Actalis S.p.A.

Manuale Operativo Posta Elettronica Certificata v.1.3

Versione: 1.3
Data approvazione: 26/07/2021
Redazione: Alessandro Capobianco, Valeria Favasuli
Verificato da: Marco Menonna, Federico Ciofi
Approvato da: Andrea Sassetti
Classificazione documento: Pubblico

Andrea Sassetti
Firmato digitalmente il 26/07/2021 14:52:41 CEST

VERS. N°	DATA	NATURA DELLA MODIFICA
ACCPEC-00-02-01	10/07/2006	Prima versione del documento
ACCPEC-00-02-02	10/07/2016	Frontespizio documento Modifica Verificatore e Approvatore del documento Paragrafo 1.3 Inserito Riferimento Codice Pa digitale Paragrafo 2.1 Modifica rappresentante legale dell'Azienda Paragrafo 3.1 Modifica Figura 1 e commenti alla figura Paragrafo 3.2.1 Inserimento riferimento al Codice riservato personale per accedere ai servizi di perdita password e richiesta informazioni sui log dei messaggi. Paragrafo 5 Inserimento commento relativo all'indipendenza del prezzo della casella dal traffico effettuato su di essa. Paragrafo 6 Eliminati i riferimenti ai protocolli di accesso alla casella di posta, in quanto descritti nei paragrafi successivi Paragrafo 6.1.1 Modifica istruzioni di creazione account di posta Paragrafo 6.1.2 Modifica istruzioni di configurazione client di posta Paragrafo 7 Inserimento commento a garanzia invio messaggi Paragrafo 10.2 Eliminato ultimo capoverso Paragrafo 10.3 Eliminato riferimento al Manuale della qualità Paragrafo 10.5.1 Eliminato riferimento al Piano per la sicurezza Paragrafo 11.1 Inserito riferimento al Codice riservato personale

ACCPEC-00-02-03	10/12/2007	Frontespizio Modifica Redattore ed Approvatore documento Paragrafo 1.3 Inserimento Circolare CNIPA [CR/51-2006] e D.lgs 196/2003 Paragrafo 2.4 Modifica responsabile Manuale Operativo Paragrafo 5 Inseriti nuovi acronimi Inserito Paragrafo Descritta la modalità di vendita on line caselle di PEC su dominio actalispec Paragrafo 8.1.2 Eliminato riferimento al [DPR 445/2000] Paragrafo 9.1 Sostituito riferimento al [DPR 445/2000] con riferimento al [D.Lgs 82] Paragrafo 10.1 Eliminati riferimenti agli standard di sicurezza BS ISO/IEC 17799:2000 BS 7799-1:2000 Paragrafo 10.4.2 Eliminati riferimenti alla policy di sicurezza delle informazioni ed inseriti riferimenti all'addestramento connesso all'erogazione del servizio Paragrafo 10.6 Eliminati riferimento alla denominazione della sala in cui sono ubicati i sistemi di monitoraggio. Paragrafo 10.6.1 e 10.6.2 Eliminati paragrafi "gestione della documentazione dei servizi" e "Gestione della capacity planning" e rassegnata la numerazione. Paragrafo 10.9 Inserite precisazioni sull'accesso fisico Paragrafi 10.12 ed 11 Eliminato riferimento all'Allegato 3 2.6 Inseriti nuovi acronimi. 3 Revisionato intero contenuto del paragrafo. 3.2.1 Eliminato riferimento ai documenti di riconoscimento 3.2.2 Inserite specifiche sull'Organizzazione. 3.3 Inserito riferimento a nuova modalità di accesso applicativo. 4.1, 4.2 Inserito riferimento alla generazione di più domini per uno stesso cliente. 4.3 Inserite precisazioni sulla facoltatività del servizio 5 Eliminata l'indicazione precisa della grandezza delle caselle di PEC. Inserita specifica sulla vendita online. 6.1 Inserite specifiche sulle porte 25 e 465 6.1.1 Inserite specifiche sui protocolli sicuri. 6.1.2 Eliminato la descrizione dettagliata della configurazione del client Outlok Express 7 Eliminato riferimento alle caselle di 100 Mb. 8.1.2 Inseriti obblighi del Cliente sulla riservatezza. 8.1.3 Inserito nuova paragrafo su informativa e consenso 9.2 Inserito contenuto ne parag. 9.3 9.2.1 Inserito nuova paragrafo su responsabilità del Gestore 9.2.3 Inserito nuova paragrafo su responsabilità contenuti e dati trasmessi 9.4 Inserito nuova paragrafo su responsabilità del cliente e degli utenti 12.8 Sostituto "cancellazione" con "disattivazione". Previsto il ripristino della casella disattivata e precisata la procedura. 2.2 Inserito nuovo paragrafo 2.5 Precisate modalità di aggiornamento
ACCPEC-00-02-04	03/10/2008	2.6 Inseriti acronimi CCIAA, SPC. Storia delle modifiche Allineati riferimenti/contenuti alle modifiche apportate con la versione 3 del documento 4.3 Specificate modalità di fruizione del servizio antispam. 3.2.1 Specificate modalità di identificazione dell'utente. 3.2.2 Specificate modalità di identificazione del titolare. 11.1 Specificate modalità di richiesta/evasione dei log dei messaggi. 4.6 Inserito paragrafo sulle liste di distribuzione 3.2.1 Integrato paragrafo 4.5 con parag. 3.2.1 4.6 Inserito paragrafo sull'archiviazione
ACCPEC-00-02-05	08/02/2010	- Modificato il frontespizio 2.4 Modificato il responsabile del Manuale Operativo 2.1 Aggiornati i dati identificativi di Actalis

ACCPEC-00-02-06	08/08/2010	-	Modificato il frontespizio
		4.5	Modificato il nome del paragrafo
		4.6	Modificato il nome del paragrafo
		4.7	Aggiunto paragrafo
		6.1.1.1	Aggiunto paragrafo
		6.1.1.2	Aggiunto paragrafo
		6.2	Modificati indirizzi delle webmail
ACCPEC-00-02-07	21/01/2011	7	Modifica limiti servizio
		2.1	Modifica Rappresentante legale
ACCPEC-00-02-08	10/09/2013	4.6	Modifica descrizione servizio
		4.7	Inserimento nuovo servizio di archivio
		4.8	Inserimenti servizio Multiutenza
		2.1	Modifica ubicazione dei server
ACCPEC-00-02-09	17/04/2013	2.1	Modifica del rappresentante legale
		7.1	Inserito Paragrafo Disaster Recovery
1.0	21/11/2017	Nuova edizione del documento sul template del gruppo Aruba	
1.1	n.a.	Non pubblicata	
1.2	15/09/2020	Eliminazione del logo Aruba Group. **1.3.** Eseguite modifiche minori alle definizioni; **2.3.** Eliminati i riferimenti ad AgID; **3:** Aggiornati i riferimenti normativi; **3:** Aggiornati i riferimenti normativi; **4.2.4:** Aggiornata la descrizione delle comunicazioni; **4.2.5:** aggiornata la descrizione del sistema antispam; **5.5:** modificata figura 3 e corretti refusi; **5.6:** modificati i riferimenti al sistema utilizzato per i riferimenti temporali; **5.9.1:** modifiche nella descrizione della connettività; da **6.2** a **6.5.4:** eseguite piccole correzioni; **6.3:** Aggiunti i riferimenti alla limitazione delle estensioni gestite; 6.**5.1:** inserita la figura del responsabile della sicurezza dei log; **6.5.2:** eseguite piccole correzioni; **6.5.4:** Modificato l'intero capitolo e la figura; **7.1:** Aggiornata la descrizione; **7.2:** eseguite piccole correzioni; **7.3**: Eliminati riferimenti obsoleti e non più attinenti; **7.3.4:** eseguite piccole correzioni; **7.3.9:** sostituito il paragrafo "*Raccomandazioni per un corretto e sicuro utilizzo del servizio*" sulle Password Policy; **7.4.1**: eliminato; **7.4.2**: eliminato**; 7.4.3:** rivista numerazione ed eseguite piccole correzioni; **7.4.4**: rivista numerazione; **7.5**: piccole modifiche agli indicatori di qualità; e **8.1**: inseriti i riferimenti al GDPR. Spostato il cap. misure di sicurezza dal 9.7 al cap. 6.3 e 6.4; **8.3** Modifiche al modello di responsabilità	
1.3	26/07/2021	**1.3:** modifiche a definizioni e acronimi e ordinamento alfabetico; **4.1:** modifiche a introduzione; **4.2:** piccole correzioni al paragrafo;**4.2.4:** modifica al paragrafo comunicazioni con indirizzi email non certificati; **5.5**: modifiche alla figura e alla descrizione dell'architettura con descrizione della componente di verifica; **6.3.1:** piccole modifiche al paragrafo; **6.3.3:** aggiunte caratteristiche di sicurezza; **7.2.2:** modifiche al paragrafo; **7.3.1:** modifiche al paragrafo; **7.3.4:** piccole correzioni al paragrafo; **7.3.6:** inserito divieto di riassegnazione; **7.3.7:** piccole modifiche al paragrafo; **7.3.9:** piccole modifiche al paragrafo; **7.4.2:** piccole modifiche al paragrafo; **8.3:** modifiche al paragrafo.	

1 Sommario

1. Informazioni di carattere generale

1.1 Scopo

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

1.2 Versione del manuale e responsabilità

Actalis è responsabile della stesura del presente documento.

La versione del manuale e le singole responsabilità dei redattori e supervisori sono riportate a pagina 1.

1.3 Definizioni ed acronimi

Agenzia per l'Italia Digitale (AgID)	Ente Nazionale per la digitalizzazione della Pubblica Amministrazione (già DIGITPA e CNIPA).
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.
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 è impossibilitato ad accettare il messaggio in ingresso, recante la motivazione per cui non è possibile accettare il messaggio e l'esplicitazione che il messaggio non potrà essere consegnato al destinatario.
Busta di anomalia	La busta, sottoscritta con la firma del Gestore di posta elettronica certificata del destinatario, nella quale è inserito un messaggio errato ovvero non di posta elettronica certificata e consegnata ad un Titolare, per evidenziare al destinatario detta anomalia.
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.
Casella di posta elettronica certificata	È la casella di posta elettronica definita all'interno di un dominio di posta elettronica certificata ed alla quale è associata una funzione che rilascia ricevute di avvenuta consegna al ricevimento di messaggi di posta elettronica certificata.
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.
Dominio di posta elettronica certificata	È un dominio, fully qualified domain name (FQDN), di posta elettronica certificata dedicato alle caselle di posta elettronica certificata.
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.
Gestore di posta elettronica certificata	È 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.
HSM	Hardware Security Module. È un dispositivo hardware per la generazione, la memorizzazione e la protezione sicura di chiavi crittografiche.
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.

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).
Indice dei Gestori di posta elettronica certificata	È 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.
LDAP	Lightweight Directory Access Protocol. È 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.
LMTP	Local Mail Transport Protocol
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.
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.
MTA	Mail Transfer Agent. È un modulo che ha il compito di effettuare il dispatching dei messaggi di posta elettronica (invio e ricezione)
NTP	Network Time Protocol
Partner (provider)	È il soggetto (Ente Pubblico, Aziende, ecc.) attraverso il quale viene offerto il servizio di Posta Elettronica Certificata di Actalis S.p.A. ai Titolari. Talvolta il partner è chiamato anche *provider.*
PEC	Posta Elettronica Certificata
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 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.
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.
Ricevuta breve di avvenuta consegna	La ricevuta nella quale sono contenuti i dati di certificazione ed un estratto del messaggio originale.
Ricevuta completa di avvenuta consegna	La ricevuta nella quale sono contenuti i dati di certificazione ed il messaggio originale.
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.
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 è inserito nella casella di posta elettronica certificata del 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 sintetica di avvenuta consegna	La ricevuta che contiene i dati di certificazione.
Riferimento temporale	Informazione contenente la data e l'ora che viene associata ad un messaggio di posta elettronica certificata.
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.
SNMP	Simple Network Management Protocol. È un protocollo utilizzato per la gestione ed il monitoring degli apparati di rete
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.
Titolare	È il soggetto a cui è assegnata una casella di posta elettronica certificata
TSA	Time Stamping Authority. Autorità che realizza il servizio di marcatura temporale di documenti informatici.
Utente	Persona che fruisce del servizio di Posta Elettronica Certificata

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 21 maggio 2009 emessa dal CNIPA (CNIPA/CR/56).

Manuale Operativo	**Circolare 21 maggio 2009, n. CNIPA/CR/56 2.1 Manuale Operativo.**
Cap. 2	**Punto a:** Dati identificativi del Gestore
Par. 2.1	**Punto b:** Indicazione del responsabile del manuale
Cap. 3	**Punto c:** Riferimenti normativi necessari per la verifica dei contenuti
Par. 2.4	**Punto d:** Indirizzo del sito web del Gestore ove il manuale è pubblicato e scaricabile
Cap. 6	**Punto e:** Indicazione delle procedure oltre che degli standard tecnologici e di sicurezza utilizzati dal Gestore nell'erogazione del servizio
Par. 1.3	**Punto f:** Definizioni, abbreviazioni e termini tecnici

Manuale Operativo	Circolare 21 maggio 2009, n. CNIPA/CR/56 2.1 Manuale Operativo.
Cap. 5, cap. 7	**Punto g:** Descrizione e modalità del servizio offerto
Par. 7.3.9	**Punto h:** Descrizione delle modalità di reperimento e di presentazione delle informazioni presenti nei log dei messaggi
Par. 7.3	**Punto i:** Indicazione delle modalità di accesso e fornitura del servizio
Par. 7.5	**Punto j:** 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
Cap. 8, Cap. 9	**Punto k:** Indicazione delle modalità di protezione dei dati dei titolari delle caselle, gli obblighi e le 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
Par. 7.7	**Punto l:** Indicazione delle procedure operative da attuare nel caso di cessazione dell'attività di gestore di posta elettronica certificata
Par. 1.2	**Punto m:** Indicazione della versione del manuale

2. Dati identificativi del Gestore

Actalis S.p.A, società del Gruppo Aruba da marzo 2009, progetta, realizza e gestisce servizi e soluzioni nel campo dei servizi fiduciari. Gestore PEC Certificato e Certification Authority accreditata presso l'AgID, opera insieme alle altre società del gruppo offrendo prodotti e servizi rivolti ad un'utenza business, sia pubblica che privata, tra cui servizi di firma digitale, posta elettronica certificata, conservazione sostitutiva e soluzioni di autenticazione e certificazione.

Gli uffici di Actalis sono a Ponte San Pietro (BG), via San Clemente 53, dove pure si trovano la sede legale e la Direzione della società.

All'erogazione dei servizi di Actalis collaborano anche risorse della società Aruba PEC S.p.A. (anch'essa, come Actalis, controllata da Aruba S.p.A.) e della capogruppo Aruba S.p.A.

Il servizio di Posta Elettronica Certificata (PEC) è erogato dall'organizzazione identificata come segue:

Dati identificativi del Gestore	
Ragione Sociale:	Actalis S.p.A.
Sede Legale:	Via San Clemente, 53 24036 – Ponte San Pietro (BG) 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

Dati identificativi del Gestore	
Sede di erogazione del servizio:	Via Piero Gobetti, 96 52100 - Arezzo (AR) Tel.: +39 0575 0500 Fax: +39 0575 862020
Partita IVA:	03358520967
Registro delle imprese:	Iscritta al registro delle imprese di Bergamo con numero 03358520967
REA:	436479
Sito web principale:	https://www.actalis.it
E-mail (generale):	info@actalis.it

2.1 Responsabile del Manuale Operativo

Il responsabile del presente manuale operativo è Andrea Sassetti.

Il responsabile può essere contattato ai recapiti

tel.: +39-0575-0500

email: info@actalis.it

indirizzo: Via San Clemente, 53 4036 Ponte San Pietro (BG)

2.2 Canali di comunicazione

Oltre ai riferimenti riportati nel precedente paragrafo, il Gestore può essere contattato attraverso i canali di seguito specificati.

2.2.1 Call Center

tel.: +39-0575-050360 (dal lunedì al venerdì, dalle 9.00 alle 13.00 e dalle 14.30 alle 17.30)

web: www.actalis.it

2.2.2 Assistenza tecnica sul servizio

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

tel.: +39-0575-050360 (dal lunedì al venerdì, dalle 9.00 alle 13.00 e dalle 14.30 alle 17.30)

web: www.actalis.it

2.2.3 Network Operations Center (NOC)

Emergenze tecniche tra Gestori

tel.: +39-0575-050012

fax: +39-0575-862020

email: noc@comunicazioni.pec.aruba.it

web: www.actalis.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 Actalis.

Actalis 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.

2.4 Indirizzo web del Gestore dal quale scaricare il manuale

All'interno del sito web del Gestore (www.actalis.it) è disponibile la copia in formato pdf del presente documento. Il file può essere scaricato all'indirizzo https://www.actalis.it/area-download.aspx.

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

2.5 Certificazioni ISO

Il sistema di gestione della qualità (QMS) di Actalis è certificato conforme allo standard ISO 9001:2015, ed è aggiornato alla revisione 2015 della norma.

Actalis ha definito e posto in opera un SGSI (Sistema di Gestione della Sicurezza delle Informazioni) conforme alla norma ISO/IEC 27001:2013 che copre tutte le aree aziendali, incluse quelle coinvolte nello sviluppo ed erogazione del servizio PEC. Tale SGSI è certificato ISO/IEC 27001:2013.

La situazione aggiornata delle certificazioni aziendali può essere visionata sia alla pagina https://www.actalis.it/chi-siamo/certificazioni-iso.aspx che sul sito della capogruppo Aruba S.p.A. all'indirizzo https://www.aruba.it/certificazioni.aspx.

3. Riferimenti normativi

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

[2] Il Decreto del Presidente della Repubblica 28 dicembre 2000 n. 445 e s.m.i. – Testo Unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa.

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

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

[5] Il Decreto Ministeriale del 2 novembre 2005 "Regole Tecniche per la formazione, la trasmissione e la validazione, anche temporale, della posta elettronica certificata e allegato **Regole tecniche del servizio di trasmissione di documenti informatici** mediante posta elettronica certificata.

[6] Circolare CNIPA **n. 56 del 21 maggio 2009** - Modalità per la 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] Il Decreto legge n. 185 del 29/11/2008 convertito nella legge n. 2 del 28/01/2009 Misure urgenti per il sostegno a famiglie, lavoro, occupazione e impresa e per ridisegnare in funzione anti-crisi il quadro strategico nazionale convertito nella **Legge 28 gennaio 2009, n. 2** - Conversione in legge, con modificazioni, del decreto-legge 29 novembre 2008, n. 185, recante misure urgenti per il sostegno a famiglie, lavoro, occupazione e impresa e per ridisegnare in funzione anti-crisi il quadro strategico nazionale.

[8] Circolare CNIPA 7 dicembre 2006, n. 51 - Espletamento della vigilanza e del controllo sulle attività esercitate dagli iscritti nell'elenco dei gestori di posta elettronica certificata (PEC), di cui all'articolo 14 del decreto del Presidente della Repubblica 11 febbraio 2005, n. 68, «Regolamento recante disposizioni per l'utilizzo della posta elettronica certificata, a norma dell'articolo 27 della legge 16 gennaio 2003, n. 3».

[9] Regolamento (UE) 2016/679 ("GDPR") del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE.

[10] Regolamento (UE) 2014/910 ("EIDAS") del Parlamento Europeo e del Consiglio del 23 luglio 2014 in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE.

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 non identifica né il mittente né il destinatario ma certifica soltanto il canale di comunicazione tra gli stessi.

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 AgID (già CNIPA e DIGITPA). 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.

4.2 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 certificati e vengono evidenziati in rosso i percorsi del messaggio originale dal mittente al destinatario ed in verde i percorsi della ricevuta.

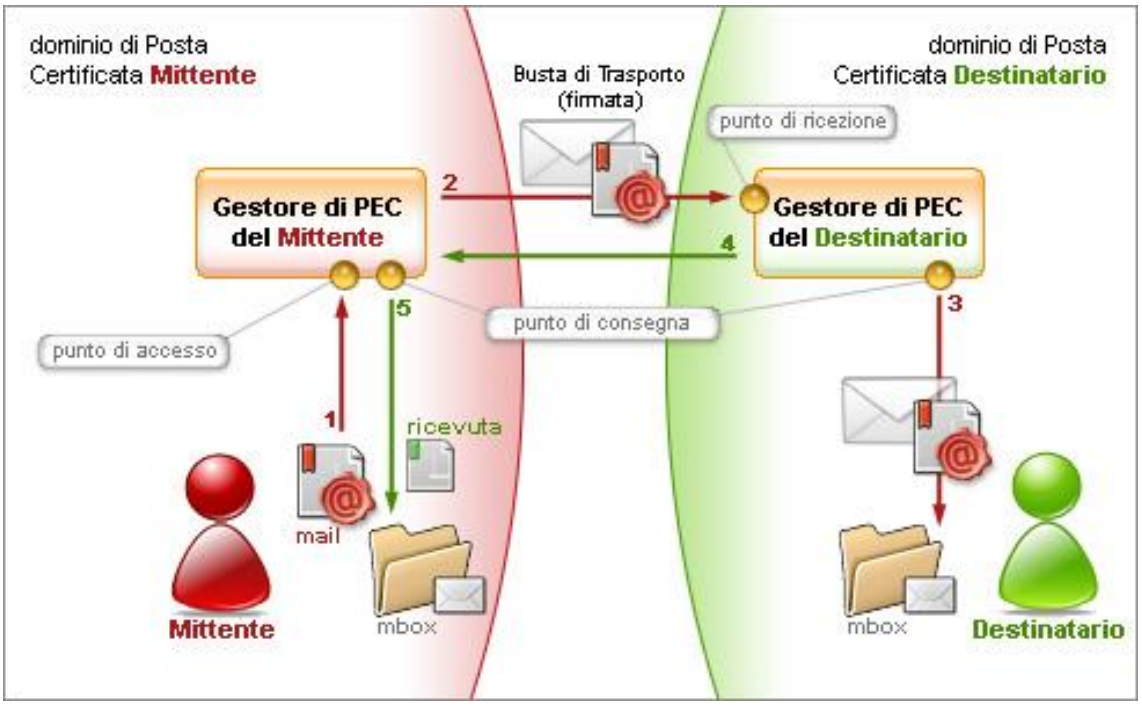


Figura 1 - Funzionamento di un sistema di PEC

Nel dettaglio: quando il mittente possessore di una casella di PEC invia un messaggio ad un altro indirizzo di posta elettronica certificata (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, il messaggio viene indirizzato 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.

4.2.1 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**.

4.2.2 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**.

In accordo a quanto definito dalle "Istruzioni per la conservazione dei Log dei messaggi e dei messaggi di Posta elettronica certificata con Virus", v.1.0. pubblicate da AgID il 5 luglio 2016, i log dei messaggi contenenti virus vengono conservati per un periodo di 30 mesi.

4.2.3 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***.

4.2.4 Comunicazioni con indirizzi email non certificati

Messaggi da caselle PEC a caselle di posta elettronica ordinaria

Nel caso di invio di email da caselle di PEC a caselle di posta elettronica ordinaria, la casella PEC riceverà la Ricevuta di Accettazione ma non quella di Avvenuta Consegna.

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

Messaggi da caselle di posta elettronica ordinaria a caselle PEC

Per quanto riguarda i messaggi di posta elettronica ordinaria (non PEC), il Titolare del servizio ha la possibilità di decidere tramite il pannello di Gestione Mail PEC se accettarli oppure scartarli.

Nel caso in cui decida di accettarli, potrà scegliere la cartella verso cui spostarli; in questo caso è possibile (ed è consigliato) attivare il filtro antispam.

Nel caso in cui decida di non accettarli, può decidere di rifiutarli oppure di inoltrarli ad una casella a sua scelta.

4.2.5 Antispam

È possibile utilizzare il servizio antispam per filtrare i messaggi di posta tradizionale in arrivo alle caselle PEC del Gestore. In tal caso il Titolare ha la possibilità di scegliere l'azione da intraprendere ogni qual volta venga rilevato un possibile caso di spamming:

- spostare il messaggio sotto un'apposita cartella Spam;
- eliminare il messaggio.

L'Utente esperto ha infine la possibilità di affinare le regole antispam impostando, ad esempio, il grado di sensibilità del filtro, le lingue dalle quali riceve abitualmente le comunicazioni, ecc.

5. Descrizione della soluzione tecnica definita da ACTALIS

5.1 Principali caratteristiche

La soluzione di Actalis presenta le seguenti caratteristiche:

- È conforme alle specifiche AgID/DIGITPA/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 una Time Stamping Authority 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*).

5.2 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.

5.3 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://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf)

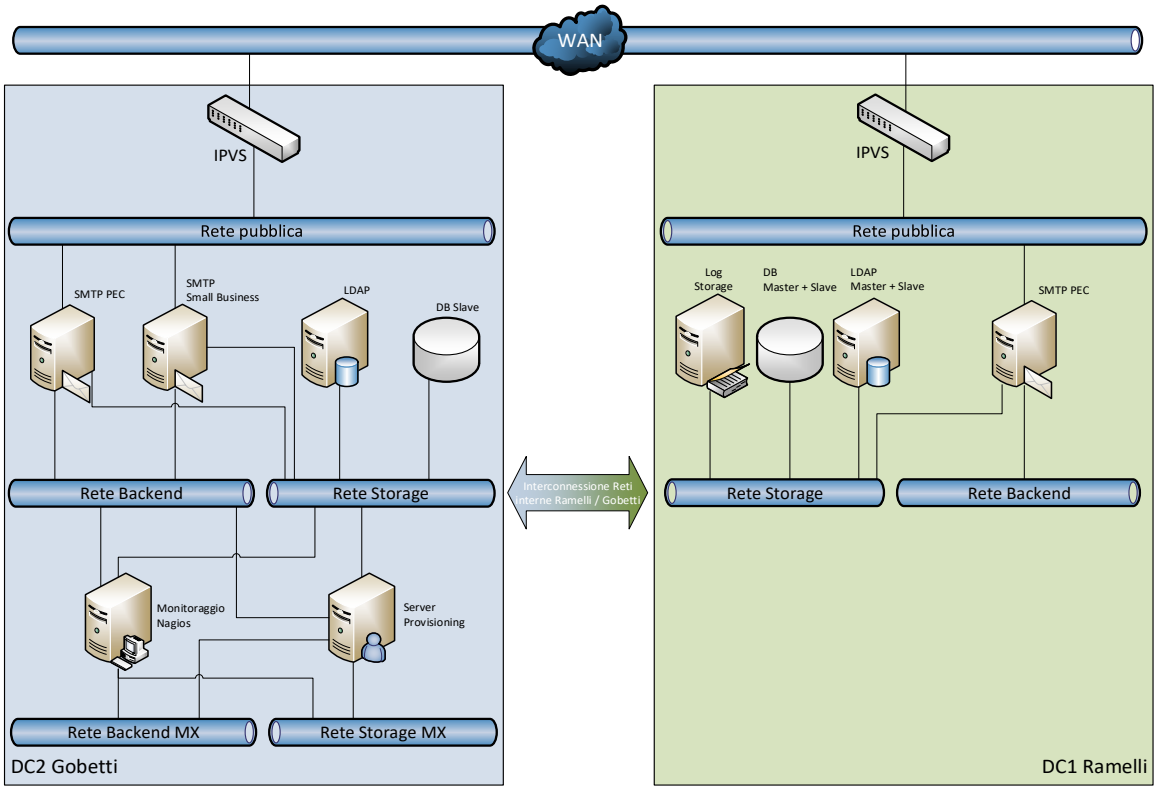
Inoltre, i dispositivi HSM utilizzati possiedono anche la certificazione Common Criteria livello EAL4+ (https://www.commoncriteriaportal.org/products/).

5.4 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 vedere dallo schema riportato di seguito il sistema è strutturato *logicamente* su 3 livelli.



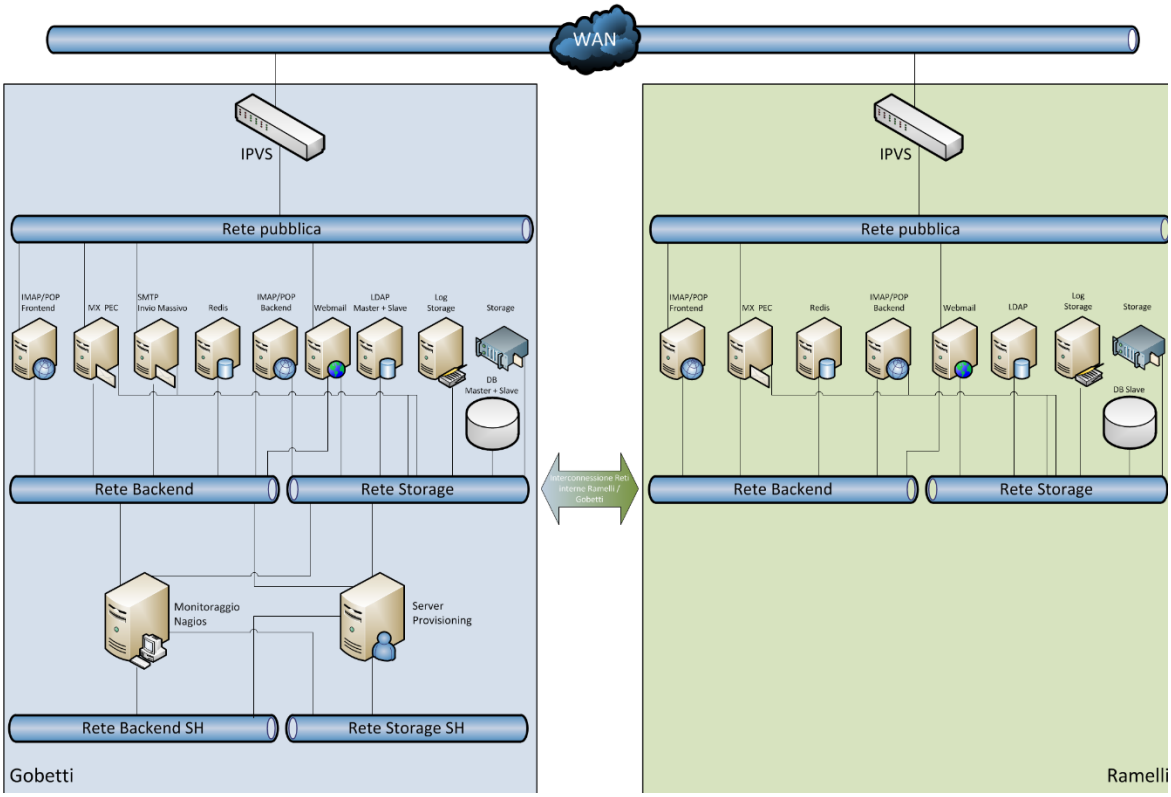


Figura 2 - Architettura di massima del sistema

5.4.1 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.

5.4.2 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 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 attraverso il protocollo NTP fornito dall'istituto nazionale di ricerca metrologica –INRiM (http://rime.inrim.it/labtf/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.

5.4.3 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 (AgID).

5.5 Architettura della soluzione

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

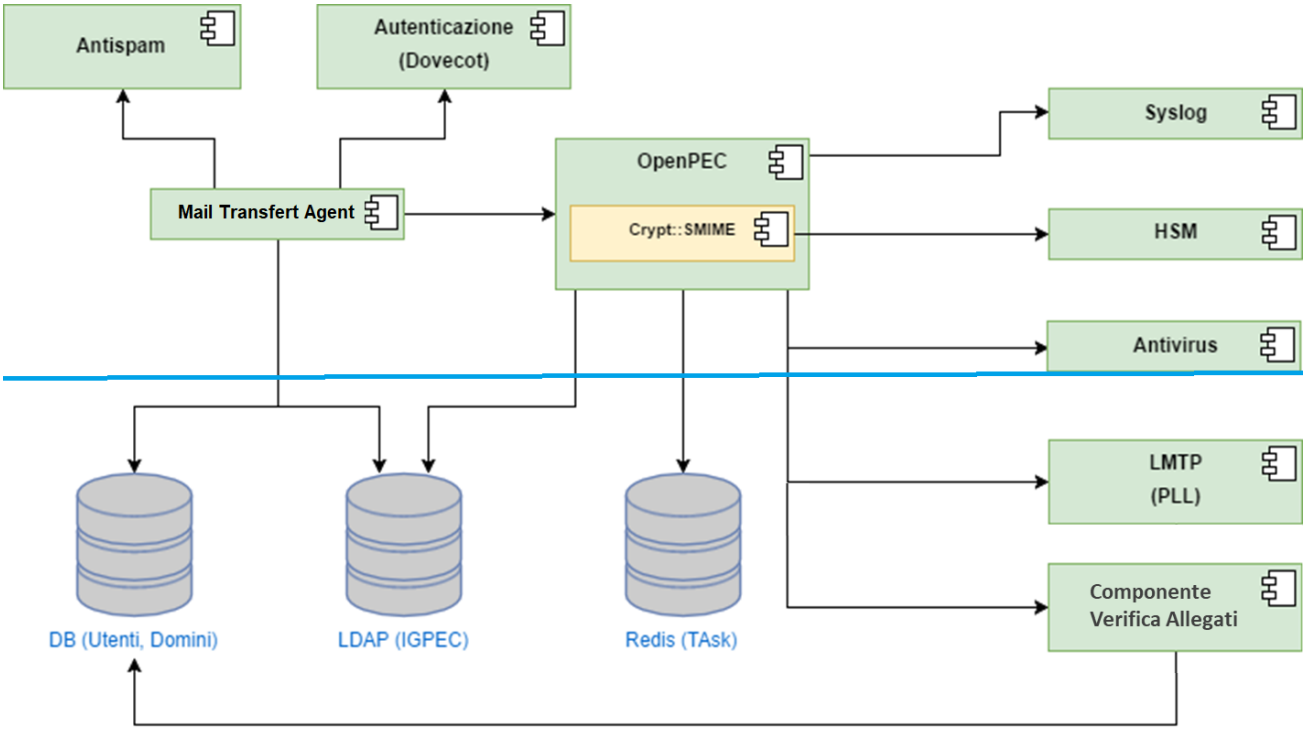


Figura 3 - Componenti del sistema

Come è possibile vedere dallo schema, OpenPEC rappresenta il nucleo centrale del sistema e si interfaccia con gli altri moduli: il Mail Transfer Agent che si incarica del routing delle mail, i sistemi Antivirus, i database dove sono memorizzati i dati relativi alle caselle (utenti, domini, titolari, …), i server LDAP che contengono i mirror dell'indice dei gestori, il server LMTP, i moduli HSM utilizzati per la firma dei messaggi, il server POP-IMAP (Dovecot) e la componente di verifica per gli allegati alle PEC.

Relativamente al comportamento della componente di verifica:

- per i messaggi in uscita, la componente di verifica effettua una serie di controlli specifici sui file allegati, sul mime type, sulla presenza di macro ed eventualmente aggiunge gli header necessari;
- se è un messaggio in uscita, incapsula il messaggio 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.

5.6 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 fornito dall'istituto nazionale di ricerca metrologica –INRiM (http://rime.inrim.it/labtf/ntp/).

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.

5.7 Storicizzazione dei Log e apposizione della marca temporale

Al fine della conservazione dei log dei messaggi, di cui alle deliberazioni AgID 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 soluzione 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 Time Stamping Authority fidata, di una firma digitale così detta di marcatura temporale (time stamping), 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.

5.8 Conservazione dei messaggi contenenti virus e relativa informativa al mittente

Il sistema di Actalis, 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 AgID in materia di riproduzione e conservazione dei documenti.

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 ecc.

A partire dall'11 aprile 2017, in osservanza del DPCM 3 dicembre 2013 sulla Conservazione e del documento AgID del 5 luglio 2016 "istruzioni per la conservazione dei log legali e dei messaggi di posta elettronica certificata con virus", i log legali vengono inviati in conservazione digitale.

5.9 Descrizione Data Center

Per la gestione della propria infrastruttura tecnologica per il sistema PEC, Actalis si avvale dei servizi di gestione data center erogati dalla capogruppo Aruba S.p.A., la quale è responsabile dell'housing e della connettività ad Internet dei sistemi, nonché della sicurezza fisica e, in parte, della sicurezza logica (network security).
Riportiamo di seguito le principali caratteristiche dei Data Center utilizzati (Data Center di via Ramelli (AR) e Data Center di via Gobetti (AR)).

5.9.1 Connettività

La connessione alla rete Internet è fondamentale per il funzionamento dei due data center.

Per questo scopo sono state realizzate connessioni multiple con diversi fornitori, utilizzando le migliori tecnologie disponibili.

Ogni connessione ha un punto di ingresso negli edifici ed un percorso geografico diverso rispetto alle altre, in modo da ridurre drasticamente la possibilità di guasti simultanei.

Inoltre la combinazione di fornitori italiani ed esteri oltre alla connessione diretta al principale punto di scambio italiano garantiscono non solo ridondanza ma anche le massime prestazioni possibili.

La connettività viene fornita da carrier indipendenti ed in più è presente una connessione diretta al Mix di Milano. Il routing viene gestito direttamente da Aruba S.p.A. tramite il proprio Autonomous System.

Due router di sistema, sia per la sede di via Gobetti che per quella di via Ramelli, sono connessi ai vari carrier.

In questo modo viene garantito un alto livello di tolleranza ai guasti nel caso in cui si verifichino problemi nella connessione verso uno dei carrier.

Dietro i router sono presenti sia per la sede di Via Ramelli che per quella di Gobetti degli apparati switch che gestiscono i link verso i router e rappresentano i root switch dell'intera rete.

Dietro gli switch sono presenti sistemi di load balancing e di monitoring.

Gli apparati hanno la funzione di bilanciare il carico per tutte le macchine della rete e di monitorare i processi dell'intero sistema. Nel caso di malfunzionamento di una macchina, oltre alla segnalazione del problema al Network Operations Center (NOC), è presente un meccanismo automatico di esclusione della macchina stessa (failover).

5.9.2 Data Center di Via Ramelli (DC IT 2)

Alimentazione:

- Stazione di trasformazione da 5 MVA (due trasformatori da 2.500kVA) connessa ad Enel tramite linee in media tensione. La stazione è connessa al ai due power center interni dove sono presenti 4+4 UPS da 500Kva in parallelo ridondato ed i relativi gruppi di batterie che garantiscono la presenza immediata di alimentazione elettrica d'emergenza e l'isolamento della rete elettrica esterna. In caso di interruzione dell'energia da parte di Enel i due generatori diesel intervengono entro 60 secondi ed hanno notevole autonomia anche in assenza di rifornimenti. Inoltre la rete di distribuzione interna fornisce 4 diverse linee di alimentazione ad ogni armadio rack.
- 2 Generatori di elettricità (G.E. da 1.650 kVa cadauno), 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.
- Cabina elettrica di proprietà, collegata alla rete elettrica di ENEL, che assicura scalabilità ed espandibilità degli oltre 2500Kva attualmente installati.
- 4 UPS da 500Kva in parallelo ridondato su ciascuno dei due power center (8 UPS totali) che garantiscono una totale sicurezza ed un'ulteriore garanzia di continuità oltre alla protezione da sbalzi, microinterruzioni e variazioni di tensione.
- Quadri elettrici per la distribuzione di energia con doppia linea.
- Apparati S.T.S. (Static Transfer Switch) per garantire in qualsiasi situazione la disponibilità di entrambe le linee di alimentazione.

Condizionamento:

- Sistema d'aria condizionata flessibile ed espandibile, dotato di sistema "free-cooling" che garantisce una temperatura ed umidità costanti.
- Nelle sale dati la temperatura media è mantenuta a 21 gradi circa.

- Unità di condizionamento a doppia alimentazione con switch automatico.
- Sistema di condizionamento protetto da UPS.

Sicurezza:

- Sicurezza fisica e degli accessi:
  - sale dati ed "aree" sensibili protette da accesso tramite badge+pin;
  - registrazione di ciascun visitatore e rilascio di specifico badge;
  - data center presidiato 24 ore su 24, 7 giorni su 7.
- Telecamere a circuito chiuso.
- Sistema di rilevazioni fumi a gas inerte (Azoto e Argon), n tutte le sale dati e nei locali power center.
- Impianto di rilevamento liquidi e antiallagamento.
- Le attrezzature antincendio (estintori, idratanti esterni, impianto centralizzato ad Azoto) sono ubicate in modo da essere facilmente raggiungibili e da proteggere tutta l'area. Tali impianti sono mantenuti e verificati regolarmente.

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 Titolari e dei Partner 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.

5.9.3 Data Center di Via Gobetti (DC IT 1)

Alimentazione:

- 4 gruppi di trasformazione M.T./B.T., 2 per l'alimentazione dei Power Center "Sale Dati" e 2 per l'alimentazione dei Power Center "Condizionamento", collegati all'anello in M.T.
- 2 gruppi di trasformazione dedicati alle sale dati costituiti da 2 trasformatori M.T/B.T. da 3150 kVA ciascuno.
- 2 gruppi di trasformazione dedicati al sistema di raffreddamento costituiti da 2 trasformatori M.T/B.T. da 3150 kVA ciascuno.
- Ogni gruppo di trasformazione è collegato ad un Power Center completamente indipendente dagli altri, in completa ridondanza 2*N.
- 4 gruppi elettrogeni Diesel in grado di erogare una potenza continua pari a quella dei trasformatori M.T/B.T. Ciascun gruppo elettrogeno ha una potenza pari a 1650 kVA; il sistema è modulare e prevede già il parallelo di più gruppi, in modo che sia possibile una crescita di numero degli stessi al crescere del carico che debbono alimentare, senza alcun disservizio per il sistema esistente e mantenendo una completa ridondanza del sistema dei Gruppi Elettrogeni. all'aumentare del carico.
- Stoccaggio di carburante costituito da 4 cisterne interrate da 25.000 litri ciascuna, per un totale di 100.000 litri di gasolio, sufficienti a garantire il funzionamento del datacenter in assenza di energia elettrica Enel ed in assenza di rifornimento per oltre 48 ore con data center a pieno carico.
- Sistema STS è in grado di alimentare - qualora per qualsiasi motivo (guasto o intervento di manutenzione) venga a mancare l'alimentazione elettrica proveniente da uno dei due Power Center - istantaneamente e senza interruzioni avvertibili dai server entrambe le PDU presenti in ciascun armadio della sala dati, dal power center superstite, realizzando pertanto una ridondanza completa di tipo 2*n.

Condizionamento:

- Tipologia di impiantistica che permette parzializzazione e modularità, ovvero un funzionamento anche a carichi parziali ed una modularità che permetta successive espansioni da poter realizzare senza fermo impianto.
- Impianto di climatizzazione dotato di macchine ad alta efficienza (EER>3,5 kW/kW), del tipo ad espansione diretta, con ricorso a sistemi di free cooling diretto.
- Distribuzione dell'aria in modalità "UNDER" supportata dall'elevata altezza del pavimento flottante (50 cm, aumentato a 60 cm nei punti di passaggio cavi principali) che consente di ridurre al minimo le perdite di carico anche in presenza di passerelle e cavi.

- Sistema di condizionamento dell'aria sovradimensionato per la creazione di ridondanza e in modo che, anche a pieno carico, venga garantito comunque il raffreddamento adeguato anche in caso di guasto di due macchine di condizionamento (ridondanza di tipo “n+2”).
- Ridondanza di tipo “2*n” nel caso dei Power Center che debbono dissipare l’energia prodotta dai sistemi UPS e STS.
- Controllo e gestione della temperatura e dell’umidità dell’ambiente realizzati mediante l’impiego di climatizzatori di precisione costituiti da unità autonome di condizionamento ad espansione diretta condensate ad aria, ad alta efficienza, funzionanti con gas refrigerante R407C, del tipo UNDER con mandata aria sotto pavimento e con aspirazione dalla parte superiore dell’unità direttamente dall’ambiente.
- Sistema di condizionamento protetto da n.4 UPS da 500kVA

Sicurezza:

- Sicurezza fisica e degli accessi:
  - porte esterne di tipo blindato;
  - finestre e superfici vetrate a piano terra dotate di vetro antiproiettile;
  - griglie per il passaggio dell’aria di raffreddamento delle sale dati protette da sbarre trasversali in acciaio;
  - accesso visitatori tramite “bussola” a due ante rotanti interbloccate, dotata di vetri antiproiettile ed attraverso varchi motorizzati apribili esclusivamente apposito badge;
  - sale dati ed “aree” sensibili protette da accesso tramite badge+pin;
  - registrazione di ciascun visitatore e rilascio di specifico badge;
  - data center presidiato 24 ore su 24, 7 giorni su 7;
- telecamere a circuito chiuso;
- Sistema di rilevazione fumi
- Sistema di spegnimento incendio a gas inerte (Azoto e Argon), in tutte le sale dati e nei locali power center
- Impianto di rilevamento liquidi e antiallagamento.
-
- le attrezzature antincendio (estintori, idratanti esterni, impianto centralizzato ad Azoto) sono ubicate in modo da essere facilmente raggiungibili e da proteggere tutta l’area. Tali impianti sono mantenuti e verificati regolarmente. Gli impianti elettrici sono realizzati in modo da minimizzare i rischi di incendio.

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 Titolari e dei Partner 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.

6. Standard tecnologici, procedurali e di sicurezza adottati

6.1 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)

6.2 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.

Actalis si avvale dei servizi di gestione data center (certificati ISO/IEC 27001) erogati dalla società capo-gruppo Aruba S.p.A., dalla data 03/02/2016 il certificato di riferimento è quello multi-sito del Gruppo Aruba. Lo standard di sicurezza ISO 27001 garantisce la sicurezza delle informazioni attraverso l'adozione di procedure, norme comportamentali, misure e corsi di formazione adeguati.

Inoltre Aruba S.p.A. è responsabile dell'housing, della connettività ad Internet e della sicurezza fisica dei sistemi di elaborazione utilizzati e garantisce ad Actalis:

- controllo accessi fisici;
- continuità di alimentazione elettrica;
- sistemi antincendio ed antiallagamento;
- ventilazione e condizionamento ottimali;
- connettività ad Internet ridondata e di capacità almeno doppia del minimo necessario;
- un Network Operation Center (NOC), presidiato H24 per 365 giorni/anno da personale sistemistico qualificato, che assicura il costante monitoraggio dell'infrastruttura e dei servizi ed il tempestivo intervento in caso di necessità.

Lo standard di sicurezza ISO 27001 garantisce la sicurezza delle informazioni 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, ridurre, contenere, evitare, trasferire il rischio di sicurezza di cui è eventualmente affetto il sistema.

6.3 Misure di sicurezza

Il sistema di posta elettronica certificata di Actalis 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 all'AgID e redatto in base alle disposizioni delle circolari dell'agenzia stessa.

6.3.1 Accesso ai locali di erogazione del servizio

Le apparecchiature utilizzate per l'erogazione del servizio sono situate all'interno di aree ad accesso controllato. L'ingresso nei locali e agli armadi con HSM è consentito solo a personale autorizzato in possesso di apposito badge+pin (cfr. paragrafo 5.9).

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.

6.3.2 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 (vedi punto 6.4.1).

6.3.3 Sicurezza di tipo informatico

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

- Presenza di firewall con definizione di policy di accesso (vengono abilitate le sole porte strettamente necessarie al funzionamento del sistema PEC).
- Sistema di antivirus costantemente ed automaticamente aggiornato sia per quanto riguarda le firme di virus riconosciuti che l'engine dell'antivirus, in modo 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 degli HSM e 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.
- Partecipazione al sistema di Infosharing MISP (Malware Information Sharing Platform) per contrastare fenomeni di Malspam e Phishing.
- Sistema Breach Monitoring che monitora l'esposizione di caselle in conseguenza di data breach pubblici.
- Controllo sulle estensioni dei file allegati a una PEC. L'obiettivo è di impedire l'invio tramite PEC di file con estensioni considerate potenzialmente pericolose, sia perché direttamente utilizzate nelle campagne di

diffusione malware, sia perché legate all'esecuzione di codice che può avere ripercussioni sull'integrità dei sistemi.

- Verifica della presenza di macro all'interno dei file allegati a una PEC. In caso positivo, i sistemi Aruba inseriscono uno specifico header che consente al Gestore destinatario di individuare in maniera automatica i messaggi contenti macro; inoltre aggiungono una notifica di cortesia all'interno della busta di trasporto di modo da segnalare al destinatario della PEC il contenuto potenzialmente dannoso del file.
- Gestione avvisi per mancato controllo di determinati allegati. Se l'allegato è cifrato o inserito in un archivio compresso e protetto da password, il suo contenuto non può essere sottoposto a scansione antivirus. In quel caso, i sistemi Aruba inseriscono uno specifico header che consente al Gestore destinatario di individuare in maniera automatica i messaggi con mancato controllo degli allegati; viene inoltre aggiunta una notifica di cortesia all'interno della busta di trasporto per segnalare al destinatario del messaggio l'impossibilità di effettuare il controllo di sicurezza sul contenuto dei file cifrati;
- Inoltre Actalis, per motivi di sicurezza, ha implementato delle restrizioni alle estensioni che non è possibile allegare ad un messaggio PEC. Il dettaglio di queste limitazioni è pubblicato nella sezione delle guide PEC online ed è rinvenibile al link: https://www.actalis.it/news-eventi/tipi-di-file-che-non-e-possibile-allegare-ad-un-messaggio-pec.aspx.

6.3.4 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 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.

6.3.5 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 ACTALIS.

6.3.6 Misure di sicurezza degli ambienti fisici

Actalis 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 5.9.

6.3.7 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.

6.4 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

6.4.1 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 mailing 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.

6.4.2 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 previa cancellazione dei dati ove ancora leggibili. Nel frattempo la macchina potrà, se necessario, essere sostituita da una macchina analoga.

6.4.3 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. 6 sono anche i responsabili del personale che opera all'interno di quel servizio.

6.4.4 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 ACTALIS 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.

6.4.5 Atti dolosi

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

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 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, ACTALIS 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, ecc.;
- indagare per capire se le altre macchine possono aver subito dei danni;
- denunciare l'attacco agli organi competenti, se ritenuto opportuno.

6.4.6 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 ACTALIS 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.

6.4.7 Azioni promosse dal Gestore in caso di malfunzionamento

In base alla circolare CNIPA (ovvero l'attuale AgID) n.51 del 7 dicembre 2006, il Gestore è tenuto a informare l'AgID 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

Tipologia	Codice	Descrizione
	1B Rilevato da terzi	funzioni base (trattamento del messaggio originario, ricevute ed avvisi) per il quale non è circoscritto il potenziale impatto
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, ricevute ed avvisi) per il quale è circoscritto il potenziale impatto
	2B Rilevato da terzi	
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 AgID 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 a AgID una relazione dettagliata su quanto accaduto e sui provvedimenti adottati.

6.5 Procedure operative

Per l'erogazione del servizio di posta elettronica certificata Actalis 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.

6.5.1 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;
- 1 responsabile della sicurezza dei log dei messaggi;
- 1 responsabile del sistema di riferimento temporale.

Le figure sopra elencate si avvalgono 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 Actalis in particolare.

Tutti gli operatori ed i responsabili riferiscono inoltre al responsabile del servizio che coordina l'intero team, definisce le strategie con la direzione e si interfaccia con l'Agenzia per l'Italia Digitale.

6.5.2 Gestione backup

I backup dei dati (di tutte le macchine che implementano il sistema PEC) vengono effettuato in maniera automatica su disco.

I dati relativi alle caselle di posta vengono storicizzati su storage dedicati (che garantiscono una replica attiva/attiva su cluster, e geografica tra i DC1 Ramelli e DC2 Gobetti) per i quali viene garantito almeno 1 giorno di conservazione; i log legali che vengono storicizzati localmente in ciascun server, e giornalmente marcati temporalmente e trasferiti su un sistema di conservazione centralizzato e i dati del database (mailbox), salvati localmente, e replicati in ciascuna macchina appartenente al cluster per un periodo di almeno 30 giorni.

I file di log che costituiscono la traccia di tutte le comunicazioni fatte dagli utenti di PEC che fanno capo al Gestore vengono memorizzati sul file system dell'unità storage. Da qui vengono copiati su storage configurati in replica con ridondanza geografica su 2 (due) Data Center.

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 ecc.

6.5.3 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 Actalis.

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.

6.5.4 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.

Problema segnalato da titolare/partner

La segnalazione può essere effettuata dal Titolare o dal Partner attraverso i canali disponibili per l'assistenza.

Il team di “Service Desk” (personale interno o in outsourcing) ha il compito di:

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

Il personale del service desk, rilevato l’impatto e l’urgenza, scala internamente la segnalazione allertando i reparti necessari sia per la soluzione che per la gestione della comunicazione nei confronti di organi competenti e dei titolari/partner (ad es. Marketing, Ufficio legale, Prodotto, Sicurezza).

Fuori orario di ufficio (18:00 – 8:30 dal lunedì al venerdì; h24 sabato, domenica e festivi).

La segnalazione viene scalata al team Control room e service desk operation che effettuate le prime verifiche contatta il reperibile di turno. Sarà il reperibile ad allertare altri soggetti se necessario.

In orario di ufficio (8:30 -18:00 dal lunedì al venerdì escluso i festivi)

- La segnalazione viene scalata al team Service Run che 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 Service Desk;
- aggiorna la knowledge base.

Problema segnalato dal monitoraggio

In questo caso la segnalazione perviene dall’interno e il team Control room e service desk operation, rilevato l’alert ed effettuati i primi controlli oltre a informare il Service Desk:

Fuori orario di ufficio (18:00 – 8:30 dal lunedì al venerdì; h24 sabato, domenica e festivi) scala la segnalazione contattando il reperibile che a sua volta allerta altri soggetti se necessario.

In orario di ufficio (8:30 -18:00 dal lunedì al venerdì escluso i festivi) scala la segnalazione al team Service Run che prende in carico il problema valutandone a sua volta gravità ed urgenza.

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

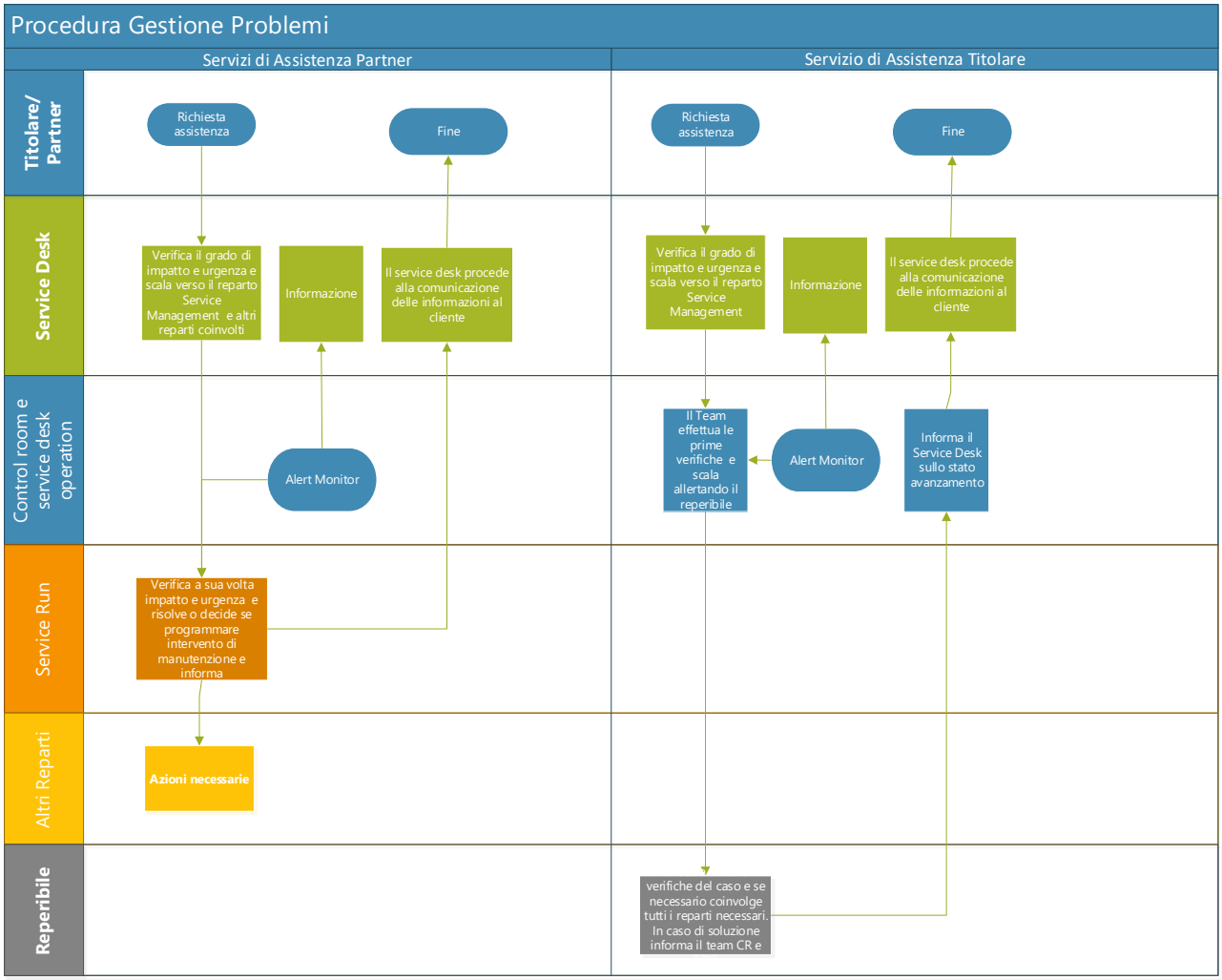


Figura 5 – Flusso di gestione dei problemi

7. Modalità di erogazione del servizio

7.1 Attivazione del Partner Actalis

Possono richiedere l'adesione al programma Partner società di diritto privato, Pubbliche Amministrazioni o liberi professionisti.

Per iscriversi è necessario prendere contatto con un commerciale del Gestore e, a seguito degli accordi presi e dell'adesione alla contrattualistica predisposta dal Gestore stesso, il reparto competente provvederà all'analisi e al controllo della documentazione inviata e procederà all'attivazione del pannello tramite l'area https://areaclienti.actalis.it/actalispec/login. In caso di documentazione errata o mancante invece invierà comunicazione al cliente tramite mail.

7.2 Tipologie di caselle

7.2.1 Caselle di Posta Elettronica Certificata sul dominio Actalis

Questa modalità di offerta è consigliata alle organizzazioni che intendono attivare una o più caselle di posta certificata sul dominio di posta certificata di Actalis, actaliscertymail, pec.actalis.it actalispec.it o cert.actalis.it. Le caselle di posta attivate saranno pertanto del tipo, user@actaliscertymail.it (es. mario.rossi@actaliscertymail.it) o utente@pec.actalis.it o utente@actalispec.it o utente@cert.actalis.it.

7.2.2 *Caselle di Posta Elettronica Certificata su un dominio dedicato al cliente.*

Il Partner ha la possibilità di richiedere la creazione di un dominio personalizzato su cui certificare le caselle di Posta Elettronica Certificata dei propri utenti (ad esempio Regione_X.it).

Il Partner dal proprio pannello di gestione potrà procedere alla creazione, sospensione, riattivazione, disdetta o modifica dati delle caselle PEC.

In base al tipo di servizio acquistato tramite il Partner, il Titolare avrà a disposizione una delle seguenti tipologie di caselle di posta elettronica certificata

- STANDARD
- PRO
- PRO PLUS

Di seguito una tabella con le principali caratteristiche dei 3 tipi di casella:

	STANDARD	**PRO**	**PRO PLUS**
Spazio Casella	1 GB	5 GB (2 GB Casella + 3 GB Archivio)	2 GB (Archiviazione Illimitata + 8 GB Archivio Offline)
Dimensione max messaggio	100 MB	100 MB	100 MB
Numero Max Destinatari	500 totali	500 totali	500 totali
Archivio di sicurezza	NO	SI	SI
Report SMS	NO	SI	SI
Notifica tramite e-mail	SI	SI	SI
Modifica password	SI	SI	SI
Antivirus	SI	SI	SI
Antispam	SI	SI	SI
Ricezione mail non certificate	SI	SI	SI
IMAP	SI	SI	SI
Accesso Webmail	SI	SI	SI
Filtri e regole messaggi	SI	SI	SI
Garanzia identità del mittente	SI	SI	SI
Ricevuta avvenuta/mancata consegna	SI	SI	SI
Validità legale dei messaggi inviati/ricevuti	SI	SI	SI
Non ripudiabilità del messaggio inviato/ricevuto	SI	SI	SI
Assistenza	Call center e ticket	Call center e ticket	Call center e ticket
Dichiarazione Certificazione casella	Gratuita	Gratuita	Gratuita

Di seguito vengono descritti gli aspetti generali per ciascuna caratteristica associata al servizio.

Spazio Casella: indica lo spazio disponibile sulla casella. Qualora si raggiunga la quota non sarà più possibile ricevere messaggi. Per liberare spazio è necessario che il Titolare provveda in modo autonomo alla cancellazione dei messaggi; in alternativa, può acquistare spazio aggiuntivo.

Dimensione massima messaggio: indica la dimensione massima che può raggiungere un messaggio in uscita (compresi gli allegati). La dimensione viene intesa come prodotto del singolo messaggio per il numero dei destinatari.

Numero massimo destinatari: indica la quantità di destinatari che possono essere indicati. Ne vengono supportati fino ad un massimo di 500 per messaggio.

Archivio di Sicurezza: il servizio consente l'archiviazione dei messaggi in entrata o in uscita. Il Titolare ha la possibilità di decidere che cosa archiviare attraverso l'impostazione di una serie di regole. In particolare potrà decidere se archiviare:

- tutte le ricevute di accettazione;
- tutte le ricevute di consegna;
- tutti i messaggi di posta certificata;
- tutti i messaggi di posta certificata inviati;
- tutte le mail inviate e ricevute sulla casella PEC.

L'archivio è fisicamente separato dalla casella del Titolare ma è visibile, come cartella, dall'interno della Webmail.

Non è possibile cancellare le mail archiviate, una volta raggiunto il limite massimo di spazio disponibile sarà possibile per procedere ad un upgrade dello spazio per poter continuare ad archiviare. In alternativa, il sistema informerà automaticamente l'Utente che verrà cancellato, prima della saturazione dell'intero archivio, parte del contenuto, riportandone lo spazio disponibile al 50%.

Report SMS: il servizio controlla quotidianamente la presenza di messaggi non letti nelle ultime 24 ore e, se presenti, invia una notifica tramite SMS al numero indicato dal Titolare. Da pannello gestione mail è possibile indicare il numero al quale ricevere la notifica e impostare l'orario nel quale il controllo deve essere effettuato.

Antivirus: il servizio antivirus è presente in tutti i tipi di caselle come previsto dalla normativa.

Ricezione mail non certificate: all'atto dell'attivazione la casella viene fornita "aperta" nel senso che le è permesso di ricevere messaggi di posta ordinaria (non PEC). Il Titolare, tramite il pannello gestione mail, può modificare tale impostazione, scegliendo di bloccare la ricezione di tali messaggi. Inoltre, il Titolare può reindirizzare tali messaggi verso una casella non PEC a sua scelta.

Inoltre, se vuole ricevere i messaggi tradizionali può farli arrivare nella propria casella "Inbox" ("Posta in Arrivo") o decidere che siano spostati automaticamente in una cartella della sua mailbox.

Antispam: il Titolare del servizio PEC ha la possibilità di attivare il servizio antispamming per filtrare i messaggi di posta ordinaria in arrivo. Ricordiamo che la normativa non consente di applicare filtri antispam ai messaggi di posta certificata per evitare la possibilità di giudicare come spam messaggi "buoni" (falsi positivi).

Sulle mail considerate spamming, il Titolare ha la possibilità di decidere se eliminarle o spostarle in una cartella denominata "spam".

È infine presente un pannello per la personalizzazione avanzata del filtro, attraverso il quale è possibile impostare il livello di sensibilità, le lingue dalle quali si ricevono normalmente le mail ecc.

Webmail: per tutte le tipologie di casella è offerto al Titolare il servizio webmail per accedere da qualunque browser.

Filtri e regole per i messaggi di arrivo: tramite questa funzione il Titolare può impostare una serie di regole sui messaggi in arrivo in modo da spostare, copiare o inoltrare le mail che soddisfano le condizioni impostate. Solo per fare alcuni esempi è possibile spostare automaticamente le ricevute sotto una cartella a scelta dell'Utente, copiare automaticamente i messaggi spediti ad un certo destinatario sotto un'altra cartella, inoltrare automaticamente i messaggi provenienti da un certo mittente ad un indirizzo (sia PEC che convenzionale) a scelta dell'Utente.

7.2.3 Personalizzazione della webmail

Qualora il cliente acquisisca un proprio dominio di posta certificata ha anche la possibilità di personalizzare la webmail, ovvero modificare l'aspetto grafico della webmail di base Actalis rendendolo aderente allo stile grafico della propria azienda.

L'obiettivo di queste personalizzazioni è quello di fornire agli utenti finali del cliente un ambiente con cui essi abbiano già familiarità, sfruttando per quanto possibile le caratteristiche grafiche a loro già note (come per es. immagini, loghi, icone, stili di formattazione) e specifiche della "Corporate identity" del cliente.

7.3 Accesso ed utilizzo del servizio

Gli utenti del servizio possono accedere alle caselle di posta certificata in due modalità: con un client di posta e/o tramite webmail.

7.3.1 Accesso ed 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, Zimbra, Mac Mail, Outlook, Outlook Express, ecc.

Per il corretto funzionamento è necessario che il Titolare abiliti il client di posta a connettersi ai server PEC attraverso i protocolli POP3/S, IMAP/S, SMTP/S. Gli indirizzi dei server ed i relativi parametri sono comunicati dal Gestore tramite messaggio di conferma attivazione del servizio.

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 (in caso di invio da casella PEC a casella PEC) 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.

7.3.2 Accesso ed utilizzo tramite webmail

L'accesso tramite webmail ha il vantaggio di non richiedere alcun tipo di configurazione del sistema: basta collegarsi all'indirizzo della webmail Actalis (https://webmail.pec.actalis.it/), inserire le proprie credenziali, e sarà possibile consultare e utilizzare la propria casella di posta certificata. La soluzione di webmail si caratterizza per la sua flessibilità e semplicità di utilizzo e consente, in particolare, di specificare la tipologia di ricevuta (breve, sintetica, completa) così come previsto dalla normativa vigente.

7.3.3 Liste di distribuzione

La lista di distribuzione è un sistema integrato nella soluzione di Posta elettronica certificata di Actalis, che permette l'invio di una mail di posta elettronica certificata ad un gruppo di destinatari appartenenti ad una lista.

Per inviare un messaggio all'elenco di destinatari appartenenti alla lista di distribuzione è necessario inviarlo ad uno speciale indirizzo e-mail, identificante la specifica lista di distribuzione, che a sua volta provvede a diffonderlo a tutti gli indirizzi appartenenti alla lista.

L'utilizzo delle liste di distribuzione permette l'invio di una mail di posta elettronica certificata ad un insieme di destinatari, senza avere l'onere di specificare tutti gli indirizzi nella mail. Essendo integrato nel sistema di posta elettronica certificata, il sistema liste di distribuzione funziona con le stesse modalità: a fronte di un invio di una mail alla lista di distribuzione il mittente riceverà nella sua casella di posta elettronica certificata una ricevuta di accettazione riportante l'elenco di tutti gli indirizzi appartenenti alla lista di distribuzione e un numero di ricevute di consegna pari al numero di caselle di posta elettronica certificata appartenenti alla lista di distribuzione.

Analogamente, in caso di mancata accettazione della mail o mancata consegna della stessa mail ad uno o più destinatari, verranno recapitate le rispettive ricevute nella casella del mittente come previsto dal sistema dii posta elettronica certificata.

La gestione di una lista (creazione, cancellazione/inserimento caselle di posta in una lista esistente, ecc.) è competenza di Actalis. In base alle proprie esigenze organizzative, un cliente Actalis può anche richiedere la generazione di più liste di distribuzione e specificare che una stessa casella di posta elettronica, certificata o ordinaria, possa fa parte di più liste di distribuzione.

Nel caso in cui un utente non autorizzato invii una mail al sistema lista di distribuzione, riceverà nella sua casella di posta elettronica certificata una ricevuta di non accettazione attestante la mancata autorizzazione all'utilizzo del sistema liste di distribuzione.

L'utilizzo del sistema liste di distribuzione permette inoltre l'invio di una mail di posta elettronica certificata firmata elettronicamente e/o cifrata dal mittente e destinata al gruppo di destinatari appartenenti alla specifica lista di distribuzione.

A richiesta Actalis fornisce un certificato digitale che consente ad una lista di distribuzione di firmare e cifrare i messaggi.

7.3.4 Modifica dati anagrafici

Successivamente all'attivazione del servizio resta possibile per il Titolare di una casella PEC modificare i dati anagrafici ad essa associati, in modo autonomo ovvero mediante espressa richiesta al proprio Partner, in base alle caratteristiche della modifica richiesta.

Qualora sia notificato al Titolare che, in sede di emissione di fattura elettronica, al Partner sono giunte evidenze formali che indicano che i dati anagrafici forniti dal Titolare in fase d'ordine non risultano esatti e/o completi e/o aggiornati, il Titolare sarà tenuto a provvedere alla loro specifica correzione e/o integrazione.

7.3.5 Cambio di Titolare

Successivamente all'attivazione del servizio resta sempre possibile per il Titolare di una casella PEC richiedere la modifica della titolarità della casella.

Per ottenere la modifica è necessario che il Titolare ne faccia espressa richiesta al proprio Partner che potrà procedere direttamente dal proprio pannello di gestione.

Il Partner potrà e dovrà modificare la titolarità di una Casella PEC solo dopo aver accertato, mediante il ricevimento dell'apposita documentazione sopra descritta sottoscritta dai soggetti coinvolti, l'effettiva volontà del Titolare della Casella PEC di cedere la medesima in favore di un soggetto Terzo, e la volontà di quest'ultimo di acquisirla alle condizioni contrattuali in vigore.

7.3.6 Cancellazione di una casella PEC da parte del Titolare

In qualsiasi momento il Titolare di una casella PEC può richiedere la cancellazione della propria casella di PEC.

Tale operazione comporta l'eliminazione, completa e irreversibile, di tutti gli eventuali dati in essa contenuti.

Nel caso di indisponibilità del Partner (es: cessazione attività, fallimento etc) il Titolare potrà richiedere la cancellazione direttamente al Gestore che provvederà facendosi inviare agli indirizzi di assistenza pec@pec.actalis.it (indirizzo mail assistenza certificato) o pec.actalis@staff.aruba.it (indirizzo mail assistenza non certificato), dalla casella PEC in questione (che dovrà essere cancellata), la richiesta.

Il Titolare può inoltre rivolgersi al proprio Partner di riferimento per richieste di assistenza di carattere amministrativo e/o gestionale (modifiche dati, cambio titolarità ecc.).

Per quanto concerne la riassegnazione di una casella PEC, che riguarda una casella dismessa (scaduta e non rinnovata), dando seguito alla Direttiva AgID del 18.12.2013, si rispetta il divieto in vigore per il Gestore di Posta Elettronica Certificata di riassegnare un indirizzo di posta elettronica certificata a soggetto diverso dal titolare originario. Quindi, qualora il richiedente non abbia lo stesso Codice Fiscale o la stessa Partita IVA che erano associate alla precedente registrazione, non potrà ottenere l'assegnazione della stessa casella PEC.

7.3.7 Assistenza

Il Titolare ha a disposizione un servizio di assistenza telefonica erogata dal Gestore attraverso i riferimenti riportati sul sito https://www.actalis.it/chi-siamo/contatti-recapiti-info.aspx dove sono riportati i riferimenti telefonici: Assistenza: +390575.050.360 dal Lunedì al Venerdì, dalle 9.00 alle 13.00 e dalle 14.30 alle 17.30.

Il sistema di trouble-ticketing è stato pensato e creato per semplificare e velocizzare al massimo tutte le richieste di supporto.

Gli indirizzi da utilizzare per l'assistenza scritta sono pec@pec.actalis.it (indirizzo mail assistenza certificato) o pec.actalis@staff.aruba.it (indirizzo mail assistenza non certificato).

Il Titolare può inoltre rivolgersi al proprio Partner di riferimento per richieste di assistenza di carattere amministrativo e/o gestionale (modifiche dati, cambio titolarità ecc.).

Per quanto riguarda l'assistenza per il canale Partner, questa viene descritta al par. 7.4.3.

7.3.8 Consultazione dei log dei messaggi da parte del Titolare

Come previsto dalla normativa in materia di PEC, il Gestore è tenuto a conservare i file di log dei messaggi di posta elettronica certificata per un periodo di almeno 30 mesi dall'invio del messaggio.

Il Titolare della casella di posta elettronica certificata potrà richiederne la consultazione aprendo una richiesta di assistenza tramite i canali dedicati.

Gli sarà dunque richiesto di inviare il "Modulo richiesta file di log", unitamente a copia del documento di identità del titolare della casella PEC.

7.3.9 Password Policy

Actalis per la fase di prima impostazione della password e per il reset della stessa, ha implementato sui propri pannelli di vendita e gestione, delle regole di composizione aventi delle caratteristiche di robustezza ritenute dal Gestore adeguate al contesto di utilizzo. Le regole per la composizione della password tengono in considerazione elementi come il numero dei caratteri, la presenza di minuscole, maiuscole, caratteri speciali e numeri. La password policy sarà applicata anche nel contesto dei clienti dei Partner di Actalis in fase di generazione delle caselle. Il Partner inoltre non è nelle condizioni di scegliere e conoscere le credenziali di prima attivazione.

La procedura di attivazione prevede la creazione di una casella protetta da password generata automaticamente (non comunicata e, conseguentemente, non conoscibile né all'utente né al Partner) e il contestuale invio all'utente di una e-mail automatica contenente il link per l'esecuzione in proprio della procedura obbligatoria di reset password.

7.4 Partner di Actalis

7.4.1 Strumenti per il Partner

I Partner hanno la possibilità di utilizzare un'apposita piattaforma con la quale possono fornire servizi di PEC ai propri utenti (c.d. "Titolari") quali p.e. creazione di caselle di posta elettronica certificata, richiesta di certificazione di un dominio, richiesta di servizi personalizzati (es. upgrade di dimensione delle caselle, personalizzazione grafica della webmail) ecc. L'acquisto dei servizi da parte del Partner può avvenire mediante credito prepagato, dal quale vengono scalati di volta in volta i crediti utilizzati oppure tramite offerta commerciale.

7.4.2 Modalità operative per il Partner

a) Richiesta da parte del Partner al Gestore di attivazione di una casella di PEC attraverso la piattaforma Partner

La richiesta da parte del Partner al Gestore di attivazione di una casella di PEC è regolata dalla seguente procedura operativa.

1. **Controllo dei dati in ingresso**

   Il Partner dovrà controllare i dati e la documentazione inviata dal proprio Utente, in particolare che quest'ultimo abbia fornito le seguenti informazioni:

   - 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 Partner dovrà verificare inoltre che sia presente e debitamente compilato il Modulo di Adesione cliente e l'eventuale ulteriore documentazione prevista.

2. **Formulazione della richiesta di attivazione**

   Per attivare una casella PEC al proprio Utente il Partner, attraverso l'apposita piattaforma Partner messa a disposizione, deve effettuare le operazioni di seguito descritte.

   a) Compilare i campi generali della casella:
      - dominio;
      - nome casella;
   b) Scegliere se la casella è destinata ad un privato o ad una persona giuridica.
   c) Indicare se si tratta di un nuovo Titolare o di uno già registrato; se il Titolare è nuovo, compilare il form con i dati richiesti.
   d) Confermare operazione assicurandosi che i dati inseriti siano corretti e corrispondano a quanto riportato nella richiesta di attivazione.
   e) Effettuare l'upload della documentazione inviata dal Titolare.

b) Richiesta da parte del Partner al Gestore di certificazione di un dominio attraverso la piattaforma Partner

Il Partner ha la possibilità di richiedere la certificazione di un dominio (FQDN) sul quale creare successivamente caselle di posta certificata per i propri utenti. Se l'Utente ha già un proprio dominio registrato, è possibile per il Partner richiedere la certificazione senza trasferire il dominio dall'attuale maintainer. È inoltre possibile certificare dominio di secondo livello (ad esempio "nomedominio.ext"), di terzo livello (ad esempio "pec.nomedominio.ext") e di quarto livello (ad esempio "pec.test.prova.ext").

Il nome del dominio sarà scelto dall'Utente tra quelli non ancora in uso.

Il Gestore si riserva comunque il diritto di rifiutare il nominativo scelto nel caso in cui lo ritenga offensivo, irrispettoso o lesivo nei confronti di terzi

La richiesta da parte del Partner al Gestore di certificazione di un dominio è regolata dalla seguente procedura operativa.

1. **Controllo dei dati in ingresso**
   Il Partner dovrà controllare i dati e la documentazione inviata dal proprio Utente, secondo quanto previsto dal flusso di cui al paragrafo 7.1, in particolare che quest'ultimo abbia fornito le seguenti informazioni:
   - 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 Partner dovrà verificare inoltre che sia presente e debitamente compilato il Modulo di Adesione cliente e l'eventuale ulteriore documentazione prevista.
2. **Formulazione della richiesta di certificazione**
   Per attivare un dominio PEC al proprio Utente il Partner, attraverso l'apposita piattaforma Partner messa a disposizione, deve effettuare le operazioni di seguito descritte.
   a) Compilare i campi generali del dominio:
      - Dominio
      - tipo:
        - Certificazione di un dominio mantenuto da Aruba,
        - trasferimento di un dominio verso Aruba e successiva certificazione,
        - certificazione di un dominio mantenuto da società diversa da Aruba.

   b) Indicare se si tratta di un nuovo Titolare o di uno già registrato; se il Titolare è nuovo compilare il form con i dati richiesti:
   c) Confermare operazione assicurandosi che i dati inseriti siano corretti e corrispondano a quanto riportato nella richiesta di attivazione.
   d) Effettuare l'upload della documentazione inviata dal Titolare.

7.4.3 Assistenza per il Partner

Il servizio di assistenza fornito da Actalis viene erogato attraverso 2 canali:

- telefono
- trouble ticketing

Il servizio è attivo in orario di ufficio (dalle ore 9.00 alle 13.00 e dalle 14.30 alle 17.30) dal lunedì al venerdì (esclusi festivi).

Il sistema di trouble-ticketing (indirizzi mail dedicati sono pec@pec.actalis.it :indirizzo mail assistenza certificato o pec.actalis@staff.aruba.it: indirizzo mail assistenza non certificato), è stato pensato e creato per semplificare e velocizzare al massimo tutte le comunicazioni in merito alle richieste di supporto tecnico, amministrativo o commerciale.

7.5 Livelli di servizio ed indicatori di qualità

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

Livelli di Servizio	
Numero massimo di destinatari contemporanei accettati	500

Livelli di Servizio	
Dimensione massima di ogni singolo messaggio (intesa come prodotto tra il numero dei destinatari e la dimensione del messaggio)	100 MB
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.

Indicatori di qualità	
Disponibilità del servizio (invio e ricezione email)	7/24/365
Disponibilità del servizio di richiesta di attivazione	7/24/365
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
Disponibilità del servizio di richiesta da parte del Titolare della traccia delle comunicazioni effettuate (log)	7/24/365
Tempo massimo per l'invio delle informazioni relative ai file di log di un messaggio di PEC dietro richiesta del Titolare (Il Titolare può comunque in qualsiasi momento ricercare e scaricare i log di interesse in autonomia direttamente dal pannello “Gestione Mail”)	5 giorni lavorativi
Sistema di monitoring con invio di messaggi di alert via email ed sms al presentarsi di malfunzionamenti e situazioni critiche	7/24/365
Servizio di assistenza al Titolare	7/24/365
Assistenza standard tramite call center (trouble ticketing)	5 giorni la settimana dal Lunedì al Venerdì, dalle 9.00 alle 13.00 e dalle 14.30 alle 17.30
Assistenza di emergenza per i Gestori tramite il Network Operations Center (NOC)	7/24/365

7.6 Interoperabilità con gli altri sistemi di PEC

Actalis 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]).

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

A questo scopo Actalis è disponibile ad assegnare caselle PEC di test ai Gestori interessati ad effettuare test di interoperabilità con il proprio sistema.

7.6.1 Assistenza su segnalazioni gravi da parte degli altri Gestori

In caso di problemi di interoperabilità con altri sistemi PEC, gli altri Gestori hanno la possibilità di contattare il Network Operations Center (NOC) 24 ore su 24, 7 giorni su 7.

7.7 Cessazione dell'attività di Gestore

Nel caso di cessazione dell'attività di Gestore PEC, Actalis comunicherà ad AgID, con adeguato preavviso, la propria volontà di cessare l'attività di Gestore, indicando nella comunicazione formale la data di cessazione e l'eventuale Gestore subentrante (se già conosciuto).

Con il medesimo preavviso il Gestore informerà, a mezzo posta elettronica certificata e/o tramite comunicazione sul sito www.actalis.it, i Titolari di caselle di Posta Elettronica Certificata e i Partner della volontà di cessare l'attività di Gestore, riportando anche le indicazioni per trasferire il servizio ad altro Gestore (se già conosciuto) oppure, ove non vi sia un Gestore subentrante, sarà specificato che le suddette caselle saranno disattivate a partire dalla data di cessazione dell'attività.

Nella comunicazione Actalis specificherà anche il periodo di tempo durante il quale le suddette caselle, pur non avendo funzionalità di invio/ricezione messaggi, saranno attive in sola lettura.

In ogni caso Actalis conserverà i log per l'arco temporale previsto dalla Normativa e pertanto per un periodo non inferiore a 30 mesi.

8. Obblighi e responsabilità

8.1 Obblighi e responsabilità del Gestore

Actalis s.p.a. 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 e del Regolamento UE 2016/679 (GDPR);
- 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 Titolari e/o Partner 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 dell'AgID 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 Actalis da ogni responsabilità in merito ai contenuti dei messaggi;
- fornire ad Actalis 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 da AgID);
- 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;
- 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. 7.3.1 e 7.3.2;
- 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

- Actalis 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;
- Actalis non assume alcun obbligo riguardo la conservazione dei messaggi inviati e trasmessi attraverso le proprie caselle di PEC. Tale responsabilità viene assunta unicamente dal Titolare;
- Actalis non ha alcuna responsabilità sui contenuti dei messaggi inviati e ricevuti attraverso le proprie caselle di PEC;
- Actalis risponde dei danni causati a qualsiasi persona fisica o giuridica in seguito al mancato adempimento degli obblighi contrattuali e di quelli previsti dalla normativa vigente in quanto applicabile;
- 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 Actalis che provochino ritardi, malfunzionamenti o interruzioni del servizio;

- Qualsiasi contestazione del Titolare relativa all'erogazione del servizio dovrà essere comunicata ad Actalis, a pena di decadenza, entro 30 giorni dalla data dell'evento mediante raccomandata a/r;
- Actalis 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 Actalis, per quanto non previsto dal presente capitolo, sono riportate nelle condizioni contrattuali di fornitura del servizio rese pubbliche nel sito del Gestore: http://www.actalis.it.

8.4 Risoluzione del contratto

Actalis, 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

Actalis 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].

9. Protezione dei dati personali

Actalis dispone l'utilizzo di adeguate misure di sicurezza al fine di preservare la riservatezza, l'integrità e la disponibilità di dati personali dell'Interessato. Specifiche misure di sicurezza sono osservate per prevenire la perdita dei dati, usi illeciti o non corretti ed accessi non autorizzati, ai sensi di quanto previsto dalla vigente normativa in materia ed in particolare dal Regolamento UE 2016/679 (GDPR).

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.

9.1 Tutela e diritti degli interessati

In ottemperanza a quanto previsto dalla vigente normativa in materia ed in particolare dal Regolamento UE 2016/679 (GDPR), art. 13 e segg., Aruba PEC rende agli Interessati idonea informativa sul trattamento dei dati personali nella quale sono riportati, oltre alle altre informazioni previste dalla citata normativa, i diritti dell'Interessato in materia e le modalità per l'esercizio dei medesimi, compresi i relativi riferimenti.