Aruba PEC S.p.A.

REMS practice statement/Practice Statement del Servizio Elettronico di Recapito Certificato Qualificato REM

Andrea Sassetti
Firmato
digitalmente il
30/07/2024
19:05:06 CEST

Versione: 1.1
Data aggiornamento: 25/07/2024
Approvato da: Andrea Sassetti
Classificazione documento: Pubblico

VERSIONE	DATA	NATURA DELLA MODIFICA
1.0	25/03/2024	Prima emissione
1.1	25/07/2024	Integrazioni Par. 7.1.1

Sommario

1. Introduzione

1.1 Informazioni di carattere generale

Il presente Manuale Operativo definisce le regole e descrive le procedure utilizzate da ARUBA PEC S.p.A. (di seguito per brevità ARUBA PEC) per l'erogazione del Servizio Elettronico di Recapito Certificato Qualificato (di seguito "Servizio") basato sullo standard REM, a norma del Regolamento (UE) n.910/2014 (Regolamento eIDAS).
Il Regolamento (UE) n. 910/2014 (eIDAS) definisce gli effetti giuridici di un servizio elettronico di recapito certificato (SERC) e i requisiti funzionali per i servizi elettronici di recapito certificato qualificati (SERCQ).
In virtù di questo, a livello europeo sono stati definiti una serie di standard con l'obiettivo di supportare lo sviluppo di servizi conformi ai requisiti specificati dal Regolamento eIDAS, in particolare relativi a "Electronic Registered Delivery Services (ERDS)" e "Registered Electronic Mail (REM) Services". All'interno degli standard ETSI sui SERC si è scelto di implementare il modello REM, un particolare servizio elettronico di recapito certificato qualificato basato su protocolli di posta elettronica e i relativi standard.
Nel contesto specifico di questo documento, vengono descritte nel dettaglio le caratteristiche e il funzionamento del Servizio che è conforme al Regolamento eIDAS, e quindi valido nell'ambito territoriale di applicazione di tale Regolamento, beneficiando delle presunzioni legali ivi previste.
Il contenuto del presente Manuale si riferisce al Servizio erogato da Aruba PEC, che soddisfa i requisiti delle Regole tecniche per i servizi di recapito certificato a norma del regolamento eIDAS n. 910/2014 e quelle adottate dall'Agenzia per l'Italia Digitale -AgID per definire i criteri di adozione dello standard ETSI avviando la transizione alla nuova REM e delle Norme ETSI relative alla fornitura dei servizi ERDS, reso disponibile mediante l'attivazione di un account di accesso al Servizio nelle modalità, con le caratteristiche e nei termini previsti dal Manuale stesso, senza distinzione per clienti e/o ambiti di applicazione.
ARUBA PEC eroga il suddetto Servizio in qualità di fornitore qualificato (QTSP o anche REMSP) come stabilito dal Regolamento eIDAS.
Il presente documento è pubblicato sul sito di Aruba PEC per garantire la massima trasparenza nei confronti degli utenti del Servizio e degli altri TSP/REMSP.
Col termine "Manuale Operativo/ Practice Statement" (anche citato con la sigla "MO" o per brevità "Manuale") si intende sempre riferirsi alla versione corrente del Manuale Operativo generale pubblicata sul sito 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 pubblicazione

ARUBA PEC è responsabile della stesura del presente documento.
La versione del presente Manuale è indicata sul frontespizio.
All'interno del sito web di Aruba PEC (https://www.pec.it) è disponibile la copia del Manuale in formato PDF firmato, in modo tale da assicurarne l'origine e l'integrità.
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.

1.3 Definizioni ed acronimi

Agenzia per l'Italia Digitale (AgID)	Ente Nazionale per la digitalizzazione della Pubblica Amministrazione.
Avviso di mancata consegna	L'avviso, emesso dal sistema, per indicare l'anomalia al mittente del messaggio originale nel caso in cui il Gestore sia impossibilitato a consegnare il messaggio nella casella di posta del destinatario.
Avviso di non accettazione	L''avviso, firmato con la chiave del Gestore 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.
Casella di posta elettronica (o solo Casella)	Casella di Posta Elettronica, valevole come recapito certificato qualificato, alla quale è associato un sistema di "trasporto" di documenti informatici che presenta delle forti similitudini con il servizio di posta elettronica "tradizionale", cui però sono state aggiunte delle caratteristiche tali da fornire agli utenti la certezza, con valore legale, della data ed ora di invio e consegna (o meno) dei messaggi e-mail al destinatario e l'identificazione del Titolare della stessa.
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 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 certificato	È un dominio, fully qualified domain name (FQDN), dedicato alle caselle REM.
ERDS	Electronic Registered Delivery Service
ERDSP	Electronic Registered Delivery Service Provider
ETSI	acronimo di "European Telecommunications Standards Institute", l'organismo internazionale, indipendente e senza fini di lucro ufficialmente responsabile della definizione e dell'emissione di standard nel campo delle telecomunicazioni nell'UE.
Firma del Gestore	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.
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).
LMTP	Local Mail Transport Protocol
Messaggio originale	Il messaggio inviato da un Utente prima del suo arrivo al punto di accesso e consegnato al Titolare destinatario per mezzo di una busta di trasporto che lo contiene.
MFA	Multi-Factor Authentication (MFA) è un metodo di autenticazione che richiede a un utente di fornire almeno due fattori di verifica per poter accedere a un servizio.
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.
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.
Partner	È il soggetto (Ente Pubblico, Azienda, Libero Professionista ecc.) che eroga ai richiedenti il Servizio oggetto del presente Manuale per conto di Aruba PEC.
Servizio	Denominazione del servizio elettronico di recapito certificato qualificato (anche SERCQ/QeRDS) offerto da Aruba PEC, oggetto del presente Manuale..
Punto di accesso	Il sistema che fornisce i servizi di accesso per l''invio e la lettura di messaggi di posta elettronica, 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 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 certificato, 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.
REM	Registered Electronic Mail: un particolare servizio elettronico di recapito certificato qualificato basato su protocolli di posta definiti ai sensi dell'art. 44 Regolamento UE n° 910/2014 - eIDAS e delle norme ETSI EN 319 521-522-531-532.
REM Baseline	Insieme minimo di requisiti volti a garantire l'interoperabilità tra i vari REM service provider che vi aderiscono, come indicato nello standard EN 319 532-4 [4], Clause C.1.
Richiedente	Il soggetto che richiede l'attivazione del Servizio

Riferimento temporale	Informazione contenente la data e l'ora che viene associata ad un messaggio trasmesso tramite SERCQ.
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.
SERCQ/QeRDS	Servizio elettronico di recapito certificato qualificato (disciplinato dagli artt. 43 e 44 Regolamento eIDAS). Nel contesto di questo Manuale, il SERCQ è denominato anche QeRDS. (Qualified electronic Registered Delivery Service).
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, ovvero del Servizio di recapito certificato qualificato fornito da ARUBA PEC, ed identificato in maniera certa.
TSA	Time Stamping Authority. Autorità che realizza il servizio di marcatura temporale di documenti informatici.
TSP/Gestore o Prestatore di servizi fiduciari qualificato	una persona fisica o giuridica che presta uno o più servizi fiduciari come prestatore di servizi fiduciari qualificato cui l'organismo di valutazione della conformità abbia assegnato tale qualifica. Nel contesto di questo Manuale, definito anche REMSP (Fornitore di servizi di posta basati su standard REM).
Utente	Persona fisica che fruisce del Servizio oggetto del presente Manuale.
Validazione temporale elettronica qualificata (comunemente definita marca temporale)	La validazione elettronica temporale qualificata è un'informazione contenente la data e l'ora associata ad uno o più documenti informatici. Il riferimento temporale è generato con un sistema che garantisce stabilmente uno scarto non superiore ad un secondo rispetto alla scala UTC. La validazione temporale elettronica qualificata applicata nell'ambito del Servizio oggetto del presente Manuale, è conforme a quanto previsto dall'art. 42 del Regolamento (UE) n. 910/2014.
Trusted list/TL	Raccoglie la lista dei SERCQ ed è un elemento essenziale e garante tra gli operatori del mercato elettronico, consentendo agli utenti di determinare

	lo stato qualificato e la cronologia dello stato dei prestatori di servizi fiduciari e dei loro servizi.

Definizioni tecniche specifiche del Servizio

REM Dispatch	Il messaggio, adeguatamente corredata di firma e timestamp qualificati, all'interno della quale sono inseriti il messaggio originale inviato dall'Utente di Posta Elettronica fornito da ARUBA PEC.
REM Submission Acceptance Evidence	La ricevuta, adeguatamente corredata di firma e timestamp qualificati, rilasciata al mittente dalla Message Submission Interface del proprio S-ERDS a fronte dell'invio di un messaggio di Posta Elettronica fornito da ARUBA PEC.
REM Content Consignment Evidence	La ricevuta, adeguatamente corredata di firma e timestamp qualificati, emessa dal R-ERDS nel momento in cui il messaggio è inserito nella casella di Posta Elettronica del destinatario.
REM Relay Acceptance Evidence	La ricevuta, adeguatamente corredata di firma e timestamp qualificati, emessa dalla Relay Interface del R-ERDS nei confronti del S-ERDS per attestare l'avvenuta presa in carico di un messaggio.
REM Relay Rejection Evidence	La ricevuta, adeguatamente corredata di firma e timestamp qualificati, emessa dalla Relay Interface del R-ERDS nei confronti del S-ERDS per attestare il rifiuto alla presa in carico di un messaggio.
REM Relay Failure Evidence	La ricevuta, adeguatamente corredata di firma e timestamp qualificati, emessa dalla Relay Interface del S-ERDS nei confronti dell''Utente mittente per attestare l'impossibilità alla presa in carico di un messaggio
REM Submission Rejection Evidence	L''avviso, firmato con la chiave del Gestore 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.
REM Content Consignment Failure Evidence	L'evidenza, adeguatamente corredata di firma e timestamp qualificati, 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.
REM Received From Non ERDS	Il messaggio, adeguatamente corredata di firma e timestamp qualificati, nella quale è inserito un messaggio errato o proveniente dall'esterno del circuito REM e consegnata ad un Titolare, per evidenziare al destinatario la provenienza non affidabile.
REM Common Service Interface	È la parte di infrastruttura condivisa che elenca e qualifica i QTSP a far parte del circuito REM.
S-ERDS - Sender's ERDS	È il servizio REM Mittente.
R-ERDS - Receiver ERDS	È il servizio REM Destinatario.

ERDS-RI - Relay Interface	La porzione del sistema ERDS adibita all'invio e alla ricezione di messaggi tra le diverse piattaforme ERDS all'interno del Dominio di interoperabilità o verso sistemi di posta all'esterno del REMID.
ERDS-MSI - Message Submission Interface	Il sistema che fornisce i servizi di accesso per l'invio di messaggi REM, nonché i servizi di identificazione ed accesso dell'Utente, di emissione della Relay Acceptance Evidence e di produzione dei REM Dispatch.
ERDS MERI - Message and Evidence Retrieval Interface	Il sistema che fornisce i servizi di accesso per la lettura di messaggi REM, nonché i servizi di identificazione ed accesso dell'Utente.
REMID - REM Interoperability Domain	Dominio di interoperabilità REM, rappresenta il circuito di servizi all'interno di cui le garanzie fornite dalla REM rimangono valide.

2. Dati identificativi del Gestore

Aruba PEC S.p.A., di seguito indicata per brevità anche solo "Gestore", è la società del Gruppo Aruba nata nel 2006 come Gestore di Posta Elettronica Certificata accreditato presso l'AgID (Agenzia per l'Italia Digitale), e Gestore del Servizio elettronico di Recapito Certificato Qualificato, che progetta, realizza e gestisce servizi e soluzioni nel campo e-security,. La sede legale di Aruba PEC è ubicata a Ponte San Pietro (BG), mentre le sedi di erogazione del Servizio sono distribuite 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

2.1 Responsabile del Manuale Operativo

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

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

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*):
  - Email noc@comunicazioni.pec.aruba.it e/o supporto.gestori@staff.aruba.it

2.3 Modifiche ed aggiornamento del 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.

La redazione e approvazione del presente Manuale segue le procedure previste dal Sistema di Gestione Qualità aziendale. Questo Manuale viene riesaminato e, se necessario, aggiornato con frequenza almeno annuale.

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 delle funzioni aziendali interessate e dal Responsabile del Servizio, tenendo conto di quanto indicato dalla norma ETSI EN 319 401 e ETSI EN 319 521, e successivamente pubblicate sul sito web di Aruba PEC come indicato al par. 1.1.

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

[4] 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.

[5] REGOLAMENTO (UE) N. 910/2014 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 23 luglio 2014 in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE (Regolamento eIDAS).

[6] Regole tecniche per i servizi di recapito certificato a norma del regolamento eIDAS n. 910/2014 – Criteri di adozione standard ETSI – REM Policy-IT (anche solo "Regole tecniche per i servizi di recapito certificato a norma del regolamento eIDAS"), adottate con Determina AGID N. 233/2022 e disponibili sul sito AgID.

Gli standard di riferimento sono elencati al par. 6.1.

4. Informazioni generali sul QeRDS

4.1 Funzionamento di un sistema QeRDS

Il titolare della casella attiva il Servizio a seguito di identificazione certa, accedendovi mediante autenticazione a due fattori (MFA), come descritto nel dettaglio al cap.7. Tutti i messaggi inviati dalla casella hanno le seguenti caratteristiche previste dagli standard europei per i servizi di recapito certificato qualificato:

- Headers, propri della REM;
- Allegati (evidence), per ogni evento generato dal flusso di invio/ricezione della REM.

Il traffico delle caselle di Posta (REM message ed evidence) sono multilingua per definizione. Esse prevedono di default la lingua inglese alla quale viene poi aggiunta la lingua italiana in quanto il Servizio, nell'ambito di questo documento, è erogato da un Gestore Italiano.

4.1.1 Rifiuto di messaggi

Nel caso in cui il messaggio inviato dal mittente non possa essere accettato per mancata conformità con gli standard di riferimento eIDAS o per motivi di sicurezza ad esempio per presenza di Virus, Malware o altre minacce il Gestore invia al proprio Utente (mittente) un Submission Rejection Evidence con cause '***Validation***' in risposta. Nel caso di presenza di virus la *cause* nella Submission Rejection Evidence cambia in '***Virus***' (Rejection con reason code RA03 da normativa eIDAS).

4.1.2 Ritardi di consegna

Nel caso in cui il Gestore del mittente non riceva alcun esito formale relativo al messaggio inviato nelle 24 ore successive alla spedizione, come previsto dalla REM Policy-IT [6] produce una Relay Failure Evidence con la quale informa il proprio Utente mittente che il messaggio ha superato i limiti di tempo per la consegna, che il messaggio non ha raggiunto la destinazione e che la spedizione deve considerarsi non andata a buon fine.

4.1.3 Comunicazioni con indirizzi email non accreditati

La REM Policy-IT [6] prevede che ogni REMSP abbia la possibilità di scegliere se consentire o meno la ricezione/invio da/verso sistemi esterni alla REM, anche in modalità selettiva: solo in ingresso o solo in uscita. Conseguentemente a tale scelta, ogni REMSP può consentire o meno all'utente di effettuare le proprie scelte di ricezione e invio di messaggi da/verso mittenti/destinatari esterni ai sistemi aderenti alla REM.

Per quanto riguarda l'invio di messaggi ad un sistema non REM, il mittente riceve una comunicazione di tipo **RelayToNonERDS** come Evidence a seguito di un invio di un messaggio ad un sistema NON REM andato a buon fine; e una comunicazione di tipo **RelayToNonERDSFailure come** Evidence a seguito di un invio di un messaggio ad un sistema NON REM non consentito o non andato a buon fine.

Per quanto riguarda la ricezione di messaggi di posta elettronica ordinaria (non REM), il Titolare del servizio ha la possibilità di decidere, tramite il pannello di Webmail, 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.
In questo caso, l'utente riceverà una comunicazione di tipo **ReceivedFromNonERDS** che presenterà nell'oggetto della mail il valore preimpostato 'REM EXTERNAL:<oggetto originale>. Per maggiori dettagli cfr. il paragrafo 4.2.

4.1.4 Antispam

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

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

L'Utente ha infine la possibilità di affinare le regole antispam impostando, ad esempio, il grado di sensibilità del filtro, le lingue dalle quali riceve abitualmente le comunicazioni, ecc.
È inoltre attivo lato server un filtro antispam applicato ai messaggi in uscita dalle caselle REM verso le caselle di posta elettronica ordinaria.

In particolare, il servizio antispam riconosce e blocca i messaggi di spam prima che questi entrino nel circuito REM, avvisando l'utente con specifici messaggi.

4.2 Dettaglio schematico Evidence REM

- Ricevute emesse da gestori REM

Tipo Evento	Evidence	Obbligatorietà	Descrizione evento
Invio (Submission)	SubmissionAcceptance	Sì	L'invio è la transazione in cui il messaggio originale, proveniente dall'esterno, passa attraverso il REM MSI (Message Submission Interface). La transazione comporta l'autenticazione del mittente.
	SubmissionRejection	Sì	
	RelayAcceptance	Sì	La presa in carico è la consegna di un
	RelayRejection	Sì	

Tipo Evento	Evidence	Obbligatorietà	Descrizione evento
Presa in carico (Relay)	RelayFailure	Sì	messaggio REM contenente il messaggio originale da un gestore REM ad un altro gestore REM tramite REM RI (Relay Interface). Solitamente è una transazione che utilizza il protocollo SMTP.
Accettazione/rifiuto da parte del destinatario	NotificationForAcceptance	No	L'accettazione o il rifiuto del messaggio sono previsti nel caso in cui il mittente e/o il destinatario utilizzano il modello Store & Forward, (previsto dalla REM Baseline e dalla Rem Policy IT al contrario della policy ETSI che permette anche lo Store & Notify).
	NotificationForAcceptanceFailure	No	
	ConsignmentAcceptance	No	
	ConsignmentRejection	No	
	AcceptanceRejectionExpiry	No	
Consegna (Consigment)	ContentConsignment	Sì	La consegna è la fase in cui il gestore del destinatario mette il messaggio del mittente a disposizione del destinatario in modo tale che quest'ultimo, dopo l'autenticazione, possa accedere al messaggio ricevuto. Il gestore del destinatario deve rilasciare le evidence sulla spedizione riuscita o non riuscita per ciascun messaggio.
	ContentConsignmentFailure	Sì	
	ConsignmentNotification	No	
	ConsignmentNotificationFailure	No	
	ContentHandover	No	

Tipo Evento	Evidence	Obbligatorietà	Descrizione evento
Passaggio di consegne (Handover)	ContentHandoverFailure	No	Il passaggio di consegne è la transazione in cui il messaggio del mittente viene reso disponibile allo User Agent a cui il destinatario si autentica per accedere alle sue mail.

- Ricevute emesse per invii tra gestore REM ed un gestore Non REM

Tipo Evento	Evidence	Obbligatorietà	Descrizione evento
Invio a destinatario non REM	RelayToNonERDS	No	Il Sistema REM può prevedere la possibilità di gestire delle evidence legate all'invio di messaggi tra un gestore REM ed un gestore Non REM. L'emissione delle ricevute previste in questo scenario consente al cliente del provider REM di capire se le mail sono state prese in carico dall'altro gestore; ciò, però, non assicura che esse siano realmente spedite al destinatario non REM
	RelayToNonERDSFailure	No	

5. Descrizione della soluzione tecnica definita da ARUBA PEC

5.1 Principali caratteristiche

Il Servizio di ARUBA PEC presenta le seguenti caratteristiche:

- È conforme alle specifiche eIDAS ed AgID ed alla normativa vigente in materia di REM.
- Fornisce le evidenze previste dagli standard ETSI e ratificate dalle attuali disposizioni AgID in materia di REM.
- Rispetta le caratteristiche di interoperabilità previsti dagli standard ETSI 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).
- Le marcature temporali sono generate secondo lo standard internazionale RFC3161 tramite l'utilizzo di una Time Stamping Authority integrata in modalità sicura. La validazione temporale elettronica qualificata utilizzata nell'ambito del servizio REM soddisfa i requisiti previsti dall'art. 42 del Reg. eIDAS;

- È interoperabile con qualsiasi Trusted Service Provider che soddisfi gli standard di interoperabilità ETSI.
- 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.
- I certificati di firma associati al servizio 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 di firme e delle marche temporali da apporre alle evidenze e ai messaggi che sono a loro volta conformi alle disposizioni eIDAS cosi come recepite nelle disposizioni AgID in materia di servizi fiduciari qualificati.

A tale scopo, la chiave privata del sistema 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 (http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf) o Common Criteria livello EAL4+ (https://www.commoncriteriaportal.org/products/).

5.4 Architettura di massima del sistema

Grazie all'installazione dei principali componenti su macchine separate è possibile 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 rappresenta: l'interfaccia verso il mondo esterno, il principale centro di elaborazione e l'interfaccia verso i dispositivi di memorizzazione.

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

Il livello contiene anche il nucleo centrale del sistema (REM Core). Inoltre il sistema si interfaccia con una Time Stamping Authority allo scopo di effettuare la marcatura giornaliera dei log e REM evidence

Il secondo livello si occupa anche di effettuare la firma dei messaggi attraverso appositi device chiamati Hardware Security Module (HSM).

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 e una cache dei dati necessari provenienti dalla Common Service Interface legati alla Trusted List.

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 REM Engine che rappresenta il nucleo centrale del sistema e si interfaccia con gli altri moduli: come il Mail Transfer Agent (MTA),, i moduli Antivirus, i database dove sono memorizzati i dati relativi alle caselle (utenti, domini, titolari, …), i server di accesso (POP3/IMAP/Webmail), la Trusted List, il server LMTP, i moduli HSM utilizzati per la firma dei messaggi, il modulo di autenticazione.

Nell'ambito di tale architettura:

- per i messaggi in uscita, la componente di verifica effettua una serie di controlli specifici sui file allegati, sul mime type, sulla presenza di macro ed eventualmente aggiunge gli header necessari;
- se è un messaggio in uscita, il REM Engine incapsulail messaggio in un documento di trasporto (REM Dispatch)appone le firme necessarie attraverso il modulo HSM e li restituisce all'MTA che li inoltra verso il destinatario;

- se è un messaggio in ingresso, il REM Engine verifica la correttezza delle firme e la validità del messaggio (provenienza da un dominio certificato), effettua il delivery verso la mailbox di destinazione attraverso il protocollo LMTP e, una volta consegnato il messaggio crea la REM Content Consignment Evidence che l'MTA invierà al mittente del messaggio originale.

Nel caso di non validità del messaggio REM Engine incapsula il messaggio in un documento di trasporto (REM Dispatch) e genera una evidenza ReceivedFromNonERDS che inoltra verso la mailbox dell'Utente;

I Log del sistema hanno valore giuridico e verranno mantenuti in appositi storage per il periodo previsto.
Il prodotto è stato progettato in modo tale da essere modulare, così da permettere future estensioni ed adattamenti.

5.6 Riferimenti temporali

Il riferimento temporale accluso alle evidenze prodotte dal servizio è prodotto in conformità a quanto previsto per le Marche temporali Qualificate dagli standard ETSI indicati dalle Regole tecniche per i servizi di recapito certificato a norma del regolamento eIDAS [5], come descritto ai par. 5.7 e 6.3.8.

5.7 Apposizione della marca temporale su log e ERDS evidence

Al fine della conservazione dei log dei messaggi, viene definito 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 sono conservati per il tempo stabilito dalla normativa (30 mesi), come meglio descritto al par. 6.3.8.In ottemperanza all'art. 44 da Regolamento eIDAS, Art. 44 punto 1/(f) e come previsto dalla REM baseline, la validazione temporale elettronica qualificata è applicata tramite firma XAdES-B-T ai REM message.

Il registro dove vengono tracciate tutte le transazioni relative agli eventi che innescano la conseguente generazione di ogni evidenza ad essi correlata (le cosiddette ERDS evidence) viene denominato "official log". Esso contiene gli eventi definiti dalle Regole tecniche per i servizi di recapito certificato a norma del regolamento eIDAS [5].

Il Gestore assolve alla funzionalità di memorizzazione e conservazione a lungo termine dell'official log per il periodo e le modalità stabilite dalle norme correnti (pari ad una durata di 30 mesi).

5.8 Gestione dei messaggi contenenti malware e relativa informativa al mittente

Il sistema di ARUBA PEC, compatibilmente con la normativa, verifica la presenza dei virus nei messaggi di posta elettronica nella fase immediatamente successiva alla spedizione del messaggio originale, e nella fase di ricezione dal sistema di posta 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 verrà generata una ricevuta con evidenza di tipo SubmissionRejection destinata al mittente del messaggio corrotto, mentre se è stato individuato alla ricezione verrà generata una ricevuta di RelayRejection destinata al Gestore del sistema mittente, una ricevuta con evidenza di ContentConsignmentFailure destinati al mittente. Il sistema inoltre, conserva i messaggi contenenti virus mettendo in condizioni il Gestore di mantenerli secondo le disposizioni normative vigenti. 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.

5.9 Descrizione Data Center di ARUBA PEC

Riportiamo di seguito le principali caratteristiche dei Data Center ARUBA PEC.

5.9.1 Infrastrutture di rete

L'infrastruttura di rete Aruba è composta da 2 piattaforme principali.

La prima piattaforma, denominata TBB (Transport Back Bone), ha il compito di collegare, tra loro, tutti i data center Aruba oltre garantire l'accesso ai punti di interconnessione (Internet Exchange) con i principali operatori di telecomunicazione nazionali ed internazionali.

Ogni PoP/Data Center ha almeno 3 vie che garantiscono l'affidabilità dei servizi di trasporto, i collegamenti sono ad altissima velocità (es. 100Gb/s), i percorsi sono stati studiati per diminuire la latenza al minimo possibile e, inoltre, nella piattaforma TBB vengono implementate tecnologie allo stato dell'arte come Segment Routing e TI-LFA per garantire la riprotezione del traffico, in caso di malfunzione di un collegamento, su un percorso alternativo, entro 50 ms.

Particolare attenzione è stata posta nella valutazione dell'ingresso dei collegamenti ai datacenter Aruba, in maniera da garantire una effettiva differenziazione geografica utilizzando accessi stradali indipendenti.

La seconda piattaforma, denominata IPBB (Internet Protocol BackBone), ha il compito di gestire i servizi di accesso e interconnessione alla rete Internet, combinandosi con il TBB, l'IPBB è in grado di scambiare traffico "Internet" con i principali operatori di livello 1 (tier one). Queste interconnessioni avvengono con accordi puntuali e. quindi, collegamenti dedicati studiati per offrire la massima diversificazione operatore/punto d'interconnessione (città) o anche tramite la partecipazione ai punti di scambio internet (Internet Exchange) come MIX, Minap, Namex e VSIX, anch'essi localizzati in diversi punti geografici del territorio nazionale.

Entrambe le piattaforme sono equipaggiate con hardware di ultima generazione e sono ridondate localmente tramite la presenza di due apparati per ogni livello o servizio di rete. Tali sistemi, nei data center Aruba, vengono installati in sale distinte e indipendenti.

La distribuzione di rete all'interno dei data center avviene tramite una "switch fabric", anch'essa ridondata. Sistemi di load balancing hanno la funzione di bilanciare il carico per tutte le macchine deputate all'erogazione dei servizi. Il sistema è complessivamente gestito da una unica piattaforma di monitoraggio, 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.

Raffreddamento:

- 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 con 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 un 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.

Raffreddamento:

- 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 un qualsiasi problema.

5.9.4 Data Center - sito a freddo

Presso tale Datacenter è presente un backup dei soli dati delle caselle (backup a freddo).

Alimentazione:
Viste le grandi dimensioni e la notevole potenza elettrica IT prevista pari a 12 MW, gli impianti sono stati strutturati su moduli da 1MW ridondato installati nel tempo in base alle effettive necessità. Ad oggi il data center è totalmente allestito con i 12MW.
I moduli elettrici sono realizzati all'interno di soluzioni containerizzate che consentono trasportabilità, scalabilità e rapida sostituzione
Ogni modulo è composto da:

- 1+1 trasformatore MT/BT da 1600kVA. Tutti i trasformatori sono collegati a due cabine di connessione alla rete MT pubblica a 15kVA
- 1+1 gruppi elettrogeni da 1700kVA, dotati di tutti i sistemi atti a garantire la massima affidabilità: doppio set di batterie e doppio motorino di avviamento, scaldiglie di preriscaldamento, filtrazione continua del carburante stoccato a bordo, doppia linea e doppia pompa di rifornimento dalle riserve esterne di carburante, dimensionate per il funzionamento continuo per almeno 48 ore a pieno carico e costituiti da due cisterne da 8.000 litri . Sono stati predisposti accordi di reperibilità con i fornitori di carburante con rifornimento completo entro 12 ore.

- 1+1 Sistema UPS costituito da 3+3 unità statiche da 500kVA in parallelo (N+1) con batterie dimensionate per un'autonomia di 15 minuti a pieno carico. Monitoraggio batterie per singolo monoblocco.
- 1+1 Sistema UPS da 160kVA al servizio degli impianti di condizionamento, in particolare delle unità di condizionamento interne (CRAH) e delle pompe di circolazione.
- Sistema STS è in grado di alimentare - qualora per qualsiasi motivo (guasto o intervento di manutenzione) venga a mancare l'alimentazione elettrica proveniente da uno dei due Power Center - istantaneamente e senza interruzioni avvertibili dai server entrambe le linee presenti in ciascun armadio della sala dati, dal power center superstite, realizzando pertanto una ridondanza completa di tipo 2*n.

Raffreddamento:

Il data center dispone di un particolare impianto di raffreddamento che utilizza la grande disponibilità locale di acqua di falda alle temperature idonee al raffrescamento delle sale in tutti i periodi dell'anno con elevata efficienza energetica.
Il sistema preleva da una serie di pozzi l'acqua a temperatura variabile dai 7 ° C dell'inverno ai 15 dell'estate e la fa circolare attraverso una serie di scambiatori passivi acqua acque dove avviene il recupero del calore proveniente dalle sale. L'acqua così riscaldatasi viene reimmessa in falda attraverso una seconda serie di pozzi detti perdenti in modo da non alterare i livelli della falda stessa.
Questo impianto è poi ridondato da una serie di gruppi frigoriferi elettrici acqua aria (chiller) in grado di avviarsi e di inserirsi in automatico in modo da sopperire ad eventuali inefficienze parziali e/o totali del sistema da acqua di falda.
Il sistema è composto da due linee ognuna suddivisa in due circuiti per un totale di 4 circuiti indipendenti.
Anche in questo caso viste le grandi dimensioni dell'impianto lo stesso è stato strutturato su moduli che vengono installati assieme a quelli elettrici.
Ogni modulo è composto da:

- 1+1 sistema scambiatore con dispositivi di regolazione (Skid) da 750KW.
- 1+1 chiller acqua aria da 500kW.
- Distribuzione dell'aria in modalità "UNDER" supportata dall'elevata altezza del pavimento flottante (200 cm) che consente di ridurre la velocità dell'aria e conseguentemente 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 del 50% delle macchine di condizionamento (ridondanza di tipo 2N).
- 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 acqua con mandata aria sotto pavimento e con aspirazione dall'aria calda dal controsoffitto mediante opportune compartimentazioni.

Sicurezza:

- Sicurezza fisica e degli accessi:
- Presenza di 7 perimetri di sicurezza

  - porte esterne di tipo blindato;
  - accesso visitatori tramite “bussola” a due ante 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 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.
- Facility Operations Center (FOC) attivo 24/7/365.
- Assistenza a disposizione dei Titolari e dei Partner per e-mail, per telefono oppure tramite trouble-ticketing on-line.
- Monitoraggio in tempo reale dello stato di ogni singolo server con alert al rilevamento di un qualsiasi problema.

6. Standard tecnologici, procedurali e di sicurezza adottati

6.1 Standard tecnologici di riferimento

- RFC 1847 (Security Multiparts for MIME: Multipart/Signed and Multipart/Encrypted)
- RFC 1891 (SMTP Service Extension for Delivery Status Notifications)
- RFC 1912 (Common DNS Operational and Configuration Errors)
- RFC 2252 (Lightweight Directory Access Protocol (v3): Attribute Syntax Definitions)
- RFC 2315 (PKCS 7: Cryptographic Message Syntax Version 1.5)
- RFC 2633 (S/MIME Version 3 Message Specification)
- RFC 2660 (The Secure Hyper Text Transfer Protocol)
- RFC 2821 (Simple Mail Transfer Protocol)
- RFC 2822 (Internet Message Format)
- RFC 2849 (The LDAP Data Interchange Format (LDIF) – Technical Specification)
- RFC 3174 (US Secure Hash Algorithm 1 - SHA1)
- RFC 3207 (SMTP Service Extension for Secure SMTP over Transport Layer Security)
- RFC 3280 (Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List-CRL Profile)
- RFC 3161 (TSP Time Stamp Protocol)
- ETSI 319 (Electronic Signatures and Infrastructures (ESI);)
- ETSI EN 319 401 General Policy Requirements for Trust Service Providers;
- ETSI 319 512 (Policy and security requirements for Electronic Registered Delivery Service Providers)
- ETSI EN 319 521 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Electronic Registered Delivery Service Providers
- ETSI 319 522 (Electronic Registered Delivery Services;)
- ETSI 319 522-1 (Part 1: Framework and Architecture)
- ETSI 319 522-2 (Part 2: Semantic contents)
- ETSI 319 522-3 (Part 3: Formats)
- ETSI 319 522-4 (Part 4: Bindings;) Sub-part 1: Message delivery bindings
- ETSI 319 522-4-1 (Sub-part 1: Message delivery bindings)
- ETSI 319 522-4-2 (Sub-part 2: Evidence and identification bindings)
- ETSI 319 531 (Policy and security requirements for REMSP)
- ETSI 319 532 (Registered Electronic Mail (REM) Services;)
- ETSI 319 532-1 (Part 1: Framework and architecture)
- ETSI 319 532-2 (Part 2: Semantic contents)
- ETSI 319 532-3 (Part 3: Formats)
- ETSI 319 532-4 (Part 4: Interoperability profiles)

Ulteriori documenti di riferimento:

- ENISA - Article 19 Incident reporting – March 2017
- ENISA - Technical Guideline on Incident Guideline on Incident reporting under the ECCC – March 2021
- AgID – Indicazioni per la notifica di incidenti, malfunzionamenti o interruzioni di servizio (SV_QM_Notifiche_1.0 - 21/12/2021).

6.2 Standard di sicurezza

I device HSM utilizzati per la firma e verifica dei messaggi REM sono certificati FIPS 140 -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.

6.3 Misure di sicurezza

Il Servizio 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, in un documento riservato e redatto in base alle disposizioni delle circolari AgID.

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 MFA (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 REM 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 REM viene periodicamente controllato attraverso attività di auditing interno. Ogni operatore riferisce ad uno dei responsabili previsti dalla normativa (vedi punto 6.5.1).

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 e redatto in base alle disposizioni delle circolari AgID. Presenza di firewall con definizione di policy di accesso (vengono abilitate le sole porte strettamente necessarie al funzionamento del sistema REM).
- Sistema di antivirus costantemente ed automaticamente aggiornato in modo da rendere il sistema protetto contro attacchi da parte di software malevolo.
- 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 (SMTPS, HTTPS, POP3S, IMAPS) e tra un Gestore e l’altro (SMTP/STARTTLS).
- Firma dei messaggi con i dispositivi HSM certificati FIPS 140 -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:
    - Controllo sulle estensioni dei file allegati a una REM che è realizzato:
        - In fase di caricamento dell’allegato qualora l’utente utilizzi gli strumenti messi a disposizione da Aruba PEC e, nel caso di file non autorizzati, segnalato dal messaggio "Per motivi di sicurezza, non è possibile caricare il file allegato"
        - In fase di invio, qualora l’utente utilizzi client terzi per l’invio dei propri messaggi e, nel caso di file non autorizzati, generando un Avviso di Mancata Accettazione per errori formali

      Il controllo è in grado di individuare gli allegati non ammessi anche se questi sono stati precedentemente rinominati (ad esempio, modificando un’estensione .exe in una .txt), se sono contenuti in archivi compressi o se sono contenuti in un messaggio REM che si intende inoltrare.

    - Verifica della presenza di macro all’interno dei file allegati a un messaggio sia attraverso gli strumenti di Aruba PEC che client terzi. Inoltre, la verifica avviene anche in caso di inoltro o di file contenuti in un archivio compresso. In caso positivo, i sistemi Aruba inseriscono uno specifico header che consente al Gestore destinatario di individuare in maniera automatica i messaggi contenti macro.
    - Gestione avvisi per mancato controllo di determinati allegati. Se l’allegato è cifrato o inserito in un archivio compresso e protetto da password, il suo contenuto non può essere sottoposto a scansione antivirus. In questo caso, i sistemi Aruba inseriscono uno specifico header che consente al Gestore destinatario di individuare in maniera automatica i messaggi con mancato controllo degli allegati.
- Tramite la sezione Gestione Account: è possibile accedere alla sezione “Storico accessi” tramite la quale visualizzare dispositivi e cronologia degli accessi effettuati alla casella REM (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 REM 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 REM (cfr. 7.2.11).

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 verifica durante le quali viene analizzato l'intero sistema con lo scopo di verificarne la sicurezza ed individuare eventuali punti vulnerabili; tale analisi viene eseguita almeno ogni 12 mesi, o prima in caso di eventi significativi. Durante tali verifiche 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 sia protetto e sicuro.

6.3.5 Trasmissione e accesso ai dati da parte dell'Utente

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

- gli utenti che usufruiranno del servizio dovranno identificarsi con 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 per il Servizio.

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 REM possono essere suddivisi in:

- Guasti di normale entità
- Guasti di grande rilevanza

<u>Guasti di normale entità</u>

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.

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.

Al par. 6.4 sono analizzate tutte le tipologie di malfunzionamento e, per ognuna di esse, sono evidenziati il livello di criticità e la modalità con cui può essere risolto il problema ed effettuato il ripristino del sistema.

6.3.8 Sistema di marcatura temporale

Come già descritto al par. 5.7, Aruba PEC utilizza, monitorando nel tempo la conformità normativa, un servizio di marca temporale qualificato ai sensi del Regolamento eIDAS [5].

In particolare, è prevista l'integrazione del servizio qualificato di Time Stamping Authority (TSA) fornito dal prestatore del servizio fiduciario qualificato Aruba PEC S.p.A. secondo le modalità disciplinate nel Manuale operativo del servizio di validazione temporale elettronica qualificata disponibile su https://www.pec.it/termini-condizioni.aspx.

6.3.9 Certificati di firma digitale

L'oggetto costituente il REM message e le ERDS evidence sono firmate digitalmente dall' ERDSP in accordo alla REM baseline, come prescritto nello standard EN 319 532-4, utilizzando una catena gerarchica di tre certificati digitali in accordo alle seguenti convenzioni:

- utilizzando lo stesso certificato digitale "foglia" (end-entity certificate) per firmare sia gli XML che rappresentano ERDS evidence (firma XAdES-B-T), sia gli EML che rappresentano i REM message (firma S/MIME CAdES-B-B);
- tale certificato di firma (S/MIME) è l'ultimo di una catena di tre certificati composti da una root CA e una intermediate CA (in accordo alla struttura riportata nella best practice della REM baseline in EN 319 532-4, Clause D.2.2.2);
- la root CA (top-level Root CA) è riconosciuta a livello mondiale dai sistemi operativi e browser client (in accordo con le best practice della REM baseline) e appartiene al QTSP Actalis S.p.A., la Certification Authority del Gruppo Aruba membro del CAB Forum e riconosciuta Qualified Trust Service Provider per la fornitura di QWAC e QSealC;
- in accordo a EN 319 521 (Clause 7.5) la chiave privata associata al suddetto certificato digitale "foglia" è mantenuta ed usata dallo stesso ERDSP all'interno di un secure cryptographic device (HSM) che dispone di certificazione FIPS PUB 140-2 level 3 o Common Criteria livello EAL4+, in accordo allo standard EN 319 411-1.

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 del Servizio.

6.4.1 Azioni promosse dal Gestore in caso di incidenti e malfunzionamenti

In linea con quanto definito da 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 Struttura Organizzativa ed attribuzione delle Responsabilità

La struttura organizzativa adottata per l'erogazione dei servizi fiduciari da parte di Aruba PEC è composta nel rispetto delle previsioni di cui allo standard ETSI EN 319 401 ed alle specifiche definite da ETSI EN 319 521.

In particolare, il personale impiegato ha esperienza almeno quinquennale per le rispettive aree di competenza ed incarico e riceve con cadenza annuale formazione relativamente alla sicurezza informatica, al trattamento dei dati personali ed alle regole per l'erogazione dei servizi fiduciari adeguata alle funzioni che sono chiamati ad esercitare.

I ruoli di responsabilità comprendono:

1. **Security Officers**: hanno la responsabilità di amministrare ed implementare I processi di sicurezza;
2. **System Administrators**: sono autorizzati ad installare, configurare e mantenere l'infrastruttura di servizi fiduciari, ivi inclusi i sistemi di recovery;
3. **System Operators**: sono responsabili del funzionamento dell'infrastruttura di servizi fiduciari su base quotidiana;
4. **System Auditors**: sono autorizzati alla visualizzazione degli archivi e dei logs di audit dell'infrastruttura dei servizi fiduciari;
5. **Identity Verification Officer**: con il compito di assicurare che i processi di verifica dell'identità eseguiti siano conformi a quelli previsti.

6.5.2 Gestione backup

I backup dei dati (di tutte le macchine che implementano il sistema REM) vengono effettuati in maniera automatica su storage configurati in replica con ridondanza geografica sul sito primario e secondario.
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 REM, 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 dei Data center Aruba. 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.

<u>Problema segnalato da titolare/partner</u>
La segnalazione può essere effettuata dal Titolare o dal Partner attraverso i canali disponibili per l'assistenza.
Il team di "Service Desk" (personale interno o in outsourcing) ha il compito di:

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

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

Fuori orario di ufficio (18:00 – 8:30 dal lunedì al venerdì; h24 sabato, domenica e festivi).
La segnalazione viene scalata al team Control room e service desk operation che effettuate le prime verifiche contatta il reperibile di turno. Sarà il reperibile ad allertare altri soggetti se necessario.

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

- La segnalazione viene scalata al team Service Run che prende in carico il problema valutandone a sua volta gravità ed urgenza;
- decide se è necessario scalare il problema verso tutti i livelli superiori fino al responsabile del servizio ed all'amministratore delegato;
- decide se il problema deve essere risolto nell'immediatezza o se può essere programmato un intervento di manutenzione da svolgere nel futuro;
- analizza il problema ed identifica le possibili soluzioni;
- decide se far intervenire risorse esterne (aziende che forniscono assistenza);
- comunica l'avvenuta risoluzione del problema al Service Desk;
- aggiorna la knowledge base.

Problema segnalato dal monitoraggio

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

Fuori orario di ufficio (18:00 – 8:30 dal lunedì al venerdì; h24 sabato, domenica e festivi) scala la segnalazione contattando il reperibile che a sua volta allerta altri soggetti se necessario. In orario di ufficio (8:30 -18:00 dal lunedì al venerdì escluso i festivi) scala la segnalazione al team Service Run che prende in carico il problema valutandone a sua volta gravità ed urgenza.

7. Modalità di erogazione del Servizio

7.1 Attivazione del Servizio

ARUBA PEC eroga il proprio Servizio sia direttamente che attraverso una rete di Partner.

Il flusso per la richiesta di attivazione da parte del Richiedente è comunque in generale il seguente:

1. il Richiedente formula la richiesta di attivazione del Servizio direttamente sul sito del Gestore o presso un Partner di ARUBA;
2. il Gestore, ovvero il Partner, verificata la correttezza e completezza della richiesta, procede (nel caso del Partner, tramite gli strumenti forniti da Aruba), all'attivazione del Servizio.

Per poter attivare, e successivamente accedere alla casella, il titolare della casella deve realizzare obbligatoriamente due passaggi:

1. **Identificazione certa**
2. **Attivazione dell'Autenticazione a più fattori – MFA**

1.Identificazione certa del titolare della casella

Per l'attivazione della casella, il titolare deve confermare la propria identità eseguendo il processo di riconoscimento scegliendo, tra i metodi descritti più nel dettaglio al par. 7.1.2.

2. Attivazione dell'autenticazione a più fattori

Per l'accesso alla casella è necessario attivare la verifica in 2 passaggi (anche nota come autenticazione a due fattori) cfr. par. 7.3.11.

Si specifica a tal proposito che, per quanto riguarda l'Italia, in relazione alla transizione tra il sistema PEC e l'avvio del sistema REM:

- Le caselle PEC che hanno acquisito, prima dell'avvio del SERCQ a livello nazionale, i requisiti minimi indispensabili previsti dalla REM Baseline (punti 1 e 2 del presente paragrafo), al momento dell'avvio non devono procedere ad ulteriori passaggi aggiuntivi, poiché saranno automaticamente attive all'interno del circuito REM.
- I titolari di caselle PEC che, prima dell'avvio del SERCQ a livello nazionale, non hanno effettuato l'identificazione certa (cft. 7.1.1) non potranno ricevere e/o inviare messaggi di posta fino ad identificazione certa del titolare.
- I titolari di caselle PEC che, prima dell'avvio del SERCQ a livello nazionale, hanno effettuato l'identificazione certa (cft. 7.1.1) ma non hanno attivato l'autenticazione a più fattori (cft. 7.1.2.), avranno la casella attiva ma per accedere ed utilizzare il Servizio dovranno obbligatoriamente attivare l'autenticazione a più fattori.

7.1.1 Processo di identificazione del titolare del Servizio

Il presente paragrafo descrive le modalità di identificazione certa del titolare della casella (persona fisica o giuridica).

Nel caso di casella intestata a persona giuridica, si applica quanto segue:

- La richiesta di identificazione del titolare è a carico della persona fisica (rappresentante legale) che rappresenta la persona giuridica, la quale è identificata secondo le stesse procedure individuate per le persone fisiche (descritte di seguito);
- I poteri di rappresentanza della persona giuridica, dichiarati dalla persona fisica richiedente l'identificazione, saranno verificati dal Gestore; qualora i controlli su fonti autoritative svolti dal Gestore per la verifica dei poteri di rappresentanza non dovessero dare esito positivo, verrà richiesta della documentazione aggiuntiva comprovante i poteri di rappresentanza.

I poteri di rappresentanza della persona giuridica, dichiarati dalla persona fisica richiedente, sono dimostrati tramite verifica di documentazione attestante lo stato di rappresentante legale del soggetto richiedente per conto della persona giuridica, come risultante da una banca dati ufficiale (es. Registro delle Imprese), ove disponibili. In particolare:

- per le persone giuridiche tenute a rispettare forme di pubblicità obbligatoria e/o iscritte in banche dati pubbliche, Aruba PEC esegue controlli automatici per la verifica dei poteri di rappresentanza del richiedente, anche avvalendosi di intermediari autorevoli operanti nel settore, consultando i registri disponibili (ad es: Registro Imprese, RUNTS, Indice IPA, etc…) e conservandone le evidenze come descritto nel prosieguo del presente paragrafo.

- negli altri casi non rientranti nelle ipotesi di cui al precedente punto, oppure nel caso in cui le verifiche di cui al punto che precede restituiscano esito negativo, Aruba PEC verifica i poteri di rappresentanza del richiedente tramite procedure che prevedono l'acquisizione di idonea documentazione, comprovante la carica rivestita e conservandone le evidenze come descritto nel prosieguo del presente paragrafo.
  La documentazione richiesta ed acquisita varia in ragione della tipologia di persona giuridica coinvolta (ad es: visura camerale aggiornata, verbale di nomina, etc.).
  Il QTSP verifica la documentazione acquisita e procede al riconoscimento della persona fisica come descritto di seguito.

I dettagli tecnico-operativi possono variare secondo la modalità e strumenti informatici utilizzati per l'identificazione del titolare. In tutti i casi, in fase di richiesta è necessario che il Titolare della casella:

1. si assuma esplicitamente gli obblighi previsti dalle norme vigenti e dal contratto col Gestore, con contestuale accettazione delle Condizioni Generali di contratto e del presente Manuale;
2. prenda visione dell'informativa privacy fornita da Aruba PEC.

Il Gestore deve identificare con certezza l'identità del titolare della casella. Il processo di identificazione può essere svolto dal titolare mediante varie modalità, elencate di seguito e descritte più nel dettaglio al par. 7.1.2:

- identificazione "De visu" (o "in presenza") svolta direttamente dal Gestore o da soggetti esterni incaricati, e basata sulla presenza fisica del soggetto titolare (**modalità 1**);
- identificazione a distanza tramite utilizzo di un dispositivo TS-CNS, CNS o CIE oppure tramite le identità rilasciate nel contesto del sistema SPID, ovvero in base a un mezzo di identificazione elettronica preesistente notificato dallo Stato Membro ai sensi dell'articolo 9 del Regolamento eIDAS, di livello significativo o elevato, o altro schema di identificazione elettronica (e-ID) nazionale non notificato che fornisca una garanzia equivalente alla presenza fisica sotto il profilo dell'affidabilità (**modalità 2**);
- identificazione a distanza tramite firma elettronica qualificata, ovvero basata sul riconoscimento effettuato da un Prestatore di Servizi Fiduciari Qualificato (**modalità 3**);
- tramite video-riconoscimento da remoto (anche detta DVO - "de visu online") svolto dal Gestore o da soggetti esterni incaricati, attraverso metodi di identificazione riconosciuti a livello nazionale, che assicurano livelli di affidabilità pari alla presenza fisica (**modalità 4**).

Al fine di ampliare le possibilità operative, le funzioni di registrazione ed identificazione possono essere svolte anche da terze parti delegate, con sedi distribuite sul territorio, sulla base di appositi accordi stipulati con il Gestore. Tali terze parti (anche dette "Centri di Registrazione Locale", abbreviato CDRL) operano secondo procedure concordate con il Gestore. I CDRL sono responsabili nei confronti del Gestore della corretta e sicura registrazione e identificazione dei titolari delle caselle REM, nonché del trattamento dei loro dati nel pieno rispetto della normativa sulla privacy. Il Gestore si riserva la possibilità di effettuare delle verifiche presso i CDRL o direttamente presso i propri incaricati, riguardo alla corretta esecuzione delle attività affidate nonché riguardo al rispetto delle istruzioni impartite. Il Gestore rimane a sua volta pienamente responsabile delle operazioni di registrazione ed identificazione dei titolari, siano esse svolte in proprio oppure dai CDRL.

Il Gestore o la terza parte delegata (CDRL) può rigettare la richiesta di identificazione del titolare della casella nel caso in cui le informazioni fornite dal Titolare della casella siano giudicate non affidabili, inesatte, incomplete o incoerenti; nel caso di dubbi sull'identità del titolare della casella (o della persona giuridica da questi presumibilmente rappresentata) o per qualsiasi altra ragione che configuri una non conformità al presente documento.

Per le modalità di identificazione per le quali è prevista l'esibizione di un documento di identità, nel rispetto di quanto previsto dal DPR 28 dicembre 2000, n. 445 e s.m.i [2], sono ammessi i seguenti documenti di identità e di riconoscimento equipollenti tra di loro:

- carta di identità italiana;
- patente di guida italiana;
- passaporto.

Nel rispetto di quanto previsto dallo standard ETSI EN 319-521 (par. 5.4 dello standard), il Gestore archivia tutte le prove di identificazione per il periodo di tempo previsto dalla normativa vigente, anche al fine di poter fornire prova in eventuali procedimenti giudiziari. In particolare vengono archiviati:

1. i moduli di richiesta del Servizio con relativa accettazione. L'accettazione delle condizioni di contratto, delle clausole vessatorie ed eventuale documentazione aggiuntiva a supporto dell'identificazione (es. documento d'identità del richiedente, ecc.);

2. oltre al punto 1, nel caso di identificazione tramite SPID (prevista nella modalità 2), il modulo di richiesta comprendente la response SAML dell'IdP è conservato firmato con sigillo PAdES;
3. nel caso di identificazione da remoto (modalità 4), in aggiunta a quanto indicato al punto 1, anche i file audio-video e metadati strutturati in formato elettronico.

Le evidenze del riconoscimento archiviate da Aruba sono conservate dal Gestore per un periodo di 10 anni dalla data di cessazione del Servizio, in conformità con l'art. 2220 c.c.

La richiesta di identificazione è formalizzata attraverso un "Modulo di Richiesta" (il nome esatto del modulo può variare). In seguito, per brevità, si fa riferimento a questo documento con "modulo di richiesta".

In certi casi il modulo di richiesta viene generato in formato PDF dal sistema informativo del Gestore o suo delegato e precompilato coi dati anagrafici del Titolare, quindi reso disponibile al Titolare per essere accettato in ogni sua parte.

Il modulo di richiesta dev'essere sottoscritto dal Richiedente, con firma autografa oppure elettronica. Nel caso di sottoscrizione elettronica, il Gestore prevede i seguenti tipi di accettazione:

A) firma elettronica avanzata basata su un certificato qualificato o firma qualificata ai sensi del Regolamento eIDAS;
B) firma elettronica apposta mediante il certificato di autenticazione presente sulla carta CIE/CNS/CRS (Carta di Identità Elettronica, Carta Nazionale o Regionale dei Servizi) del Titolare;
C) firma elettronica basata su un dato riservato conosciuto solo dal Titolare, oltre che dal Gestore (per esempio una password dinamica (OTP) che il Gestore invia al telefono cellulare del Titolare mediante SMS o con altre modalità);
D) altre forme di firma elettronica o firma elettronica avanzata ai sensi delle norme vigenti;

Per quanto riguarda il punto D, il Gestore si riserva di accettare firme elettroniche solamente per i casi in cui accerti l'integrità e la sicurezza delle specifiche procedure autorizzate e messe in atto all'interno del processo di identificazione, ovvero nei casi in cui la procedura di accettazione o sottoscrizione è messa a disposizione dal Gestore stesso.

Nei casi di identificazione de visu del Titolare (modalità 1), l'incaricato al riconoscimento appone al modulo la propria controfirma digitale (o fornisce altra evidenza elettronica affidabile che attesti l'identità dell'operatore che ha effettuato il riconoscimento); inoltre, in questo caso, il modulo include anche la dichiarazione dell'incaricato che la firma elettronica del Titolare è avvenuta in sua presenza nell'ambito dell'identificazione de visu.

I contratti stipulati con ciascun Centro di Registrazione Locale (CDRL) sono conservati da Aruba. Per quanto riguarda i file di log dei messaggi di posta elettronica certificata si rimanda al par. 7.3.8.

7.1.2 Modalità di identificazione del titolare della casella

Le modalità di identificazione del titolare della casella sono descritte come richiamato all'interno delle Regole tecniche per i servizi di recapito certificato a norma del regolamento eIDAS e dallo standard ETSI EN 319-521. Relativamente alle modalità di identificazione descritte di seguito, il Gestore verifica direttamente, o affidandosi a terzi, l'identità del Titolare della casella. Nelle descrizioni che seguono, il termine "Titolare" si riferisce al soggetto che è intestatario della casella, come persona fisica o persona giuridica. Nel caso di persona giuridica, l'identificazione è a carico del legale rappresentante, (in quanto persona fisica che rappresenta la persona giuridica).

Per garantire la tutela ed il trattamento dei dati personali in conformità alla normativa applicabile in materia, Aruba adotta idonee misure e strumenti a tutela degli interessati e rende disponibile l'informativa che definisce le modalità di trattamento dei dati trattati.

Modalità 1

L'identificazione prevede la presenza fisica (de-visu) del Titolare della casella, che dev'essere maggiorenne, dinnanzi ad un soggetto abilitato a eseguire il riconoscimento e che provvede ad accertare la sua identità attraverso la verifica formale e sostanziale di un documento di riconoscimento tra quelli descritti ad inizio paragrafo, integro e in corso di validità, esibito in originale dal Soggetto stesso.

Le operazioni d'identificazione dei Titolari sono svolte, in base al modello organizzativo di riferimento, da uno dei seguenti soggetti abilitati al riconoscimento:

- direttamente dal Gestore;
- da una terza parte denominata Centro di Registrazione Locale (CDRL) dinnanzi ad un incaricato del CDRL, denominato Incaricato al Riconoscimento (IR).

I CDRL possono operare successivamente alla stipula di un accordo e di un mandato con cui il Gestore denominerà gli incaricati del CDRL quali IR, che eseguono le pratiche relative al processo di identificazione. L'autorizzazione e successivamente la qualificazione degli IR come abili alle operazioni di identificazione, avviene tipicamente mediante corso di formazione e superamento di una verifica scritta. A seguito della firma da parte dei rispettivi legali rappresentanti del Gestore e del CDRL e previa qualificazione degli IR, il Gestore rende disponibili agli IR stessi gli strumenti telematici sicuri per consentire lo svolgimento delle attività di identificazione. I privilegi di accesso agli strumenti telematici sicuri e le operazioni degli IR sono sotto il costante controllo del Gestore. Gli IR possono operare successivamente alla stipula di un mandato direttamente con il Gestore, o tramite nomina di un CDRL, nel contesto delle pratiche operative definite dal Gestore stesso e limitatamente allo svolgimento delle attività di identificazione.

Modalità 2

L'identificazione del titolare della casella viene effettuata attraverso un mezzo di identificazione elettronica preesistente in base al riconoscimento effettuato da corrispondente autorità pubblica o soggetto privato emittente, ovvero uno schema notificato da uno Stato Membro ai sensi del regolamento eIDAS e compreso nell'elenco pubblicato dalla Commissione, a norma dell'articolo 9 del regolamento eIDAS, o altro schema di identificazione elettronica (e-ID) nazionale con garanzie equivalenti alla presenza fisica sotto il profilo dell'affidabilità [5]. Nello specifico riferimento al

contesto italiano, tale verifica dell'identità del Soggetto richiedente titolare della casella si avvale di un dispositivo TS-CNS, CNS o CIE oppure di un processo di autenticazione SPID con credenziali di livello 2 o 3.

Modalità 3

L'identificazione si basa sul riconoscimento (già) effettuato da un Prestatore di Servizi Fiduciari Qualificato per il rilascio di un certificato qualificato a norma del Regolamento eIDAS. L'identità del Titolare della casella è accertata attraverso procedure di identificazione informatica basate sull'acquisizione di un modulo di adesione o di altro insieme di dati in forma elettronica (comunque sottoposto dal Gestore), firmato elettronicamente con il certificato qualificato, ancora in corso di validità, le cui chiavi di firma sono contenute nel dispositivo sicuro (QSCD) in possesso del Soggetto stesso titolare della casella (persona fisica o, nel caso della persona giuridica, del rappresentante legale).

Modalità 4

In tale modalità l'identificazione viene effettuata mediante l'ausilio di un sistema di videoconferenza e prevede che il Titolare della casella, che dev'essere maggiorenne, sia dotato di una webcam correttamente collegata ad un dispositivo con sistema audio e video funzionante (pc, tablet o smartphone).
Le operazioni d'identificazione dei Titolari sono svolte, in base al modello organizzativo di riferimento, da uno dei seguenti soggetti abilitati al riconoscimento:

- direttamente dal Gestore;
- da una terza parte denominata Centro di Registrazione Locale (CDRL) dinnanzi ad un incaricato del CDRL;
- un soggetto terzo denominato Incaricato al Riconoscimento (IR).

L'operatore segue particolari procedure – che per ragioni di sicurezza sono riservate – volte a garantire l'autenticità della richiesta di identificazione del corso della sessione in videoconferenza. L'operatore, tra l'altro, richiede al Titolare di esibire un documento di riconoscimento in corso di validità tra quelli indicati all'inizio del paragrafo. L'Operatore può escludere l'ammissibilità del documento presentato dal Titolare se ritenuto carente delle caratteristiche elencate. L'operatore può inoltre sospendere, o non avviare, il processo di identificazione nel caso in cui la qualità audio/video sia scarsa o ritenuta non adeguata a soddisfare i requisiti indicati all'Art. 24 del Regolamento eIDAS e dallo standard ETSI EN 319-521 (al par. 5.2 dello standard).

Al momento dell'identificazione, il Titolare deve confermare:

- la volontà di voler effettuare l'identificazione tramite webcam per il rilascio del Servizio;
- i dati identificativi ed anagrafici registrati ed associati alla casella di cui è Titolare;

La sessione di videoconferenza è interamente registrata (audio e immagini-video). I dati di identificazione, costituiti dal file audio-video e metadati strutturati in formato elettronico, sono conservati come indicato all'inizio del presente paragrafo.

7.2 Accesso ed utilizzo del servizio

Il Servizio fornito dal Gestore può essere utilizzato mediante le modalità di seguito riportate e descritte.

7.2.1 Accesso ed utilizzo tramite client di posta

Il sistema è compatibile con tutti i principali client di posta che supportano i formati previsti dallo standard S/MIME.

Per il corretto funzionamento è necessario abilitare il client di posta a connettersi ai server REM attraverso i protocolli POP3/S, IMAP/S, SMTP/S. Gli indirizzi dei server ed i relativi parametri sono comunicati dal Gestore all' attivazione del Servizio e comunque resi disponibili sul sito del Gestore.

L'accesso alla casella tramite client di posta, in quanto necessaria l'autenticazione a più fattori (MFA), avviene mediante l'inserimento di utenza e relativa chiave auto-generata dal sistema REM. Tale chiave, che può essere generata direttamente dall'utente tramite le modalità messe a disposizione dal Gestore, consente l'utilizzo del client con autenticazione a due fattori attiva e ha un periodo di validità limitato nel tempo, come previsto dalle Regole tecniche per i servizi di recapito certificato a norma del regolamento eIDAS [5].

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 a casella) il mittente riceve una evidence di tipo Submission Acceptance ed una evidence di tipo ContentConsignment; il destinatario, riceve il messaggio originale imbustato in un messaggio di trasporto il cui oggetto ha un prefisso del tipo "**REM dispatch:**", seguito dal subject originale.

Sul sito del Gestore vengono descritte le modalità di configurazione dei principali client di posta.

7.2.2 Accesso ed utilizzo tramite webmail

Il Titolare ha la possibilità di accedere alla casella di posta tramite applicazione webmail, alla quale può autenticarsi inserendo le proprie credenziali (indirizzo e-mail e password), e confermare l'autenticazione tramite un secondo fattore (es: push ,OTP etc.). L'accesso alla webmail offre la possibilità di:

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

È possibile effettuare l'accesso tramite webmail via browser anche tramite QRcode, ovvero inquadrando il QRCode che appare sulla maschera di login del Servizio tramite l'App Mobile Aruba PEC (cft. 7.2.3). Tale modalità di accesso è caratterizzata dai seguenti requisiti:

1. l'utente deve aver abilitato l'utilizzo del fattore biometrico (impronta digitale o impronta facciale) per l'accesso all'App Mobile di Aruba PEC dal proprio dispositivo (smartphone/tablet);

2. l'utente deve aver effettuato l'accesso alla casella REM dall'App Mobile di Aruba PEC con la quale intende inquadrare il QRCode, e deve inquadrare il QRCode dal medesimo dispositivo associato alla casella REM per l'autenticazione a più fattori (cft. 7.2.11);

3. effettuato l'accesso all'App Mobile di 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 REM solo tramite inserimento delle credenziali (indirizzo email, password e secondo fattore).

L'autenticazione con QRCode tramite App Mobile di 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 REM.

7.2.3 Accesso ed utilizzo tramite App Aruba PEC

Disponibile per Dispositivi IOS e Android, la App consente di:

- accedere alla casella da smartphone e tablet;
- configurare più account di posta 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 https://guide.pec.it/posta-pec/webmail/webmail-pec.aspx;
- visionare le informazioni relative alla casella, la "Scadenza", lo spazio a disposizione e quello occupato, ecc..

L'App è scaricabile da tutti gli store come descritto su https://guide.pec.it/app-aruba-pec/caratteristiche-download-compatibilita/scaricare-applicazione-da-store.aspx.

Di seguito le compatibilità: https://guide.pec.it/app-aruba-pec/caratteristiche-compatibilita.aspx

7.2.4 Accesso al servizio in delega

È possibile che il Titolare del Servizio permetta, tramite le funzionalità e le procedure messe a disposizione dal Gestore, ad uno o più utenti registrati di accedere e utilizzare il Servizio.

Infatti, come previsto dalle Regole tecniche per i servizi di recapito certificato qualificato a norma del regolamento eIDAS [5], il processo di registrazione al Servizio, una volta identificato il titolare, prevede che vengano rilasciate delle credenziali personali, una per ognuno degli utenti che accederanno al Servizio.

Il Titolare può definire e modificare le utenze associate alla casella in qualsiasi momento, stabilendo inoltre i permessi da associare a tali utenze aggiuntive.

7.2.5 Modifica dati anagrafici

Successivamente all'attivazione del servizio alcuni dei dati anagrafici associati alla casella possono essere modificati, in base alle caratteristiche e alla tipologia della modifica richiesta, dal Titolare o da persona da esso autorizzato, in modo autonomo o tramite assistenza, così come descritto al link https://guide.pec.it/posta-pec/modifica-dati/riepilogo-dati-modifiche-consentite.aspx. Invece per quelle acquistate tramite Partner, la modifica potrà essere effettuata tramite richiesta il proprio Partner (cft. 7.3).

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.

7.2.6 Cambio di Titolare

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

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 tutte le informazioni richieste relative ai dati del nuovo e vecchio titolare e il modulo di richiesta firmato.

Il Partner potrà e dovrà modificare la titolarità di una casella solo dopo aver accertato, mediante il ricevimento dell'apposita documentazione sopra descritta sottoscritta dai soggetti coinvolti, l'effettiva volontà del Titolare della casella 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, sospensione di eventuali accessi in delega (cft. 7.2.4);
- la dissociazione del dispositivo collegato alla verifica in 2 passaggi: il nuovo titolare al primo accesso potrà eseguire l'associazione con il proprio dispositivo;
- l'obbligo, in capo al nuovo Titolare, di effettuare l'identificazione certa per poter accedere ed utilizzare la casella, realizzando obbligatoriamente i passaggi descritti al par. 7.1 del presente Manuale.

Come comunicato in fase di cambio titolarità, il Titolare cedente la casella, provvede autonomamente alla cancellazione del contenuto della casella, cioè eventuali messaggi e contatti, salvo un diverso accordo tra il cedente ed il subentrante. Aruba PEC, nelle operazioni di trasferimento della casella, non compie alcuna attività in relazione al contenuto della medesima.

7.2.7 Cancellazione di una casella da parte del Titolare

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

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 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, che riguarda una casella dismessa (scaduta e non rinnovata), dando seguito alle direttive fornite da AgID, si rispetta il divieto in vigore per il Gestore di riassegnare una stessa casella ad un 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. In ogni caso, il Titolare della casella può scegliere di richiedere la modifica della titolarità come previsto al par. 7.2.6.

7.2.8 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. 7.3.2.

7.2.9 Consultazione dei log dei messaggi da parte del Titolare

Come previsto dalla normativa in materia di REM, il Gestore è tenuto a conservare i file di log dei messaggi del SERCQ per un periodo di 30 mesi dall'invio del messaggio. Il Titolare del servizio può procedere in autonomia alla consultazione dei log di suo interesse. Per far ciò, deve:

- accedere alla propria Webmail (cft. 7.2.2);
- selezionare la specifica voce per consultare i log, quindi impostare la ricerca secondo i parametri di suo interesse (data inizio, data fine, evento, oggetto del messaggio, destinatario, ecc.);
- visualizzare i risultati, che possono essere esportati (in formato CSV o PDF).

Per maggiori dettagli cft. paragrafo 5.7.

Nel caso di cancellazione della casella 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.

7.2.10 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 per eventuali utenze aggiuntive in delega (cft. 7.2.4) e 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.

7.2.11 Autenticazione a più fattori (MFA)

L' attivazione del secondo fattore di autenticazione (autenticazione forte) è obbligatoria per l'accesso alla casella REM.

Il secondo fattore di autenticazione permette, tramite l'associazione di un dispositivo in possesso dell'utente (smartphone, token fisico, etc.), di accedere al QeRDS. L'autenticazione a due fattori prevede infatti l'accesso sicuro al Servizio attraverso l'inserimento della password associata ad un secondo fattore di autenticazione veicolato dal dispositivo associato (come notifica push, OTP, sms).

Tale associazione avviene mediante modalità sicure che hanno l'obiettivo di accertare il reale possesso del dispositivo utilizzato dall'utente (es. invio di un OTP al numero di telefono, inserimento del seriale del token fisico).

Qualora l'utente abbia smarrito e/o non sia in grado di recuperare le credenziali di accesso tramite i metodi sicuri messi a disposizione dal Gestore (reset password), lo stesso si riserva la possibilità di mettere a disposizione ulteriori pratiche per il recuperodell'indirizzo email e del numero di telefono associati alla casella, mediante procedure specifiche che prevedono la ri-validazione dell'identità del titolare della casella stessa, da svolgere mediante le medesime modalità previste per la prima attivazione (cft. Par. 7.1).

7.3 Partner ARUBA PEC

7.3.1 Modalità operative per il Partner

A. Richiesta da parte del Partner al Gestore di attivazione di una casella attraverso la piattaforma Partner

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

1.Controllo dei dati in ingresso

Il Partner dovrà controllare i dati e la documentazione fornita dal Titolare della casella, secondo quanto previsto dal flusso di cui al paragrafo 7.1.

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

2. Formulazione della richiesta di attivazione

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

1. Compilare i campi generali della casella;
   - dominio;
   - nome casella.

2. Scegliere se la casella è destinata ad un privato o ad una persona giuridica.

3. Indicare se si tratta di un nuovo Titolare o di uno già registrato; se il Titolare è nuovo, compilare i dati richiesti (cft. punto 1);

4.Confermare operazione assicurandosi che i dati inseriti siano corretti e corrispondano a quanto riportato nella richiesta di attivazione.

5. Effettuare l'upload della documentazione fornita dal Titolare.

3. Completamento della richiesta di attivazione

Per completare l'attivazione della casella sarà necessario che il Titolare porti a compimento i passaggi obbligatori previsti al par. 7.1 del presente documento. Una volta compiuti i passaggi obbligatori, la casella verrà attivata.

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 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 e di quarto livello.

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.

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

2. Formulazione della richiesta di certificazione

Per attivare un dominio al proprio richiedente, il Partner, attraverso l'apposita piattaforma Partner messa a disposizione, deve effettuare le operazioni di seguito descritte.

1. 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.

    2.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 (cft. punto 1);

    3.Confermare operazione assicurandosi che i dati inseriti siano corretti e corrispondano a quanto riportato nella richiesta di attivazione.

4. Effettuare l'upload della documentazione inviata dal Titolare.

Il Gestore provvederà all'inserimento del dominio certificato in Trusted list.

7.3.2 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 sul Servizio di posta (valore legale, funzionamento, interoperabilità con gli altri Gestori, interazioni con la pubblica amministrazione), configurazione del client di posta, funzionamento della webmail ecc.

7.4 Livelli di servizio ed indicatori di qualità

Per l'erogazione del Servizio ARUBA PEC garantisce il rispetto dei seguenti livelli di servizio:

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 REM Content Consignment Evidence 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 SERCQ su dominio del gestore (dalla ricezione di tutta la documentazione necessaria)	2 giorni lavorativi
Tempo massimo per l'attivazione di un nuovo account SERCQ 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 dietro richiesta del Titolare (Il Titolare può comunque in qualsiasi momento ricercare e scaricare i log di interesse in autonomia direttamente dalla propria Webmail)	5 giorni lavorativi

Indicatori di qualità	
Sistema di monitoring con invio di messaggi di alert via email ed sms al presentarsi di malfunzionamenti e situazioni critiche	7/24/365
Servizio di Assistenza 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

7.5 Interoperabilità con gli altri sistemi REM

ARUBA PEC si impegna a garantire l'interoperabilità del proprio Servizio REM con gli altri Gestori REM che rispettano la baseline eIDAS e sono censiti sulla trusted list, secondo quanto stabilito dalla normativa di settore.

ARUBA PEC inoltre si impegna a verificare periodicamente l'interoperabilità del proprio sistema con gli altri Gestori REM accreditati attraverso uno scambio concordato di email.

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

7.5.1 Assistenza su segnalazioni gravi da parte degli altri Gestori

In caso di problemi di interoperabilità con altri sistemi, gli altri Gestori hanno la possibilità di contattare la Control Room 24 ore su 24, 7 giorni su 7 ai riferimenti indicati al par. 2.2.

7.6 Cessazione dell'attività del QTSP

Di seguito si descrivono le attività che saranno svolte qualora Aruba PEC decida, per qualsiasi ragione, di cessare il proprio Servizio.

Prima della effettiva cessazione:

- almeno 60 giorni prima della data pianificata di cessazione del Servizio, sarà inviata una informativa a tutti i clienti del Servizio, nonché all'organismo di supervisione (AgID), all'organismo di verifica della conformità (CAB), alle terze parti coinvolte e agli altri Gestori.
- con preavviso minimo di 60 giorni, il Gestore invierà una comunicazione a tutti gli eventuali subappaltatori (informandoli che alla scadenza del termine non saranno più autorizzati ad eseguire attività collegate al Servizio);
- con preavviso minimo di 60 giorni, sarà pubblicata in modo evidente una nota informativa sul sito web del Gestore;
- se individuato, la responsabilità della conservazione delle evidenze e dei log sarà trasferita ad un altro soggetto affidabile che ne possa garantire la conservazione per un tempo adeguato. In caso di mancata individuazione, il Gestore mantiene la conservazione delle evidenze e dei log, per il periodo previsto dalla norma.

Sarà fornita contestualmente agli interessati un'informativa sul trasferimento dei dati personali all'eventuale TSP subentrante, rimanendo comunque fermo il diritto dell'Interessato di non procedere al trasferimento ad altro Gestore.

La pianificazione delle attività di cessazione permette di gestire l'erogazione del Servizio fino alla fase di dismissione e di garantire agli utenti tutte le informazioni necessarie al governo del Servizio acquisito.

Alla data di cessazione, il TSP cessante provvederà a distruggere (mediante cancellazione logica) le chiavi private nonché il materiale annesso (se presente) che ne consente il ripristino; queste operazioni si svolgeranno nel rispetto delle procedure in vigore presso il TSP cessante relativamente alla gestione delle chiavi.
Alla data di cessazione:

Al termine della fase di trasferimento, una volta avuto conferma e accettazione formale da parte dell'eventuale Gestore subentrante, si procede alla dismissione e distruzione delle evidenze (dedicati al sistema SERCQ), al fine di rendere definitivamente indisponibile qualsiasi dato conservato.

8. Obblighi e responsabilità

8.1 Obblighi e responsabilità del QTSP

ARUBA PEC si impegna a rispettare la normativa tempo per tempo vigente, relativa al Servizio, in particolare a:

- garantire i livelli di servizio previsti dalla normativa vigente e dalle disposizioni di dettaglio emanate dalle competenti Autorità di settore;
- assicurare l'interoperabilità con gli altri Operatori, secondo quanto previsto dalla normativa vigente e dalle disposizioni di dettaglio emanate dalle competenti Autorità di settore;
- informare i titolari sulle modalità di accesso al servizio e sui necessari requisiti tecnici;
- fornire al mittente le risultanze relative alla trasmissione del messaggio, come previsto dalla normativa vigente e dalle disposizioni di dettaglio emanate dalle competenti Autorità di settore (salvo nel caso di eventi disastrosi improvvisi);
- comunicare al Titolare della casella la mancata consegna del messaggio nei tempi e con le modalità previste normativa vigente e dalle disposizioni di dettaglio emanate dalle competenti Autorità di settore (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) [4];
- 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 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 REM;
- 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;
- identificare in maniera certa il Titolare della casella secondo le modalità previste dal Reg. eIDAS [5] prevedendo che, nei casi in cui l'identificazione dovesse decadere per i casi previsti dal presente documento, il Servizio sia sospeso;
- imporre all'utente della casella, il requisito dell'accesso alla stessa tramite autenticazione a due fattori (cft. 7.2.11).

8.2 Obblighi e responsabilità dei titolari

- Sollevare ARUBA PEC da ogni responsabilità in merito ai contenuti dei messaggi;

- fornire ad ARUBA PEC tutte le informazioni necessarie ad identificare la persona ed attivare il servizio, garantendo, sotto la propria responsabilità, la veridicità dei dati comunicati 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 recapito certificato qualificato erogato da Prestatori accreditati;
- i privati che intendono utilizzare il Servizio 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 tramite SERCQ 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 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 Obblighi terze parti coinvolte

Aruba PEC può delegare le funzioni di attivazione del Servizio e di riconoscimento a soggetti esterni (detti Partner Aruba PEC) previo corso di formazione e sottoscrizione della documentazione contrattuale ai fini dell'adesione al programma partner o in qualità di CDRL;
Ai fini dell'esecuzione delle attività di riconoscimento di cui al precedente paragrafo 7.1, i Partner incaricati saranno nominati CDRL.
In ogni caso, i Partner sono tenuti al pieno rispetto del contratto stipulato con Aruba PEC, tra cui:

- alla corretta e sicura Identificazione dei Titolari, nel rispetto del Reg UE 2016/679 [4] e degli Accordi intercorsi con Aruba PEC nonchè alla corretta attivazione del Servizio;
- alla diligente conservazione di tutte le evidenze raccolte (salvo diverso e specifico accordo con Aruba PEC) per tutto il tempo previsto dal contratto stesso;
- ad utilizzare gli strumenti ed i canali di comunicazione messi loro a disposizione secondo correttezza e diligenza, nel rispetto delle istruzioni fornite da Aruba PEC.

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 REM. Tale responsabilità viene assunta unicamente dal Titolare;
- ARUBA PEC non ha alcuna responsabilità sui contenuti dei messaggi inviati e ricevuti attraverso le proprie caselle REM;
- Aruba PEC risponde dei danni causati a qualsiasi persona fisica o giuridica in seguito al mancato adempimento degli obblighi contrattuali e di quelli previsti dalla normativa vigente in quanto applicabile;
- il Gestore non potrà in alcun modo essere ritenuto responsabile, a titolo esemplificativo ma non esaustivo, per danni derivanti da cause di forza maggiore, caso fortuito, eventi catastrofici (incendi, terremoti, esplosioni) o comunque non imputabili ad ARUBA PEC che provochino ritardi, malfunzionamenti o interruzioni del servizio;
- Qualsiasi contestazione del Titolare relativa all'erogazione del Servizio dovrà essere comunicata ad ARUBA PEC, a pena di decadenza, entro 30 giorni dalla data dell'evento mediante raccomandata a/r;
- Il Servizio garantisce l'invio o la trasmissione di dati nei limiti e nelle condizioni previste dal Contratto, con divieto nei confronti dell'utente di adoperare per il loro invio o trasmissione programmi software automatizzati o comunque senza intervento diretto dell'utente stesso, salvo diversa previsione indicata nel Contratto, da intendersi come il complesso dei documenti che regolano il rapporto con il cliente e descrivono il funzionamento del Servizio;
- ARUBA PEC si riserva la facoltà di modificare il presente manuale nel caso in cui vengano apportate modifiche tecniche al sistema, variazioni all'offerta commerciale, o adeguamenti normativi. Le limitazioni agli indennizzi stabilite da ARUBA PEC, per quanto non previsto dal presente capitolo, sono riportate nelle condizioni contrattuali di fornitura del servizio rese pubbliche nel sito del Gestore: http://www.pec.it.

8.5 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 ovvero delle policy di utilizzo servizi Aruba, potrà risolvere il contratto con le modalità indicate nello stesso.

8.6 Polizza assicurativa

ARUBA PEC si impegna a mantenere attiva una idonea polizza assicurativa per la copertura dei rischi e dei danni causati a terzi nell'esercizio dell'attività di Prestatore del Servizio, in conformità alla normativa tempo per tempo vigente, per tutto il periodo di erogazione del Servizio.

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) [4].
In particolare, le misure di sicurezza adottate, tra le quali quelle di cui al Cap. 6 hanno l'obiettivo di assicurare:

- 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.