Aruba PEC S.p.A.

Manuale Operativo Posta Elettronica Certificata

Versione: 3.8
Data aggiornamento: 13/02/2025
Approvato da: Andrea Sassetti
Classificazione documento: pubblico

Andrea Sassetti
Firmato digitalmente il 13/02/2025 21:09:43 CET

VERSIONE N°	DATA	NATURA DELLA MODIFICA
1.0	04/07/2007	Prima emissione
1.1	06/05/2008	**Cap. 2**: Modificata Sede Legale, Capitale Sociale e numeri fax, **Par. 2.5:** Aggiunte certificazioni ISO, **Cap. 5**: Modificata dim. minima delle caselle PEC e procedure per la richiesta del servizio, **Par. 5.5**: Modificata procedura di richiesta rigenerazione password in caso di smarrimento, **Par. 5.6**: Modificata procedura di richiesta cancellazione caselle PEC, **Par. 5.9**: Modificata procedura di richiesta log, **Par. 9.7.7**: Aggiunte azioni promosse dal Gestore in caso di malfunzionamento, **Tutto:** Correzioni varie.
1.2	10/10/2008	**Cap. 2**: Modificato sito di riferimento, **Par. 2.2, 2.2.1, 2.2.2**: Modificato sito di riferimento del servizio, **Par. 4.3.4**: Aggiunti dettagli sul trattamento dei messaggi di posta, elettronica tradizionale (non PEC, **Par. 5.1**: Modificate le tipologie di servizio offerto, **Par. 5.3.1**: Aggiunta procedura per attivazioni di caselle su dominio del Gestore, **Par. 5.4.1**: Aggiunti dettagli sui client di posta in merito alla compatibilità con gli algoritmi di firma RSA, **Par. 6.9**: Aggiornate caratteristiche Webfarm, **Par 8.1**: Aggiunti e modificati obblighi per il Gestore, **Par 8.2**: Aggiunti e modificati obblighi per il Titolare, **Par. 8.4**: Aggiunta clausola di risoluzione del contratto.
1.3	07/11/2008	Modificato rappresentante legale di ArubaPEC, **Cap. 2**, **Par. 2.1, 2.2, 2.2.1, 2.2.2**: modificati indirizzi email per contattare il gestore.
1.4	20/02/2009	Modificato sito di riferimento del Gestore in www.pec.it, **Cap. 3** Aggiunto nuovo riferimento normativo, **Par. 5.1**: Modificate le tipologie di servizio offerto.

1.5	20/07/2011	**Par. 4.3.4**: modificate comunicazioni con le caselle di posta convenzionale, **Par. 4.3.5**: Aggiunto paragrafo su antispamming, **Cap. 5**: Aggiunte nuove tipologie di caselle, certificazione domini, come diventare Partner, strumenti per i Partner, modificate modalità di attivazione di caselle e domini, caratteristiche assistenza, interoperabilità con altri sistemi PEC, livelli di servizio.
2.0	29/04/2016	**Par. 1.2**: aggiornati riferimenti su responsabilità, **Par. 1.3**: riportate in questo paragrafo le definizioni di cui al **par. 4.2 v. 1.5** ed aggiornata definizione Titolare, **Par. 1.4**: aggiornata tabella di riferimento, **Cap. 2**: aggiunta sede erogazione servizio e aggiornati riferimenti telefonici assistenza e riferimento a email NOC, **Par. 2.5**: aggiornato scopo certificati ISO e relativi riferimenti, **Par. 4.2**: rimosse definizione, sostituito contenuto del paragrafo con paragrafo successivo "Funzionamento di un sistema di Posta Elettronica Certificata", aggiornati riferimenti a schema e schema stesso, **da Cap. 5 a Cap. 7**: riorganizzata struttura documento da cap. 5 a cap. 7 e modificato ordine capitoli (cap. 5 v.1.5. diventato cap. 7 in v.2.0, cap. 6 v1.5 diventato cap. 5 in v.2.0, cap. 7 v.1.5 diventato cap. 6 in v.2.0), **Cap. 5.9**: aggiornati riferimenti a strutture data center, **Par. 6.2**: aggiornati riferimenti a certificazioni ISO, **Par. 6.3:** aggiornato riferimento normativo, **Par. 6.3.1**: inserito riferimento a p.5.9, **Par. 6.3.3**: aggiornati riferimenti a sistema antivirus, **Cap. 7**: revisione completa dei contenuti, **Cap. 8.5**: aggiornato importo polizza e descrizione, **Cap. 9.6.2**: corretto riferimento a paragrafo, **Cap. 9.7.3**: corretto riferimento a paragrafo, **Tutto il documento**: modificato template documento, sostituiti riferimenti, ove attinenti, CNIPA o DigitPA con AGID.
2.1	22/05/2017	**Tutto il documento**: modificato il template documento; modificati i riferimenti a TSA. **Cap. 2**: modificato indirizzo Sede Legale, **Par. 2.1:** Aggiornato indirizzo Responsabile del Manuale Operativo **Par. 4.2.2**.: indicato periodo di conservazione dei log con virus, **Par.3.4** aggiornato collegamento al FIPS PUB 140-2 e inseriti riferimenti a certificazione Common Criteria **Par. 5.5**. Aggiornata Figura 3: componenti del sistema e relativa descrizione; rimossa figura 4. **Par. 5.8**. Specificate modalità di conservazione. **Par 7.4.2**: inserita possibilità offerta commerciale partner.
3.0	06/05/2019	**Tutto il documento**: modificato il template documento ed effettuate correzioni formali. Inoltre: **Par.1.3:** inserito riferimento a GDPR, **Cap.2:** aggiornati riferimenti Gestore, **Par.2.1:** modificato nominativo responsabile Manuale, **Par.2.2:** aggiornati canali di contatto, **Par.2.4:** aggiornato indirizzo web per download Manuale, **Cap.3:** inserito riferimento a GDPR, **Par.4.2.4:** inserite precisazioni su comunicazioni con indirizzi email non certificati, **Par.4.2.5:** inserite precisazioni su funzionalità antispam, **Par.5.9.1:** aggiornati dettagli connettività dei DC IT 1 e 2, **Par.5.9.2:** aggiornati riferimenti a alimentazione elettrica e sistema antincendio di DC IT 2, **Par.5.9.3:** aggiornati riferimenti a sistema antincendio di DC IT 1, **Par.6.3.1:** corretta modalità di accesso a sale dati, **Par.6.3.5:** inserito riferimento a GDPR, **Par.6.4 e 6.5:** spostato ex 9.6, **Par.7.2:** aggiornata tabella con caratteristiche casella e descrizione delle caratteristiche, **Par.7.3.3:** modificato paragrafo con inserimento descrizione accesso ed utilizzo tramite app Aruba Pec Mobile, **Par.7.3.4:** aggiornate modalità di modifica dei dati anagrafici Titolare, **Par.7.3.7:** aggiornati riferimenti per l'assistenza, **Par.7.3.8:** aggiornato intero paragrafo con consultazione dei log dei messaggi da parte del Titolare, **Par.7.5:** integrati indicatori di qualità su assistenza, **Par.8.2:** inserito riferimento a GDPR, **Cap.9 e Par.9.1-9-5:** revisionati in riferimento a GDPR.

3.1	20/11/2019	**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; **6.4.5:** eseguite piccole correzioni; **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; **7.2:** eseguite piccole correzioni; **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.
3.2	15/09/2020	Modifiche al modello di responsabilità
3.3	26/07/2021	**1.3:** modifiche a definizioni e acronimi e ordinamento alfabetico**; 4.1:** modifiche a introduzione**; 4.2**: modifiche 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**: aggiunte caratteristiche di sicurezza; **6.3.3**: aggiunte caratteristiche di sicurezza; **7.1:** modifiche al paragrafo;**7.2**: modifiche al punto ricezione email non certificate e numero massimo destinatari; **7.3:** modifiche al paragrafo; **7.3.1:** modifiche al paragrafo; **7.3.2**: modifiche a accesso e utilizzo tramite webmail; **7.3.3:** modifiche al paragrafo; **7.3.4:** aggiunte modifiche dati anagrafici; **7.3.5:** aggiunte a cambio di titolare; **7.3.6:** modifiche al paragrafo e inserimento divieto di riassegnazione casella PEC; **7.3.7:** modifiche al paragrafo; **7.3.8:** aggiunto riferimento richiesta log di una casella cancellata; **7.3.9**: aggiunte caratteristiche di sicurezza password; **7.4.1:** modifiche al paragrafo; **8.3**: modifiche al paragrafo.
3.4	20/07/2022	**Modifiche ai paragrafi:** 5.5; 6.3.3; 6.3.5; 7.2; 7.3.1; 7.3.2; 7.3.3; 7.3.5; 7.3.8; 7.5; 8.2. **Aggiunto paragrafo**: 7.3.10
3.5	05/08/2022	**7.7:** modifiche al paragrafo.
3.6	02/05/2023	**P. 1.2**: riformulazione del paragrafo; **P.1.3:** inserite definizioni di Fattore Biometrico e QRCode; **P. 2:** riformulazione del paragrafo e modifica dell'email generale del Gestore; **P. 2.5** confluito in **P. 6.2**; **P.5.3 – 5.4 – 5.4.2 - 5.5 – 5.9 (e sotto-paragrafi) – 6.3.1 – 6.3.3 – 6.3.5:** riformulazione paragrafi e sotto-paragrafi per garantire sicurezza e riservatezza di dati sensibili; **P. 6.4** e **P. 6.4.7** (che diventa **6.4.1**) riscrittura completa del paragrafo; **P. 7.3.2 – 7.3.10:** aggiornamento paragrafo per accesso con QRCode; **Aggiunto P. 7.3.11:** Autenticazione con QRCode; **P. 5.9.1 – 5.9.2 – 5.9.3 – 7.6.1 – 7.5:** inseriti riferimenti alla Control Room;
3.7	15/04/2024	**1.3:** inserita definizione di Richiedente; **7.1:** aggiornamento di alcuni passaggi del paragrafo; **7.2**: aggiornamento dei passaggi relativi allo spazio di archivio e agli avvisi; **7.3.4:** riformulazione del paragrafo; **7.3.8:** inserito chiarimento su conservazione a norma dei log e inserimento richiesta log Gestore cessante Actalis S.p.A.; **8.2:** aggiornamento di alcuni passaggi del paragrafo.
3.8	13/02/2025	**4.2.5**: integrazioni al paragrafo riguardo le misure antispam e antiphishing; **6.3.3**: integrazioni al paragrafo riguardo le misure antispam e antiphishing; **8.3:** revisione completa del paragrafo. Modifiche e correzione minori di refusi e di formattazione del documento.

Sommario

1. Informazioni di carattere generale

1.1 Scopo

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

1.2 Versione del manuale e responsabilità

ARUBA PEC è responsabile della stesura del presente documento.
La versione del manuale è riportata nel frontespizio e nel piè pagina.

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.

Fattore biometrico	Caratteristiche biometriche degli individui quali Impronta digitale o facciale (della retina o dell'iride), su cui si basa l'autenticazione per l'accesso a determinati sistemi.
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.
OTP – One time password	Il codice OTP è una password valida solo per una singola sessione di accesso/transazione che garantisce elevati standard di sicurezza
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	È il soggetto (Ente Pubblico, Aziende, Libero Professionista ecc.) attraverso il quale viene offerto il servizio di Posta Elettronica Certificata di Aruba PEC S.p.A. ai Titolari.
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.
QRCode	Quick response Code. Codice a barre bidimensionale che memorizza informazioni leggibili da un dispositivo, mediante un'apposita applicazione.
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.

Richiedente	Il soggetto che richiede l'attivazione del servizio di Posta Elettronica Certificata.
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 intestatario della 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 CNIPA
Cap. 2	Circolare 21 maggio 2009, n. CNIPA/CR/56 2.1 Manuale Operativo. **Punto a:** Dati identificativi del Gestore
Par. 2.1	Circolare 21 maggio 2009, n. CNIPA/CR/56 2.1 Manuale Operativo. **Punto b:** Indicazione del responsabile del manuale
Cap. 3	Circolare 21 maggio 2009, n. CNIPA/CR/56 2.1 Manuale Operativo. **Punto c:** Riferimenti normativi necessari per la verifica dei contenuti
Par. 2.4	Circolare 21 maggio 2009, n. CNIPA/CR/56 2.1 Manuale Operativo.

Manuale Operativo	Circolare CNIPA
	Punto d: Indirizzo del sito web del Gestore ove il manuale è pubblicato e scaricabile
Cap. 6	Circolare 21 maggio 2009, n. CNIPA/CR/56 2.1 Manuale Operativo. **Punto e:** Indicazione delle procedure oltre che degli standard tecnologici e di sicurezza utilizzati dal Gestore nell'erogazione del servizio
Par. 1.3	Circolare 21 maggio 2009, n. CNIPA/CR/56 2.1 Manuale Operativo. **Punto f:** Definizioni, abbreviazioni e termini tecnici
Cap. 5, cap. 7	Circolare 21 maggio 2009, n. CNIPA/CR/56 2.1 Manuale Operativo. **Punto g:** Descrizione e modalità del servizio offerto
Par. 7.3.8	Circolare 21 maggio 2009, n. CNIPA/CR/56 2.1 Manuale Operativo. **Punto h:** Descrizione delle modalità di reperimento e di presentazione delle informazioni presenti nei log dei messaggi
Par. 7.3	Circolare 21 maggio 2009, n. CNIPA/CR/56 2.1 Manuale Operativo. **Punto i:** Indicazione delle modalità di accesso e fornitura del servizio
Par. 7.5	Circolare 21 maggio 2009, n. CNIPA/CR/56 2.1 Manuale Operativo. **Punto j:** Indicazione dei 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	Circolare 21 maggio 2009, n. CNIPA/CR/56 2.1 Manuale Operativo. **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	Circolare 21 maggio 2009, n. CNIPA/CR/56 2.1 Manuale Operativo. **Punto l:** Indicazione delle procedure operative da attuare nel caso di cessazione dell'attività di gestore di posta elettronica certificata
Par. 1.2	Circolare 21 maggio 2009, n. CNIPA/CR/56 2.1 Manuale Operativo. **Punto m:** Indicazione della versione del manuale

2. Dati identificativi del Gestore

Aruba PEC S.p.A., società del Gruppo Aruba nata nel 2006 come Gestore di Posta Elettronica Certificata accreditato presso l'AgID (Agenzia per l'Italia Digitale), progetta, realizza e gestisce servizi e soluzioni nel campo e-security, essendo altresì accreditata presso AgID anche come Certification Authority, Conservatore a Norma e Gestore dell'Identità Digitale.
La sede legale di Aruba PEC è ubicata a Ponte San Pietro (BG), mentre l'erogazione del servizio è distribuita su due data center (primario e secondario) di proprietà del Gruppo Aruba.
Di seguito si riportano in dettaglio i dati identificativi di Aruba PEC:

Dati identificativi del Gestore	
Ragione Sociale:	Aruba PEC S.p.A.
Sede Legale:	Via San Clemente, 53 24036 – Ponte San Pietro (BG)
Partita IVA:	01879020517
Iscrizione registro delle imprese:	Iscritta al registro delle imprese di Bergamo con numero 01879020517
REA:	445886
Capitale sociale:	€ 6.500.000 (interamente versati)
Siti web:	www.pec.it
Email:	CPS-requests@ca.arubapec.it

2.1Responsabile del Manuale Operativo

Il soggetto responsabile del presente Manuale Operativo all'interno di Aruba PEC è:

- **Andrea Sassetti (Responsabile del Servizio PEC)**

Richieste di informazioni o chiarimenti sul presente Manuale Operativo possono essere inviate tramite posta elettronica all'indirizzo CPS-requests@ca.arubapec.it.

2.2 Canali di comunicazione

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

- Call center e assistenza tecnica sul servizio:
  - secondo le specifiche riportate sul sito https://assistenza.aruba.it
- Emergenze tecniche tra i Gestori (*solo per Gestori*):
  - Telefono +39-0575050012
  - Email noc@comunicazioni.pec.aruba.it e/o supporto.gestori@staff.aruba.it

2.3 Modifiche al manuale

Il presente manuale potrà, nel futuro, subire modifiche dettate dalla necessità di adattare il sistema a nuove normative che verranno emesse da parte degli organi competenti. Il manuale sarà inoltre

aggiornato nel caso in cui si rendano necessarie modifiche ed ottimizzazioni al sistema o cambiamenti relativi alle modalità di erogazione del servizio e dell'offerta da parte di ARUBA PEC.
ARUBA PEC garantisce in qualsiasi momento la coerenza del manuale con la versione del sistema.
Tutte le future modifiche del Manuale verranno sottoposte a verifica ed approvazione interna ad opera dei responsabili del servizio.

2.4 Indirizzo web del Gestore dal quale scaricare il manuale

All'interno del sito web del Gestore (https://www.pec.it) è disponibile la copia in formato pdf del presente documento. Il file può essere scaricato all'indirizzo https://www.pec.it/termini-condizioni.aspx.
ARUBA PEC garantisce che sul sito sia sempre pubblicata l'ultima versione esistente ed approvata del manuale operativo.

3. Principali riferimenti normativi

[1] Decreto Legislativo 30 giugno 2003, n. 196 e s.m.i. – Codice in materia di protezione dei dati personali.

[2] 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] 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] Decreto Legislativo 7 marzo 2005, n. 82 e s.m.i. - Codice dell'Amministrazione Digitale (CAD).

[5] 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 presentazione della domanda di iscrizione nell'elenco pubblico dei gestori di posta elettronica certificata (PEC) di cui all'articolo 14 del decreto del Presidente della Repubblica 11 febbraio 2005, n. 68.

[7] Decreto-legge del 29 novembre 2008, n. 185 - 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.

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.

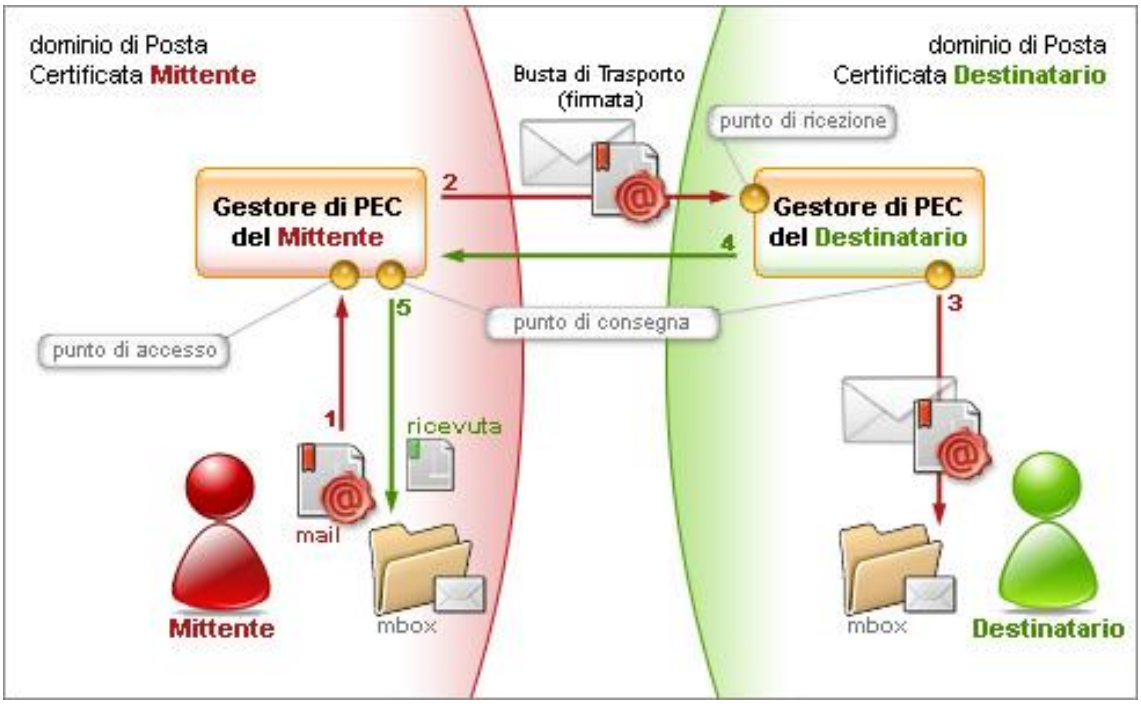

Figura 1 - Funzionamento di un sistema di PEC

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.

L'elenco delle estensioni che non è possibile veicolare attraverso messaggi PEC è riportato al link https://guide.pec.it/posta-pec/sicurezza-servizio-pec/limitazioni-alle-estensioni-degli-allegati-pec.aspx

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 ARUBA PEC 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 la Webmail 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 Messaggi contenenti spam e phishing

Il Gestore Aruba PEC si impegna a preservare la sicurezza del sistema PEC a tutela degli utenti e delle terze parti che vi fanno affidamento analizzando i messaggi in entrata e in uscita.

Nel caso di messaggi in entrata, il Gestore intercetta contenuti di spam e phishing contrassegnandoli con apposito *tag* e spostandoli automaticamente nella cartella spam dedicata.

In aggiunta, a fronte di rilevazione di caselle PEC che veicolano acclarate campagne phishing di tipo malevolo, i messaggi inviati da tale casella non verranno consegnati generando un avviso di mancata consegna.

Nel caso di messaggi originati da posta elettronica ordinaria, l'utente 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,
- di disattivare o abilitare le regole antispam, fornite di default.

Per gli invii di messaggi da PEC a le caselle di posta elettronica ordinaria è inoltre attivo un filtro antispam applicato ai messaggi in uscita che riconosce e blocca i messaggi spam, avvisando l'utente con specifici messaggi.

5. Descrizione della soluzione tecnica definita da ARUBA PEC

5.1 Principali caratteristiche

La soluzione di ARUBA PEC 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)

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.
Il sistema è strutturato logicamente su tre livelli, descritti di seguito:

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 e rappresenta: l'interfaccia verso il mondo esterno, il principale centro di elaborazione, l'interfaccia verso i dispositivi di memorizzazione e sincronizzazione temporale delle macchine.

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

L'architettura della soluzione è descritta nel dettaglio all'interno di documentazione riservata.

In generale il corretto funzionamento del Servizio è garantito dal nucleo centrale del sistema che si interfaccia con gli altri moduli, come il Mail Transfer Agent, i moduli Antivirus, i database dove sono memorizzati i dati relativi alle caselle (utenti, domini, titolari, …), i server LDAP, il server LMTP, i moduli HSM utilizzati per la firma dei messaggi, il modulo di autenticazione. Nell'ambito di tale architettura, inoltre, la componente di verifica prevede il controllo:

- di allegati con estensioni o mime type non validi;
- di macro all'interno di allegati con formato Office;
- di allegati non verificabili quali ad esempio archivi cifrati o archivi compressi protetti da password.
- antivirus.

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 del CNIPA in materia di riproduzione e conservazione dei documenti su supporto ottico, è necessario definire un intervallo temporale unitario, non superiore alle ventiquattro ore, entro il quale eseguire senza 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 ARUBA PEC, compatibilmente con la normativa, verifica la presenza dei virus nei messaggi di posta elettronica al Punto di Accesso, ossia nella fase immediatamente successiva alla spedizione del messaggio originale, e al Punto di Ricezione, nella fase di ricezione dal sistema di posta certificato del mittente.
L'individuazione del virus fa scattare una serie di operazioni finalizzate ad avvertire il soggetto che ha introdotto il virus ed alla conservazione del messaggio per eventuali verifiche successive.
Se il virus è individuato al Punto di Accesso verrà generato un "Avviso di rilevazione di virus informatici" destinato al mittente del messaggio corrotto mentre se è stato individuato al Punto di Ricezione verrà generato un "*Avviso di non accettazione per virus informatici*" destinato al Gestore del sistema certificato del mittente e un "*Avviso di mancata consegna per rilevazione di virus informatici*" destinato al mittente.
Il sistema inoltre, conserva i messaggi contenenti virus su supporto ottico o magnetico mettendo in condizioni il Gestore di mantenerli per un periodo non inferiore a trenta mesi secondo le modalità indicate nelle deliberazioni 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 di ARUBA PEC

Riportiamo di seguito le principali caratteristiche dei due Data Center ARUBA PEC che permettono l'erogazione del Servizio PEC. (Data Center primario e secondario).

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, per ciascun Data Center, 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 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 alla Control Room), è presente un meccanismo automatico di esclusione della macchina stessa (failover).

5.9.2 Data Center primario

Alimentazione:

Aruba utilizza per i propri servizi esclusivamente server ed apparati dotati di doppia alimentazione. All'uscita di ogni singolo Power Center vi sono dispositivi STS (Static Transfer Switch) in grado di garantire comunque continuità dell'alimentazione elettrica di entrambe le linee presenti, garantendo così il funzionamento anche dei server ed apparati che non dispongono di doppio alimentatore. L'alimentazione fornita ai server è completamente ridondata grazie a due Power Center separati. Ogni Power Center ha la capacità di alimentare tutte le sale dati presenti all'interno dei data center proprietari, anche a pieno carico, ed è dotato di sistemi UPS a doppia conversione ad altissima efficienza energetica (per il Data center primario, ridondanza di tipo 2N+1). I sistemi di alimentazione dei data center partner sono anch'essi completamente ridondati e dotati di sistemi UPS a doppia conversione.

Climatizzazione:

- 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, 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 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 ed 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, del tipo UNDER con mandata aria sotto pavimento e con aspirazione dalla parte superiore dell'unità direttamente dall'ambiente.

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 controllato;
  - 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 antincendio a gas inerte (Azoto), rilevamento elettronico, sistema antifumo;
- impianto di rilevamento liquidi e sistema 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 e di distribuzione del gas inerte 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.
- Control Room attiva 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 qualsiasi problema.

5.9.3 Data Center secondario

Alimentazione:

Aruba utilizza per i propri servizi esclusivamente server ed apparati dotati di doppia alimentazione. All'uscita di ogni singolo Power Center vi sono dispositivi STS (Static Transfer Switch) in grado di garantire comunque continuità dell'alimentazione elettrica di entrambe le linee presenti, garantendo così il funzionamento anche dei server ed apparati che non dispongono di doppio alimentatore. L'alimentazione fornita ai server è completamente ridondata grazie a due Power Center separati. Ogni Power Center ha la capacità di alimentare tutte le sale dati presenti all'interno dei data center proprietari, anche a pieno carico, ed è dotato di sistemi UPS a doppia conversione ad altissima efficienza energetica (per il Data center secondario, ridondanza di tipo 2N+1). I sistemi di alimentazione dei data center partner sono anch'essi completamente ridondati e dotati di sistemi UPS a doppia conversione.

Climatizzazione:

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

Sicurezza:

- Sicurezza fisica e degli accessi:
  - sale dati ed "aree" sensibili protette da accesso controllato;
  - 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 antincendio a gas inerte (Azoto e Argon), rilevamento elettronico, sistema antifumo.
- Impianto di rilevamento liquidi e sistema 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 e di distribuzione del gas inerte 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.
- Control Room attiva 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 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.
ARUBA PEC ha conseguito la certificazione **ISO 27001** in data 28 settembre 2007. Successivamente in data 03/02/2016 il certificato è stato inserito all'interno del certificato 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.
Lo standard si basa sui seguenti principi:

- **Information Security**: preservare confidenzialità, integrità e garantire la disponibilità delle informazioni.
- **Confidentiality**: assicurarsi che le informazioni siano accessibili solo a coloro che sono autorizzati.
- **Integrity**: salvaguardare l'accuratezza e la completezza delle informazioni e preservare la tecnica con la quale le informazioni vengono processate.
- **Availability**: assicurarsi che informazioni siano disponibili ed accessibili al personale autorizzato, quando necessario.

- **Risk Assessment, Risk Analysis**: rilevare le minacce ed il loro impatto sul sistema, analizzare la vulnerabilità delle informazioni e dei processi, calcolare la probabilità che gli eventi accadano.
- **Risk Management**: identificare, controllare, contenere, eliminare il security risk di cui è eventualmente affetto il sistema.

ARUBA PEC ha inoltre conseguito la certificazione **ISO 9001** (Qualità) in data 05 ottobre 2007. Successivamente in data 08/01/2016 il certificato è stato inserito all'interno del certificato multi-sito del Gruppo Aruba.
Il dominio di certificazione comprende sia per ISO 9001 che per ISO 27001 anche i servizi di Posta Elettronica Certificata ed è riportato in modo completo sia sul sito del Gestore ARUBA PEC all'indirizzo https://www.pec.it/ChiSiamo.aspx che sul sito della capogruppo Aruba S.p.A. all'indirizzo https://www.aruba.it/certificazioni.aspx .

6.3 Misure di sicurezza

Il sistema di posta elettronica certificata di ARUBA PEC presenta tutte le garanzie di sicurezza compatibili con la tipologia di servizio erogato, sia a livello fisico che a livello informatico.
Riportiamo di seguito le principali misure di sicurezza adottate per garantire l'integrità, la protezione e la riservatezza dei dati. Tali misure sono riportate, in maniera approfondita, nel **Piano della Sicurezza**, un documento riservato, consegnato 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 2FA (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.

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 periodo 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 ARUBA PEC viene realizzata attraverso l'adozione di una serie di misure di sicurezza descritte di seguito in modo sintetico.
Tali misure sono poi 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.

- Presenza di firewall con definizione di policy di accesso.

- Sistema di antivirus, antispam e antiphishing, costantemente ed automaticamente aggiornato in modo da proteggere il sistema PEC contro le varie tipologie di attacchi informatici.
- Prodotti software costantemente aggiornati.
- 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.
- Componente di verifica che prevede il controllo di allegati con estensioni o mime type non validi; di macro all'interno di allegati con formato Office; di allegati non verificabili quali ad esempio archivi cifrati o archivi compressi protetti da password; e antivirus.
- Tramite la sezione Gestione Account: è possibile accedere alla sezione "Storico accessi" tramite la quale visualizzare dispositivi e cronologia degli accessi effettuati alla casella PEC (nei sei mesi precedenti) e segnalare eventuali accessi che non si riconoscono come propri; è inoltre possibile modificare ed attivare la scadenza password, e verificare (o modificare) i contatti (email e cellulare) associati alla casella PEC ed utilizzati per compiere operazioni e ricevere eventuali avvisi relativi alla sicurezza. Tramite la sezione Gestione Account, è inoltre possibile attivare/disattivare l'autenticazione a due fattori per l'accesso alla casella PEC (cfr. 7.3.10).

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.

6.3.5 Trasmissione e accesso ai dati da parte dell'Utente

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 credenziali personali;

- le credenziali di accesso ed i profili di accesso degli utenti sono gestiti da procedure supportate da strumenti software e/o hardware idonea a rendere sicura l'identificazione dell'Utente;
- gli utenti autorizzati sono responsabili dell'osservanza delle procedure e delle misure di sicurezza definite da ARUBA PEC.

6.3.6 Misure di sicurezza degli ambienti fisici

ARUBA PEC 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

A garanzia dell'esaustività dell'elenco di minacce, è presa come riferimento la lista di minacce dello standard ISO/IEC 27005, a cui si aggiungono le considerazioni prodotte e pubblicate da ENISA a valle dei suoi studi in materia. Le categorie di minacce comprese nello standard ISO/IEC 27005 sono le seguenti:

- physical damage;
- natural events;
- compromise of functions;
- human error;
- loss of essential services;
- disturbance due to radiation;
- technical failures;
- compromise of information;
- unauthorised actions.

Le singole minacce, sono successivamente raggruppate in scenari di rischio realistici per il contesto analizzato della PEC. Per maggiori dettagli rispetto alle analisi condotte sugli scenari di rischio specifici del servizio si rimanda al Piano di sicurezza.

6.4.1 Azioni promosse dal Gestore in caso di incidenti e malfunzionamenti

In linea con quanto definito dall' art. 14bis, comma 2, lettera i) del decreto legislativo 7 marzo 2005, n. 82 e successive modifiche ("CAD") e sulla base delle indicazioni della circolare CNIPA n.51/2006, ed alle successive indicazioni di AgID, ARUBA PEC informa AgID dei malfunzionamenti e degli incidenti riscontrati nel proprio sistema.
Inoltre, a seconda della gravità dell'incidente e sempre in accordo con le indicazioni dell'Agenzia per l'Italia Digitale, Aruba PEC potrà autosospendere il servizio e 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. e fino a quando il problema è stato risolto.

6.5 Procedure operative

Per l'erogazione del servizio di posta elettronica certificata ARUBA PEC mette in atto una serie di procedure tecniche ed organizzative che hanno l'obiettivo di garantire un livello di servizio elevato e costante nel tempo.
L'obiettivo viene raggiunto con un'organizzazione attenta del personale, una gestione programmata dei backup, un accurato e costante monitoraggio del sistema e con l'applicazione di procedure e metodologie di risoluzione dei problemi precise e consolidate.

6.5.1 Organizzazione del personale

Come previsto dal DM del 2 novembre 2005 [5], 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 ARUBA PEC 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 effettuati in maniera automatica 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 ARUBA PEC.
Una importante caratteristica del sistema di Monitoring è la capacità di escludere automaticamente gli apparati del sistema nel caso in cui ne venga accertato il malfunzionamento.

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).

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

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

- 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.

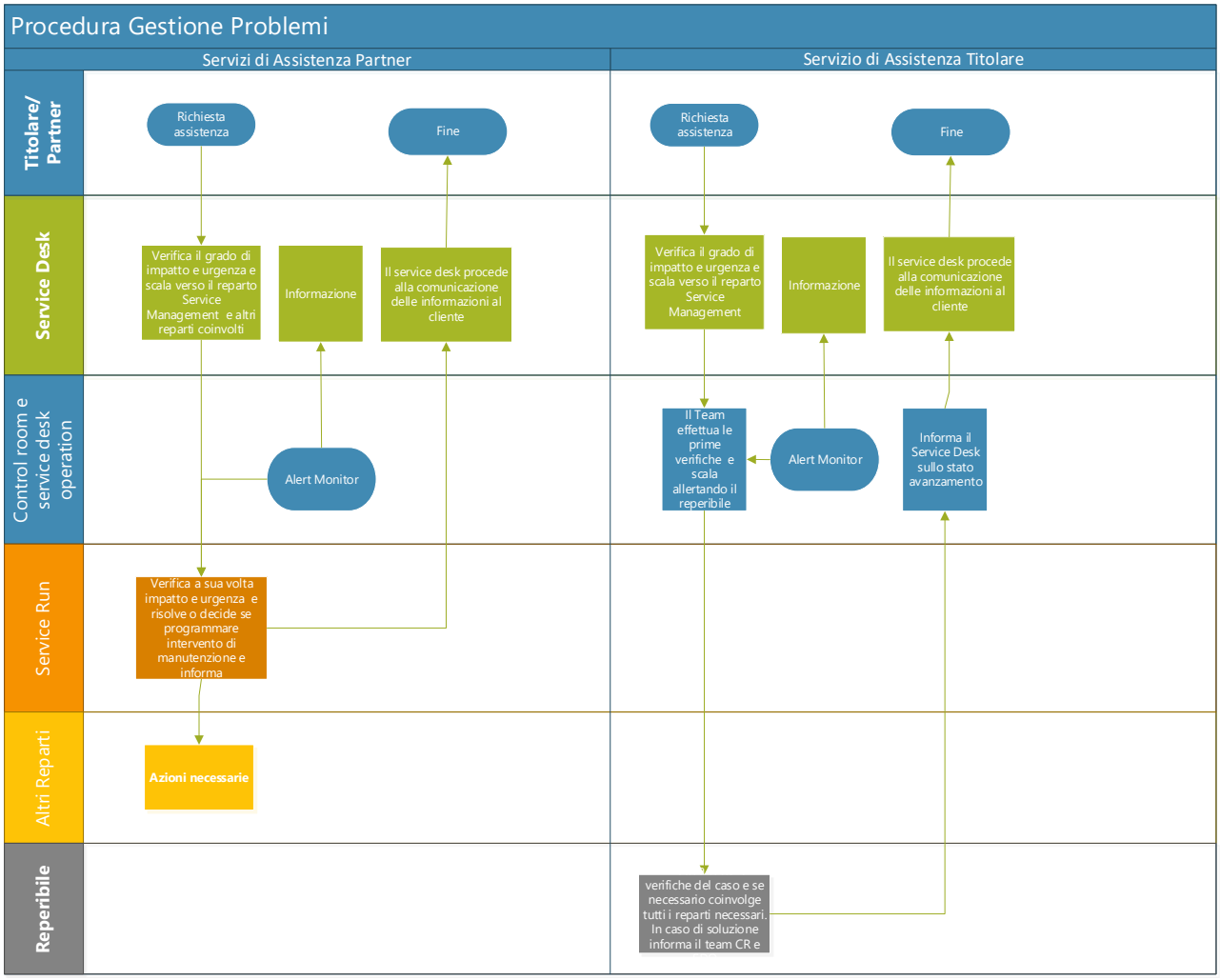

Figura 2 – Flusso di gestione dei problemi

7. Modalità di erogazione del servizio

7.1 Attivazione del Servizio

ARUBA PEC vende i propri servizi di Posta Elettronica Certificata sia direttamente che attraverso una rete di Partner, ovvero di soggetti interessati ad offrire ai propri utenti la soluzione di Posta Elettronica Certificata definita da ARUBA PEC.
Il flusso per la richiesta di attivazione di una casella PEC o di un dominio certificato da parte del Richiedente è , in generale, il seguente:

1. Il Richiedente formula la richiesta di attivazione del servizio ad un Partner di ARUBA PEC;
2. Il Partner, verificata la correttezza e completezza della richiesta, procede, tramite gli strumenti forniti dal Gestore, all'attivazione del servizio.

7.2 Tipologie di caselle

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
- PREMIUM

Al seguente link si possono visualizzare le principali caratteristiche dei 3 tipi di casella: https://www.pec.it/acquista-posta-elettronica-certificata.aspx

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

Spazio Casella: indica lo spazio che a livello contrattuale è disponibile sulla casella PEC per ricevere ed inviare messaggi. Al raggiungimento della quota contrattuale, se la casella è attiva è configurata in modo tale che sia possibile accedervi e ricevere i messaggi in entrata senza poterne inviare di nuovi fino all'adeguamento dello spazio casella. Per liberare spazio è necessario che il Titolare provveda in modo autonomo alla cancellazione dei messaggi; in alternativa, può acquistare spazio aggiuntivo o modificare la tipologia di casella, salvo diversi accordi contrattuali.
Avvisi via email/SMS: il servizio controlla quotidianamente la presenza di messaggi ricevuti e non letti nelle ultime 24 ore e, se presenti, invia un sms/email al canale indicato dal Titolare. Da webmail PEC è possibile gestire il servizio e impostare l'orario nel quale il controllo deve essere effettuato.
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. È altresì possibile abilitare, tramite la Webmail PEC, l'accesso all'archivio tramite IMAP. Inoltre, sempre tramite la Webmail PEC, è possibile attivare la cancellazione manuale dei messaggi, tramite la quale il cliente può autonomamente liberare spazio nell'archivio.

Notifica tramite email: Accedendo alla Webmail PEC è possibile indicare che si desidera ricevere una notifica via e-mail ad un determinato indirizzo tutte le volte che si riceve un messaggio di posta certificata.
Leggi Fatture: è la funzionalità per leggere dalla casella PEC le fatture elettroniche ricevute. Attivando questa funzione dalla Webmail PEC:

- tutte le fatture elettroniche ricevute vengono raccolte all'interno di una specifica cartella, che viene automaticamente creata all'interno della Webmail PEC e dell'app Aruba PEC;
- le PEC contenenti fatture elettroniche vengono contrassegnate da un'apposita icona, così da renderle immediatamente visibili nella posta in arrivo
- la fatture elettroniche (che sono in formato .xml) possono essere visualizzate in formato leggibile cliccando sul pulsante "Visualizza fattura" che viene mostrato nell'email

Aruba PEC App: è l'app che consente di inviare, ricevere e gestire la PEC direttamente da smartphone e tablet
Antivirus: il servizio antivirus è presente in tutti i tipi di caselle come previsto dalla normativa.
Antispam: il Titolare del servizio PEC ha la possibilità di attivare il servizio antispamming per filtrare i messaggi di posta ordinaria in arrivo.
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.
Ricezione mail non certificate: all'atto dell'attivazione la casella viene fornita "chiusa" nel senso che non le è permesso di ricevere messaggi di posta ordinaria (non PEC). Il Titolare, tramite **la Webmail PEC**, può modificare tale impostazione, scegliendo di consentire la ricezione di tali messaggi. Nel caso in cui il Titolare intenda lasciare l'impostazione iniziale e non ricevere messaggi tradizionali può reindirizzare tali messaggi verso una casella non PEC a sua scelta.
Se invece 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.
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.
Dichiarazione certificazione Casella: Per ogni casella certificata acquistata viene rilasciata la dichiarazione di certificazione casella che attesta che la casella è attiva.
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.
Webmail: per tutte le tipologie di casella è offerto al Titolare il servizio webmail per accedere da qualunque browser.

7.3 Accesso ed utilizzo del servizio

Il servizio di PEC fornito dal Gestore può essere utilizzato dal Titolare sia attraverso i più diffusi client di posta, attraverso un'applicazione webmail e tramite app con le modalità di seguito riportate.

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 e comunque resi disponibili sul sito del Gestore.
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.
Sul sito del Gestore vengono descritte le modalità di configurazione dei principali client di posta.
In caso di attivazione dell'autenticazione a due fattori (strong authentication, cfr. par. 7.3.10), sarà possibile accedere al client di posta elettronica solamente attraverso un token generato dal sistema secondo le procedure previste da AgID[1].
In qualsiasi momento, l'utente della casella PEC può gestire l'abilitazione dei protocolli di posta alternativi (POP3/S, IMAP/S, SMTP/S). Si ricorda che l'accesso alla webmail e all'app (cfr. par. 7.3.2 e 7.3.3.) è sempre garantito indipendentemente dalla configurazione effettuata sui protocolli di cui sopra.

7.3.2 Accesso ed utilizzo tramite webmail

Il Titolare ha la possibilità di accedere alla casella di PEC tramite applicazione webmail, alla quale può loggarsi inserendo le proprie credenziali (indirizzo e-mail e password). Qualora dovesse essere attivata l'autenticazione a due fattori (cft. 7.3.10), l'accesso avverrà anche mediante inserimento di un secondo fattore di autenticazione (come notifica push, OTP) o, se possibile, attraverso l'autenticazione con QRcode (cft. 7.3.11).
L'accesso alla webmail offre la possibilità di:

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

Per ogni messaggio inviato da casella PEC a casella PEC il Titolare ha la possibilità di scegliere il tipo di ricevuta di avvenuta consegna che intende ottenere dal destinatario. La ricevuta può essere completa (contiene il messaggio originale), breve (contiene una codifica hash del messaggio originale) o sintetica (contiene i soli dati di certificazione).

[1] L'accesso alla casella è garantito attraverso uno speciale token di sicurezza, che può essere inserito dall'utente in un qualsiasi client di posta elettronica standard, in luogo del campo "password", abilitandolo così ad accedere al servizio fornito dal Gestore PEC attraverso l'uso esclusivo e protetto dei classici protocolli SMTP/POP3/IMAP4, secondo quanto stabilito dalla Policy IT-AgID v.1.1, Allegato Tecnico v.1.1 - al par. 2.4.2.7 "Autenticazione su client di posta elettronica standard").

7.3.3 Accesso ed utilizzo tramite App Aruba PEC

Disponibile per Dispositivi IOS (versione 10.0 e successive) e Android (versioni 6.0 e successive), la APP consente di:

- accedere alla PEC da smartphone e tablet;
- configurare più account PEC attivi e scegliere quale utilizzare;
- leggere, cercare, creare e inviare messaggi;
- visionare l'elenco delle Cartelle di sistema (In arrivo, Bozze, SPAM, Posta inviata e Cestino) ed eventuali cartelle personalizzate create su Webmail PEC;
- visionare le informazioni relative alla casella, ad esempio il "Tipo" (Standard, PRO o PREMIUM) e la "Scadenza", lo spazio a disposizione e quello occupato, ecc..

7.3.4 Modifica dati anagrafici

Successivamente all'attivazione del servizio, alcuni dei dati anagrafici associati alla casella PEC possono essere modificati, in base alle caratteristiche e alla tipologia della modifica richiesta, dal Titolare o dal Richiedentein modo autonomo o tramite assistenza,così come descritto nel dettaglio al link https://guide.pec.it/posta-pec/modifica-dati/riepilogo-dati-modifiche-consentite.aspx,.
Invece per quelle acquistate tramite Partner, occorre effettuare la richiesta al proprio Partner.
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.
Attraverso il canale online, le modalità di cambio del Titolare sono descritte al seguente link: https://guide.pec.it/posta-pec/modifica-dati/modifica-titolare-casella-pec.aspx.
Attraverso il canale Partner, per ottenere la modifica è necessario che il Titolare ne faccia espressa richiesta al proprio Partner di riferimento avendo cura di fornire le seguenti informazioni:

1. I dati anagrafici del vecchio Titolare:
   - nome e cognome;
   - indirizzo di residenza (via, numero civico, città e CAP);
   - codice fiscale o partita iva.
2. Una copia del documento di identità del vecchio Titolare.
3. I dati anagrafici del nuovo Titolare:
   - nome e cognome;
   - indirizzo di residenza (via, numero civico, città e CAP);
   - codice fiscale o partita iva.
4. Una copia del documento di identità del nuovo Titolare;
5. Modulo cambio titolarità firmato da vecchio e nuovo Titolare;
6. Contatti di riferimento (email e cellulare) del nuovo Titolare.

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.

In ogni caso, si ricorda che il cambio intestatario di una casella comporta:

- l'attivazione automatica di meccanismi di sicurezza associati alla casella (come ad es. l'obbligo di reset password da parte del nuovo titolare);
- la disassociazione del dispositivo collegato alla verifica in 2 passaggi se attiva; il nuovo titolare al primo accesso potrà eseguire l'associazione con il proprio dispositivo;

L'attuale titolare provvede autonomamente alla cancellazione del contenuto della casella PEC, cioè eventuali messaggi e contatti. Aruba PEC, nelle operazioni di trasferimento della casella, non compie alcuna attività in relazione al contenuto della medesima.

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 PEC.
Per le caselle attivate tramite il canale Partner, il Titolare può richiedere al Partner la cancellazione: tale operazione comporta l'eliminazione, completa e irreversibile, di tutti gli eventuali dati in essa contenuti.
Per quanto riguarda la clientela online, per chiedere la disdetta del servizio PEC prima della data di scadenza dello stesso è necessario inviare ad Aruba specifica documentazione. Le procedure, alternative tra loro, sono indicate in modo dettagliato al link https://guide.pec.it/posta-pec/disdetta-servizio/disdetta-caselle-pec.aspx.

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 che viene erogato dal Gestore attraverso i riferimenti riportati sul sito https://assistenza.aruba.it.
A disposizione del Titolare vi sono inoltre pagine web che contengono le risposte a tutte le domande frequenti, oltre alle soluzioni ed alle guide per l'utilizzo dei servizi.
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. 7.4.2.

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 può procedere in autonomia alla consultazione dei log di suo interesse. Per far ciò, deve:

- accedere alla propria Webmail PEC;
- selezionare la specifica voce "PecLog", quindi impostare la ricerca secondo i parametri di interesse (data inizio, data fine, evento, oggetto del messaggio, destinatario, ecc.);
- visualizzare i risultati, che possono essere esportati (in formato CSV o PDF).

Nel caso di cancellazione della casella PEC entro i 30 mesi in cui il Gestore è tenuto a conservare i file di log, è possibile richiedere i Log dei messaggi che identificano la traccia dell'avvenuta transazione (non il contenuto dei messaggi), attraverso una richiesta di assistenza dal Portale di assistenza Aruba. In osservanza 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.
Aruba PEC conserva il registro dei log dei messaggi del gestore PEC cessante Actalis S.p.a., ai quali il titolare della casella può accedere mediante specifica richiesta ai canali di assistenza dedicati.

7.3.9 Password Policy

Aruba PEC 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. Vengono inoltre effettuati ulteriori controlli di sicurezza (impostazione della scadenza, riutilizzo ed altro) per garantire la corretta gestione delle password nel tempo. La password policy sarà applicata anche nel contesto dei clienti dei Partner di Aruba PEC 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.

7.3.10 Autenticazione a due fattori (2FA)

Per l'accesso alla casella PEC è possibile attivare il secondo fattore di autenticazione (autenticazione forte/2FA).
L'attivazione dell'autenticazione forte permette all'utente, tramite il possesso di un dispositivo personale associato a un numero di cellulare verificato, di accedere alla propria casella PEC tramite l'inserimento della password e di un secondo fattore di autenticazione (come notifica push, OTP).
L'attivazione dell'autenticazione a due fattori è opzionale, in quanto l'utente in ogni momento può decidere di abilitare/disabilitare il secondo fattore di autenticazione.
Qualora l'autenticazione a due fattori dovesse essere abilitata, è possibile accedere al client di posta elettronica solamente attraverso un token (cfr. par. 7.3.1).

7.3.11 Autenticazione con QRCode

È possibile effettuare l'accesso alla propria casella PEC via browser anche tramite autenticazione con QRcode, ovvero inquadrando il QRCode che appare sulla maschera di login del Servizio tramite l'App Aruba PEC (cft. 7.3.3).
Tale modalità di accesso è caratterizzata dai seguenti requisiti:

1. l'utente deve aver impostato l'autenticazione a due fattori per l'accesso alla casella PEC (cft. 7.3.10), e deve aver abilitato l'utilizzo del fattore biometrico (impronta digitale o impronta facciale) per l'accesso all'App Aruba PEC dal proprio dispositivo (smartphone/tablet);
2. l'utente deve aver effettuato l'accesso alla casella PEC dall'App Aruba PEC con la quale intende inquadrare il QRCode, e deve inquadrare il QRCode dal medesimo dispositivo associato alla casella PEC per l'autenticazione a due fattori (cft. 7.3.10);

3. effettuato l'accesso all'App Aruba PEC, l'utente deve ripetere l'inserimento del fattore biometrico per autorizzare l'accesso con QRCode via browser.

In caso di assenza, disabilitazione o fallimento del fattore biometrico per l'utilizzo dell'autenticazione con QRCode, l'utente potrà accedere alla casella PEC solo tramite inserimento delle credenziali (indirizzo email, password e OTP).
L'autenticazione con QRCode tramite App Aruba PEC viene inoltre inibita qualora il fattore biometrico sia stato modificato rispetto al precedente utilizzo. Per poterla utilizzare nuovamente, sarà necessario eseguire un nuovo accesso tramite le credenziali della casella PEC.

7.4 Partner ARUBA PEC

7.4.1 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, 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 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 (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.

7.4.2 Assistenza per il Partner

Il servizio di assistenza fornito da ARUBA PEC al Partner viene erogato attraverso 2 canali:

- telefono
- trouble ticketing

Il servizio è attivo in orario di ufficio (dalle ore 8.30 alle 18.00) dal lunedì al venerdì (esclusi festivi).
Il sistema di trouble-ticketing è stato pensato e creato per semplificare e velocizzare al massimo tutte le comunicazioni in merito alle richieste di supporto tecnico, amministrativo o commerciale.
Ad ogni variazione di stato delle richieste il Partner riceverà notifica via email.
ARUBA PEC mette a disposizione del Partner una pagina web che contiene le risposte allele domande più, oltre alle soluzioni ed alle guide per l'utilizzo dei servizi.

Il Partner può chiamare durante i suddetti orari per ottenere supporto sulle problematiche legate al servizio acquistato quali p.e. generalità sulla posta elettronica certificata (valore legale, funzionamento, interoperabilità con gli altri Gestori, interazioni con la pubblica amministrazione), configurazione del client di posta, funzionamento della webmail ecc.

7.5 Livelli di servizio ed indicatori di qualità

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

Livelli di Servizio	
Numero massimo di destinatari contemporanei accettati	500
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% del totale di indisponibilità previsto (considerando 0,2% il totale di indisponibilità previsto, quindi 0,1% per ogni singolo evento)
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 dalla propria Webmail PEC)	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

Indicatori di qualità	
Servizio di Assistenza Titolare	7/24/365
Servizi di Assistenza Partner	5 giorni la settimana (lun-ven) dalle ore 8.30 alle 18.00 escluso festivi
Assistenza di emergenza per i Gestori tramite la Control Room	7/24/365

7.6 Interoperabilità con gli altri sistemi di PEC

ARUBA PEC si impegna a garantire l'interoperabilità del proprio servizio di PEC con gli altri Gestori secondo quanto stabilito dalle Regole Tecniche di posta elettronica certificata (Decreto Ministeriale 2 novembre 2005 [5]).
ARUBA PEC inoltre verifica periodicamente l'interoperabilità del proprio sistema con gli altri Gestori accreditati attraverso uno scambio concordato di email.
A questo scopo ARUBA PEC 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 la Control Room 24 ore su 24, 7 giorni su 7.

7.7 Cessazione dell'attività di Gestore

Nel caso di cessazione dell'attività di Gestore PEC, ARUBA PEC 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.pec.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.
In caso di mancata individuazione del Gestore subentrante, ARUBA PEC specificherà nella comunicazione anche il periodo di tempo durante il quale le suddette caselle, pur non avendo funzionalità di invio/ricezione messaggi, saranno attive in sola lettura. ARUBA PEC inoltre conserverà i log per l'arco temporale previsto dalla Normativa e pertanto per un periodo non inferiore a 30 mesi.
Nel caso in cui il Gestore subentrante sia stato individuato, i log verranno invece trasferiti al Gestore subentrante che dovrà conservarli per l'arco temporale previsto dalla Normativa.

8. Obblighi e responsabilità

8.1 Obblighi e responsabilità del Gestore

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

Il Titolare si impegna a:

- Sollevare ARUBA PEC da ogni responsabilità in merito ai contenuti dei messaggi;
- fornire ad ARUBA PEC tutte le informazioni necessarie ad identificare la persona ed attivare il servizio, garantendo, sotto la propria responsabilità, la veridicità dei dati comunicati nonché di procedere all'aggiornamento degli stessi;
- utilizzare in modo sicuro il sistema evitando di rivelare o cedere a terzi le credenziali di accesso;
- utilizzare il servizio per i soli usi consentiti dalla legge ed in conformità con la stessa;
- 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. Resta inteso che tale dichiarazione è di esclusiva responsabilità del Titolare della casella;
- 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. Resta inteso che tale dichiarazione è di esclusiva responsabilità del Titolare della casella;
- 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 le sole modalità di accesso descritte al capitolo 7;
- resta a cura del Titolare della casella di posta elettronica certificata la conservazione delle copie dei messaggi inviati o spediti e delle relative ricevute. Il Gestore non effettua alcun back-up dei dati/informazioni contenuti nella casella, salvo quanto previsto dal contratto.

8.3 Limitazioni ed indennizzi

Gli obblighi e le responsabilità del Gestore Aruba PEC sono esclusivamente quelli definiti dal presente documento e dal Contratto di fornitura del Servizio al quale si fa espresso rinvio.

8.4 Risoluzione del contratto

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

8.5 Polizza assicurativa

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

9. Trattamento dei dati personali

Aruba PEC 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).

In particolare, le misure di sicurezza adottate, tra le quali quelle di cui al Cap. 6 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.