Due Diligence

delle misure di sicurezza per il rilascio delle integrazioni applicative del servizio di Posta Elettronica Certificata

Versione 1.0

Aruba PEC S.p.A.
Via San Clemente 53, Ponte San Pietro 24036 (BG)
Partita I.V.A. 01879020517 | **Codice Fiscale** 01879020517
REA 445886 | **C.S.** € 6.500.000,00 i.v. | **PEC** arubapec@aruba.pec.it | **Sito** enterprise.aruba.it

SOMMARIO

Aruba PEC S.p.A.
Via San Clemente 53, Ponte San Pietro 24036 (BG)
Partita I.V.A. 01879020517 | **Codice Fiscale** 01879020517
REA 445886 | **C.S.** € 6.500.000,00 i.v. | **PEC** arubapec@aruba.pec.it | **Sito** enterprise.aruba.it

1 INTRODUZIONE E SCOPO DEL DOCUMENTO

Il presente documento descrive le misure di sicurezza adottate dal Cliente per garantire la conformità normativa e la protezione del Servizio di Posta Elettronica Certificata (PEC) quando l'accesso avviene tramite software o web-application, anche di terze parti.

La compilazione e l'accettazione del documento da parte del Cliente sono obbligatorie. L'erogazione del servizio è subordinata al parere positivo del Gestore Aruba PEC S.p.A., sulla base delle informazioni fornite dal Cliente.

Il servizio potrà essere sospeso in caso di:

- mancata approvazione da parte del Gestore;
- gravi incidenti di sicurezza che compromettano l'integrità, la disponibilità, l'immodificabilità o la riservatezza dei dati trasmessi.

Obiettivo del documento è assicurare che l'integrazione del servizio PEC con componenti software mantenga nel tempo i requisiti di sicurezza richiesti dal Gestore.

2 RUOLI E RESPONSABILITÀ

2.1 Gestore di Posta Elettronica Certificata - Aruba PEC S.p.A.

È il soggetto che eroga il servizio di Posta Elettronica Certificata verso il Cliente.

Il ruolo di Gestore del servizio di Posta Elettronica Certificata, ai sensi nella normativa vigente, è svolto da Aruba PEC S.p.A.. La descrizione completa dei compiti e delle responsabilità del certificatore è presente nel Manuale Operativo del servizio di Posta Elettronica Certificata.

Il Gestore mette a disposizione la possibilità di accesso e/o utilizzo del Servizio anche tramite soluzioni software o *web-application*, anche di terze parti, previa verifica ed approvazione delle misure di sicurezza poste in essere dal Cliente secondo quanto meglio precisato nel prosieguo del presente.

Il Gestore si riserva il diritto di effettuare audit periodici allo scopo di verificare le misure di sicurezza poste in essere dal Cliente nonché di sospendere l'erogazione del servizio di Posta Elettronica Certificata tramite Integrazioni Applicative in caso di gravi carenze e/o seguito di gravi incidenti di sicurezza che possano aver violato l'integrità, l'immodificabilità, la disponibilità e la riservatezza dei dati trasmessi tramite il servizio di Posta Elettronica Certificata così come disciplinato nelle Condizioni Generali di Contratto.

2.2 Cliente

È il soggetto che usufruisce del servizio di Posta Elettronica Certificata erogata dal Gestore anche attraverso client di posta elettronica, software applicativi o *web-application,* anche di terze parti.

Il Cliente è il destinatario del presente documento che accetta e sottoscrive quanto dettagliato in merito alle misure di sicurezza poste in essere dal Cliente stesso e oggetto di successiva valutazione da parte del Gestore.

Il Cliente è inoltre responsabile di comunicare tempestivamente al Gestore in caso di:

- eventuali incidenti di sicurezza che possano aver violato l'integrità, l'immodificabilità, la disponibilità e la riservatezza dei dati trattati dal servizio di Posta Elettronica Certificata;
- di eventuali cambiamenti infrastrutturali e/o nelle politiche e misure di sicurezza che alterino quanto indicato nel presente documento.

  In tal caso si rende necessaria una nuova compilazione e valutazione del presente documento.

Il Cliente potrà essere inoltre soggetto ad audit periodici da parte del Gestore per la verifica del rispetto dei requisiti di sicurezza previsti per l'utilizzo del servizio di Posta Elettronica Certificata.

3 DUE DILIGENCE DI SICUREZZA

Il Gestore ha messo a disposizione dei propri Clienti la possibilità di accesso ed utilizzo del servizio di Posta Elettronica Certificata tramite soluzioni basate su client di posta elettronica, software applicativi e/o *web-application,* anche di terze parti, così come già formalizzato all'interno del Manuale Operativo del servizio di Posta Elettronica Certificata.

A seconda della soluzione scelta ed adottata dal Cliente si distinguono i seguenti ***scenari***:

1. **Integrazione con *API-KEY***, nel caso in cui il Cliente utilizzi applicativi *legacy* che non supportino l'autenticazione basata su framework OAuth2;
2. **Integrazione con *modalità interattiva*[1]**, nel caso in cui i client o gli applicativi del Cliente accedano alla casella su esplicita azione dell'utente umano autorizzato all'uso della casella;
3. **Integrazione con *modalità applicativa*[1]**, nel caso in cui gli applicativi del Cliente accedano in modo completamente automatizzato alle caselle e non prevedano alcun tipo di intervento umano (*Machine to Machine - M2M*).

È richiesto al Cliente di attestare la conformità ai requisiti di sicurezza individuati dal Gestore, riportati nelle seguenti tabelle, fornendo, ove necessario o ritenuto opportuno, ulteriori chiarimenti o dettagli integrativi anche in caso di utilizzo di Servizi di Terze Parti.

NB: Nei casi in cui il Cliente preveda l'utilizzo di più scenari, o utilizzi differenti soluzioni software nell'ambito dello stesso scenario ma con differenti misure di sicurezza, è necessario provvedere alla compilazione di più questionari.

[1] Le integrazioni attraverso le modalità "*interattiva*" e "*applicativa*" sono possibili sia attraverso protocolli standard (IMAP, PO3 ed SMTP) sia attraverso API.

Aruba PEC S.p.A.
Via San Clemente 53, Ponte San Pietro 24036 (BG)
Partita I.V.A. 01879020517 | **Codice Fiscale** 01879020517
REA 445886 | **C.S.** € 6.500.000,00 i.v. | **PEC** arubapec@aruba.pec.it | **Sito** enterprise.aruba.it

Cliente: *Applicativo*:

Requisiti obbligatori per l'attivazione del Servizio			
ID	**Scenario**	**Requisito**	**Risposta**
SEC-01	API-KEY Modalità Interattiva Modalità Applicativa	Tutti gli account che permettono accesso interattivo ad applicazioni e sistemi in ambito devono essere nominali, al fine di garantire l'accountability delle azioni eseguite. Gli account non nominali e con accesso interattivo (account condivisi) che non possono essere disabilitati devono essere gestiti in modo da garantirne l'accountability, ad esempio per il tramite di macchine ponte, registrando le sessioni d'uso o tramite opportune procedure operative.	○ *Conforme* ○ *Non Conforme*
SEC-02	Modalità Interattiva Modalità Applicativa	Le chiavi private relative a certificati usati per l'autenticazione non devono essere utilizzate da più sistemi o applicazioni	○ *Conforme* ○ *Non Conforme*
SEC-03	API-KEY Modalità Interattiva Modalità Applicativa	Le chiavi private e le credenziali di autenticazione devono essere conservate sui sistemi facendo uso di tecnologie o processi operativi finalizzati al mantenimento della loro segretezza ed integrità, anche rispetto ai permessi amministrativi assegnati a utenze dei sistemi ospitanti.	○ *Conforme* ○ *Non Conforme*
SEC-04	API-KEY Modalità Interattiva Modalità Applicativa	Il livello di privilegio associato alle componenti applicative e di sistema deve essere il più basso possibile. Le applicazioni devono girare con utenza tecnica dedicata, con privilegi opportuni, e non con utenza amministrativa.	○ *Conforme* ○ *Non Conforme*
SEC-05	API-KEY Modalità Interattiva Modalità Applicativa	Tutte le trasmissioni di dati (per qualunque tipologia di accesso e per qualunque tipologia di utente) devono utilizzare protocolli di rete cifrati, robusti e non obsoleti, in particolare TLS 1.2 o 1.3 per le interfacce web e le API, SSH 2 o RDP basato su TLS 1.2 o 1.3 per l'accesso in console.	○ *Conforme* ○ *Non Conforme*
SEC-06	Modalità Interattiva Modalità Applicativa	I processi di sviluppo software delle applicazioni in ambito devono basarsi su best practice e linee guida di sviluppo sicuro al fine di garantire una qualità adeguata in termini di sicurezza delle applicazioni.	○ *Conforme* ○ *Non Conforme*

Aruba PEC S.p.A.
Via San Clemente 53, Ponte San Pietro 24036 (BG)
Partita I.V.A. 01879020517 | **Codice Fiscale** 01879020517
REA 445886 | **C.S.** € 6.500.000,00 i.v. | **PEC** arubapec@aruba.pec.it | **Sito** enterprise.aruba.it

Requisiti obbligatori a 30 giorni dall'attivazione del Servizio			
ID	**Scenario**	**Requisito**	**Risposta**
SEC-07	API-KEY Modalità Interattiva Modalità Applicativa	Tutti gli elementi applicativi utilizzati per l'accesso al servizio devono essere individuati e censiti opportunamente, insieme ai ruoli operativi dei singoli elementi e ai dati trattati.	○ *Conforme* ○ *Parzialmente Conforme* ○ *Non Conforme*
SEC-08	API-KEY Modalità Interattiva Modalità Applicativa	Tutte le componenti sistemistiche e applicative (sistemi operativi, database, etc.) devono essere opportunamente sottoposte ad hardening come da best practice di mercato, attivando solo i servizi strettamente necessari.	○ *Conforme* ○ *Parzialmente Conforme* ○ *Non Conforme*
SEC-09	API-KEY Modalità Interattiva Modalità Applicativa	Sui sistemi che ospitano le applicazioni in ambito devono essere previste l'installazione, la manutenzione costante ed il monitoraggio dei presidi di sicurezza di base quali come EDR o soluzioni antimalware.	○ *Conforme* ○ *Parzialmente Conforme* ○ *Non Conforme*

Requisiti obbligatori a 90 giorni dall'attivazione del Servizio			
ID	**Scenario**	**Requisito**	**Risposta**
SEC-10	API-KEY Modalità Interattiva Modalità Applicativa	Gli account di sistema di default con privilegi amministrativi (e.g. root, administrator, etc.) devono essere resi inutilizzabili. Se non è possibile disabilitarli, è necessario che sia definita una procedura di controllo stringente sul loro utilizzo.	○ *Conforme* ○ *Parzialmente Conforme* ○ *Non Conforme*
SEC-11	API-KEY Modalità Interattiva Modalità Applicativa	I diritti di accesso su sistemi e applicazioni in ambito devono essere assegnati agli utenti in base ai compiti loro attribuiti, seguendo il principio dei privilegi minimi e le necessità effettive di accesso.	○ *Conforme* ○ *Parzialmente Conforme* ○ *Non Conforme*
SEC-12	API-KEY Modalità Interattiva Modalità Applicativa	L'accesso a funzionalità privilegiate deve essere limitato alle sole necessità previste dal ruolo assegnato all'utente.	○ *Conforme* ○ *Parzialmente Conforme* ○ *Non Conforme*
SEC-13	API-KEY Modalità Interattiva Modalità Applicativa	Le applicazioni in ambito devono essere installate in segmenti di rete opportunamente segregati e raggiungibili unicamente dalle postazioni di lavoro o da sistemi autorizzati.	○ *Conforme* ○ *Parzialmente Conforme* ○ *Non Conforme*
SEC-14	API-KEY Modalità Interattiva Modalità Applicativa	Per tutti i sistemi e le componenti software in ambito deve essere previsto un processo di patching finalizzato a mantenere un adeguato livello di sicurezza.	○ *Conforme* ○ *Parzialmente Conforme* ○ *Non Conforme*

Requisiti obbligatori a 180 giorni dall'attivazione del servizio			
ID	**Scenario**	**Requisito**	**Risposta**
SEC-15	Modalità Interattiva Modalità Applicativa	Le utenze che accedono ad applicazioni e sistemi in ambito e le relative modalità di autenticazione devono essere gestite tramite strumenti tecnici e/o procedure operative in grado di garantire il controllo centralizzato dei permessi di accesso, segregando i ruoli degli utenti da quelli degli amministratori	○ *Conforme* ○ *Parzialmente Conforme* ○ *Non Conforme*
SEC-16	API-KEY Modalità Interattiva Modalità Applicativa	L'architettura di rete deve essere organizzata in almeno tre livelli: ○ livello di front-end che contiene l'interfaccia utente e rappresenta il punto di ingresso dell'applicazione ○ livello di back-end, che contiene la logica per la gestione delle richieste ○ livello database per la memorizzazione dei dati. Ogni livello deve essere separato fisicamente o logicamente dagli altri per evitare l'accesso non autorizzato tra di essi.	○ *Conforme* ○ *Parzialmente Conforme* ○ *Non Conforme*
SEC-17	API-KEY Modalità Interattiva Modalità Applicativa	La segregazione di rete deve essere ottenuta tramite firewall configurati per filtrare il traffico di rete tra i diversi ambienti e livelli e devono essere definite delle politiche di sicurezza per consentire solo le comunicazioni necessarie tra le diverse componenti.	○ *Conforme* ○ *Parzialmente Conforme* ○ *Non Conforme*
SEC-18	API-KEY Modalità Interattiva Modalità Applicativa	Tutti gli eventi rilevanti per l'erogazione del servizio o per l'integrità di sistemi e applicazioni devono generare dei log di sicurezza; in particolare: • Tutte le interazioni con i meccanismi di autenticazione, come ad esempio: ○ autenticazione; ○ cambio password; ○ reset password; ○ recupero username; ○ modifica della propria modalità di autenticazione (e.g. abilitazione o disabilitazione 2FA); ○ modifica anagrafica; ○ delega di privilegio di accesso ad altri utenti; • Tutte le cancellazioni o modifiche alle configurazioni rilevanti dei servizi, modificabili dall'utente; • Tutti gli eventi generati a seguito di attività amministrative, ad esempio: ○ creazione, modifica o cancellazione di account; ○ creazione, modifica o cancellazione di gruppi e di appartenenza a gruppi; ○ concessione, modifica o rimozione di autorizzazioni ad account e gruppi; ○ modifica della modalità di autenticazione di un utente (e.g. abilitazione o disabilitazione 2FA); ○ cancellazione o modifica alle configurazioni; ○ uso dei privilegi; ○ attivazione o disattivazione del meccanismo di logging; ○ cambio del livello di dettaglio del logging.	7 ○ *Conforme* ○ *Parzialmente Conforme* ○ *Non Conforme*
SEC-19	API-KEY Modalità Interattiva Modalità Applicativa	Tutti i log relativi agli eventi descritti in precedenza devono essere protetti da manipolazione o cancellazione e conservati separatamente rispetto ai sistemi che li hanno generati per un appropriato periodo di retention. I log devono essere resi disponibili al Gestore in caso di ispezione.	○ *Conforme* ○ *Parzialmente Conforme* ○ *Non Conforme*
SEC-20	API-KEY Modalità Interattiva Modalità Applicativa	L'accesso alle impostazioni di logging deve essere limitato esclusivamente agli utenti con privilegi di amministrazione dei sistemi, apparati e applicazioni.	○ *Conforme* ○ *Parzialmente Conforme* ○ *Non Conforme*
SEC-21	API-KEY Modalità Interattiva Modalità Applicativa	L'accesso al contenuto dei log deve essere limitato esclusivamente agli utenti all'uopo autorizzati.	○ *Conforme* ○ *Parzialmente Conforme* ○ *Non Conforme*

4 LIMITAZIONI DI RESPONSABILITÀ E VERIFICHE

Il Gestore rimane responsabile esclusivamente per le attività di propria competenza, come descritte nell'Allegato Tecnico e/o nella Scheda Prodotto, e secondo le modalità previste nelle Condizioni Generali, alle quali si rinvia.

Il Cliente è l'unico responsabile delle dichiarazioni rese nel presente documento e risponde integralmente di eventuali dichiarazioni false, incomplete o parziali, nonché di tutte le conseguenze pregiudizievoli che possano derivarne nei confronti del Gestore, del Titolare o di terzi.

Il Cliente è altresì tenuto a comunicare tempestivamente al Gestore, secondo le modalità previste nelle Condizioni Generali:

- ogni mutamento o evoluzione della soluzione qui descritta;
- qualsiasi incidente di sicurezza che possa compromettere l'integrità, l'immodificabilità, la disponibilità o la riservatezza dei dati trattati tramite il Servizio.

Al fine di dimostrare l'osservanza degli obblighi assunti, il Cliente acconsente sin d'ora allo svolgimento di audit da parte del Gestore. A tal fine, il Cliente si impegna a mettere a disposizione di Aruba PEC S.p.A. tutta la documentazione, le evidenze e le attestazioni necessarie, inclusa, ove richiesto, la descrizione delle procedure di identificazione adottate, atte a dimostrare la corretta identificazione dei propri dipendenti.

Qualora il Cliente deleghi, anche solo parzialmente e in conformità al presente documento, l'esecuzione di determinate attività a soggetti terzi, lo stesso si impegna a regolamentare tale rapporto mediante apposito accordo scritto. Tale accordo dovrà prevedere, in favore del Gestore e a carico del terzo incaricato, gli stessi diritti di accesso, ispezione e verifica stabiliti nel presente documento.

Il Cliente, inoltre, manleva fin d'ora il Gestore da qualsivoglia conseguenza pregiudizievole derivante dall'inadempimento proprio o di terzi e si obbliga al risarcimento di eventuali danni recati al Gestore nonché eventuali sanzioni comminate dalle Autorità competenti a causa di tali inadempimenti.

5 ACCETTAZIONE DEL DOCUMENTO

Io sottoscritto/a _____,

codice fiscale _____,

in qualità di _____ della _____, (specificare carica ricoperta e nome dell'organizzazione di appartenenza / rappresentata), come già identificato nel modulo d'ordine se presente.

dichiaro

di aver letto e compreso il documento "*Due Diligence delle misure di sicurezza per il rilascio delle integrazioni applicative del servizio di Posta Elettronica Certificata*". Con la presente accettazione mi impegno a rispettare e far rispettare i requisiti da tutti i soggetti coinvolti nella gestione ed utilizzo della soluzione implementata ciascuno per quanto di propria competenza. Mi impegno, altresì, a porre in essere entro il termine massimo di sei mesi dalla sottoscrizione del presente documento, le opportune azioni correttive volte al superamento delle parziali non conformità dichiarate, dandone opportuna comunicazione al Gestore.

Data _____ **Firma** _____

Dichiaro inoltre, anche ai sensi degli artt. 1341 e 1342 c.c., di aver preso esatta visione e di approvare in modo specifico le seguenti clausole del documento “Requisiti per soluzioni di firma basate su riconoscimento con modalità 6 del CPS” articolo 3 “Requisiti tecnico-operativi” articolo 5 “Limitazioni di responsabilità e verifiche”.

Data _____ **Firma** _____

Aruba PEC S.p.A.
Via San Clemente 53, Ponte San Pietro 24036 (BG)
Partita I.V.A. 01879020517 | **Codice Fiscale** 01879020517
REA 445886 | **C.S.** € 6.500.000,00 i.v. | **PEC** arubapec@aruba.pec.it | **Sito** enterprise.aruba.it