali componenti della soluzione:

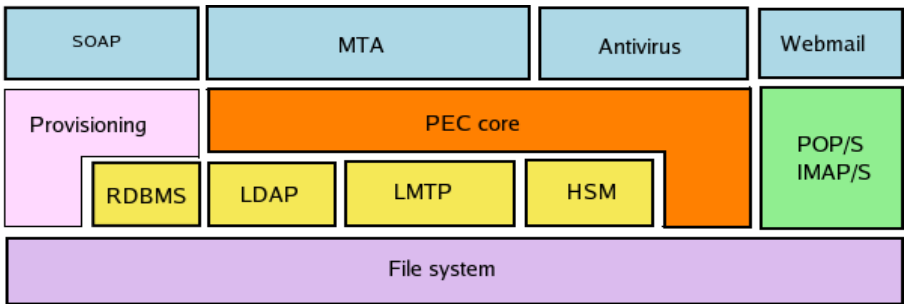


Figura 6 - Componenti del sistema

Come descritto nello schema, esiste un nucleo centrale del sistema (PEC Core) che si interfaccia con tutti gli altri moduli: il Mail Transfer Agent (MTA) che si incarica del "dispatching" delle mail, il modulo Antivirus, il server LDAP (che contiene gli account ed il mirror dell'indice dei Gestori), il server LMTP, i moduli HSM utilizzati per la firma dei messaggi, lo storage (file system), il server POP-IMAP. Nel sistema è presente un modulo di provisioning (per la creazione/modifica degli account) richiamabile attraverso interfaccia SOAP, ed una web mail.

Per descrivere a grandi linee il funzionamento del sistema utilizziamo la figura seguente nella quale sono evidenziate le interazioni tra i principali componenti.

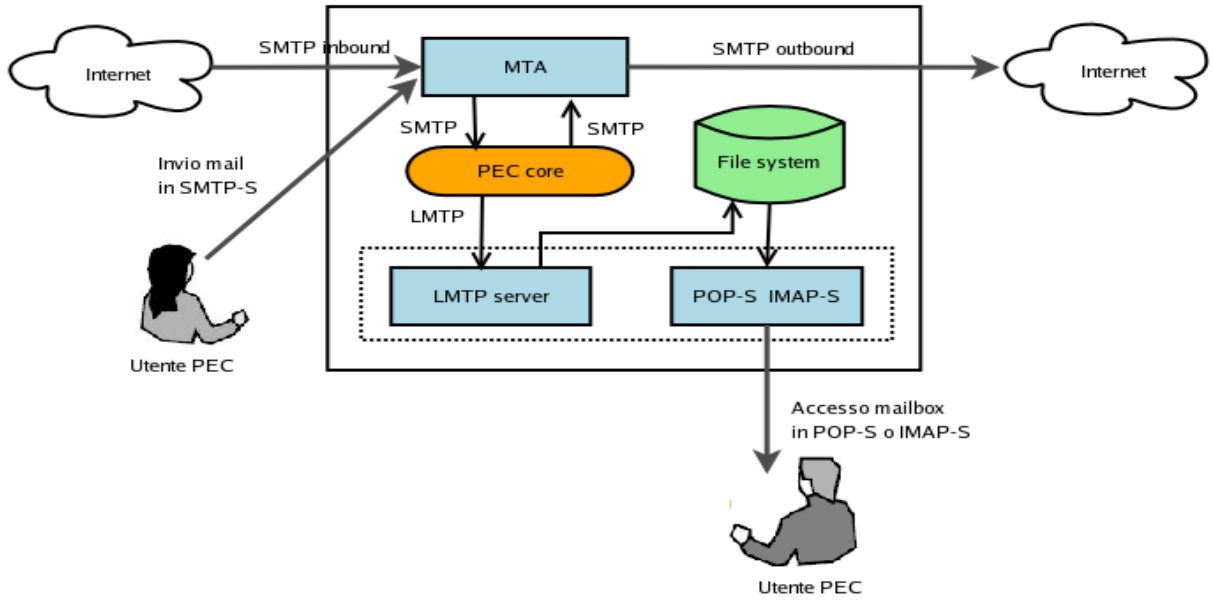


Figura 7 – Interazioni tra i moduli del sistema

Per ogni messaggio in ingresso all'MTA:

- se è un messaggio in uscita lo incapsula in un documento di trasporto, lo firma elettronicamente attraverso il modulo HSM e lo restituisce all'MTA che lo inoltra verso il destinatario
- se è un messaggio in ingresso verifica la correttezza della firma (attraverso il modulo HSM) e la validità del messaggio (provenienza da un dominio certificato), effettua il delivery verso la mailbox di destinazione attraverso il protocollo LMTP e, una volta consegnato il messaggio crea la ricevuta di avvenuta consegna che l'MTA invierà al mittente del messaggio originale. Nel caso di non validità del messaggio genera un messaggio di anomalia di trasporto che inoltra verso la mailbox dell'utente.

I Log del sistema hanno valore giuridico e verranno mantenuti in appositi storage per il periodo previsto.

Il prodotto è stato progettato in modo tale da essere modulare, così da permettere future estensioni ed adattamenti.

6.6 Riferimenti temporali

Come previsto dalla normativa (Decreto ministeriale del 2 novembre 2005) su ogni messaggio viene apposto un riferimento temporale, sia esso il messaggio di trasporto, una ricevuta o un avviso.

Tutti gli eventi che costituiscono la transazione nel punto di accesso, nel punto di ricezione e nel punto di consegna utilizzano un unico valore temporale calcolato all'interno della transazione stessa. In questo modo l'indicazione dell'istante di elaborazione del messaggio risulta univoca all'interno dei log, delle ricevute, degli avvisi e dei messaggi generati dal sistema.

Il riferimento temporale viene generato con un sistema che garantisce uno scarto non superiore ad 1 minuto secondo rispetto alla scala di riferimento UTC (Coordinated Universal Time).

Il formato della data è ***gg/mm/aaaa*** dove ***gg*** sono le 2 cifre del giorno, ***mm*** le 2 cifre del mese e ***aaaa*** le 4 cifre dell'anno.

Il formato dell'ora è ***hh:mm:ss*** dove ***hh*** sono le 2 cifre delle ore (su 24 ore), ***mm*** le 2 cifre dei minuti, ***ss*** le 2 cifre dei secondi.

Al dato temporale viene fatto seguire, tra parentesi tonde, la **zona**, ossia la differenza, in ore e minuti, tra l'ora legale ed il riferimento UTC. Il valore di tale differenza è preceduto da un segno + o – che indica la differenza positiva o negativa rispetto ad UTC.

Facciamo un esempio:

07/06/2006 17:27:21 (+0100)

indica il 7 giugno 2006, ore 17, 27 minuti e 21 secondi, con

1 ora avanti rispetto al riferimento UTC.

Per garantire la massima precisione sui riferimenti temporali apportati ai messaggi, il sistema si sincronizza attraverso il protocollo NTP con l'Istituto Elettrotecnico Nazionale Galileo Ferraris di Torino (IEN).

L'orologio di sistema viene mantenuto permanentemente sincronizzato con quello di riferimento compensando anche la deriva e le fluttuazioni causate ad esempio dalle variazioni dei parametri ambientali, dal carico di lavoro del sistema, ecc.

6.7 Storicizzazione dei Log e apposizione della marca temporale

Al fine della conservazione dei log dei messaggi, di cui alle deliberazioni del CNIPA in materia di riproduzione e conservazione dei documenti su supporto ottico, è necessario definire un intervallo temporale unitario, non superiore alle ventiquattro ore, entro il quale eseguire senza soluzioni di continuità il salvataggio dei log dei messaggi generati in ciascun intervallo temporale.

Ai file generati da ciascuna operazione di salvataggio deve essere apposta la relativa marca temporale. Le marche temporali sono messaggi firmati digitalmente che legano in modo sicuro e verificabile un qualsiasi documento informatico ad un riferimento affidabile di tempo, data e ora. La validazione temporale di un documento informatico consiste nella generazione, da parte di una "*trusted third party*" (terza parte fidata), di una firma digitale così detta di "*time stamping*" (marcatura temporale), dalla quale è possibile acquisire la certezza della data ed ora di emissione. Le marche temporali possono risolvere dispute in merito al tempo (data/ora) in un cui un dato documento è stato prodotto.

Per il servizio di marca temporale è prevista l'integrazione di un servizio di **Time Stamping Authority** (**TSA**) esterno attraverso il protocollo standard RFC 3161 (http://www.ietf.org/rfc/rfc3161.txt). I file generati conservati per il tempo stabilito dalla normativa (30 mesi).

Nel caso in cui venisse revocato il certificato di un firmatario di un documento di cui si ha la marca temporale, è possibile determinare quando la firma è stata apposta, in particolare si riesce a determinare se ciò è avvenuto prima o dopo la revoca e definire quindi se si tratta di una firma affidabile.

6.8 Conservazione dei messaggi contenenti virus e relativa informativa al mittente

Il sistema di ARUBA PEC, compatibilmente con la normativa, verifica la presenza dei virus nei messaggi di posta elettronica al Punto di Accesso, ossia nella fase immediatamente successiva alla spedizione del messaggio originale, e al Punto di Ricezione, nella fase di ricezione dal sistema di posta certificato del mittente.

L'individuazione del virus fa scattare una serie di operazioni finalizzate ad avvertire il soggetto che ha introdotto il virus ed alla conservazione del messaggio per eventuali verifiche successive.

Se il virus è individuato al Punto di Accesso verrà generato un "Avviso di rilevazione di virus informatici" destinato al mittente del messaggio corrotto mentre se è stato individuato al Punto di Ricezione verrà generato un "Avviso di non accettazione per virus informatici" destinato al Gestore del sistema certificato del mittente e un "Avviso di mancata consegna per rilevazione di virus informatici" destinato al mittente.

Il sistema inoltre, conserva i messaggi contenenti virus su supporto ottico o magnetico mettendo in condizioni il Gestore di mantenerli per un periodo non inferiore a trenta mesi secondo le modalità indicate nelle deliberazioni del CNIPA in materia di riproduzione e conservazione dei documenti.

6.9 Descrizione Webfarm di ARUBA PEC

Riportiamo qui di seguito le principali caratteristiche della Webfarm:

Connettività:

- 32 Gbit/s di connettività nazionale ed internazionale.
- Collegamenti fisici con 3 diversi fornitori di connettività (carrier) ridondati, e collegamento diretto con il MIX anch'esso ridondato.
- 2 router CISCO classe 12.000 e 2 switch CISCO Catalyst 6513 in bilanciamento assicurano connettività anche in caso di guasto di un componente.
- Rete LAN interna di classe GIGABIT con cablaggio cat. 6 certificato.

Alimentazione:

- Cabina elettrica dedicata, collegata alla rete elettrica di ENEL, che assicura scalabilità ed espandibilità degli oltre 5 MVA attualmente installati.
- Generatore di elettricità di pari capacità, con motori diesel in grado di sopperire in qualsiasi momento e per qualsiasi periodo di tempo ad eventuali mancanze nelle erogazioni di energia elettrica da parte di ENEL.
- 5 gruppi di UPS da 500 Kva ciascuno in configurazione parallelo ridondato "n + 2" con durata 2 ore garantiscono una totale sicurezza ed un'ulteriore garanzia di continuità oltre alla protezione da sbalzi, microinterruzioni e variazioni di tensione.

Climatizzazione:

- Sistema d'aria condizionata flessibile ed espandibile, garantisce una temperatura ed umidità costanti.
- Nelle sale dati la temperatura media è mantenuta a 23 gradi circa.

Sicurezza:

- Sicurezza agli accessi
- Telecamere a circuito chiuso
- Sistema antincendio ad NitrArgon rilevamento elettronico, sistema antifumo

- Le attrezzature antincendio (estintori, idratanti esterni, impianto centralizzato a gas NitrArgon) sono ubicate in modo da essere facilmente raggiungibili e da proteggere tutta l'area. Tali impianti sono mantenuti e verificati regolarmente. Gli impianti elettrici e di distribuzione del gas sono realizzati in modo da minimizzare i rischi di incendio e di esplosione.

Assistenza:

- Personale qualificato presente 24 ore su 24 ore, 7 giorni su 7 per garantire controllo, manutenzione ed assistenza.
- Network Operations Center (NOC) attivo 24/7/365 per i Gestori.
- Assistenza a disposizione dei clienti per e-mail, per telefono oppure tramite trouble ticketing on-line.
- Monitoraggio in tempo reale dello stato di ogni singolo server con alert al rilevamento di un qualsiasi problema.

7 – Standard tecnologici, procedurali e di sicurezza adottati

7.1 Standard tecnologici di riferimento

- RFC 1847 (Security Multiparts for MIME: Multipart/Signed and Multipart/Encrypted)
- RFC 1891 (SMTP Service Extension for Delivery Status Notifications)
- RFC 1912 (Common DNS Operational and Configuration Errors)
- RFC 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 Hyper Text Transfer Protocol)
- RFC 2821 (Simple Mail Transfer Protocol)
- RFC 2822 (Internet Message Format)
- RFC 2849 (The LDAP Data Interchange Format (LDIF) – Technical Specification)
- RFC 3174 (US Secure Hash Algorithm 1 - SHA1)
- RFC 3207 (SMTP Service Extension for Secure SMTP over Transport Layer Security)
- RFC 3280 (Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List - CRL Profile)
- RFC 3161 (TSP Time Stamp Protocol)

7.2 Standard di sicurezza

I device HSM utilizzati per la firma e verifica dei messaggi di PEC sono certificati **FIPS 2 – Level 3**. Con questa sigla si intendono i Requisiti Standard di Sicurezza (pubblicati dal NIST, il National Institute of Standards and Technology) che devono essere rispettati dai moduli crittografici utilizzati all'interno di un sistema di sicurezza ove si trattino dati/informazioni sensibili. In particolare fanno parte di questa gamma le specifiche dei moduli crittografici e relative interfacce, le regole, i servizi e il processo di autenticazione. Tra i requisiti, vengono trattati anche i vincoli di sicurezza a livello fisico ed il processo del Key Management.

Lo Standard si compone di quattro livelli qualitativi di sicurezza, dal Level 1 a 4 per coprire un'ampia gamma di requisiti, dal design all'implementazione dei moduli crittografici.

Il **Level 1** riguarda essenzialmente i requisiti minimali di sicurezza per i moduli crittografici, in particolare per quanto riguarda gli algoritmi, senza alcun vincolo sulla sicurezza fisica.

Il **Level 2** aggiunge, ai precedenti, requisiti fisici di sicurezza (ad es. è richiesto l'utilizzo di rivestimenti e/o etichette al fine di ottenere un livello fisico **"**tamper-evident**").**

Il **Level 3** aggiunge, ai meccanismi di "tamper evidence" presenti anche nei livelli precedenti altri meccanismi per garantire la "tamper proofness". I dispositivi, infatti, rispondono ai tentativi d'accesso non autorizzato cancellando la memoria del modulo crittografico. Inoltre, al meccanismo di autenticazione basato sui ruoli previsto dal livello 2, il livello 3 aggiunge anche un meccanismo basato

sull'identità: il modulo crittografico autentica l'identità di un operatore e verifica che sia associato ad un ruolo previsto e lo autorizza alla gestione di servizi specifici.

ARUBA PEC ha conseguito la certificazione **ISO 27001:2005** in data 28 settembre 2007. Lo standard di sicurezza ISO 27001:2005 garantisce la sicurezza dei dati attraverso l'adozione di procedure, norme comportamentali, misure e corsi di formazione adeguati.

Lo standard si basa sui seguenti principi:

- **Information Security**: preservare confidenzialità, integrità e garantire la disponibilità delle informazioni.
- **Confidentiality**: assicurarsi che le informazioni siano accessibili solo a coloro che sono autorizzati.
- **Integrity**: salvaguardare l'accuratezza e la completezza delle informazioni e preservare la tecnica con la quale le informazioni vengono processate.
- **Availability**: assicurarsi che informazioni siano disponibili ed accessibili al personale autorizzato, quando necessario.
- **Risk Assessment, Risk Analysis**: rilevare le minacce ed il loro impatto sul sistema, analizzare la vulnerabilità delle informazioni e dei processi, calcolare la probabilità che gli eventi accadano.
- **Risk Management**: identificare, controllare, contenere, eliminare il security risk di cui è eventualmente affetto il sistema.

Aruba Pec ha inoltre conseguito la certificazione **ISO 9001:2000** (Qualità) in data 05 ottobre 2007.

7.3 Misure di sicurezza

Il sistema di posta elettronica certificata di ARUBA PEC presenta tutte le garanzie di sicurezza compatibili con la tipologia di servizio erogato, sia a livello fisico che a livello informatico.

Riportiamo di seguito le principali misure di sicurezza adottate per garantire l'integrità, la protezione e la riservatezza dei dati. Tali misure sono riportate, in maniera approfondita, nel **Piano della Sicurezza**, un documento riservato, consegnato al CNIPA e redatto in base alle disposizioni della circolare CNIPA n. 49 del 24 novembre 2005.

7.3.1 Accesso ai locali di erogazione del servizio

Le apparecchiature utilizzate per l'erogazione del servizio sono situate all'interno di un'area ad accesso controllato. L'ingresso nei locali è consentito solo a personale autorizzato tramite sistema a controllo biometrico.

L'intera area è monitorata da telecamere a circuito chiuso e presidiata 24 ore su 24.

I locali sono dotati dei più moderni dispositivi antincendio, antifumo, antri intrusione e condizionamento.

Le visite di clienti o visitatori occasionali sono possibili solo su prenotazione e nei tempi e modi definiti dall'azienda. Duranti tali visite, il visitatore è sempre accompagnato da personale interno.

7.3.2 Personale adibito alla gestione del sistema

Il personale adibito al sistema PEC viene istruito opportunamente mediante corsi di formazione interni attraverso i quali gli incaricati imparano a svolgere le mansioni loro assegnate. Durante la formazione viene dato particolare risalto all'importanza ed alla criticità del servizio erogato in modo che gli

operatori si sentano responsabilizzati e si dedichino con particolare cura ed attenzione al proprio lavoro.

Ogni nuovo incaricato viene seguito, nel primo periodi di attività, da un tutor che ne controlla l'operato. In generale tutto il personale adibito alla PEC viene periodicamente controllato attraverso attività di auditing interno.

Ogni operatore riferisce ad uno dei responsabili previsti dalla normativa:

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

7.3.3 Sicurezza di tipo informatico

Dal punto di vista prettamente informatico, la sicurezza del sistema di ARUBA PEC viene realizzata attraverso l'adozione di una sere di misure quali:

- Presenza di 2 livelli di firewall con definizione di policy di accesso (vengono abilitate le sole porte strettamente necessarie al funzionamento del sistema PEC).
- Sistema di antivirus aggiornato più volte al giorno (minimo 4), così da rendere il sistema protetto contro attacchi da parte di software malevolo.
- Prodotti software costantemente aggiornati (al rilascio di un nuovo prodotto o di una patch, dopo una fase di test su un ambiente di staging, viene aggiornato il prodotto in ambiente di produzione).
- Separazione fisica del livello di front-end dal livello di back end e storage in modo da proteggere ulteriormente i dati da accessi indesiderati.
- Ulteriore protezione delle macchine che contengono i dati degli utenti attraverso firewall locali.
- Sistema ridondato in ogni sua parte in modo da evitare "single point of failure".
- Meccanismo di auto esclusione degli apparati non funzionanti con conseguente dirottamento del traffico sugli altri nodi "gemelli".
- Utilizzo di storage di rete esterni al sistema per aumentare la protezione delle informazioni degli utenti.
- Sistema di backup su doppio supporto per ridurre il rischio di perdita dei dati.
- Utilizzo di protocolli sicuri per il colloquio tra l'utente ed il proprio Gestore (SMTP/S, POP3/S, IMAP/S) e tra un Gestore e l'altro (STARTTSL).
- Firma dei messaggi con i dispositivi HSM certificati FIPS-2 Level 3.

7.3.4 Controllo dei livelli di sicurezza

I livelli di sicurezza vengono costantemente controllati attraverso opportune attività di monitoring sui principali componenti del sistema.

Inoltre sono previste delle attività di auditing con cadenza massima annuale durante le quali viene analizzato l'intero sistema con lo scopo di verificarne la sicurezza ed individuare eventuali punti vulnerabili. Durante l'auditing viene analizzata la storia passata dedicando particolare attenzione agli eventuali problemi riscontrati. Vengono inoltre controllati gli apparati di rete, i firewall e tutti i componenti del sistema allo scopo di accertarsi che il sistema è protetto e sicuro.

Durante l'auditing vengono interrogati i responsabili del servizio in relazione all'operato del personale adibito al sistema PEC. Gli incaricati che verranno giudicati non idonei, verranno prontamente sostituiti.

Al termine delle attività viene compilato un rapporto nel quale vengono evidenziati i controlli effettuati e vengono descritti gli eventuali aspetti da migliorare.

7.3.5 Protezione dei dati

I dati personali degli utenti sono trattati, conservati e protetti da ARUBA PEC conformemente da quanto previsto dal Decreto legislativo n. 196 del 30 giugno 2003 "Codice in materia di protezione dei dati personali" e s.m.i [1] (per i dettagli si rimanda al Cap. 9 –).

Adottando le misure, le procedure, i processi ed i controlli di sicurezza descritti nei precedenti paragrafi, ARUBA PEC è in grado di assicurare, ai propri clienti, un continuo e costante livello di protezione dei propri dati.

7.4 Procedure operative

Per l'erogazione del servizio di posta elettronica certificata ARUBA PEC mette in atto una serie di procedure tecniche ed organizzative che hanno l'obiettivo di garantire un livello di servizio elevato e costante nel tempo.

L'obiettivo viene raggiunto con un'organizzazione attenta del personale, una gestione programmata dei backup, un accurato e costante monitoraggio del sistema e con l'applicazione di procedure e metodologie di risoluzione dei problemi precise e consolidate.

7.4.1 Organizzazione del personale

Come previsto dal DM del 2 novembre 2005, per l'erogazione del servizio sono state definite le seguenti figure professionali:

- 1 responsabile della registrazione dei titolari
- 1 responsabile dei servizi tecnici
- 1 responsabile delle verifiche e delle ispezioni (auditing)
- 1 responsabile della sicurezza, dei log dei messaggi e del sistema di riferimento temporale

Le figure sopra elencate si avvarranno di tecnici ed operatori per l'esercizio di tutte le attività necessarie all'erogazione del servizio.

Tutto il personale adibito alla gestione del sistema possiede le competenze tecniche necessarie ed è formato sulle problematiche di natura tecnica e giuridica legate alla posta elettronica certificata in generale, ed al servizio di ARUBA PEC in particolare.

7.4.2 Gestione backup

I backup dei dati (di tutte le macchine che implementano il sistema PEC) vengono effettuato in maniera automatica su doppio dispositivo: disco e nastro LT04.

I backup ottenuti vengono conservati all'interno di locali fisici diversi in modo da garantire un più alto livello di sicurezza nel caso di eventi catastrofici quali incendi, terremoti, etc.

Vengono effettuati dei backup incrementali con cadenza giornaliera e dei backup completi con cadenza settimanale.

7.4.3 Monitoring del sistema

Tutti i servizi utilizzati all'interno della soluzione PEC, siano essi hardware o software, vengono costantemente supervisionati attraverso un'applicazione di monitor. Per ogni servizio vengono definiti, a seconda dei casi, dei valori di soglia o dei trigger che servono a stabilire quando il sistema si trova in una situazione critica che può dare origine a malfunzionamenti. Al superare dei valori di soglia, o allo scattare dei trigger, il sistema di monitor segnala, con la presenza di una lista di eventi, lo specifico malfunzionamento che è stato rilevato.

I segnali di alert vengono raccolti 7 giorni su 7, 24 ore su 24 dal personale addetto, sempre presente all'interno della web farm di ARUBA PEC.

Una importante caratteristica del sistema di Monitoring è la capacità di escludere automaticamente gli apparati del sistema nel caso in cui ne venga accertato il malfunzionamento.

7.4.4 Gestione e risoluzione dei problemi

La procedura di gestione dei problemi si basa sulla suddivisione del personale in team, ognuno dei quali ha un proprio compito ben preciso all'interno dell'organizzazione.

Il problema segnalato dal cliente o rilevato dal sistema di monitoring viene assegnato al team di "**primo soccorso**" che ha il compito di:

- individuare la gravità del problema
- individuarne l'urgenza
- individuare la persona o le persone (team di risoluzione) più indicate per la sua risoluzione
- attivare i meccanismi di comunicazione interni (team di risoluzione, customer care) ed esterni (customer are)
- aprire (se non già aperto dal cliente) un trouble ticket
- chiudere il ticket a richiesta completata.

Una volta classificato il problema secondo i livelli di urgenza e gravità previsti il problema viene assegnato al "**team di risoluzione**", il quale:

- prende in carico il problema valutandone a sua volta gravità ed urgenza
- decide se è necessario scalare il problema verso tutti i livelli superiori fino al responsabile del servizio ed all'amministratore delegato
- decide se il problema deve essere risolto nell'immediatezza o se può essere programmato un intervento di manutenzione da svolgere nel futuro
- analizza il problema ed identifica le possibili soluzioni
- decide se far intervenire risorse esterne (aziende che forniscono assistenza)

- comunica l'avvenuta risoluzione del problema al team di primo soccorso ed al customer care
- aggiorna la knowledge base

Il team di "**customer care**" ha il compito di:

- comunicare ai clienti della presa in carico dei problemi da loro assegnati
- comunicare ai clienti gli orari e le date degli interventi di manutenzione programmata che possano causare interruzioni o temporanee disfunzioni del sistema
- comunicare ai clienti il termine degli interventi di manutenzione programmata
- comunicare ai clienti l'avvenuta risoluzione dei problemi segnalati

Nella figura seguente una schematizzazione del flusso informativo tra i team che concorrono a risolvere un problema rilevato all'interno del sistema.

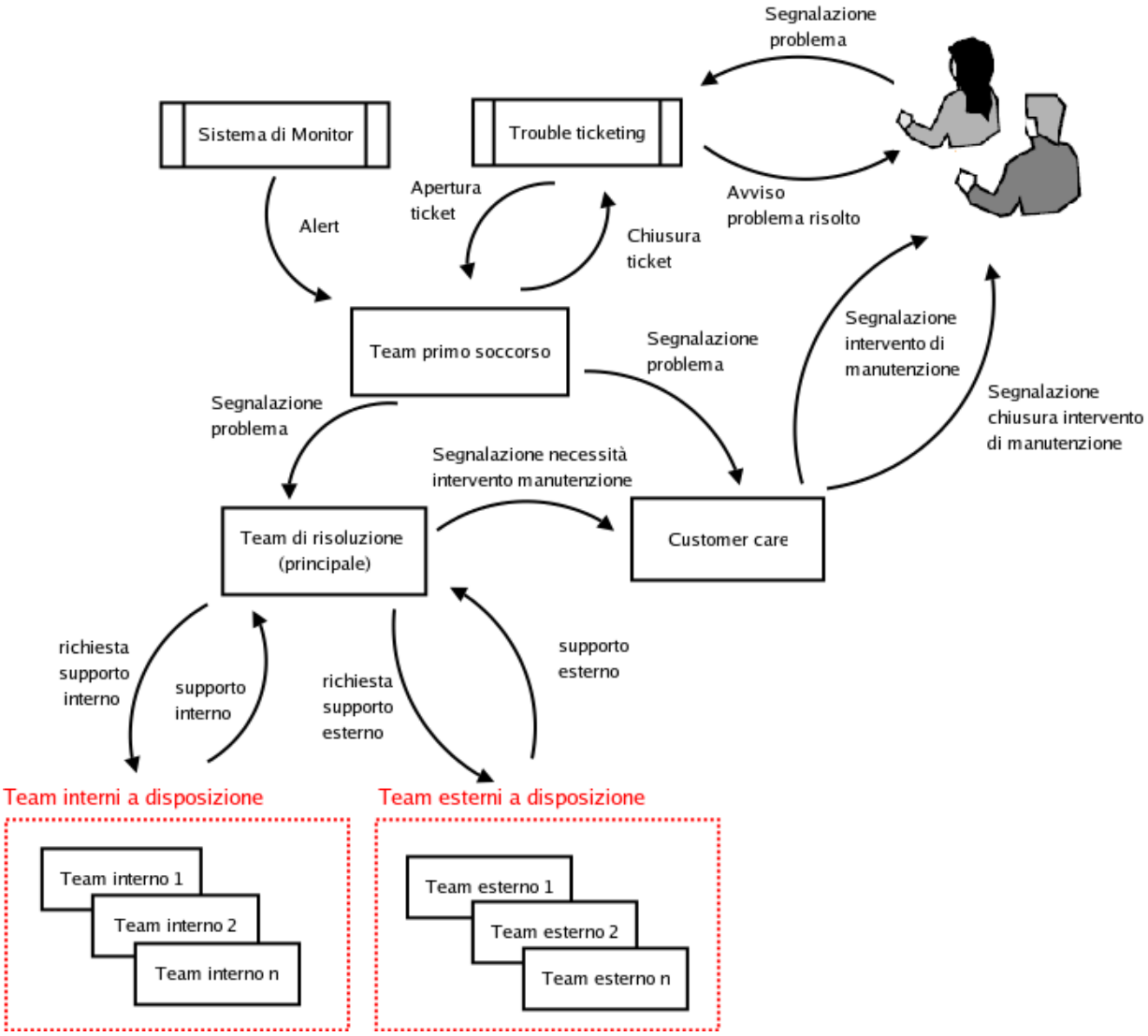


Figura 8 – Flusso di gestione dei problemi

8 – Obblighi e responsabilità

8.1 Obblighi e responsabilità del Gestore

ARUBA PEC si impegna a rispettare la normativa vigente e le Regole Tecniche contenute nel Decreto Ministeriale 2 novembre 2005 [5], in particolare a:

- garantire i livelli di servizio previsti;
- assicurare l'interoperabilità con gli altri Gestori accreditati;
- informare i titolari sulle modalità di accesso al servizio e sui necessari requisiti tecnici;
- fornire al mittente la ricevuta di presa in carico, accettazione e di avvenuta consegna del messaggio di posta elettronica certificata (salvo nel caso di eventi disastrosi improvvisi);
- comunicare al Titolare della casella di posta elettronica certificata la mancata consegna del messaggio entro le 24 ore dall'invio (salvo nel caso di eventi disastrosi improvvisi);
- apporre su ogni messaggio un riferimento temporale, sia esso il messaggio di trasporto, una ricevuta o un avviso (salvo nel caso di eventi disastrosi improvvisi);
- apporre la relativa marca temporale ai log dei messaggi generati dal sistema;
- effettuare la corretta trasmissione dal mittente al destinatario conservando l'integrità del messaggio originale nella relativa busta di trasporto (salvo nel caso di eventi disastrosi improvvisi);
- rilasciare avviso di rilevazione di virus informatici;
- rilevare la presenza di virus o eccezioni formali nei messaggi mediante avviso di non accettazione;
- rilasciare avviso di mancata consegna per superamento dei tempi massimi previsti (salvo nel caso di eventi disastrosi improvvisi);
- agire nel rispetto delle norme previste dal Decreto legislativo 30 giugno 2003, n. 196 Codice in materia di protezione dei dati personali;
- adottare misure atte ad evitare inserimento di codici eseguibili dannosi nei messaggi (virus);
- prevedere procedure e servizi di emergenza che assicurino il completamento della trasmissione anche in caso di incidenti (salvo nel caso di eventi disastrosi improvvisi);
- registrare ed associare un riferimento temporale ad ogni fase di trasmissione del messaggio sui file log, conservare e rendere disponibili detti log per gli usi e nelle modalità previste dalla legge;
- garantire la riservatezza, integrità e inalterabilità nel tempo dei file di log;assicurare la segretezza della corrispondenza trasmessa attraverso il proprio sistema;
- conservare i messaggi contenenti virus informatici per il periodo previsto dalla normativa;
- conservare le informazioni relative agli accordi stipulati con i clienti nel rispetto della normativa vigente;

- effettuare la disattivazione di una casella PEC dopo aver verificato l'autenticità della richiesta;
- fornire informazioni sulle modalità di richiesta, reperimento e presentazione all'utente dei log dei messaggi;
- utilizzare protocolli sicuri allo scopo di garantire la segretezza, l'autenticità, l'integrità delle informazioni trasmesse attraverso il sistema PEC;
- attivare la procedura di sostituzione dei certificati elettronici relativi alle proprie chiavi di firma con una tempistica tale da non causare interruzioni di servizio;
- richiedere la revoca dei certificati relativi alle chiavi utilizzate per la firma dei messaggi e per la connessione sicura al sito del CNIPA in caso di loro compromissione;
- operare in modo che non sia consentita la duplicazione abusiva e incontrollata delle chiavi private di firma o dei dispositivi che le contengono;
- consentire l'esportazione cifrata delle chiavi private di firma in modo da non diminuirne il livello di sicurezza;
- non consentire l'utilizzo delle chiavi private per scopi diversi dalla firma dei messaggi previsti dalla normativa;
- comunicare tempestivamente ai propri utenti l'eventuale cessazione o interruzione del servizio;
- consentire l'accesso logico e fisico al sistema alle sole persone autorizzate;
- utilizzare un sistema di riferimento temporale che garantisca stabilmente una sincronizzazione delle macchine coinvolte con uno scarto non superiore al minuto secondo rispetto alla scala di Tempo Universale Coordinato UTC;
- utilizzare dispositivi di firma conformi con la normativa.

8.2 Obblighi e responsabilità dei titolari

- Sollevare ARUBA PEC da ogni responsabilità in merito ai contenuti dei messaggi
- Fornire ad ARUBA PEC tutte le informazioni necessarie ad identificare la persona ed attivare il servizio, garantendo, sotto la propria responsabilità, la veridicità dei dati comunicati;
- utilizzare in modo sicuro il sistema evitando di rivelare a terzi le credenziali di accesso;
- utilizzare il servizio per i soli usi consentiti dalla legge;
- utilizzare soltanto il servizio di posta elettronica certificata erogato da Gestori accreditati (presenti nell'elenco pubblico dei Gestori tenuto dal CNIPA);
- i privati che intendono utilizzare il servizio di posta elettronica certificata nei rapporti con la Pubblica Amministrazione, devono espressamente dichiarare il proprio indirizzo. Tale dichiarazione obbliga solo il dichiarante e può essere revocata;
- le imprese, nei rapporti tra loro intercorrenti, possono dichiarare la esplicita volontà di accettare l'invio di posta elettronica certificata mediante indicazione nell'atto di iscrizione al registro delle imprese. Tale dichiarazione obbliga solo il dichiarante e può essere revocata;
- dare il consenso all'utilizzo dei propri dati personali ai sensi del DLgs 196/03;
- informare le persone abilitate all'utilizzo delle caselle sulle tematiche di sicurezza concernenti il loro uso onde evitare un uso non autorizzato;

- adottare misure atte ad evitare inserimento di codici eseguibili dannosi nei messaggi (virus);
- utilizzare, per accedere al servizio, la webmail messa a disposizione dal Gestore o i client di posta di cui al par. 5.4.1 .
- resta a cura del Titolare della casella di posta elettronica certificata la conservazione delle copie dei messaggi inviati o spediti e delle relative ricevute.

8.3 Limitazioni ed indennizzi

- ARUBA PEC non risponderà in alcun caso ai danni causati direttamente o indirettamente dagli utilizzatori del servizio imputabili ad un utilizzo improprio del sistema ed al mancato rispetto delle regole e degli obblighi contenuto nel presente manuale;
- il Gestore non potrà in alcun modo essere ritenuto responsabile, a titolo esemplificativo ma non esaustivo, per danni derivanti da cause di forza maggiore, caso fortuito, eventi catastrofici (incendi, terremoti, esplosioni) o comunque non imputabili ad ARUBA PEC che provochino ritardi, malfunzionamenti o interruzioni del servizio;
- ARUBA PEC non assume alcun obbligo riguardo la conservazione dei messaggi inviati e trasmessi attraverso le proprie caselle di PEC. Tale responsabilità viene assunta unicamente dal cliente cliente/Titolare;
- ARUBA PEC non ha alcuna responsabilità sui contenuti dei messaggi inviati e ricevuti attraverso le proprie caselle di PEC;
- la responsabilità di ARUBA PEC per ogni tipo di danno derivato dall'utilizzo del servizio, fatti salvi i casi di dolo o colpa grave, sarà limitata al doppio del corrispettivo pagato e/o dovuto per la singola casella dal Titolare secondo gli accordi contrattuali;
- qualsiasi contestazione del Titolare e/o cliente relativa all'erogazione del servizio dovrà essere comunicata ad ARUBA PEC, a pena di decadenza, entro 30 giorni dalla data dell'evento mediante raccomandata a/r;
- ARUBA PEC si riserva la facoltà di modificare il presente manuale nel caso in cui vengano apportate modifiche tecniche al sistema, variazioni all'offerta commerciale, o adeguamenti normativi.

Le limitazioni agli indennizzi stabilite da ARUBA PEC, per quanto non previsto dal presente capitolo, sono riportate nelle condizioni contrattuali di fornitura del servizio rese pubbliche nel sito del Gestore: http://www.pec.it .

8.4 Risoluzione del contratto

ARUBA PEC, nel caso in cui il servizio venga utilizzato per finalità contrarie a leggi, regolamenti, disposizioni o in violazione degli obblighi contrattuali, potrà risolvere il contratto con le modalità indicate nel contratto.

8.5 Polizza assicurativa

ARUBA PEC ha stipulato una polizza assicurativa per la copertura dei rischi e dei danni causati a terzi nell'esercizio dell'attività di Gestore di posta elettronica certificata secondo quanto previsto nel DPR n. 68 del 2005 [3]. La polizza copre i rischi derivanti dall'attività ed eventuali danni causati a terzi ai sensi del DPR 11 Febbraio 2005, n. 68 [3] con il seguente massimale:

€ 1.000.000,00	Per ogni singolo atto illecito per anno assicurativo per tutte le perdite patrimoniali derivanti da tutte le richieste di risarcimento presentate contro tutti gli assicurati per tutte le coperture assicurative combinate.

9 – Protezione dei dati personali

l presente capitolo del manuale operativo ha lo scopo di illustrare le procedure e le modalità operative adottate da ARUBA PEC, in qualità di Titolare del trattamento dei dati personali, nello svolgimento della propria attività. I dati personali relativi al richiedente la registrazione, al Titolare di certificati, al terzo interessato e a chiunque acceda al servizio, sono trattati, conservati e protetti da ARUBA PEC conformemente da quanto previsto dal Decreto Legislativo n. 196 del 30 giugno 2003 "Codice in materia di protezione dei dati personali" [1].

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

- per **Titolare del trattamento dati** si intende la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro Titolare le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza
- per **Responsabile** si intende la persona fisica, la persona giuridica., la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal Titolare, al trattamento dei dati personali
- per **Incaricato** si intende la persona fisica autorizzata a compiere operazioni di trattamento dal Titolare del trattamento dati o dal responsabile
- per **Interessato** si intende la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali

In particolare ARUBA PEC

- potrà nominare uno o più responsabili del trattamento mediante formale incarico scritto con il quale sono indicati i compiti che dovrà assolvere ai sensi del DLgs 196/03
- individua e nomina gli incaricati del trattamento che operano sotto la diretta autorità del Titolare o del responsabile attenendosi alle istruzioni impartite.

9.1 Definizione di dato personale

Ai sensi dell'art. 1 comma 2 lett. B del DLgs per dato personale si intende "qualunque informazione relativa a persona fisica, persona giuridica, ente o associazione, identificati o identificabili, anche mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale".

Dati personali saranno anche quelli relativi all'utente ovvero ad eventuali terzi e contenuti nei campi informativi presenti sui moduli e negli archivi – elettronici e/o cartacei – di registrazione, di richiesta di sospensione, di riabilitazione, di revoca, di cambio anagrafica e nei certificati di cui al presente manuale operativo.

9.2 Tutela e diritti degli interessati

In materia di trattamento dei dati personali ARUBA PEC garantisce la tutela degli interessati in ottemperanza al DLgs 196/03 e s.m.i. In particolare:

1. agli interessati sono fornite le necessarie informazioni ai sensi dell'art. 13 DLgs 196/03

2. nella suddetta informativa gli utenti saranno informati sui diritti di accesso ai dati personali ed altri diritti. (art. 7 DLgs 196/03)
3. Agli interessati verrà chiesto il consenso scritto al trattamento dei propri dati personali da parte di ARUBA PEC.

9.3 Modalità del trattamento

I dati personali sono trattati con strumenti automatizzati per il tempo strettamente necessario a conseguire gli scopi per cui sono stati raccolti.

Specifiche misure di sicurezza, come descritte nel presente manuale operativo, sono osservate per prevenire la perdita dei dati, usi illeciti o non corretti ed accessi non autorizzati.

I dati in formato elettronico sono conservati in appositi data server adibiti allo scopo.

I dati in formato cartaceo saranno conservati negli archivi cartacei di ARUBA PEC, a tali dati avranno diritto di accesso solo gli incaricati a ciò espressamente autorizzati.

9.4 Finalità del trattamento

Le finalità del trattamento sono:

1. Erogazione del servizio e gestione del rapporto contrattuale.
2. Eventuali controlli sulla qualità dei servizi e di sicurezza del sistema senza procedere, in alcun modo, al "profiling" dei dati.
3. Scopi di natura commerciale, quindi ARUBA PEC potrà utilizzare le coordinate di posta elettronica fornite al momento della sottoscrizione del contratto per inviare comunicazioni relative a prodotti e/o servizi analoghi a quelli acquistati salva in ogni caso la possibilità dell'interessato di opporsi a tale trattamento.

9.5 Altre forme di utilizzo dei dati

ARUBA PEC, per motivi d'ordine pubblico, nel rispetto delle disposizioni di legge per la sicurezza e difesa dello Stato, per la prevenzione, accertamento e/o repressione dei reati, i dati forniti potranno essere usati con altre finalità rispetto alla fornitura dei servizi ed essere comunicati a soggetti pubblici, quali forze dell'ordine, Autorità Pubbliche e Autorità Giudiziaria, per lo svolgimento delle attività di loro competenza.

9.6 Sicurezza dei dati

Come previsto dalle norme vigenti in materia, ARUBA PEC adotta idonee e preventive misure di sicurezza al fine di ridurre al minimo:

- i rischi di distruzione o perdita, anche accidentale, dei dati, di danneggiamento risorse hardware su cui sono registrati ed i locali ove vengono custoditi
- l'accesso non autorizzato ai dati stessi
- le modalità di trattamento non consentite dalla legge o dai regolamenti aziendali
- Le misure di sicurezza adottate assicurano:
- l'integrità dei dati, da intendersi come salvaguardia dell'esattezza dei dati, difesa da manomissioni o modifiche da parte di soggetti non autorizzati

- la disponibilità dei dati da intendersi come la certezza che l'accesso sia sempre possibile quando necessario; indica quindi la garanzia di fruibilità dei dati e dei servizi, evitando la perdita o la riduzione dei dati e dei servizi anche accidentale utilizzando un sistema di backup e di disaster recovery.
- la riservatezza dei dati da intendersi come garanzia che le informazioni siano accessibili solo da persone autorizzate e come protezione delle trasmissioni e controllo degli accessi stessi.

9.6.1 Trasmissione e accesso ai dati da parte dell'utente

Tutti i colloqui attraverso l'interfaccia web e il client di posta elettronica utilizzato tra l'utente ed il sistema avvengono attraverso protocolli e connessioni sicure come SMTP/S, IMAP/S, POP3/S e HTTPS, conseguentemente:

- gli utenti che usufruiranno del servizio dovranno identificarsi con username e password personali
- le credenziali di accesso ed i profili di accesso degli utenti sono gestiti da procedure supportate da strumenti software e/o hardware idonea a rendere sicura l'identificazione dell'utente.
- gli utenti autorizzati sono responsabili dell'osservanza delle procedure e delle misure di sicurezza definite da Aruba Pec.

9.6.2 Misure di sicurezza degli ambienti fisici

Aruba PEC S.p.A. garantisce idonee misure di sicurezza tramite la predisposizione ed il mantenimento di un ambiente fisico che impedisca la perdita, la sottrazione, la falsificazione o l' alterazione dei dati.

I dettagli sono elencati al paragrafo 6.9.

9.6.3 Gestione emergenze

I guasti che possono verificarsi nel sistema di PEC possono essere suddivisi in:

- guasti di normale entità
- guasti di grande rilevanza

Guasti di normale entità

I guasti di normale entità sono i guasti tipici di un sistema informatico e generalmente sono causati da malfunzionamenti software o hardware. Si tratta di problemi che non creano danni irreparabili ai dati ed ai componenti del sistema e che, nella maggior parte dei casi, possono essere risolti con interventi di manutenzione più o meno complessi.

Gli interventi possono, in genere, essere pianificati in modo da non causare fermi del servizio di PEC.

Guasti di grande rilevanza

I guasti di grande rilevanza sono i guasti che possono causare gravi danni all'intero sistema ed alle informazioni trattate, fino a rendere il servizio non disponibile anche per lunghi periodi di tempo. I guasti di grande rilevanza possono arrecare danni irreparabili e permanenti alle apparecchiature ed alle infrastrutture di rete utilizzate.

I guasti gravi possono essere causati da negligenza o incompetenza, da interventi dolosi o da eventi catastrofici etc.

Analizziamo nel seguito tutte le tipologie di malfunzionamento e, per ognuna di esse, evidenziamo il livello di criticità e la modalità con cui può essere risolto il problema ed effettuato il ripristino del sistema.

9.7 Analisi dei rischi e procedure di ripristino

I rischi di malfunzionamento possono essere catalogati in 6 macro-categorie:

1. malfunzionamenti software
2. malfunzionamenti hardware
3. inefficienza o incapacità del personale
4. inadeguatezza tecnologica
5. atti dolosi
6. eventi catastrofici

9.7.1 Malfunzionamenti software

I malfunzionamenti software possono coinvolgere tutti i componenti del sistema PEC e interazioni tra di essi, da comportamenti inusuali in presenza di carico, da eventi sporadici, ecc.

Per evitare i malfunzionamenti software il Gestore adotta le seguenti strategie:

- testing funzionale e di carico dell'intero sistema
- monitoring continuo dei singoli moduli che lo compongono
- aggiornamento del personale continuo sulle nuove release rilasciate dei prodotti
- usati e sui bug rilevati e segnalati nei forum e nelle maililng list
- utilizzo di un sistema di staging presso il quale provare le nuove release dei prodotti
- prima di installarle in produzione
- ridondanza delle applicazioni
- possibilità di estendere in qualsiasi momento l'architettura (data la sua modularità)

Data la ridondanza del sistema gli eventuali interventi di manutenzione e di upgrade dei moduli software possono essere svolti in tempi diversi sulle singole macchine evitando, in questo modo, dei fermi servizio.

9.7.2 Malfunzionamenti hardware

I malfunzionamenti hardware possono coinvolgere tutte le macchine ed i dispositivi di rete coinvolte nell'erogazione del servizio.

Come descritto dall'architettura riportata al par. 5.4, il sistema è altamente ridondato e non esiste alcun servizio che venga erogato su una singola macchina.

In caso di malfunzionamento di una apparecchiatura il sistema continua a funzionare mentre il device viene inviato al servizio di assistenza tecnica. Nel frattempo la macchina potrà, se necessario, essere sostituita da una macchina analoga.

9.7.3 Inefficienza o incapacità del personale

Il personale adibito al sistema PEC viene istruito opportunamente attraverso corsi di formazione interni attraverso i quali gli incaricati imparano ad operare sul sistema e ad utilizzare le procedure di manutenzione, gestione, assistenza e ripristino previste dalle particolari mansioni loro assegnate.

Durante la formazione viene dato particolare risalto all'importanza ed alla criticità del servizio erogato ed alla necessità di prestare la maggior cura ed accortezza possibile nello svolgimento dei compiti assegnati.

I responsabili dei singoli servizi elencati al cap. 7 sono anche i responsabili del personale che opera all'interno di quel servizio.

9.7.4 Inadeguatezza tecnologica

Il sistema proposto risulta sovradimensionato rispetto alle previsioni iniziali di carico ed alle reali esigenze del servizio.

Riteniamo pertanto che la soluzione di ARUBA PEC sia tecnicamente valida e tecnologicamente adeguata per svolgere le funzioni per le quali è stata creata.

Precisiamo comunque che il sistema è modulare ed altamente scalabile sia in direzione orizzontale che verticale come descritto al par. 5.4 e può pertanto, in qualsiasi momento, essere esteso ed adeguato alle esigenze di performance e carico che dovessero nascere nel futuro.

9.7.5 Atti dolosi

I malfunzionamenti del sistema possono essere causati da atti dolosi provenienti dall'interno e dall'esterno della struttura operativa di ARUBA PEC.

Vengono adottati i seguenti accorgimenti per contrastare eventuali atti dolosi **interni**:

- cura ed attenzione nella scelta del personale da adibire alle mansioni inerenti la PEC
- immediato intervento di rimozione e sostituzione del personale in caso di
- comportamenti sleali
- accesso controllato (sistema a controllo biometrico) ai locali nei quali viene erogato il servizio

Gli atti dolosi **esterni** possono essere prevenuti con:

- un sistema di Firewall/ Intrusion Detection efficiente ed aggiornato
- un sistema antivirus aggiornato
- un controllo continuo e sistematico delle macchine e degli apparati di rete idoneo a rilevare eventuali intrusioni indesiderate.

Nel caso in cui venga registrato un attacco esterno che provochi un malfunzionamento al sistema PEC, ARUBA PEC si adopererà per:

- risolvere in tempi rapidi il problema utilizzando tutti i mezzi a disposizione: dalla esclusione delle macchine che presentano malfunzionamenti, all'aggiunta di nuove apparecchiature, all'utilizzo delle copie di backup, ecc.
- indagare per capire se le altre macchine possono aver subito dei danni
- denunciare l'attacco agli organi competenti, se ritenuto opportuno.

9.7.6 Eventi catastrofici

Come eventi catastrofici intendiamo tutti quegli eventi imprevedibili ed indipendenti dall'attività del Gestore quali incendi, terremoti, allagamenti (e in genere calamità naturali), guasti alle linee elettriche o dei carrier, ecc..

L'infrastruttura di ARUBA PEC prevede una serie di accorgimenti per contrastare, prevenire e, dove possibile, superare i problemi causati da eventi esterni

- ridondanza della connettività
- presenza di più gruppi elettrogeni
- dispositivi di rilevazione fumo ed incendio
- presenza estintori
- ridondanza sistemi di refrigerazione.

I tempi di ripristino del sistema non sono ovviamente pronosticabili e dipendono, quasi esclusivamente, dai danni provocati. Come tempo massimo di ripristino possiamo prendere in considerazione il caso peggiore nel quale l'intero sistema sia inutilizzabile. In tal caso il tempo di ripristino corrisponde al tempo di messa in opera di un sistema ex-novo che possiamo stimare in 48 ore.

9.7.7 Azioni promosse dal Gestore in caso di malfunzionamento

In base alla circolare CNIPA n.51 del 7 dicembre 2006, il Gestore è tenuto a informare il CNIPA dei malfunzionamenti riscontrati nel proprio sistema entro 30 minuti dal suo presentarsi. Nella segnalazione il Gestore deve fornire anche "una prima valutazione dell'incidente e descrivere le eventuali misure adottate a riguardo".

I disservizi vengono catalogati in base alla seguente tabella:

Tipologia	Codice	Descrizione
Comportamento Anomalo non circoscritto	1A rilevato dal Gestore	Comportamento difforme dalle regole tecniche di cui all'art. 17 del DPR 11 febbraio 2005, n.68, relativo alle funzioni base (trattamento del messaggio originario, ricevute ed avvisi) per il quale non è circoscritto il potenziale impatto
	1B rilevato da terzi	
Comportamento Anomalo circoscritto	2A rilevato dal Gestore	Comportamento difforme dalle regole tecniche di cui all'art. 17 del DPR 11 febbraio 2005, n.68, relativo alle funzioni base (trattamento del messaggio originario,

Tipologia	Codice	Descrizione
	2B rilevato da terzi	ricevute ed avvisi) per il quale è circoscritto il potenziale impatto
Malfunzionamento bloccante	3A rilevato dal Gestore	Tipologia di malfunzionamento a causa del quale le funzionalità del sistema PEC, come definite nelle regole tecniche di cui all'art. 17 del DPR 11 febbraio 2005, n.68, non possono essere utilizzate in tutto o in parte dagli utenti
	3B rilevato da terzi	
Malfunzionamento grave	4A rilevato dal Gestore	Tipologia di malfunzionamento a causa del quale in alcune circostanze le funzionalità del sistema PEC, come definite nelle regole tecniche di cui all'art. 17 del DPR 11 febbraio 2005, n.68, non possono essere utilizzate in tutto o in parte dagli utenti
	4B rilevato da terzi	
Malfunzionamento	5B rilevato dal Gestore	Situazione a causa della quale le funzionalità del sistema PEC, come definite nelle regole tecniche di cui all'art. 17 del DPR 11 febbraio 2005, n.68, in tutto o in parte, risultano degradate ovvero il sistema ha un comportamento anomalo in situazioni circoscritte e per funzionalità secondarie (esclusi: la procedura di identificazione, i messaggi originari, le ricevute, gli avvisi e le buste)
	5B rilevato da terzi	

Le segnalazioni degli utenti vengono catalogati in base ai seguenti codici identificativi:

Codice	Descrizione
RC	Segnalazione di un reclamo relativo al rapporto contrattuale
AL	Segnalazione di un reclamo relativo alla procedura di accesso ai log
SA	Segnalazione di anomalia/disservizio non imputabili al Gestore (client, collegamento a internet, gestione utenze decentrate)

Nei casi 1A e 1B il Gestore auto-sospenderà il servizio informando i propri utenti e gli altri Gestori.

Nei casi 2A e 2B i CNIPA può decidere di sospendere il servizio del Gestore fino a quando il problema è stato risolto. In entrambi i casi il Gestore attua la sospensione producendo un "avviso di non accettazione per eccezioni formali" e non producendo la "ricevuta di presa in carico".

Nel caso di sospensione il Gestore, una volta eliminato il disservizio può riprendere l'attività. In tal caso deve inviare al CNIPA una relazione dettagliata su quanto accaduto e sui provvedimenti adottati.

10 – Bibliografia

[1] Decreto Legislativo 30 giugno 2003, n. 196, "Codice in materia di protezione dei dati personali".

[2] Decreto del Presidente della Repubblica N. 445 del 28/12/2000: Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa

[3] Decreto del Presidente della Repubblica N. 68 del 11/2/2005: "Regolamento recante disposizioni per l'utilizzo della posta elettronica certificata, a norma dell'articolo 27 della legge 16 gennaio 2003, n.3.

[4] Decreto Legislativo del 7 marzo 2005 n. 82 "Codice dell'Amministrazione Digitale

[5] Decreto Ministeriale del 2 novembre 2005: "Regole tecniche per la formazione, la trasmissione, la validazione, anche temporale, della posta elettronica certificata"

[6] Circolare CNIPA N. 49 del 24 novembre 2005: 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.

[7] Decreto legge n. 185 del 29/11/2008 convertito nella legge n. 2 del 28/01/2009.

Arezzo, 20/02/2009

Aruba PEC S.p.A.
Il legale rappresentante
(Simone Braccagni)