Aruba PEC S.p.A.

Addendum al Manuale Operativo Posta Elettronica Certificata

Servizio telematico di domicilio digitale attestato su impresa.italia.it

Versione: 1.1
Data: 20/07/2022
Redazione: Nicole Mazzoni, Valeria Favasuli
Verificato da: Federico Ciofi
Approvato da: Andrea Sassetti
Classificazione documento: Pubblico

Andrea Sassetti
Firmato digitalmente il 20/07/2022 10:36:19 CEST

VERSIONE N°	DATA	NATURA DELLA MODIFICA
1.0	09/08/2021	Prima emissione.
1.1	20/07/2022	**2.5:** inserimento paragrafo; **7.2**: modifiche al nome dell'app Aruba PEC; **7.3.3**: modifiche al nome dell'app Aruba PEC; **7.5**: modifiche al paragrafo.

Sommario

1. Informazioni di carattere generale

1.1 Scopo

Questo documento è un'Integrazione del Manuale Operativo Aruba PEC (in seguito citato con la sigla MO) che 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 MO vale per tutte le caselle di posta elettronica certificata erogate da Aruba PEC, senza distinzione per clienti e/o ambiti di applicazione.

Come parte del MO di Aruba PEC, questo documento si riferisce al contesto della PEC d'ufficio erogata dalle Camere di Commercio avvalendosi dei servizi informatici di InfoCamere, ed è sottoposto all'approvazione dell'AGID e pubblicato sul sito web di Aruba PEC.
Per tutto quanto non espressamente specificato nel presente documento, resta valido quanto descritto nel MO, al quale si rimanda (anche per i riferimenti normativi e tecnici eventualmente non riportati). Per agevolare la verifica incrociata, in questo documento è stata conservata, ove possibile, la stessa struttura e titolazione del MO.

Nel contesto specifico di questo documento, vengono descritte nel dettaglio le caratteristiche del servizio sperimentale telematico di "domicilio digitale attestato su impresa.italia.it" fornito ad InfoCamere da ArubaPEC, gestore accreditato di Posta Elettronica Certificata dal 12/10/2006 iscritto all'elenco pubblico gestito dall'Agenzia per l'Italia Digitale (AgID). Tale servizio consente di rispondere alle indicazioni previste all'art. 37, comma 1, lettera b del Decreto Semplificazioni (D.L. n. 76/2020 convertito, con modificazioni, dalla L. n. 120/2020), in cui viene affidato alle Camere di Commercio, Industria, Agricoltura ed Artigianato il compito di attribuire d'ufficio di un domicilio digitale (PEC d'ufficio) con sola funzione di ricezione, attestato presso il cassetto digitale dell'imprenditore (impresa.italia.it), sia alle imprese che non ne siano dotate, sia a quelle il cui domicilio digitale segnalato presso il registro delle imprese risulti inattivo.

Col termine "Manuale Operativo" (anche citato con la sigla MO) s'intende sempre riferirsi alla versione corrente del Manuale Operativo generale pubblicata sul portale web di Aruba PEC all'indirizzo https://www.pec.it/termini-condizioni.aspx#pec
I riferimenti alla normativa e agli standard sono riportati tra parentesi quadre.

1.2 Versione del manuale e responsabilità

ARUBA PEC è responsabile della stesura del presente documento.

Il presente documento è un'integrazione al Manuale Operativo relativo al servizio PEC d'ufficio erogato da InfoCamere. La versione di riferimento del MO è quella pubblicata sul sito web di Aruba PEC (si veda il par. 1.2 del MO).

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.
Conservatore del Registro delle imprese	Soggetto posto a capo dell'Ufficio del Registro delle imprese di ciascuna Camera di Commercio, Industria, Agricoltura ed Artigianato, ai sensi dell'art. 2188 del codice civile e dell'art. 8 della l. n. 580/1993. e.

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.
Domicilio Digitale	Un indirizzo elettronico eletto presso un servizio di posta elettronica certificata o un servizio elettronico di recapito certificato qualificato, come definito dal regolamento (UE) 23 luglio 2014 n. 910 «Regolamento eIDAS», valido ai fini delle comunicazioni elettroniche aventi valore legale.
Dominio di posta elettronica certificata	È un dominio, fully qualified domain name (FQDN), di posta elettronica certificata dedicato alle caselle di posta elettronica certificata.
Firma del Gestore di posta elettronica certificata	La firma elettronica avanzata, basata su un sistema di chiavi asimmetriche, che consente di rendere manifesta la provenienza e di assicurare l'integrità e l'autenticità dei messaggi del sistema di posta elettronica certificata, generata attraverso una procedura informatica che garantisce la connessione univoca al Gestore e la sua univoca identificazione, creata automaticamente con mezzi che garantiscano il controllo esclusivo da parte del Gestore.
Gestore di posta elettronica certificata	È il soggetto che gestisce uno o più domini di posta elettronica certificata con i relativi punti di accesso, di ricezione e di consegna, Titolare della chiave usata per la firma delle ricevute e delle buste e che si interfaccia con altri Gestori di posta elettronica certificata per l'interoperabilità con altri titolari.
HSM	Hardware Security Module. È un dispositivo hardware per la generazione, la memorizzazione e la protezione sicura di chiavi crittografiche.
HTML	HTML (acronimo per Hyper Text Mark-Up Language) è un linguaggio usato per descrivere i documenti ipertestuali disponibili su Internet. Non è un linguaggio di programmazione, ma un linguaggio di markup, ossia descrive il contenuto, testuale e non, di una pagina web.
HTTPS	Con il termine HTTPS ci si riferisce al protocollo HTTP (Hyper Text Transfer Protocol) utilizzato in combinazione con lo strato SSL (Secure Socket Layer).

Indice dei Gestori di posta elettronica certificata	È il sistema, che contiene l'elenco dei domini e dei Gestori di posta elettronica certificata, con i relativi certificati corrispondenti alle chiavi usate per la firma delle ricevute, degli avvisi e delle buste, realizzato per mezzo di un server Lightweight Directory Access Protocol, di seguito denominato LDAP, posizionato in un'area raggiungibile dai vari Gestori di posta elettronica certificata e che costituisce, inoltre, la struttura tecnica relativa all'elenco pubblico dei Gestori di posta elettronica certificata.
InfoCamere S.C.p.A	La società consortile delle Camere di Commercio italiane per l'innovazione digitale che gestisce per conto delle medesime la struttura informatica del sistema camerale. Di seguito anche solo InfoCamere.
INI-PEC	Il pubblico elenco dei domicili digitali di imprese e professionisti, denominato "Indice nazionale dei domicili digitali" (INI-PEC), istituito presso il Ministero dello sviluppo economico.
LDAP	Lightweight Directory Access Protocol. È un protocollo di rete utilizzato per la ricerca e memorizzazione di informazioni su un Directory Server. Una directory server LDAP è un albero di entità costituite da attributi e valori. Un classico utilizzo di un directory server è la memorizzazioni degli account email o degli utenti registrati ad un sito.
LMTP	Local Mail Transport Protocol.
Marca temporale	Evidenza informatica con cui si attribuisce, ad uno o più documenti informatici, un riferimento temporale opponibile ai terzi secondo quanto previsto dal decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 e dal decreto del Presidente del Consiglio dei Ministri 13 gennaio 2004, pubblicato nella Gazzetta Ufficiale n. 98 del 27 aprile 2004.
Messaggio originale	Il messaggio inviato da un Utente di posta elettronica certificata prima del suo arrivo al punto di accesso e consegnato al Titolare destinatario per mezzo di una busta di trasporto che lo contiene.
MTA	Mail Transfer Agent. È un modulo che ha il compito di effettuare il dispatching dei messaggi di posta elettronica (invio e ricezione)
NTP	Network Time Protocol.
Partner	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.

PEC d'ufficio	La casella di Posta Elettronica Certificata assegnata e attivata dal Conservatore del Registro delle Imprese per il ricevimento di comunicazioni e notifiche ai sensi dell'art. 37 del D.L. n. 76/2020 convertito, con modificazioni, dalla L. n. 120/2020.
Punto di accesso	Il sistema che fornisce i servizi di accesso per l'invio e la lettura di messaggi di posta elettronica certificata, nonché i servizi di identificazione ed accesso dell'Utente, di verifica della presenza di virus informatici all'interno del messaggio, di emissione della ricevuta di accettazione e di imbustamento del messaggio originale nella busta di trasporto.
Punto di consegna	Il sistema che compie la consegna del messaggio nella casella di posta elettronica certificata del Titolare destinatario, verifica la provenienza e la correttezza del messaggio ed emette, a seconda dei casi, la ricevuta di avvenuta consegna o l'avviso di mancata consegna.
Punto di ricezione	Il sistema che riceve il messaggio all'interno di un dominio di posta elettronica certificata, effettua i controlli sulla provenienza e sulla correttezza del messaggio ed emette la ricevuta di presa in carico, imbusta i messaggi errati in una busta di anomalia e verifica la presenza di virus informatici all'interno dei messaggi di posta ordinaria e delle buste di trasporto.
Ricevuta breve di avvenuta consegna	La ricevuta nella quale sono contenuti i dati di certificazione ed un estratto del messaggio originale.
Ricevuta completa di avvenuta consegna	La ricevuta nella quale sono contenuti i dati di certificazione ed il messaggio originale.
Ricevuta di accettazione	La ricevuta, firmata con la chiave del Gestore di posta elettronica certificata del mittente, contenente i dati di certificazione, rilasciata al mittente dal punto di accesso a fronte dell'invio di un messaggio di posta elettronica certificata.
Ricevuta di avvenuta consegna	La ricevuta, firmata con la chiave del Gestore di posta elettronica certificata del destinatario, emessa dal punto di consegna al mittente nel momento in cui il messaggio è inserito nella casella di posta elettronica certificata del destinatario.

Ricevuta di presa in carico	La ricevuta, firmata con la chiave del Gestore di posta elettronica certificata del destinatario, emessa dal punto di ricezione nei confronti del Gestore di posta elettronica certificata mittente per attestare l'avvenuta presa in carico del messaggio da parte del sistema di posta elettronica certificata di destinazione, recante i dati di certificazione per consentirne l'associazione con il messaggio a cui si riferisce.
Ricevuta sintetica di avvenuta consegna	La ricevuta che contiene i dati di certificazione.
Riferimento temporale	Informazione contenente la data e l'ora che viene associata ad un messaggio di posta elettronica certificata.
Registro delle imprese	Un registro pubblico informatico previsto dal Codice Civile, che ha avuto completa attuazione a partire dal 1993 con la Legge n. 580/1993 relativa al riordino delle Camere di Commercio e con il successivo Regolamento di attuazione.
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

2. Dati identificativi del Gestore

Il servizio PEC è erogato da Aruba PEC S.p.A., identificata come riportato nel MO.

2.1 Responsabile del Manuale Operativo

Il responsabile del presente documento è il medesimo del MO (cfr. il paragrafo 2.1 del MO).

2.2 Canali di comunicazione

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

- Emergenze tecniche tra i Gestori (*solo per Gestori*):
  - Telefono +39-0575050012
  - Email noc@comunicazioni.pec.aruba.it e/o gestori@staff.aruba.it

Per assistenza al servizio della PEC d'ufficio InfoCamere si rimanda ai canali descritti nel par. 7.3.7

2.3 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#pec

ARUBA PEC garantisce che sul sito sia sempre pubblicata l'ultima versione esistente ed approvata del manuale operativo e del presente documento.

2.4 Certificazioni ISO

ARUBA PEC ha conseguito la certificazione di qualità ISO 9001 in data 05 ottobre 2007. Ha conseguito inoltre la certificazione ISO 27001 in data 28 settembre 2007. Successivamente in data 08/01/2016 e 03/02/2016 i due certificati sono stati inseriti 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 .

2.5 Modifiche all'Addendum

Il presente documento potrà, nel futuro, subire modifiche dettate dalla necessità di adattare il sistema a nuove normative che verranno emesse da parte degli organi competenti. Il documento 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 documento con la versione del sistema. Tutte le future modifiche del documento verranno sottoposte a verifica ed approvazione interna ad opera dei responsabili del servizio.

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.

[10] Decreto-legge del 16 luglio 2020, n.76 - Misure urgenti per la semplificazione e l'innovazione digitale (Decreto Semplificazioni) convertito con modificazioni dalla L. 11 settembre 2020. n. 120.

4. Informazioni generali sulla Posta Elettronica Certificata

4.1 Introduzione

Il funzionamento del sistema di Posta Elettronica Certificata (PEC) è il medesimo descritto all'interno del paragrafo del MO.

4.2 Funzionamento di un sistema di Posta Elettronica Certificata

Il funzionamento del sistema di Posta Elettronica Certificata (PEC) è il medesimo descritto all'interno del paragrafo del MO, con la differenza che nel contesto della PEC d'ufficio le caselle di Posta elettronica certificata saranno abilitate solamente alla ricezione di messaggi di posta certificati, per cui non è possibile effettuare l'invio di alcun messaggio di posta.

4.2.1 Messaggio formalmente non corretto

Resta valido nella sua interezza quanto descritto all'interno del paragrafo del MO, al quale si rimanda.

4.2.2 Presenza virus

Resta valido nella sua interezza quanto descritto all'interno del paragrafo del MO, al quale si rimanda.

4.2.3 Ritardi di consegna

Resta valido nella sua interezza quanto descritto all'interno del paragrafo del MO, al quale si rimanda.

4.2.4 Comunicazioni con indirizzi email non certificati

Non applicabile al contesto della PEC d'ufficio. Le caselle di Posta elettronica certificata nel contesto della PEC d'ufficio saranno abilitate solamente alla ricezione di messaggi di posta certificati.

4.2.5 Antispam

Non applicabile nel contesto della PEC d'ufficio.

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.
- L'accesso ai contenuti dei messaggi ricevuti è previsto in sola modalità autenticata via API;
- I protocolli POP3/S, IMAP/S, SMTP/S sono inibiti. Pertanto i principali client di posta tra i quali Thunderbird, Outlook, etc., non possono accedere al servizio di Posta Elettronica Certificata per la consultazione dei messaggi.
- È basata su un'infrastruttura Hardware con caratteristiche di scalabilità, modularità e sicurezza nella gestione dei dati sensibili (Chiavi di Firma).
- 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

Resta valido nella sua interezza quanto descritto all'interno del paragrafo del MO, al quale si rimanda.

5.3 Sicurezza dei dati

Resta valido nella sua interezza quanto descritto all'interno del paragrafo del MO, al quale si rimanda.

5.4 Architettura di massima del sistema

L'architettura del sistema è modulare, ossia scalabile ed estendibile. In qualsiasi momento è, infatti, possibile aggiungere, aggiornare o effettuare un upgrade delle macchine. Come per il servizio PEC, 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.
I router di sistema, sia per la sede di via Gobetti che per quella di via Ramelli, sono connessi ai vari carrier, garantendo così un alto livello di tolleranza ai guasti nel caso in cui si verifichino problemi nella connessione verso uno dei 2 carrier stessi.
Dietro i router sono presenti, sia per la sede di Via Ramelli che per quella di Gobetti, degli apparati switch che gestiscono i link verso i router e rappresentano i root switch dell'intera rete.
Dietro gli switch sono presenti sistemi di load balancing e di monitoring.
Gli apparati hanno la funzione di bilanciare il carico per tutte le macchine della rete e di monitorare i processi dell'intero sistema. Nel caso di malfunzionamento di una macchina, oltre alla segnalazione del problema al Network Operations Center (NOC), è presente un meccanismo automatico di esclusione della macchina stessa (failover).

Il sistema è altamente ridondato e garantisce quindi un elevato livello di tolleranza ai guasti. Oltre alla ridondanza della rete elettrica e della connettività viene infatti assicurata anche la ridondanza di tutte le macchine coinvolte. Ogni servizio erogato viene svolto da almeno 2 macchine che, al presentarsi di eventuali problemi, possono essere temporaneamente escluse.

5.5 Architettura della soluzione

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

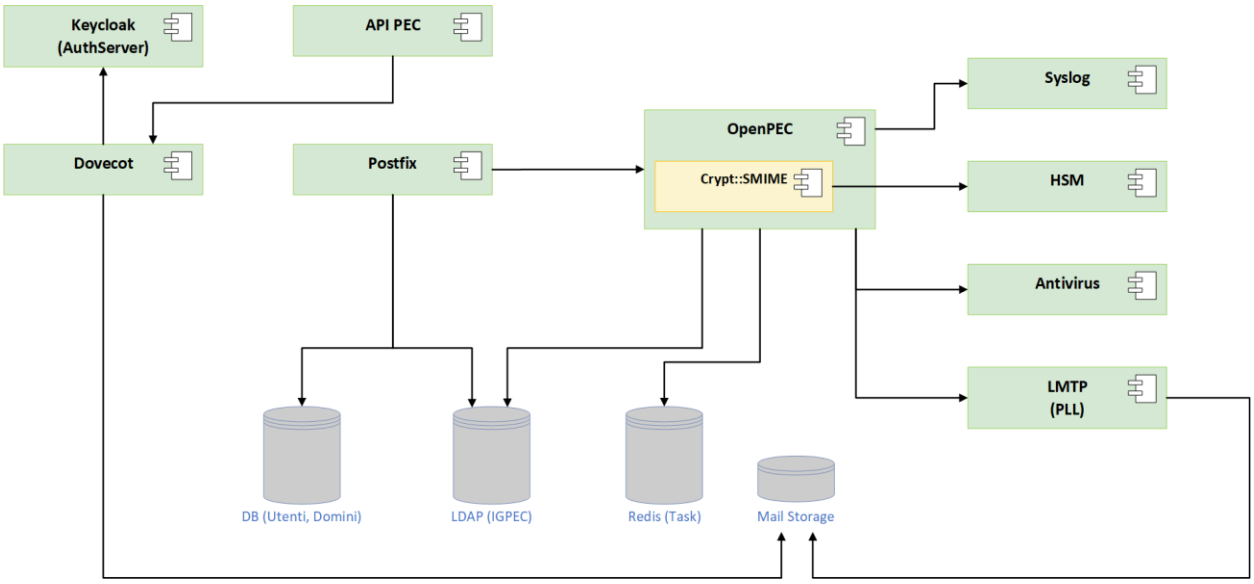

Figura 1 - Componenti del sistema

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

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.

L'accesso alle caselle del domicilio digitale dell'impresa in sola lettura sarà mediato da specifiche API con autenticazione OAuth2; i server di InfoCamere otterranno un token, per conto dell'utente autenticato sul portale impresaitalia.it, dall'IdentityProvider Keycloak e lo useranno per richiamare le API di lettura.

A livello di trasporto i servizi di autenticazione e di lettura delle caselle PEC saranno protetti da mutual TLS e controllo su IP chiamante.

5.6 Riferimenti temporali

Resta valido nella sua interezza quanto descritto all'interno del paragrafo del MO, al quale si rimanda.

5.7 Storicizzazione dei Log e apposizione della marca temporale

Resta valido nella sua interezza quanto descritto all'interno del paragrafo del MO, al quale si rimanda.

5.8 Conservazione dei messaggi contenenti virus e relativa informativa al mittente

Resta valido nella sua interezza quanto descritto all'interno del paragrafo del MO, al quale si rimanda.

5.9 Descrizione Data Center di ARUBA PEC

Resta valido nella sua interezza quanto descritto all'interno del paragrafo del MO, al quale si rimanda.

5.9.1 Connettività

Resta valido nella sua interezza quanto descritto all'interno del paragrafo del MO, al quale si rimanda.

5.9.2 Data Center di Via Ramelli (DC IT 2)

Resta valido nella sua interezza quanto descritto all'interno del paragrafo del MO, al quale si rimanda.

5.9.3 Data Center di Via Gobetti (DC IT 1)

Resta valido nella sua interezza quanto descritto all'interno del paragrafo del MO, al quale si rimanda.

6. Standard tecnologici, procedurali e di sicurezza adottati

6.1 Standard tecnologici di riferimento

Resta valido nella sua interezza quanto descritto all'interno del paragrafo del MO, al quale si rimanda.

6.2 Standard di sicurezza

Resta valido nella sua interezza quanto descritto all'interno del paragrafo del MO, al quale si rimanda.

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. In riferimento al contesto della PEC d'ufficio, ulteriori specifiche caratteristiche di sicurezza sono state riportate in maniera approfondita all'interno del relativo addendum del Piano della Sicurezza, anch'esso documento riservato.

6.3.1 Accesso ai locali di erogazione del servizio

Resta valido nella sua interezza quanto descritto all'interno del paragrafo del MO, al quale si rimanda.

6.3.2 Personale adibito alla gestione del sistema

Resta valido nella sua interezza quanto descritto all'interno del paragrafo del MO, al quale si rimanda.

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 quali:

- Presenza di firewall con definizione di policy di accesso (vengono abilitate le sole porte strettamente necessarie al funzionamento del sistema PEC).
- Sistema di antivirus costantemente ed automaticamente aggiornato sia per quanto riguarda le firme di virus riconosciuti che l'engine dell'antivirus, in modo da rendere il sistema protetto contro attacchi da parte di software malevolo.
- Prodotti software costantemente aggiornati (al rilascio di un nuovo prodotto o di una patch, dopo una fase di test su un ambiente di staging, viene aggiornato il prodotto in ambiente di produzione).
- Separazione fisica degli HSM, e del livello di front-end dal livello di back end e storage in modo da proteggere ulteriormente i dati da accessi indesiderati.
- Ulteriore protezione delle macchine che contengono i dati degli utenti attraverso firewall locali.
- Sistema ridondato in ogni sua parte in modo da evitare “single point of failure”.
- Meccanismo di auto esclusione degli apparati non funzionanti con conseguente dirottamento del traffico sugli altri nodi “gemelli”.
- Utilizzo di storage di rete esterni al sistema per aumentare la protezione delle informazioni degli utenti.
- Sistema di backup su doppio supporto per ridurre il rischio di perdita dei dati.
- Utilizzo del canale sicuro in fase di lettura di un messaggio (HTTPS).
- 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 veicolati tramite il servizio PEC d’ufficio.
- Sistema Breach Monitoring che monitora l’esposizione di caselle in conseguenza di data breach pubblici.

6.3.4 Controllo dei livelli di sicurezza

Resta valido nella sua interezza quanto descritto all'interno del paragrafo del MO, al quale si rimanda.

6.3.5 Trasmissione e accesso ai dati da parte dell’Utente

L’applicazione di accesso alle caselle PEC d’ufficio sarà messa a disposizione da InfoCamere a cui è demandata l’autenticazione utente; l’accesso ai sistemi PEC d’ufficio prevede un’autenticazione server OAuth2 su canale protetto da mutual TLS e controllo di indirizzo IP.

6.3.6 Misure di sicurezza degli ambienti fisici

Resta valido nella sua interezza quanto descritto all'interno del paragrafo del MO, al quale si rimanda.

6.3.7 Gestione emergenze

Resta valido nella sua interezza quanto descritto all'interno del paragrafo del MO, al quale si rimanda.

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 d'ufficio. Per maggiori dettagli rispetto agli scenari di rischio specifici del servizio si rimanda all'addendum del Piano della Sicurezza dedicato.
La metodologia di analisi dei rischi seguita fa riferimento alla tabella delle minacce comprese nello standard ISO/IEC 27005.

ISO 27005									
Threat				Origin			Perdita RID		
Threat Type_ID	Threat Type_ID	Threat Classification	Threat Class_ID	Accidental	Deliberate	Enviromental	R	I	D
T1	Physical damage	Fire	T1.1	X	X	X			X
		Water damage	T1.2	X	X	X			X
		Pollution	T1.3	X	X	X			X
		Major accident	T1.4	X	X	X			X

		Destruction of equipment or media	T1.5	X	X	X			X
		Dust, corrosion, freezing	T1.6	X	X	X			X
	Natural events	Climatic phenomenon	T1.7			X			X
		Seismic phenomenon	T1.8			X			X
		Volcanic phenomenon	T1.9			X			X
		Meteorological phenomenon	T1.10			X			X
		Flood	T1.11			X			X
T2	Compromise of functions	Abuse of rights	T2.1	X	X			X	
		Forging of rights	T2.2		X			X	
		Denial of actions	T2.3		X				X
		Breach of personnel availability	T2.4	X	X	X			X
		Dependency on a service provider	T2.5 (2.32)	X					X
		Violazione DLgs 196/2003	T2.6 (2.37)	X	X		X		
		Lack of, or inadequate, training of teleworkers	T2.7 (2.38)		X		X		
		Relevant statutory, regulatory and contractual violation	T2.8 (2.40)		X		X		
		Lack of law compliance	T2.9 (2.49)	X	X		X		
		Damage to files and data media due to an inadequate transport	T2.10 (2.23)	X	X				X
		Unauthorized use of copyrighted materia	T2.11 (2.18)		X		X		
		Damage to storage media	T2.12 (2.25)	X	X				X

		in the event of an emergency due to inadequate process of backup							
		Damage caused by third party	T2.13 (2.35)	X					X
		Information leakage	T2.14	X	X		X		
T3	Human error	Error in use	NA	X				X	
		Negligent destroying of equipment or data	T3.1 (3.2)	X	X				X
		Inadvertent damaging of cables	T3.2 (3.4)	X	X				X
		Hazards posed by cleaning staff or outside staff	T3.3 (3.5)	X	X				X
		Inadequate configuration of active network components	T3.4 (3.11)	X	X			X	
		Errors in configuration and operation	T3.5 (3.16)	X	X			X	
		Carelessness in handling information	T3.6 (3.17)		X			X	
		Inapropriate handling of passwords	T3.7 (3.18)		X		X		
T4	Loss of essential services	Failure of air-conditioning or water supply system	T4.1	X	X				X
		Loss of power supply	T4.2	X	X	X			X
		Failure of telecommunication equipment	T4.3	X	X				X
		Disturbance due to radiation	T4.4	X	X	X			X

	Disturbance due to radiation	Thermal radiation	T4.5	X	X	X			X
		Electromagnetic pulses	T4.6	X	X	X			X
	Technical failures	Equipment failure	T4.7	X					X
		Equipment malfunction	T4.8	X					X
		Saturation of the information system	T4.9	X	X				X
		Software malfunction	T4.10	X					X
		Breach of information system maintainability	T4.11	X	X				X
T5	Compromise of information	Interception of compromising interference signals	T5.1		X		X		
		Remote spying	T5.2		X		X		
		Eavesdropping	T5.3		X		X		
		Theft of media or documents	T5.4		X		X		
		Theft of equipment	T5.5		X		X		
		Retrieval of recycled or discarded media	T5.6		X		X		
		Disclosure	T5.7	X	X		X		
		Data from untrustworthy sources	T5.8	X	X			X	
		Tampering with hardware	T5.9		X			X	
		Tampering with software	T5.10	X	X			X	
		Position detection	T5.11		X		X		
	Unauthorised actions	Unauthorised use of equipment	T5.12		X			X	
		Fraudulent copying of software	T5.13		X		X		
		Use of counterfeit or	T5.14	X	X			X	

		copied software							
		Corruption of data	T5.15		X			X	
		Illegal processing of data	T5.16		X			X	

6.4.1 Azioni promosse dal Gestore in caso di malfunzionamento

Resta valido nella sua interezza quanto descritto all'interno del paragrafo del MO, al quale si rimanda.

6.5 Procedure operative

Resta valido nella sua interezza quanto descritto all'interno del paragrafo del MO, al quale si rimanda.

6.5.1 Organizzazione del personale

Resta valido nella sua interezza quanto descritto all'interno del paragrafo del MO, al quale si rimanda.

6.5.2 Gestione backup

Resta valido nella sua interezza quanto descritto all'interno del paragrafo del MO, al quale si rimanda.

6.5.3 Monitoring del sistema

Resta valido nella sua interezza quanto descritto all'interno del paragrafo del MO, al quale si rimanda.

6.5.4 Gestione e risoluzione dei problemi

Nel caso specifico della PEC d'ufficio per la gestione dell'assistenza si rimanda al par. 7.3.7.

7. Modalità di erogazione del servizio

7.1 Attivazione del Servizio

Il servizio di Posta Elettronica Certificata PEC d'ufficio sarà erogato dalle Camere di Commercio avvalendosi dei servizi informatici di InfoCamere, direttamente alle imprese [10].

Il servizio non potrà essere richiesto dal rappresentate legale dell'impresa, ma sarà assegnato d'ufficio dal Conservatore del Registro Imprese secondo quanto previsto nella normativa di riferimento [10].

7.2 Tipologie di caselle

Il servizio offrirà alle imprese una casella di Posta elettronica certificata in modalità SOLA LETTURA, senza una data di scadenza e con spazio illimitato.

Di seguito la tabella con le principali caratteristiche di una singola casella:

Servizi	
Spazio casella	Illimitato
Notifica SMS	NO
Archivio di sicurezza	NO
Notifica tramite email	NO
Leggi Fatture	NO
Aruba PEC App	NO
Antivirus	SI
Antispam	NO
IMAP	NO
Ricezione Email non certificate	NO
Filtri e regole messaggi	NO
Ricevute avvenuta/mancata consegna	NO
Validità legale messaggi ricevuti	SI

Non ripudiabilità del messaggio ricevuto	SI
Dichiarazione Certificazione casella	Gratuita
Conformità alla normativa vigente (DPR 11 febbraio 2005 n.68, DM 2 novembre 2005)	SI
Accesso webmail	NO
Accesso dai più comuni client di posta (Outlook, Outlook Express, Thunderbird, Eudora)	NO
Traffico	Illimitato
Dimensione max messaggio ricevuto (compresi allegati)	100 MB

Di seguito vengono descritti gli aspetti generali per le caratteristiche associate al servizio.

Spazio Casella: indica lo spazio disponibile sulla casella.

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

7.3 Accesso ed utilizzo del servizio

Il servizio di PEC d'ufficio può essere utilizzato solamente attraverso il Cassetto Digitale dell'impresa, gestito da InfoCamere per conto delle Camere di Commercio, autenticandosi tramite SPID o CNS, ai sensi dell'art. 64 del CAD [4]. Non sono previste credenziali quali username e password.

In particolare:

- Nel caso di utilizzo di SPID (persona fisica) o CNS, si verifica che il codice fiscale associato corrisponda a quello del Rappresentante legale associato all'impresa o ad altro soggetto abilitato ad accedere alle informazioni della stessa;
- Se si utilizza SPID (persona giuridica), si verifica che la Partita IVA associata a SPID corrisponda a quella dell'impresa a cui è stata assegnata la PEC d'ufficio.

Aruba fornirà ad InfoCamere un layer applicativo di API di Provisioning che consente di gestire tutto il ciclo di vita delle caselle: attivazione, disattivazione e modifica.

Aruba fornirà ad InfoCamere un layer applicativo di API di Accesso ai Messaggi che consente di gestire tutte le operazioni di base relative ai messaggi: ricerca, lettura, verifica stato.

L'accesso alle caselle PEC d'ufficio sarà garantito tramite un Identity Provider (fornito da Aruba a InfoCamere S.C.p.A.) che avrà il compito di autenticare l'utente ed autorizzarlo ad accedere alla propria casella di posta per la consultazione dei messaggi.

7.3.1 Accesso ed utilizzo tramite client di posta

Per il dominio ***impresa.italia.it*** i protocolli POP3/S, IMAP/S, SMTP/S saranno inibiti. Pertanto i principali client di posta tra i quali Thunderbird, Zimba, Mac Mail, Outlook, Outlook Express, etc, non potranno accedere al servizio di posta elettronica certificata per la consultazione dei messaggi.

7.3.2 Accesso ed utilizzo tramite webmail

Per il dominio ***impresa.italia.it*** non sarà disponibile l'applicazione Webmail, in quanto la consultazione dei messaggi di posta elettronica certifica avverrà solo attraverso il Cassetto Digitale d'Impresa gestito da InfoCamere.

7.3.3 Accesso ed utilizzo tramite App Aruba Pec

Per il dominio ***impresa.italia.it*** non sarà disponibile l'applicazione Aruba Pec, in quanto la consultazione dei messaggi di posta elettronica certifica avverrà solo attraverso il Cassetto Digitale d'Impresa gestito da InfoCamere.

7.3.4 Modifica dati anagrafici

Qualora dovesse verificarsi un cambio di anagrafica di un utente abilitato ad accedere al cassetto digitale di una società, tale cambiamento non comporta alcun tipo di modifica alla casella PEC d'ufficio, in quanto associata all'impresa e non ad utenti specifici.

7.3.5 Cambio di Titolare

Non applicabile nel contesto della PEC d'ufficio in quanto la casella PEC viene assegnata d'ufficio all'impresa dal Conservatore del Registro Imprese secondo quanto previsto nella normativa di riferimento [10].

7.3.6 Cancellazione di una casella PEC da parte del Titolare

Secondo quanto stabilito dal Decreto Semplificazioni [10], in caso di cessazione dell'impresa o nel caso in cui quest'ultima dovesse comunicare al Conservatore del Registro delle Imprese l'elezione di un nuovo domicilio digitale, InfoCamere S.C.p.A. potrà disattivare la casella PEC d'ufficio su richiesta firmata del Conservatore. Una volta disattivata, la PEC d'ufficio non potrà più ricevere

comunicazioni formali, ma è comunque resa disponibile all'interno del cassetto digitale per 180 giorni, per permettere la consultazione in sola lettura (con possibilità di download) dei messaggi di posta ricevuti fino al momento della disattivazione. Decorso tale periodo di tempo, la PEC d'ufficio sarà disabilitata e non sarà possibile procedere, in un momento successivo, alla riattivazione della stessa. In conseguenza di ciò, qualora trascorso detto periodo (180 giorni) l'impresa ricada nuovamente nell'ambito di applicazione di cui all'art. 37 del D.L. n. 76/2020 convertito, con modificazioni, dalla L. n. 120/2020, verrà attivato un nuovo e diverso Domicilio Digitale (PEC d'ufficio).

Aruba manterrà anche traccia di tutto il ciclo di vita di ogni singola casella PEC d'ufficio tramite file di audit all'interno dei quali saranno riportate tutte le operazioni di lettura dei messaggi e tutto il ciclo di vita della casella.

7.3.7 Assistenza

Per l'utenza di impresa.italia.it, InfoCamere rende disponibili:

- il numero di telefono dedicato 06 64892323, attivo dal lunedì al venerdì dalle 09:00 alle 18:00 per assistenza al primo accesso, utilizzo del cassetto digitale e domicilio digitale, per le imprese alle quali è attribuito.
- un web form per la compilazione di richieste di assistenza sulle categorie:
    - Informazioni generali
    - Accesso al servizio
    - Utilizzo del servizio
    - Domicilio Digitale art 37 l.n.120/2020
- un assistente virtuale, basato su interfaccia conversazionale, per fornire l'aiuto necessario alla configurazione e uso del dispositivo CNS in possesso dell'utente.
- pagina FAQ con le domande più frequenti e risposte liberamente consultabili dall'utenza con sezione speciale dedicata al Domicilio Digitale

7.3.8 Consultazione dei log dei messaggi da parte del Titolare

Aruba conserva i log delle PEC per un periodo pari a 30 mesi, come previsto dalla normativa di riferimento. Il titolare può richiedere l'accesso a tali informazioni inoltrando la richiesta di esibizione direttamente tramite i servizi o i canali messi a disposizione da InfoCamere S.C.p.A.

7.3.9 Password Policy

Non applicabile nel contesto della PEC d'ufficio in quanto l'accesso al servizio avverrà solamente tramite credenziali SPID o CNS.

7.4 Partner ARUBA PEC

7.4.1 Modalità operative per il Partner

Non applicabile nel contesto della PEC d'ufficio.

7.4.2 Assistenza per il Partner

Non applicabile nel contesto della PEC d'ufficio.

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	N.A.*
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)*	N.A.*

* Non applicabile nel contesto della PEC d'ufficio. Le caselle di Posta elettronica certificata nel contesto della PEC d'ufficio saranno abilitate solamente alla ricezione di messaggi di posta certificati [10].

Riportiamo qui di seguito gli indicatori di qualità del servizio.

Indicatori di qualità	
Recovery Time Objective (RTO): tempo necessario per il pieno recupero dell'operatività di un sistema	4 ore
Recovery Point Objective (RPO): tolleranza ai guasti del sistema informatico.	0 ore
Disponibilità del servizio di richiesta tramite InfoCamere da parte del Titolare della traccia delle comunicazioni effettuate (log)	7/24/365
Tempo massimo per l'invio da parte di Aruba PEC delle informazioni relative ai file di log di un messaggio di PEC dietro richiesta del Titolare ad InfoCamere e poi inoltrata ad Aruba PEC	5 giorni lavorativi
Servizio di assistenza telefonica reso da InfoCamere	06 64892323 - attivo dal lunedì al venerdì dalle 09:00 alle 18:00
Servizio di assistenza attraverso webform reso da InfoCamere	7/24/365
Servizio di assistenza tramite assistente virtuale reso da InfoCamere	7/24/365
Servizio di assistenza attraverso FAQ reso da InfoCamere	7/24/365

7.6 Interoperabilità con gli altri sistemi di PEC

ARUBA PEC si impegna a garantire l'interoperabilità del servizio di PEC d'ufficio 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 d'ufficio di test ai Gestori interessati ad effettuare test di interoperabilità con il proprio sistema.

7.6.1 Assistenza su segnalazioni gravi da parte degli altri Gestori

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

7.6.2 Passaggio a nuovo Gestore per fornitura PEC d'ufficio

Al termine del periodo di erogazione del servizio, il Gestore renderà disponibili i propri sistemi e strumenti per garantire il passaggio a nuovo gestore al fine di migrare le PEC d'ufficio assegnate ed il loro contenuto. Come previsto dalla normativa, il gestore uscente conserverà per 30 mesi i log dei messaggi e metterà a disposizione i propri canali per inoltrare eventuali richieste di accesso.

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, InfoCamere S.C.p.A. 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 salvo indicazione di InfoCamere di un nuovo Gestore.

Nella comunicazione ARUBA PEC specificherà anche il periodo di tempo durante il quale le suddette caselle saranno attive.

In ogni caso ARUBA PEC conserverà i log per l'arco temporale previsto dalla Normativa e pertanto per un periodo pari a 30 mesi.

8. Obblighi e responsabilità

8.1 Obblighi e responsabilità del Gestore

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

- garantire i livelli di servizio previsti;
- assicurare l'interoperabilità con gli altri Gestori accreditati;
- informare i titolari sui necessari requisiti tecnici;
- apporre la relativa marca temporale ai log dei messaggi generati dal sistema;
- rilasciare avviso di rilevazione di virus informatici;
- rilevare la presenza di virus o eccezioni formali nei messaggi mediante avviso di non accettazione;
- 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 InfoCamere nel rispetto della normativa vigente;
- effettuare la disattivazione di una casella PEC dopo aver verificato l'autenticità della richiesta;
- fornire informazioni sulle modalità di richiesta, reperimento e presentazione all'Utente dei log dei messaggi;
- utilizzare protocolli sicuri allo scopo di garantire la segretezza, l'autenticità, l'integrità delle informazioni trasmesse attraverso il sistema PEC;
- attivare la procedura di sostituzione dei certificati elettronici relativi alle proprie chiavi di firma con una tempistica tale da non causare interruzioni di servizio;
- richiedere la revoca dei certificati relativi alle chiavi utilizzate per la firma dei messaggi e per la connessione sicura al sito dell'AgID in caso di loro compromissione;
- operare in modo che non sia consentita la duplicazione abusiva e incontrollata delle chiavi private di firma o dei dispositivi che le contengono;

- consentire l'esportazione cifrata delle chiavi private di firma in modo da non diminuirne il livello di sicurezza;
- non consentire l'utilizzo delle chiavi private per scopi diversi dalla firma dei messaggi previsti dalla normativa;
- comunicare tempestivamente ai propri utenti l'eventuale cessazione o interruzione del servizio;
- consentire l'accesso logico e fisico al sistema alle sole persone autorizzate;
- utilizzare un sistema di riferimento temporale che garantisca stabilmente una sincronizzazione delle macchine coinvolte con uno scarto non superiore al minuto secondo rispetto alla scala di Tempo Universale Coordinato UTC;
- utilizzare dispositivi di firma conformi con la normativa.

8.2 Obblighi e responsabilità dei titolari

- Sollevare ARUBA PEC da ogni responsabilità in merito ai contenuti dei messaggi;
- utilizzare il servizio per i soli usi consentiti dalla legge;
- utilizzare soltanto il servizio di posta elettronica certificata erogato da Gestori accreditati (presenti nell'elenco pubblico dei Gestori tenuto da AgID);
- 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);
- resta a cura del Titolare della casella di posta elettronica certificata la conservazione delle copie dei messaggi ricevuti.

8.3 Obblighi e responsabilità di InfoCamere

- fornire ad Aruba PEC tutte le informazioni necessarie ad identificare il titolare ed attivare il servizio, garantendo, sotto la propria responsabilità che le medesime coincidano con quelle comunicate dalle Camere di Commercio;
- fornire ad Aruba PEC le richieste di attivazione sottoscritte dal Conservatore del registro nei tempi e modi concordati con il Gestore;
- fornire ad Aruba PEC le richieste di disattivazione sottoscritte dal Conservatore del registro nei tempi e modi concordati con il Gestore;
- informare i Titolari delle PEC d'ufficio e gli utilizzatori circa le regole d'uso del servizio;
- comunicare ad Aruba PEC le richieste di log legali, previa verifica della titolarità della richiesta stessa;
- garantire la corretta autenticazione al portale impresa.italia dei soli utenti abilitati alla consultazione della PEC d'ufficio;
- fornire assistenza di primo livello al titolare della PEC d'ufficio;

8.4 Limitazioni ed indennizzi

- ARUBA PEC non risponderà in alcun caso ai danni causati direttamente o indirettamente dagli utilizzatori del servizio imputabili ad un utilizzo improprio del sistema ed al mancato rispetto delle regole e degli obblighi contenuto nel presente manuale;
- ARUBA PEC non assume alcun obbligo riguardo la conservazione dei messaggi inviati e trasmessi attraverso le proprie caselle di PEC. Tale responsabilità viene assunta unicamente dal Titolare;
- ARUBA PEC non ha alcuna responsabilità sui contenuti dei messaggi inviati e ricevuti attraverso le proprie caselle di PEC;
- Aruba PEC risponde dei danni causati a qualsiasi persona fisica o giuridica in seguito al mancato adempimento dei propri obblighi indicati nel presente MO e di quelli previsti dalla normativa vigente in quanto applicabile;
- il Gestore non potrà in alcun modo essere ritenuto responsabile, a titolo esemplificativo ma non esaustivo, per danni derivanti da cause di forza maggiore, caso fortuito, eventi catastrofici (incendi, terremoti, esplosioni) o comunque non imputabili ad ARUBA PEC che provochino ritardi, malfunzionamenti o interruzioni del servizio;
- Qualsiasi contestazione del Titolare relativa all'erogazione del servizio dovrà essere comunicata ad InfoCamere, a pena di decadenza, entro 30 giorni dalla data dell'evento mediante raccomandata a/r o posta elettronica certificata;
- ARUBA PEC si riserva la facoltà di modificare il presente manuale nel caso in cui vengano apportate modifiche tecniche al sistema, variazioni all'offerta commerciale, o adeguamenti normativi. Le limitazioni di responsabilità, per quanto non previsto dal presente capitolo, sono riportate all'interno del documento di informativa sull' utilizzo del servizio PEC d'ufficio messo a disposizione al Titolare nel cassetto digitale dell'imprenditore.

8.5 Risoluzione del contratto

Non applicabile nel contesto della PEC d'ufficio in quanto la casella PEC viene assegnata d'ufficio all'impresa dal Conservatore del Registro Imprese secondo quanto previsto nella normativa di riferimento [10].

8.6 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

Resta valido nella sua interezza quanto descritto all'interno del paragrafo del MO, al quale si rimanda.

9.1 Tutela e diritti degli interessati

Non applicabile al contesto della PEC d'ufficio.