Aruba PEC S.p.A.

Addendum al Manuale Operativo Posta Elettronica Certificata

Servizio PEC adeguata agli standard europei

Versione: 1.1
Data: 08/08/2022
Redazione: Valeria Favasuli
Verificato da: Federico Ciofi, Andrea Panichi, Nicole Mazzoni
Approvato da: Andrea Sassetti
Classificazione documento: Pubblico

Andrea Sassetti
Firmato digitalmente il 08/08/2022 10:24:10 CEST

VERSIONE N°	DATA	NATURA DELLA MODIFICA
1.0	20/07/2022	Prima emissione.
1.1	08/08/2022	3 e 7.1.2: aggiornamento policy IT AgiD versione 1.2. 7.1.1: modifica paragrafo. 7.7: modifica paragrafo.

Sommario

1. Informazioni di carattere generale 4
1.1 Scopo 4
1.2 Versione dell'Addendum e responsabilità 5
1.3 Definizioni ed acronimi dell'Addendum 5
1.4 Tabella di corrispondenza 6
2. Dati identificativi del Gestore 6
2.1 Responsabile dell'Addendum 6
2.2 Canali di comunicazione 6
2.3 Modifiche all'Addendum 6
2.4 Indirizzo web del Gestore dal quale scaricare l'Addendum 7
2.5 Certificazioni ISO 7
3. Principali riferimenti normativi 8
4. Informazioni generali sulla Posta Elettronica Certificata 9
4.1 Introduzione 9
4.2 Funzionamento di un sistema di Posta Elettronica Certificata adeguata agli standard europei 9
5. Descrizione della soluzione tecnica definita da ARUBA PEC 10
5.1 Principali caratteristiche 10
5.2 Scalabilità e Affidabilità 11
5.3 Sicurezza dei dati 11
5.4 Architettura di massima del sistema 11
5.5 Architettura della soluzione 12
5.6 Riferimenti temporali 13
5.7 Storicizzazione dei Log e apposizione della marca temporale 13
5.8 Conservazione dei messaggi contenenti virus e relativa informativa al mittente 13
5.9 Descrizione Data Center di ARUBA PEC 14
6. Standard tecnologici, procedurali e di sicurezza adottati 14
6.1 Standard tecnologici di riferimento 14
6.2 Standard di sicurezza 14
6.3 Misure di sicurezza 14

6.4 Analisi dei rischi e procedure di ripristino 14
6.5 Procedure operative 14
7. Modalità di erogazione del servizio 15
7.1 Attivazione del Servizio 15
7.1.1 Processo di identificazione del titolare della casella PEC 15
7.1.2 Modalità di identificazione del titolare della casella PEC 18
7.2 Tipologie di caselle 21
7.3 Accesso ed utilizzo del servizio 21
7.3.4 Modifica dati anagrafici 21
7.3.5 Cambio di Titolare 21
7.3.10 Autenticazione a due fattori (2FA) 23
7.4 Partner ARUBA PEC 23
7.4.1 Modalità operative per il Partner 23
7.4.2 Assistenza per il Partner 23
7.5 Livelli di servizio ed indicatori di qualità 23
7.6 Interoperabilità con gli altri sistemi di PEC 23
7.6.1 Assistenza su segnalazioni gravi da parte degli altri Gestori 23
7.7 Cessazione dell'attività di Gestore 24
8. Obblighi e responsabilità 24
8.1 Obblighi e responsabilità del Gestore 24
8.2 Obblighi e responsabilità dei titolari 26
8.3 Limitazioni ed indennizzi 27
8.4 Risoluzione del contratto 27
8.5 Polizza assicurativa 27
9. Trattamento dei dati personali 27
9.1 Tutela e diritti degli interessati 27

1. Informazioni di carattere generale

1.1 Scopo

Questo documento è un'Integrazione del Manuale Operativo Aruba PEC (in seguito citato con la sigla MO) che definisce le regole e descrive le procedure utilizzate dal Gestore ARUBA PEC S.p.A. (di seguito per brevità ARUBA PEC) per l'erogazione del servizio di Posta elettronica certificata adeguata agli standard europei.

Col termine "Manuale Operativo" s'intende sempre riferirsi alla versione corrente del Manuale Operativo generale pubblicata sul portale web di Aruba PEC all'indirizzo https://www.pec.it/termini-condizioni.aspx#pec

Il Manuale Operativo vale per tutte le caselle di posta elettronica certificata erogate da Aruba PEC, senza distinzione per clienti e/o ambiti di applicazione.

Resta inteso che il Servizio di Posta Elettronica Certificata è disciplinato dal Manuale Operativo e che le previsioni del presente Addendum sono applicabili esclusivamente al Servizio di Posta elettronica certificata adeguata agli standard europei.

Per tutto quanto non espressamente specificato nel presente Addendum resta valido quanto descritto nel Manuale Operativo, al quale si rimanda (anche per i riferimenti normativi e tecnici eventualmente non riportati). Per agevolare la lettura, in questo documento è stata conservata, ove possibile, la stessa struttura e titolazione del Manuale Operativo. I paragrafi di cui al presente Addendum sostituiscono, con riferimento al Servizio di posta elettronica certificata adeguata agli standard europei, i corrispondenti paragrafi del MO.

Il presente Addendum è pubblicato alla medesima pagina web del MO.

I riferimenti alla normativa e agli standard sono riportati tra parentesi quadre.

Il Decreto-legge 14 dicembre 2018, n. 135 impone l'adozione delle misure necessarie per garantire la conformità dei Servizi di Posta Elettronica Certificata al regolamento (UE) n. 910/2014 (eIDAS) [10] che 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 e l'Italia, tra questi standard, ha scelto di implementare il modello REM che si basa su protocolli di posta elettronica e risulta la soluzione con modalità di fruizione più simili alla PEC.

Con la guida dell'Agenzia per l'Italia Digitale (AgID), i vari Gestori PEC hanno potuto implementare delle strategie di migrazione da PEC a REM. Nell'attesa che si realizzi la transizione dall'attuale sistema PEC al modello REM, inteso come un sistema di recapito certificato qualificato conforme al regolamento eIDAS, è quindi possibile che il soggetto titolare di una casella PEC possa richiedere al Gestore Aruba PEC l'adeguamento agli standard europei della propria casella PEC, in modo tale che sia conforme alle regole tecniche dell'attuale servizio PEC e disponga, inoltre, di caratteristiche tecniche aggiuntive (add-on) che la rendono adeguata ai nuovi standard europei.

Nel contesto specifico di questo documento, vengono descritte nel dettaglio le caratteristiche del servizio conforme agli standard europei fornito su richiesta dell'utente titolare della casella PEC, da Aruba PEC gestore accreditato di Posta Elettronica Certificata dal 12/10/2006 iscritto all'elenco pubblico gestito dall'Agenzia per l'Italia Digitale (AgID).

1.2 Versione dell'Addendum e responsabilità

ARUBA PEC è responsabile della stesura del presente documento. La versione dell'Addendum e le singole responsabilità dei redattori e supervisori sono riportate a pagina 1.

1.3 Definizioni ed acronimi dell'Addendum

Add-on	Caratteristiche tecniche aggiuntive (allegati/evidence ed headers) del servizio di Posta elettronica certificata adeguata agli standard europei
Autenticazione a due fattori/ Verifica in 2 passaggi	Definita anche 2FA o MFA (Multi-Factor Authentication) metodo di autenticazione effettuato tramite due o più fattori di autenticazione indipendenti e diversi tra loro (esempio: password + OTP).
Casella di posta elettronica certificata adeguata agli standard europei	È la casella di posta elettronica certificata, comprensiva degli Add-on ed associata ad un Titolare debitamente identificato, per la quale sia stata attivata la verifica in 2 passaggi.
CDRL	Centro di Registrazione Locale
IR	Incaricato al Riconoscimento
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, Aziende, Libero Professionista ecc.) attraverso il quale viene offerto il servizio di Posta Elettronica Certificata di Aruba PEC S.p.A. ai Titolari.

PEC adeguata agli standard europei	Posta Elettronica Certificata, comprensivo degli Add-on, che prevede l'identificazione certa del Titolare e l'attivazione dell'Autenticazione a due fattori.
REM	Registered Electronic Mail è un tipo specifico di servizio di recapito elettronico registrato (ERDS), che si basa sui formati, sui protocolli e sui meccanismi utilizzati nella normale messaggistica di posta elettronica.
Titolare	È il soggetto intestatario della casella di posta elettronica certificata adeguata agli standard europei, la cui identità è stata verificata come previsto dal presente Addendum
Utente	Persona che fruisce del servizio di Posta Elettronica Certificata adeguata agli standard Europei.

1.4 Tabella di corrispondenza

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

2. Dati identificativi del Gestore

Il servizio PEC oggetto del presente documento è erogato da Aruba PEC S.p.A., identificata come riportato nel corrispondente paragrafo del MO.

2.1 Responsabile dell'Addendum

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

2.2 Canali di comunicazione

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

2.3 Modifiche all'Addendum

Per ogni eventuale modifica al presente documento resta valido nella sua interezza quanto descritto all'interno del corrispondente paragrafo del MO, al quale si rimanda.

2.4 Indirizzo web del Gestore dal quale scaricare l'Addendum

L'indirizzo web dove poter visionare il MO e il presente Addendum è riportato al par.1.1.

2.5 Certificazioni ISO

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

3. Principali riferimenti normativi

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

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

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

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

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

[6] Circolare CNIPA n. 56 del 21 maggio 2009 - Modalità per la presentazione della domanda di iscrizione nell'elenco pubblico dei gestori di posta elettronica certificata (PEC) di cui all'articolo 14 del decreto del Presidente della Repubblica 11 febbraio 2005, n. 68.

[7] Decreto-legge del 29 novembre 2008, n. 185 - Misure urgenti per il sostegno a famiglie, lavoro, occupazione e impresa e per ridisegnare in funzione anti-crisi il quadro strategico nazionale convertito nella Legge 28 gennaio 2009, n. 2 - Conversione in legge, con modificazioni, del decreto-legge 29 novembre 2008, n. 185, recante misure urgenti per il sostegno a famiglie, lavoro, occupazione e impresa e per ridisegnare in funzione anti-crisi il quadro strategico nazionale.

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

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

[10] 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).

[11] REM SERVICES – Criteri di adozione degli standard ETSI – Policy IT Versione 1.2. Documento per i servizi di recapito certificato qualificato a norma eIDAS, disponibile sul sito AgID.

4. Informazioni generali sulla Posta Elettronica Certificata

4.1 Introduzione

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

4.2 Funzionamento di un sistema di Posta Elettronica Certificata adeguata agli standard europei

Resta valido nella sua interezza quanto descritto all'interno del corrispondente paragrafo del MO al quale si rimanda. In riferimento alle caselle PEC adeguate agli standard europei, si aggiunge quanto segue:

Caratteristiche tecniche aggiuntive per la PEC adeguata agli standard europei

Una volta che il titolare della casella PEC effettuato i passaggi necessari per l'adeguamento della casella agli standard europei (cfr. 7.1), tutti i messaggi inviati dalla casella PEC adeguata agli standard europei avranno caratteristiche tecniche aggiuntive (add-on), previste dagli standard europei per i servizi di recapito certificato qualificato (SERCQ). Tali caratteristiche tecniche aggiuntive sono:

- Headers, propri della REM, in aggiunta agli altri headers della PEC.
- Allegati (evidence) aggiuntivi (oltre al daticert.xml), per ogni evento generato dal flusso di invio/ricezione della PEC adeguata agli standard europei.

Allegati ed headers aggiuntivi sono coerenti per ogni tipologia di messaggio (mappatura tra messaggi PEC e REM, disponibile nella documentazione Policy IT AgID) [11].

Tali add-on sono previsti verso utenti di Gestori che hanno aderito alla PEC adeguata agli standard europei. Negli altri casi si opera in modalità PEC standard.

Quanto sopra riportato descrive il funzionamento di un sistema di PEC nel caso in cui non si verifichino problemi durante la spedizione. Con riferimento ai casi di:

- messaggio formalmente non corretto,

- presenza di virus
- ritardi di consegna
- comunicazioni con indirizzi email non certificati
- Antispam

Si rinvia integralmente ai corrispondenti paragrafi del Manuale Operativo. Vediamo nel seguito alcuni casi particolari.

Comunicazioni tra indirizzi PEC e indirizzi PEC adeguati agli standard europei

Messaggi da caselle PEC a caselle PEC adeguate agli standard europei e viceversa

Le caselle PEC adeguate agli standard europei possono comunque ricevere PEC da caselle PEC non adeguate e viceversa, in quanto i due sistemi sono compatibili.

5. Descrizione della soluzione tecnica definita da ARUBA PEC

5.1 Principali caratteristiche

La soluzione di ARUBA PEC per il servizio di posta elettronica certificata adeguata agli standard europei presenta le seguenti caratteristiche:

- È conforme alle specifiche AgID/DIGITPA/CNIPA ed alla normativa vigente in materia di PEC.
- Fornisce le evidenze previste dalle attuali disposizioni AgID/DIGITPA/CNIPA in materia di REM
- Rispetta le caratteristiche di interoperabilità ed è conforme, per quanto riguarda la sicurezza, alla normativa vigente.
- È basata su un'infrastruttura Hardware con caratteristiche di scalabilità, modularità e sicurezza nella gestione dei dati sensibili (Chiavi di Firma).
- È compatibile con tutti i client di posta (Thunderbird, Outlook, ecc.) che soddisfano i requisiti minimi stabiliti dalle regole tecniche.
- Le marcature temporali sono generate secondo lo standard internazionale RFC3161 tramite l'utilizzo di una Time Stamping Authority integrata in modalità sicura.
- È interoperabile con qualsiasi Certification Authority che soddisfa gli standard di interoperabilità.
- Si integra semplicemente alle tipologie di rete più diffuse sul mercato, Microsoft, Linux, ecc. Si integra in maniera trasparente a qualsiasi tipologia di rete eterogenea.

- Il certificato e la chiave di firma associati a ciascun dominio di posta elettronica certificata, nonché le procedure che espletano tutte le operazioni crittografiche necessarie durante la firma e/o la verifica dei messaggi risiedono su dispositivi HSM non suscettibili di alterazione (tamper-proof ,tamper-evident).

5.2 Scalabilità e Affidabilità

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

5.3 Sicurezza dei dati

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

5.4 Architettura di massima del sistema

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

5.5 Architettura della soluzione

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

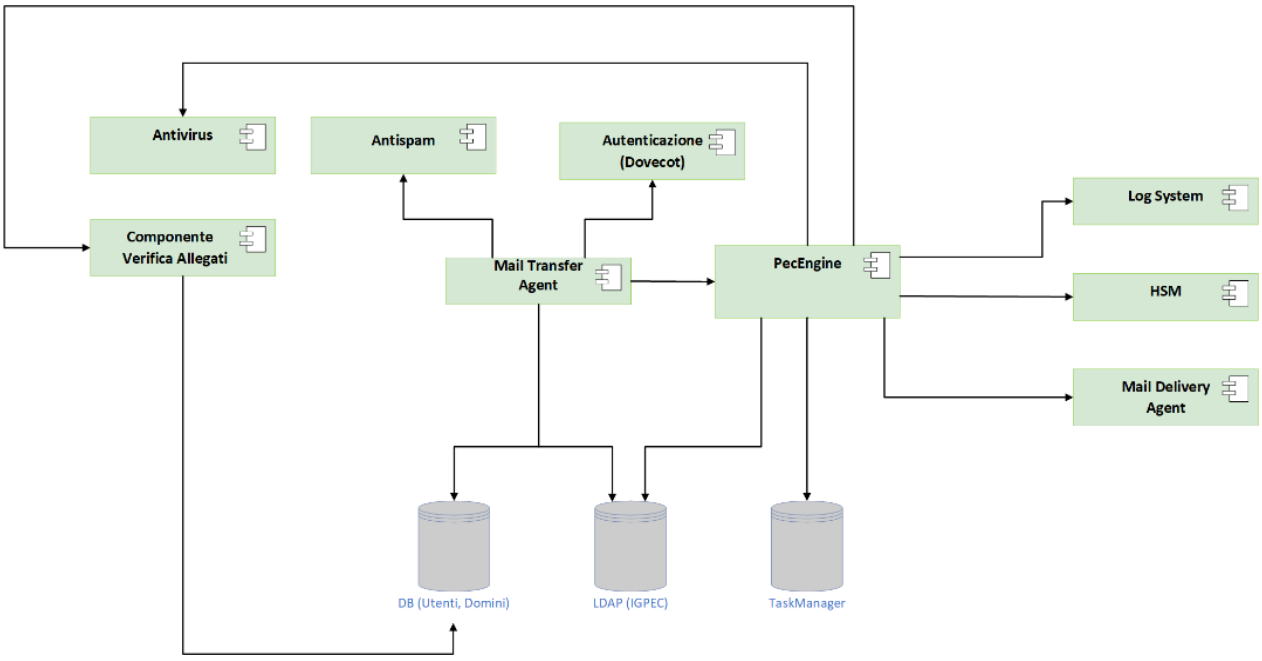

Figura 1 - Componenti del sistema

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

Relativamente al comportamento della componente di verifica:

- per i messaggi in uscita, la componente di verifica effettua una serie di controlli specifici sui file allegati, sul mime type, sulla presenza di macro ed eventualmente aggiunge gli header necessari;
- se è un messaggio in uscita, incapsula il messaggio in un documento di trasporto e di un 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, verifica la correttezza delle firme (attraverso il modulo HSM) e la validità del messaggio (provenienza da un dominio certificato), effettua il delivery verso la mailbox di destinazione attraverso il protocollo LMTP e, una volta consegnato il

messaggio crea la ricevuta di avvenuta consegna che l'MTA invierà al mittente del messaggio originale.

Nel caso di non validità del messaggio genera un messaggio di anomalia di trasporto e di 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

Resta valido nella sua interezza quanto descritto all'interno del corrispondente paragrafo del MO al quale si rimanda, specificando che il riferimento temporale accluso alle evidenze prodotte dal servizio è prodotto in conformità a quanto previsto per il servizio di Marche temporali Qualificate.

5.7 Storicizzazione dei Log e apposizione della marca temporale

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

5.8 Conservazione dei messaggi contenenti virus e relativa informativa al mittente

Il sistema di ARUBA PEC, compatibilmente con la normativa, verifica la presenza dei virus nei messaggi di posta elettronica adeguata agli standard europei al Punto di Accesso, ossia nella fase immediatamente successiva alla spedizione del messaggio originale, e al Punto di Ricezione, nella fase di ricezione dal sistema di posta certificato del mittente. L'individuazione del virus fa scattare una serie di operazioni finalizzate ad avvertire il soggetto che ha introdotto il virus ed alla conservazione del messaggio per eventuali verifiche successive. Se il virus è individuato al Punto di Accesso verranno generati un "Avviso di rilevazione di virus informatici" e una evidenza di tipo "SubmissionRejection" destinato al mittente del messaggio corrotto mentre se è stato individuato al Punto di Ricezione verrà generato un "Avviso di non accettazione per virus informatici" destinato al Gestore del sistema certificato del mittente, un "Avviso di mancata consegna per rilevazione di virus informatici" e una evidenza "ContentConsignmentFailure" destinati al mittente. Il sistema inoltre, conserva i messaggi contenenti virus su supporto ottico o magnetico mettendo in condizioni il Gestore di mantenerli per un periodo non inferiore a trenta mesi secondo le modalità indicate nelle deliberazioni AgID in materia di riproduzione e conservazione dei documenti. I backup ottenuti vengono conservati all'interno di locali fisici diversi in modo da garantire un più alto livello di sicurezza nel caso di eventi catastrofici quali incendi, terremoti ecc.

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

5.9 Descrizione Data Center di ARUBA PEC

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

6. Standard tecnologici, procedurali e di sicurezza adottati

6.1 Standard tecnologici di riferimento

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

6.2 Standard di sicurezza

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

6.3 Misure di sicurezza

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

6.4 Analisi dei rischi e procedure di ripristino

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

6.5 Procedure operative

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

7. Modalità di erogazione del servizio

7.1 Attivazione del Servizio

Una volta in possesso di una o più caselle di Posta Elettronica Certificata, il titolare delle caselle attive in quel momento può richiedere il passaggio al servizio di adeguamento agli standard europei. Per procedere all'adeguamento, il titolare della casella deve realizzare due passaggi:

1. Identificazione certa del titolare della casella
2. Attivazione della verifica in 2 passaggi

Al termine dei due step previsti dall'adeguamento della casella PEC, la casella conforme agli standard europei è contrassegnata visivamente. Di conseguenza, se una delle due condizioni indicate dovesse decadere (cfr. 7.3.5 e 7.3.10), la casella PEC non risulterà adeguata agli standard europei, operando come PEC. La casella, in questo caso, non sarà contrassegnata visivamente.

1.Identificazione certa del titolare della casella

Il titolare della PEC deve confermare la propria identità eseguendo il processo di riconoscimento, e scegliendo tra i seguenti metodi descritti più nel dettaglio al par. 7.1.2.

Qualora un utente risulti titolare di più caselle PEC, il processo di identificazione sarà associato a tutte le caselle attive in quel momento.

2. Attivazione della verifica in 2 passaggi (Autenticazione a due fattori)

Per il completo adeguamento della casella agli standard europei è necessario attivare la verifica in 2 passaggi (autenticazione a due fattori) per l'accesso alla casella, qualora questa non fosse già stata attivata per ciascuna casella PEC tramite la sezione Gestione Account (cfr. par. 7.3.10 del MO).

7.1.1 Processo di identificazione del titolare della casella PEC

Questo paragrafo descrive le modalità di identificazione dell'identità del titolare delle caselle PEC attive al momento dell'identificazione (persona fisica o giuridica).

Nel caso di caselle PEC intestate a persone giuridiche, si applica quanto segue:

- La richiesta di identificazione del titolare è a carico della persona fisica 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 PEC; qualora i controlli su fonti autoritative svolti dal Gestore PEC per la verifica dei poteri di rappresentanza non dovessero dare esito positivo, verrà richiesta della documentazione aggiuntiva comprovante i poteri di rappresentanza.

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:

a) si assuma esplicitamente gli obblighi previsti dalle norme vigenti e dal contratto il Gestore PEC, con contestuale accettazione delle Condizioni Generali di contratto e del presente Addendum al MO;

b) acconsenta al trattamento dei propri dati personali nel rispetto della normativa vigente.

Per il servizio Newsletter, se viene attivato dal titolare di una casella PEC che ha effettuato il processo di identificazione, la casella '_news' risulterà automaticamente riconosciuta anch'essa.

Prima di procedere all'adeguamento della casella PEC, il Gestore PEC deve identificare con certezza l'identità del titolare della casella PEC. Per consentire una più ampia diffusione sul territorio del servizio PEC ed una semplificazione dello stesso, ove possibile, tramite meccanismi di riconoscimento a distanza, le funzioni di identificazione possono essere svolte con varie modalità, 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 videoconferenza (anche detta DVO - "de visu online") svolta 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 identificazione possono essere svolte anche da terze parti delegate, con sedi distribuite sul territorio, sulla base di appositi accordi stipulati con il Gestore PEC. Tali terze parti (anche dette "Centri di Registrazione Locale", abbreviato CDRL) operano secondo procedure concordate con il Gestore PEC. I CDRL sono

responsabili nei confronti del Gestore della corretta e sicura identificazione dei titolari delle caselle PEC, nonché del trattamento dei loro dati nel pieno rispetto della normativa sulla privacy. Il Gestore si riserva la possibilità di effettuare verifiche presso i CDRL della corretta esecuzione delle attività affidate nonché il rispetto dell'istruzioni impartite. Il Gestore PEC rimane a sua volta pienamente responsabile delle operazioni di identificazione dei titolari, siano esse svolte in proprio oppure dai CDRL.

Il Gestore PEC o la terza parte delegata (CDRL) può rigettare la richiesta di identificazione del titolare della casella PEC 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 italiana,
- passaporto.

Nel rispetto di quanto previsto dallo standard ETSI EN 319-521 (par. 5.4), il Gestore PEC 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 PEC adeguata agli standard europei con relativa accettazione. L'accettazione delle condizioni di contratto 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 generate da Aruba sono conservate a norma per un periodo di 10 anni dalla data di cessazione del servizio.

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 PEC 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 PEC 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.

I contratti stipulati con ciascun Centro di Registrazione Locale (CDRL) sono conservati dall'ufficio legale di Aruba PEC. 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 PEC

Le modalità di identificazione del titolare della casella PEC sono descritte come richiamato all'interno della Policy IT v.1.2 di AgID e dallo standard ETSI EN 319-521 [11]. Relativamente alle modalità di identificazione descritte di seguito, il Gestore PEC verifica direttamente, o affidandosi a terzi, l'identità del Titolare della casella PEC. Nelle descrizioni che seguono, il termine "Titolare" si riferisce al soggetto che è intestatario della/e casella/e PEC attiva/e in quel momento per sé o per l'organizzazione che egli/ella rappresenta (in quanto persona fisica che rappresenta la persona giuridica).

Modalità 1

L'identificazione prevede la presenza fisica (de-visu) del Titolare della casella PEC, 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 d'identificazione, 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 PEC;
- 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 mandato con il Gestore PEC in cui la terza parte indica il proprio personale, che sarà definito IR, che dovrà operare nel contesto delle pratiche operative 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 PEC e del CDRL e previa qualificazione degli IR, il Gestore PEC 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 PEC. Gli IR possono operare successivamente alla stipula di un mandato direttamente con il Gestore PEC, o tramite nomina di un CDRL, nel contesto delle pratiche operative definite dal Gestore PEC stesso e limitatamente allo svolgimento delle attività di identificazione.

Modalità 2

L'identificazione del titolare della/e casella/e PEC 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 [10]. Nello specifico riferimento al contesto italiano, tale verifica dell'identità del Soggetto richiedente titolare della/e casella/e PEC 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 Richiedente 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 PEC), 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/e casella/e PEC (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/e casella/e PEC che si vuole adeguare agli standard europei, 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 PEC;
- da una terza parte, incaricata dal Gestore PEC, denominata Centro di Registrazione Locale (CDRL) dinnanzi ad un incaricato del CDRL;
- da un soggetto terzo, incaricato dal Gestore PEC denominato Incaricato al Riconoscimento (IR).

L'incaricato al riconoscimento 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'incaricato, 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'incaricato 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 [10] e dallo standard ETSI EN 319-521 (al par. 5.2).

Al momento dell'identificazione, il Titolare deve confermare:

- la volontà di voler effettuare l'identificazione tramite webcam per l'adeguamento della PEC agli standard europei;
- i dati identificativi ed anagrafici registrati ed associati alla/e caselle PEC di cui è Titolare al momento dell'identificazione;

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.

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.

7.2 Tipologie di caselle

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

7.3 Accesso ed utilizzo del servizio

Resta valido nella sua interezza quanto descritto all'interno del paragrafo del MO, al quale si rimanda. Si prevedono, nell'ambito del presente Addendum, le aggiunte descritte di seguito:

7.3.4 Modifica dati anagrafici

Resta valido nella sua interezza quanto descritto all'interno del corrispondente paragrafo del MO, al quale si rimanda, specificando che qualora le modifiche dei dati anagrafici dovessero comportare il cambio di titolarità della casella PEC adeguata agli standard europei, si applica quanto previsto dal par. 7.3.5.

7.3.5 Cambio di Titolare

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

Nel caso si volesse cambiare la Titolarità di caselle PEC conformi agli standard europei, occorre precisare che:

- le caselle che sono in fase di riconoscimento (per le quali è in corso un processo di identificazione così come descritto al par. 7.1.2) non possono essere trasferite ad altro Titolare;
- le caselle che sono in fase di trasferimento non possono essere riconosciute (il nuovo Titolare della casella dovrà attendere la conclusione del trasferimento di titolarità per avviare il processo di identificazione descritto al par. 7.1.2).

Come specificato al par. 7.1, il cambio di titolarità comporta che le caselle PEC conformi agli standard europei opereranno come PEC, in attesa che il nuovo titolare effettui il processo di identificazione.
Attraverso il canale online, le modalità di cambio del Titolare sono descritte al seguente link: https://guide.pec.it/posta-pec/modifica-dati/modifica-titolare-casella-pec.aspx

Attraverso il canale Partner, per ottenere la modifica è necessario che il Titolare ne faccia espressa richiesta al proprio Partner di riferimento avendo cura di fornire le seguenti informazioni:

1. I dati anagrafici del vecchio Titolare:

- nome e cognome;
- indirizzo di residenza (via, numero civico, città e CAP);
- codice fiscale o partita iva.

2. Una copia del documento di identità del vecchio Titolare.

3. I dati anagrafici del nuovo Titolare:

- nome e cognome;
- indirizzo di residenza (via, numero civico, città e CAP);
- codice fiscale o partita iva.

4. Una copia del documento di identità del nuovo Titolare;

5. Modulo cambio titolarità firmato da vecchio e nuovo Titolare;

6. Contatti di riferimento (email e cellulare) del nuovo Titolare.

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

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

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

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

7.3.10 Autenticazione a due fattori (2FA)

Resta valido nella sua interezza quanto descritto all'interno del paragrafo del MO al quale si rimanda, con la specifica che per quanto riguarda l'accesso e l'utilizzo di caselle PEC adeguate agli standard europei, è obbligatorio attivare l'autenticazione a due fattori. Infatti, come specificato al par. 7.1, disattivando l'autenticazione a due fattori, la casella PEC interessata non sarà conforme agli standard europei ed opererà dunque come PEC.

7.4 Partner ARUBA PEC

7.4.1 Modalità operative per il Partner

Resta valido nella sua interezza quanto descritto all'interno del corrispondente paragrafo del MO, al quale si rimanda, specificando che, qualora il Partner esegua i riconoscimenti ai fini dell'attivazione del Servizio di posta elettronica certificata conforme agli standard europei, si applica quanto previsto ai paragrafi 7.1.1 e 7.1.2 del presente Addendum.

7.4.2 Assistenza per il Partner

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

7.5 Livelli di servizio ed indicatori di qualità

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

7.6 Interoperabilità con gli altri sistemi di PEC

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

7.6.1 Assistenza su segnalazioni gravi da parte degli altri Gestori

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

7.7 Cessazione dell'attività di Gestore

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

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

In caso di mancata individuazione del Gestore subentrante, ARUBA PEC specificherà nella comunicazione anche il periodo di tempo durante il quale le suddette caselle, pur non avendo funzionalità di invio/ricezione messaggi, saranno attive in sola lettura. ARUBA PEC inoltre conserverà i log per l'arco temporale previsto dalla Normativa e pertanto per un periodo non inferiore a 30 mesi. In caso di mancata individuazione del Gestore subentrante, verranno conservate da ARUBA PEC anche le evidenze relative al riconoscimento dei Titolari per il tempo richiesto dalla normativa vigente.

Nel caso in cui il Gestore subentrante sia stato individuato, le evidenze relative al riconoscimento dei Titolari e i log verranno invece trasferiti al Gestore subentrante che dovrà conservarli per l'arco temporale previsto dalla Normativa.

8. Obblighi e responsabilità

8.1 Obblighi e responsabilità del Gestore

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

- garantire i livelli di servizio previsti;
- assicurare l'interoperabilità con gli altri Gestori accreditati;
- informare i titolari sulle modalità di accesso al servizio e sui necessari requisiti tecnici;
- fornire al mittente la ricevuta di presa in carico, accettazione e di avvenuta consegna del messaggio di posta elettronica certificata (salvo nel caso di eventi disastrosi improvvisi);
- comunicare al Titolare della casella di posta elettronica certificata la mancata consegna del messaggio entro le 24 ore dall'invio (salvo nel caso di eventi disastrosi improvvisi);

- apporre su ogni messaggio un riferimento temporale, sia esso il messaggio di trasporto, una ricevuta o un avviso (salvo nel caso di eventi disastrosi improvvisi);
- apporre la relativa marca temporale ai log dei messaggi generati dal sistema;
- effettuare la corretta trasmissione dal mittente al destinatario conservando l'integrità del messaggio originale nella relativa busta di trasporto (salvo nel caso di eventi disastrosi improvvisi);
- rilasciare avviso di rilevazione di virus informatici;
- rilevare la presenza di virus o eccezioni formali nei messaggi mediante avviso di non accettazione;
- rilasciare avviso di mancata consegna per superamento dei tempi massimi previsti (salvo nel caso di eventi disastrosi improvvisi);
- agire nel rispetto delle norme previste dal Decreto legislativo 30 giugno 2003, n. 196 Codice in materia di protezione dei dati personali e del Regolamento UE 2016/679 (GDPR);
- adottare misure atte ad evitare inserimento di codici eseguibili dannosi nei messaggi (virus);
- prevedere procedure e servizi di emergenza che assicurino il completamento della trasmissione anche in caso di incidenti (salvo nel caso di eventi disastrosi improvvisi);
- registrare ed associare un riferimento temporale ad ogni fase di trasmissione del messaggio sui file log, conservare e rendere disponibili detti log per gli usi e nelle modalità previste dalla legge;
- garantire la riservatezza, integrità e inalterabilità nel tempo dei file di log;
- assicurare la segretezza della corrispondenza trasmessa attraverso il proprio sistema;
- conservare i messaggi contenenti virus informatici per il periodo previsto dalla normativa;
- conservare le informazioni relative agli accordi stipulati con i Titolari e/o Partner nel rispetto della normativa vigente;
- effettuare la disattivazione di una casella PEC dopo aver verificato l'autenticità della richiesta;
- fornire informazioni sulle modalità di richiesta, reperimento e presentazione all'Utente dei log dei messaggi;
- utilizzare protocolli sicuri allo scopo di garantire la segretezza, l'autenticità, l'integrità delle informazioni trasmesse attraverso il sistema PEC;
- attivare la procedura di sostituzione dei certificati elettronici relativi alle proprie chiavi di firma con una tempistica tale da non causare interruzioni di servizio;
- richiedere la revoca dei certificati relativi alle chiavi utilizzate per la firma dei messaggi e per la connessione sicura al sito dell'AgID in caso di loro compromissione;
- operare in modo che non sia consentita la duplicazione abusiva e incontrollata delle chiavi private di firma o dei dispositivi che le contengono;
- consentire l'esportazione cifrata delle chiavi private di firma in modo da non diminuirne il livello di sicurezza;
- non consentire l'utilizzo delle chiavi private per scopi diversi dalla firma dei messaggi previsti dalla normativa;

- comunicare tempestivamente ai propri utenti l'eventuale cessazione o interruzione del servizio;
- consentire l'accesso logico e fisico al sistema alle sole persone autorizzate;
- utilizzare un sistema di riferimento temporale che garantisca stabilmente una sincronizzazione delle macchine coinvolte con uno scarto non superiore al minuto secondo rispetto alla scala di Tempo Universale Coordinato UTC;
- utilizzare dispositivi di firma conformi con la normativa;
- identificare in maniera certa il Titolare della casella PEC adeguata agli standard europei secondo le modalità previste dal Reg. eIDAS prevedendo che, nei casi in cui l'identificazione dovesse decadere per i casi previsti dal presente documento, la PEC tornerebbe standard e di conseguenza non adeguata al Reg. eIDAS;
- imporre all'utente della casella PEC adeguata alla normativa europea, il requisito dell'accesso alla stessa tramite autenticazione a due fattori, prevedendo che in caso di disattivazione di tale metodologia di autenticazione secondo quanto previsto dal presente documento, la PEC tornerebbe standard e di conseguenza non adeguata al Reg. eIDAS.

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 per l'identificazione certa del Titolare della casella, garantendo, sotto la propria responsabilità, la veridicità e la correttezza, ai sensi dell'art. 46 DPR 445/2000 e s.m.i.;
- utilizzare in modo sicuro il servizio evitando di rivelare a terzi le credenziali di accesso, adottando tutte le precauzioni e misure atte a preservare la sicurezza delle credenziali e sporgere immediatamente denuncia alle Autorità competenti in caso di smarrimento o sottrazione delle Credenziali e fornire tempestivamente ad Aruba PEC tale notizia;
- adottare tutte le misure idonee a garantire la custodia del dispositivo personale utilizzato per l'autenticazione a due fattori;
- utilizzare il servizio per i soli usi consentiti dalla legge;
- utilizzare soltanto il servizio di posta elettronica certificata erogato da Gestori accreditati (presenti nell'elenco pubblico dei Gestori tenuto da AgID);
- i privati che intendono utilizzare il servizio di posta elettronica certificata nei rapporti con la Pubblica Amministrazione, devono espressamente dichiarare il proprio indirizzo. Tale dichiarazione obbliga solo il dichiarante e può essere revocata;
- le imprese, nei rapporti tra loro intercorrenti, possono dichiarare la esplicita volontà di accettare l'invio di posta elettronica certificata mediante indicazione nell'atto di iscrizione al registro delle imprese. Tale dichiarazione obbliga solo il dichiarante e può essere revocata;
- informare le persone abilitate all'utilizzo delle caselle sulle tematiche di sicurezza concernenti il loro uso onde evitare un uso non autorizzato;

- adottare misure atte ad evitare inserimento di codici eseguibili dannosi nei messaggi (virus);
- utilizzare le sole modalità di accesso descritte al capitolo 7;
- resta a cura del Titolare della casella di posta elettronica certificata la conservazione delle copie dei messaggi inviati o spediti e delle relative ricevute.

8.3 Limitazioni ed indennizzi

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

8.4 Risoluzione del contratto

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

8.5 Polizza assicurativa

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

9. Trattamento dei dati personali

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

9.1 Tutela e diritti degli interessati

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