Aruba PEC S.p.A.

Service Practice Statement – Remote Automatic Identity Proofing – ***RAIP & S-RAIP***

Versione: 1.2
Data aggiornamento: 08/04/2026
Approvato da: Andrea Sassetti
Classificazione documento: Pubblico

Sassetti
Andrea
15.04.2026
07:00:14
UTC

VERSIONE	DATA	CHANGELOG
1.0	04/03/2025	**Prima emissione**
1.1	14/05/2025	**Par. 1.2 –** Integrazione riguardo la modalità di comunicazione degli aggiornamenti del documento verso i partner commerciali; **Par. 2.1, 2.2, 2.3, 5.4 –** Integrazione riguardo documenti di identità accettati e revisioni minori; **Cap. 3** – Inserimento nuovo capitolo relativo ai *Trusted Roles.*
1.2	08/04/2026	**Cap. 1 –** Aggiornamento dei servizi fiduciari in scope del documento, il livello target dell'identificazione e la referenza OID, integrazione delle definizioni. **Cap. 2 –** Aggiunta della nuova modalità supervisionata – *S-RAIP*; **Cap. 3 –** Inserimento nuovo *Trusted Role –Operatore Supervisore.* Ulteriori integrazioni minori a seguito dell'introduzione della modalità *S-RAIP*.

SOMMARIO

1 INTRODUZIONE E AMMINISTRAZIONE

1.1 Quadro generale

Aruba PEC S.p.A. (Aruba PEC), un Prestatore di Servizi Fiduciari (Trust Service Provider) accreditato presso l'AgID sino dal 2007, eroga servizi qualificati di certificazione di chiavi pubbliche, oltre a diversi altri servizi fiduciari (per maggiori informazioni si rimanda al sito web - https://www.pec.it).

L'identificazione degli utenti è il primo ed il principale step per l'erogazione verso gli utenti dei servizi fiduciari. Aruba PEC consente agli utenti di identificarsi in diverse modalità, così come descritto nei Manuali Operativi dei servizi di riferimento. Questo documento descrive una nuova componente, completamente automatizzata, che sfrutta tecniche di intelligenza artificiale (AI) per elaborare i dati biometrici necessari ed effettuare un'identificazione certa dell'utente. Il processo di riconoscimento senza operatore garantisce il massimo livello di fiducia e affidabilità assicurando un'esperienza *user friendly* ed adottando i migliori standard di sicurezza al fine prevenire qualsiasi tipo di frode o furto di identità nel processo di identificazione.

Lo scopo di questo documento è quello di descrivere la procedura e le regole generali del processo di identificazione implementato da Aruba PEC per consentire l'erogazione di servizi fiduciari e servizi fiduciari, anche qualificati tra cui i Servizi Elettronici di Recapito Certificato Qualificato – SERCQ – e i certificati qualificati di firma – Firma Digitale.

A tal fine, il processo di *Remote Identity Proofing* è implementato in conformità al Regolamento (UE) n. 910/2014 – eIDAS (versione vigente), alla norma ETSI EN 319 401 - *General Policy Requirements for Trust Service Providers* e allo standard norma ETSI TS 119 461 - *Policy and security requirements for trust service components providing identity proofing of trust service subject*, con particolare riferimento ai requisiti previsti per il livello *Extended Level of Identity Proofing* (**OID 0.4.0.19461.1.2**).

1.2 Amministrazione del Service Pratice Statement

1.2.1 Versione del SPS e organizzazione responsabile

La versione del presente Service Practice Statement (SPS) è indicate nella prima pagina del documento. Il documento è stato redatto, pubblicato e aggiornato da Aruba PEC S.p.A.

Il soggetto responsabile del presente manuale operativo all'interno di Aruba PEC è:

Andrea Sassetti
Direttore dei Servizi di Certificazione
Aruba PEC S.p.A.

Questo documento viene riesaminato e, se necessario, aggiornato con frequenza almeno annuale. Ogni nuova versione del documento è immediatamente pubblicata al sito web (https://www.pec.it/termini-condizioni.aspx) firmata in modalità PDF al fine di garantire l'origine e l'integrità a tutti gli utenti e le terze parti

interessate. È inoltre prevista una comunicazione verso i partner commerciali di Aruba PEC che utilizzano la *Remote Automatic Identity Proofing* per il rilascio dei servizi fiduciari qualificati.

1.2.2 Approving parties

Questo documento è approvato dalla Direzione dei servizi di CA, previa verifica da parte delle funzioni aziendali interessate e tenendo conto di quanto indicato al §6.1 della norma ETSI EN 319 401.

1.3 Definizioni

APCER	Attack Presentation Classification Error Rate. Per maggiori dettagli vedasi standard ETSI TS 119 461.
Richiedente	La persona fisica che richiede ad Aruba PEC S.p.A. un servizio fiduciario per il quale è prevista l'identificazione. Il Richiedente può rappresentare la persona giuridica.
Evidenza autorevole	Evidenza che attesta alcuni attributi del Richiedente gestita da una fonte autorevole.
Fonte autorevole	Qualsiasi fonte, indipendentemente dalla sua forma, su cui si possa fare affidamento per fornire dati, informazioni e/o prove accurate che possano essere utilizzate per dimostrare gli attributi del Richiedente.
Associazione al Richiedente	Parte del processo di riconoscimento che verifica che il richiedente sia la persona la fisica identificata dal documento presentato nel processo di riconoscimento e verifica inoltre che il documento d'identità presentato sia autentico e non clonato o copiato impedendo attacchi di spoofing (documenti stampati, immagini digitali ad alta risoluzione, chip clonati, ecc..).
BPCER	Bonafide Presentation Classification Error Rate. Per maggiori dettagli vedasi standard ETSI TS 119 461.
Documento di identità digitale	Documento di identità rilasciato in formato *machine-processable*, firmato digitalmente dall'Ente Emettitore ed in forma puramente digitale. Un documento di identità digitale può essere incluso in un documento di identità fisico, ad esempio in una carta di identità o passaporto.
Mezzi di identificazione elettronica	Un'unità materiale e/o immateriale contenente dati di identificazione personale e utilizzata per l'autenticazione per un servizio online.
Documento di identità	Documento fisico o digitale rilasciato da una fonte autorevole ed attestante l'identità del Richiedente.
Contesto di verifica dell'identità	Requisiti esterni che influenzano il processo di verifica dell'identità, dovuti dalle finalità della verifica dell'identità, dai relativi requisiti normativi e dalle conseguenti restrizioni sulla raccolta degli attributi e delle prove nonché sul processo di verifica dell'identità stesso.
Processo di verifica dell'identità	Processo di verifica dell'identità di un Richiedente mediante l'uso di evidenze che attestino gli attributi di identità richiesti.

Liveness detection	Tecnica di misura ed analisi di caratteristiche anatomiche biometriche e di reazioni volontarie o involontarie al fine di determinare se un campione biometrico è acquisito da un soggetto reale presente al momento del processo di identificazione.
Extended LoIP	Livello di Identity Proofing (LoIP) che raggiunge un elevato livello di sicurezza, basato sul soddisfacimento dei requisiti minimi del processo di identificazione. Tale livello è considerato adeguato per l'identificazione dei Richiedenti ai fini del rilascio dei certificati qualificati, delle attestazioni elettroniche qualificate di attributi ai sensi del Regolamento eIDAS. Per ulteriori informazioni si rimanda anche alla standard ETSI TS 119 461.
Documento di identità fisico	Documento di identità emesso in forma fisica ed in modalità *human-readable.*
Proof of access	Qualsiasi fonte, indipendentemente dalla sua forma, ritenuta affidabile per la raccolta di dati, informazioni e/o evidenze che possano essere usate in un processo di verifica dell'identità, a condizione che il Richiedente sia in grado di dimostrare l'accesso a tale fonte.
Sessione di identificazione	Singola sessione di identificazione in cui all'utente viene chiesto di eseguire alcune attività per fornire e convalidare la propria identità.
Componente di riconoscimento automatico senza operatore	Una specifica componente, implementata nelle applicazioni di Aruba PEC, che abilita il Richiedente all'identificazione attraverso tecniche di riconoscimento biometrico e intelligenza artificiale nonché tramite lettura NFC di un documento di identità in possesso del Richiedente.
Processo di verifica dell'identità da remoto - *Remote identity proofing*	Processo di verifica dell'identità del Richiedente effettuato in modalità remota, ovvero fisicamente lontano dal luogo fisico di verifica dell'identità. Il processo può essere eseguito in modalità completamente automatica (RAIP) o supervisionata (S-RAIP).
Trusted Register	Registro o database pubblico, o altra tipologia di fonte affidabile per la trasmissione degli attributi di identità nel contesto di verifica dell'identità del richiedente.
Validazione	Parte del processo di verifica dell'identità del Richiedente che determina se gli attributi sono convalidati dalle evidenze ottenute verificandone l'autenticità, la validità e l'affidabilità.

2 REMOTE AUTOMATIC IDENTITY PROOFING – RAIP & S-RAIP

Il processo di verifica dell'identità è un elemento fondamentale per la creazione di fiducia nei servizi digitali. Il processo di verifica dell'identità è un processo in cui un utente richiedente dimostra di essere

Il processo di verifica dell'identità può essere svolto anche a distanza, solitamente tramite una webcam o un dispositivo mobile, in cui gli utenti richiedenti mostrano il proprio volto ed esibiscono i documenti di identità in loro possesso come la carta d'identità o il passaporto, oppure tramite altri mezzi di identificazione elettronica.

Il processo di identificazione a distanza fornito da Aruba PEC è un processo di identificazione del Richiedente finalizzato all'erogazione di servizi fiduciari o servizi fiduciari qualificati. L'intero processo è orchestrato da applicazioni Aruba che integrano una specifica componente basata su intelligenza artificiale, al fine di consentire la raccolta dei dati del Richiedente necessari per un'identificazione sicura.

Il processo di identificazione a distanza può essere effettuato:

- in modalità completamente automatizzata – *denominata Remote Automatic Identity Proofing* - **RAIP**, oppure
- tramite una variante opzionale con supervisione umana – denominata *Supervised Remote Automatic Identity Proofing* - **S-RAIP**.

In quest'ultimo caso, la supervisione umana è limitata alle fasi di verifica dei dati e delle informazioni raccolte. Tali attività di supervisione sono svolte dagli *Operatori Supervisori*, formalmente nominati e periodicamente formati da Aruba PEC, in conformità alle policy e procedure interne. Tali operatori operano nel rispetto di specifiche procedure interne definite da Aruba PEC, garantendo coerenza, affidabilità e conformità ai requisiti normativi applicabili.

Il processo di identificazione senza operatore descritto in questo documento può essere riassunto in cinque passaggi:

1. **Inizializzazione del processo di riconoscimento senza operatore**
2. **Collezione degli attributi**
3. **Validazione degli attributi**
4. **Associazione al Richiedente**
5. **Emissione della "*proof*"**

Figura 1 - Fasi del processo di riconoscimento senza operatore

A seconda del contesto del riconoscimento, Aruba PEC può collezionare o validare autonomamente ulteriori attributi o evidenze dichiarate dal Richiedente attraverso interrogazioni verso *Trusted Registers*, come ad esempio i registri nazionali delle imprese o della popolazione residente, o attraverso procedure manuali. La *proof* generata al termine del processo contiene tutte le evidenze e gli attributi validati.

Nel caso della variante supervisionata S-RAIP, la supervisione umana è applicata esclusivamente durante le fasi di *Validazione degli attributi* e di *Associazione al Richiedente*, mentre tutte le altre fasi del processo rimangono completamente automatizzate.

Aruba PEC definisce e mantiene livelli obiettivo di prestazione per il False Acceptance Rate – *FAR* – e il False Rejection Rate – *FRR* – , in linea con le *best practices* di settore, per entrambe le modalità RAIP e S-RAIP. Il servizio è progettato ed erogato in modo da raggiungere valori target di FAR pari o migliori di 1/500.000 e di FRR pari 0.2. Aruba PEC definisce e mantiene inoltre livelli obiettivo di prestazione per le metriche PAD, inclusi APCER e BPCER, con riferimento agli scenari PAD dal Livello 1 al Livello 3 e al Livello 5 (injection). Il valore atteso di APCER è pari a 0% per tutti i suddetti livelli, mentre il BPCER rimane entro i valori target definiti.

Tutti tali parametri sono soggetti a monitoraggio continuo e a revisione periodica, al fine di garantire la costante conformità agli standard applicabili e l'allineamento con le *best practice* di settore.

Una descrizione più dettagliata del processo è fornita nei prossimi capitoli.

2.1 Inizializzazione del processo di riconoscimento senza operatore

Il processo di identificazione è inizializzato direttamente dal Richiedente attraverso la richiesta di un servizio fornito da Aruba PEC S.p.A., quale ad esempio un certificato di firma qualificata o sigillo qualificato conforme al Regolamento eIDAS.

La richiesta del servizio è formalizzata attraverso un *form online* dove vengono collezionati da Aruba PEC i dati dichiarati dal Richiedente utili a fine di rilascio e di successiva gestione del servizio fiduciario.

Nei casi in cui il Richiedente sia una persona fisica, viene raccolto un set minimo di dati obbligatori:

- Nome e Cognome del Richiedente[1];
- Identificativo univoco nazionale (ad esempio il Codice Fiscale o altro codice di tassazione nazionale TIN, il numero del documento di identità ecc..)
- Recapito di contatto telefonico ed indirizzo email;

Nel caso in cui il Richiedente sia una persona fisica che rappresenta una persona giuridica, in aggiunta alla lista precedente vengono richiesti anche i seguenti dati:

- Ragione sociale della persona giuridica
- Numero univoco nazionale della persona giuridica (CF o PIVA nel contesto italiano, o altro numero di registrazione nazionale)
- Paese di registrazione della persona giuridica
- Indirizzo della sede legale della persona giuridica.

A seconda della tipologia di servizio fiduciario richiesta dal Richiedente, Aruba PEC può richiedere ulteriori dati necessari per il rilascio del servizio.

Nei casi in cui il servizio fiduciario richiesto preveda l'identificazione del Richiedente, quest'ultimo potrà avvalersi di uno dei metodi messi a disposizione da Aruba PEC, inclusa la *Remote Automatic Identity Proofing*. Il Richiedente è quindi informato che la modalità di riconoscimento *Remote Automatic Identity Proofing* prevede l'utilizzo di documenti di identità conformi allo standard ICAO-9303[2], il possesso di uno smartphone abilitato alla lettura NFC e l'installazione di una specifica App fornita da Aruba PEC.

Prima di procedere con il riconoscimento, vengono mostrati al Richiedente: i Termini e Condizioni del processo di identificazione con *Remote Automatic Identity Proofing*, il presente documento e la specifica Informativa Privacy per il trattamento dei dati biometrici. Tutte le accettazioni dei suddetti documenti sono obbligatorie per procedere con il processo di identificazione con *RAIP* e sono opportunamente tracciate e storicizzate da Aruba PEC.

I documenti mostrati al Richiedente possono essere scaricati in locale e sono sempre disponibili online sul sito web di Aruba PEC https://www.pec.it/termini-condizioni.aspx e https://enterprise.aruba.it/home.aspx.

A seconda del tipo di servizio fiduciario richiesto dal Richiedente, Aruba PEC potrà applicare alcune restrizioni nel processo di registrazione e di identificazione del Richiedente.

[1] L'uso dello pseudonimo non è attualmente permesso per l'emissione di servizi fiduciari qualificati. I Richiedenti devono dichiarare la loro reale identità che deve essere verificata durante il processo di *identity proofing.* Ciò assicura la massima trasparenza tra l'identità del Richiedente ed il servizio fiduciario emesso.

[2] Al momento sono consentiti solo la Carta di Identità Elettronica (CIE) italiana ed il Passaporto Elettronico italiano.

2.2 Collezione di attributi

In questa fase il Richiedente può iniziare il processo tramite *Remote Automatic Identity Proofing*, sia nel caso di modalità automatizzata *RAIP*, sia supervisionata *S-RAIP*. La procedura è interamente guidata dall'App fornita da Aruba PEC ed installata sul dispositivo mobile in uso da parte del Richiedente[3].

L'Applicazione colleziona tutte le evidenze necessarie all'identificazione sicura del Richiedente inviandole presso i Data Center di Aruba tramite protocollo criptato TLS per i successivi step di analisi e validazione. Qualsiasi tipo di errore durante le fasi di raccolta dati o di caricamento comportano il fallimento dell'intero processo di riconoscimento. Dopo la trasmissione dei dati, l'App cancella dal dispositivo mobile tutti i dati relativi all'identificazione Richiedente.

Se il Richiedente è una persona fisica, il processo di identificazione tramite *Remote Automatic Identity Proofing* colleziona almeno il seguente set minimo di dati:

- Nome e cognome del Richiedente;
- Scansione del documento d'identità fisico utilizzato nella procedura;
- Foto del Richiedente estratta dal chip del documento digitale in possesso del Richiedente;
- Dati contenuti nel documento digitale in possesso del Richiedente (ad es. numero di documento, Codice Fiscale o TIN, validità, ente emettitore ecc..)
- Foto del volto del Richiedente (ovvero un *facescan* consistente in 60-180 frames frontali con risoluzione di almeno 640x480 e 50 frames per secondo) estratto dal processo di riconoscimento senza operatore;
- Metadati relativi alla sessione di identificazione (ID, data di inizio e fine del processo, alert, durata ecc..)
- Risultato della sessione di identificazione (success/fail).

Se il Richiedente è una persona fisica che rappresenta una persona giuridica, in aggiunta alle evidenze sopracitate per la persona fisica, Aruba PEC procede automaticamente all'interrogazione dei *Trust Registers* al fine di collezionare, come minimo, i seguenti dati:

- Ragione sociale della persona giuridica;
- Identificativo univoco della persona giuridica (CF o PIVA nel contesto italiano o altro codice univoco nazionale);
- Nome, Cognome e, quando possibile, identificativo univoco della persona fisica rappresentante la persona giuridica.

Per alcune tipologie di persona giuridica, le informazioni sopra citate non sono disponibili nei *Trust Registers* o nei registri nazionali, in tal caso Aruba PEC prevede una procedura manuale che presuppone l'upload da parte del Richiedente di specifiche tipologie di documenti e attestazioni che evidenzino il ruolo del Richiedente rispetto

[3] Le misure di sicurezza relative al dispositivo mobile sono descritte al Capitolo 4.

alla persona giuridica. A seconda del servizio richiesto dal Richiedente e dal contesto di riconoscimento, Aruba PEC mette a disposizione sul proprio sito web https://www.pec.it la lista dei documenti accettati per la verifica dei poteri di rappresentanza del Richiedente.

Tutte le comunicazioni verso i *Trust Registers* sono protette tramite l'utilizzo di protocolli di cifratura o autenticazioni.
Per maggiori dettagli si rimanda al Manuale Operativo del servizio fiduciario richiesto dal Richiedente.

2.3 Validazione degli attributi e delle evidenze

Il processo di identificazione tramite *Remote Automatic Identity Proofing* prevede due tipi di validazione delle evidenze raccolte:

- Validazione del documento fisico e digitale;
- Validazione della *liveness* e della corrispondenza del volto.

Per il primo punto, dopo l'acquisizione tramite App di copia per immagine di fronte/retro del documento fisico del Richiedente, Aruba PEC verifica che la tipologia di documento fisico sia tra quelle conformi allo standard ICAO 9303 MRTD (Passaporto elettronico italiano o CIE italiana). Questa limitazione è vincolante e assicura che i documenti presentati dal Richiedente siano autentici e pertanto non clonati o copiati in alcun modo. Questa verifica previene attacchi di *spoofing* come ad esempio documenti fotocopiati o stampati, stampe in alta qualità, chip clonati ecc.. Nel caso in cui il documento non sia conforme allo standard ICAO 9303 MRTD, il processo di riconoscimento RAIP termina immediatamente e l'intera sessione è marcata come *failed.*

In aggiunta, Aruba PEC compara i dati estrapolati dal chip del documento di identità digitale tramite lettura NFC rispetto a quelli dichiarati dal Richiedente in fase di registrazione dei dati, con particolare riferimento al Nome, Cognome e Codice Fiscale (o altro tipo di *Tax Identification Number*) o numero del documento di identità. Inoltre, è verificata da Aruba PEC la validità della firma elettronica dell'Ente Emettitore al fine di prevenire qualsiasi tipo di frode dovuta a contraffazione del documento d'identità digitale.

In caso siano presenti accenti o caratteri diacritici, per la validazione delle evidenze è applicata la translitterazione prevista dallo standard ICAO 9303 Part 3. Ogni difformità risultante nella procedura comporta la terminazione del processo di identificazione tramite RAIP.

Per quanto riguarda le verifiche di *liveness* e corrispondenza del volto, l'App Mobile esegue la verifica della *liveness* all'inizio della sessione di riconoscimento al fine di assicurarsi che il Richiedente sia una persona reale e non un tentativo di attacco tramite tecniche di *spoofing*.

Nel caso la *liveness detection* identifichi la sessione come una possibile minaccia o attacco, il processo di identificazione senza operatore termina immediatamente e la sessione è marcata come *failed.* In aggiunta, il processo di riconoscimento tramite *Remote Automatic Identity Proofing* verifica la corrispondenza tra la foto estratta dal documento digitale tramite lettura NFC con l'immagine stampata nel documento d'identità fisico e con il modello 3D del volto del Richiedente creato tramite le immagini estrapolate nella sessione di identificazione.

Nei casi in cui non venga raggiunta la soglia di affidabilità richiesta, la sessione di riconoscimento sarà terminata ed etichettata come *failed.*

Nel caso della modalità supervisionata S-RAIP, le attività di supervisione sono svolte da operatori formalmente nominati e periodicamente formati da Aruba PEC, di seguito denominati *Operatori Supervisori* che operano in conformità a rigorose procedure interne di supervisione. Tale supervisione è effettuata mediante l'utilizzo di strumenti informatici dedicati a supporto del confronto facciale, tra cui la possibilità di ingrandimento per la visualizzazione dei dettagli, e della verifica delle evidenze raccolte durante il processo di riconoscimento. Inoltre, qualora durante la fase di supervisione venga rilevata una qualsiasi incongruenza o incoerenza tra le evidenze raccolte, l'intera sessione di identificazione è respinta dall'Operatore Supervisore.

Nel caso il Richiedente sia una persona fisica che rappresenta una persona giuridica, le applicazioni di Aruba PEC, successivamente alla validazione del processo di identificazione della persona fisica tramite *Remote Automatic Identity Proofing*, verificano gli attributi e le evidenze collezionate dai *Trust Registers* rispetto ai dati della persona giuridica dichiarati in fase di registrazione. Tali evidenze possono essere oggetto delle attività di supervisione in accordo con le procedure di Aruba PEC. In caso di errori, Aruba PEC mette a disposizione una procedura manuale per l'upload da parte del Richiedente di specifici documenti e attestazioni comprovanti i poteri di rappresentanza del Richiedente rispetto alla persona giuridica; le evidenze raccolte sono in seguito verificate dagli operatori preposti di Aruba PEC. Nei casi in cui non possa essere confermato il ruolo del Richiedente rispetto alla persona giuridica, il processo di identificazione senza operatore sarà etichettato come *failed.*

L'intera fase di validazione degli attributi e delle evidenze è svolta nei Data Center di Aruba, in un ambiente protetto così come descritto nei successivi paragrafi; nessuna decisione del processo di riconoscimento tramite RAIP è implementata nell'App installata sul device utilizzato dal Richiedente così da ridurre i rischi dovuti a *injection* o codici malevoli.

2.4 Associazione al Richiedente

Dopo la fase di verifica, il processo di riconoscimento tramite *Remote Automatic Identity Proofing* associa al Richiedente tutte le evidenze collezionate e validate nelle precedenti fasi del processo tramite la creazione di una *proof of evidence* consistente in un file in formato .zip. Tutte le evidenze sono storicizzate nel file bundle secondo uno schema definito.

In particolare per la modalità RAIP, nel file *bundle .zip* sono presenti:

- Le foto del volto Richiedente effettuate durante le verifiche di *liveness detection* (facescan in alta e bassa risoluzione);
- La foto del volto del Richiedente estratta dal documento digitale in suo possesso;
- Le foto fronte/retro del documento fisico di identità del Richiedente;
- Un report complessivo della sessione di riconoscimento e dell'esito di ogni fase del processo di identificazione tramite RAIP;
- I dati estratti dal documento di identità digitale tramite lettura NFC (ID, validità, ente emettitore, ecc..)

- I metadati relativi alla sessione di riconoscimento (data e ora, durata, ID della sessione ecc..)

Nella variante supervisionata S-RAIP, in aggiunta ai precedenti elementi, il risultato delle attività di supervisione effettuate dagli Operatori Supervisori è opportunamente registrato e storicizzato nei sistemi informatici di Aruba PEC al fine di assicurare l'integrità, la completezza e la sicurezza dei dati e dei log raccolti.

Nei casi in cui il Richiedente sia una persona fisica che rappresenta una persona giuridica, Aruba PEC aggiungerà al file bundle .zip le ulteriori evidenze collezionate e validate nel processo di riconoscimento relative alla persona giuridica e ai poteri di rappresentanza della persona fisica.

2.5 Emissione della *proof of evidence*

La *proof of evidence* generata, unica e autoconsistente, è conservata a norma nei sistemi di Aruba PEC per il tempo richiesto dalla legge, a seconda della tipologia di servizio fornito al Richiedente. Alla fine del periodo di conservazione, tutte le evidenze collezionate durante il processo di identificazione saranno cancellate dai sistemi di Aruba.

Per maggiori dettagli riguardo le modalità di conservazione delle evidenze ottenute nel processo di identificazione si rimanda al par 5.5 del presente documento e ai Manuali Operativi dei servizi fiduciari forniti da Aruba PEC.

2.6 Cessazione

Aruba PEC S.p.A. può disabilitare o terminare la componente abilitante al processo di riconoscimento tramite *Remote Automatic Identity Proofing* ed il processo di riconoscimento RAIP e/o S-RAIP in qualsiasi momento e per qualsiasi ragione ritenuta opportuna. Prima dell'effettiva cessazione:

- almeno 90 giorni prima della cessazione pianificata del Servizio, sarà inviata una comunicazione all'Autorità di Vigilanza nazionale – AgID – e all'Ente di Conformità (CAB) e a tutte le terze parti interessate;
- sarà pubblicata sul sito di Aruba PEC una specifica informativa affinché l'informazione sia resa disponibile a tutti i clienti e le terze parti, compresi gli eventuali subappaltatori.
- la responsabilità della conservazione delle evidenze ottenute potrà essere trasferita ad altro soggetto affidabile affinché possa garantirne la conservazione per un periodo di tempo adeguato.

La cessazione della componente o del processo di riconoscimento tramite *Remote Automatic Identity Proofing* non implica in maniera automatica la cessazione degli altri servizi forniti da Aruba PEC, ad esempio servizi di certificazione quali firma o sigillo qualificati. In quest'ultimo caso sono forniti maggiori dettagli nel Manuale Operativo del servizio fiduciario di riferimento.

Resta inteso che Aruba PEC, in qualità di prestatore di servizio fiduciario verso il Richiedente, ha l'esclusiva responsabilità legale di definire il Piano di Cessazione del servizio.

3 RUOLI DI FIDUCIA

La struttura organizzativa è definita nel rispetto degli standard ETSI EN 319 401 ed in conformità alle norme vigenti. I ruoli di fiducia e le relative responsabilità sono assegnate formalmente dalla Direzione mediante lettere di incarico. I requisiti per il mantenimento dell'incarico vengono rivalutati con cadenza almeno annuale e a fronte di cambiamenti nella struttura organizzativa dell'azienda. Gli incaricati possono avvalersi, per lo svolgimento delle proprie attività, di addetti e collaboratori, nel rispetto delle disposizioni generali stabilite dall'azienda.

Le funzioni e le mansioni del personale sono distribuite in modo che una sola persona non sia in grado di eludere le misure di sicurezza a tutela dei sistemi di Aruba PEC; inoltre, i soggetti designati sono liberi da conflitti di interesse che potrebbero pregiudicare l'imparzialità delle attività loro assegnate.

Aruba PEC ha definito ed assegnato formalmente i seguenti ruoli di fiducia ("*trusted roles"*) all'interno del servizio di *Remote Automatic Identity Proofing* regolato da questo documento:

- **Responsabile di Sicurezza:** responsabile per l'implementazione e la gestione delle procedure di sicurezza. Questa figura corrisponde al "Responsabile per la Sicurezza" di cui alle norme vigenti;
- **Security Officers**: responsabili nel supportare il Responsabile della Sicurezza per l'implementazione e la gestione delle procedure di sicurezza;
- **Amministratore di Sistema** (*System Administrator*): responsabile dell'installazione, configurazione e manutenzione dei sistemi informatici di Aruba PEC relativi al servizio di *Remote Automatic Identity Proofing*;
- **Operatore di Sistema** (*System Operator*): responsabile del funzionamento quotidiano dei sistemi di relativi al servizio di *Remote Automatic Identity Proofing*;
- **System Auditor**: responsabile della verifica dei log e degli archivi relativi al servizio di *Remote Automatic Identity Proofing*;
- **Identity Verification Officer**: responsabile di assicurare che i processi di verifica dell'identità eseguiti tramite il processo di *Remote Automatic Identity Proofing* siano conformi a quelli previsti;
- **Operatore Supervisore**: responsabile delle verifiche di leggibilità, completezza, validità, autenticità, integrità e correttezza della documentazione e delle evidenze raccolte durante il processo di riconoscimento.

Alcune persone possono ricoprire ruoli multipli purché ciò non pregiudichi la sicurezza del Servizio e non sia vietato dalle normative e dagli standard applicabili.

4 MISURE DI SICUREZZA

Aruba ha adottato un sistema di gestione della sicurezza delle informazioni conforme e certificato allo standard ISO/IEC 27001.

Lo standard ISO 270001 assicura la sicurezza delle informazioni tramite l'attuazione di specifiche procedure, norme comportamentali e corsi di formazione.

Lo standard è basato sui seguenti principi:

- ***Sicurezza dell'informazione:*** preserva la confidenzialità, l'integrità e assicura la disponibilità dell'informazione;
- ***Confidenzialità:*** assicura che l'informazione è resa accessibile solo agli utenti autorizzati;
- ***Integrità:*** salvaguardia l'affidabilità e la completezza dell'informazione e preserva le modalità con cui sono processate;
- ***Risk Assessment e Risk Analysis***: identifica le minacce e I loro possibili impatti sul sistema, analizza le vulnerabilità delle informazioni e dei processi stimando la probabilità che un evento possa manifestarsi;
- ***Risk Management:*** identifica, controlla, mitiga ed elimina i rischi di sicurezza che possono avere impatti sul sistema.

Aruba PEC dispone di tutte le garanzie di sicurezza compatibili con il tipo di servizio erogato, sia a livello fisico che informatico.

Maggiori dettagli sulle misure di sicurezza sono riportati nel Policy Statement dei servizi forniti da Aruba PEC.

4.1 Scenari di rischio e misure di sicurezza adottate

Vengono illustrati nel seguito i principali scenari di rischio specifici per la modalità di riconoscimento tramite *Remote Automatic Identity Proofing,* in entrambe le modalità RAIP & S-RAIP, e le contromisure di sicurezza adottate da Aruba PEC.

SCENARIO DI RISCHIO	DESCRIZIONE	PRINCIPALI CONTROMISURE ADOTTATE
Consegna dell'identità digitale ad un utente non legittimo	Chiamate APP-API illegittime.	Autenticazione tramite credenziali del cliente. Univocità della sessione di riconoscimento tramite GUID con validità di 24ore. Durata massima della sessione di riconoscimento inizializzata dall'utente pari a 10 minuti.
	Manomissione del dispositivo mobile (furto del dispositivo hardware, intercettamento delle comunicazioni, reverse engineering del codice applicativo, attacchi di tipo injection o substitution nel codice etc.…)	Rilevamento del rooting/jailbreaking del dispositivo. Fingerprinting dei componenti essenziali del dispositivo. Rilevamento della presenza del blocco del dispositivo. Rilevamento di tecniche di hooking. Rilevamento dei debuggers.

SCENARIO DI RISCHIO	DESCRIZIONE	PRINCIPALI CONTROMISURE ADOTTATE
	Presenza di artefattati volti ad aggirare il sistema (stampe, sostituzioni video, maschere 3D, deepfake etc..)	Utilizzo di tecniche *Biometric Presentation Attack Detection (PAD)*.
	Documento di identità falso, clonato, rubato o modificato.	Verifica del certificato e dell'eventuale revoca. Lettura del chip di autenticazione (tramite NFC) per verificare l'autenticità del documento. Utilizzo dei soli documenti di identità elettronici conformi allo standard ICAO-9303 MRTD.
	Titolare non corrispondente al documento	Confronto tra l'immagine del documento e il video acquisito tramite APP. Il flusso di riconoscimento viene bloccato in caso di verifica negativa.
Furto o manomissione dei dati di riconoscimento e identificazione del Richiedente.	Reindirizzamento illegittimo delle chiamate API	Adozione del protocollo TLS con tecniche di certificate pinning.
	Furto o manomissione dei dati in transito.	Adozione del protocollo TLS compreso la verifica dei certificati e la crittografia dei dati inviati dall'App. Chiavi di crittografia non memorizzate sul device. Rotazione delle chiavi di crittografia ogni 90 giorni.
	Furto o manomissione dei dati memorizzati.	Nessun salvataggio di dati sul device. Memorizzazione dei dati non criptati sui sistemi centrali limitata al tempo necessario per le operazioni di riconoscimento, con cancellazione al termine del processo. Dati e documenti sono storicizzati in maniera criptata.
Compromissione della supply-chain	Mancata adozione delle best practices.	Selezione di fornitori con livello di sicurezza e certificazione adeguate (OWASP ASVS Level 2; ISO/IEC 30107-3 Level 1/2). Contrattualizzazione di specifici requisiti di sicurezza da rispettare. Esecuzione di test VA/PT.
	Introduzione di errori negli aggiornamenti software	Test di non regressione e VA/PT.

5 TERMINI GENERALI DI UTILIZZO

5.1 Introduzione

I termini e le condizioni nel seguito descritti si applicano tra l'utente richiedente ("Richiedente") e Aruba PEC, nei casi in cui il Richiedente scelga di procedere con il riconoscimento tramite "*Remote Automatic Identity Proofing*" (di seguito "Servizio"), in entrambe le modalità RAIP ed S-RAIP.

Queste condizioni regolamentano l'accesso e l'uso del Servizio fornito da Aruba PEC al Richiedente e possono essere aggiornate nel tempo. Qualsiasi cambiamento delle condizioni comporterà una nuova versione del documento e sarà esplicitata la natura delle modifiche.

5.2 Disposizioni generali

Il riconoscimento tramite *Remote Automatic Identity Proofing* è il Servizio adottato per l'emissione dei servizi fiduciari forniti da Aruba PEC previa verifica certa dell'identità del Richiedente. Il Richiedente accetta che i servizi forniti da Aruba PEC che integrano la suddetta modalità di riconoscimento siano regolati separatamente dalle specifiche condizioni di fornitura del Servizio.

5.3 Obblighi del Richiedente

Il Richiedente deve fornire le informazioni riportate ai paragrafi precedenti.

In aggiunta il Richiedente accetta e conferma che:

- L'identità verificata attraverso le informazioni dichiarate e i documenti presentanti corrispondano all'identità dichiarata nell'utilizzo dei servizi forniti da Aruba PEC;
- Tutte le informazioni fornite sono complete ed accurate;
- Il Richiedente si impegna a rispettare tutte le leggi, i regolamenti e le norme locali, nazionali e internazionali applicabili.

È fatto divieto al Richiedente di:

- Utilizzare il Servizio a scopo di frode, a scopo commerciale o per finalità diverse da quelle del rilascio del servizio fiduciario richiesto;
- Dichiarare identità non in proprio possesso o per le quali non si è autorizzati all'utilizzo per conto terzi;
- Dichiarare associazioni fasulle con altre persone o organizzazioni;
- Modificare, alterare o interferire in qualsiasi forma i contenuti e le informazioni;
- Utilizzare strumenti automatizzati, ad esempio bot o strumenti di *scraping*, per accedere, raccogliere o interagire con Aruba PEC;
- Eludere qualsiasi misura volta a prevenire le violazioni dei presenti termini e condizioni.

5.4 Requisiti di accesso e utilizzo

Il Richiedente deve essere in possesso di un dispositivo mobile (smartphone) equipaggiato con una fotocamera e videocamera correttamente funzionanti, alla lettura NFC ed aver installato l'App mobile fornita da Aruba PEC. Il Richiedente deve essere inoltre in possesso di un documento conforme allo standard ICAO 9303 MRTD, quali Carta di Identità Elettronica italiana o Passaporto Elettronico italiano ed essere collegato alla rete internet.

Al fine di garantire il massimo livello di performance e di sicurezza durante la sessione di riconoscimento tramite *Remote Automatic Identity Proofing*:

- Le immagini e i video acquisiti devono mostrare un'immagine chiara e completa sia del volto del Richiedente che dei documenti di identità richiesti. Le immagini devono essere ben nitide e correttamente illuminate, ad alto contrasto e prive di sfocature o ostruzioni;
- È raccomandato l'utilizzo dell'ultima versione dell'App fornita da Aruba PEC;
- Sul dispositivo devono essere installati tutti gli aggiornamenti di sicurezza previsti.

5.5 Tipologia di dati archiviati e periodo di conservazione

Aruba PEC memorizza le seguenti tipologie di dati: le fasi di esecuzione di ciascuna sessione di identificazione, inclusa la data/ora di inizio e fine della sessione, il risultato della sessione e il report della sessione di riconoscimento tramite *Remote Automatic Identity Proofing.*

Per ogni azione, Aruba PEC memorizza le relative evidenze:

- scansioni del volto: immagini di verifica (*audit photo*) in alta e bassa qualità;
- scansione del documento: foto fronte/retro del documento + immagine nfc + dati nfc + dati utente estrapolati tipo di dispositivo + modello di dispositivo + ip del dispositivo; - data di creazione della pratica
- data e ora di inizio della sessione di riconoscimento (ovvero quando il Richiedente inizia a scansionare con nfc);
- data e ora della fine della sessione di riconoscimento;
- l'eventuale risultato delle attività di supervisione dei riconoscimenti;
- consensi privacy.

Il periodo di conservazione dei dati può variare a seconda della tipologia del servizio fiduciario richiesto. Il periodo massimo di conservazione dei dati è previsto a 20 anni. Il periodo esatto di conservazione dei dati è descritto e riportato nella documentazione contrattuale dello specifico servizio, a cui si rimanda.

5.6 Limitazione di responsabilità

Aruba PEC non sarà responsabile di eventuali perdite o danni derivanti dall'utilizzo del sistema di riconoscimento tramite *Remote Automatic Identity Proofing*, inclusi eventuali problemi legati alla sicurezza del dispositivo, alle informazioni errate e/o ad accessi non autorizzati.

Eventuali ed ulteriori limitazioni di responsabilità relative all'uso del sistema di verifica dell'identità a distanza sono disciplinate dalle specifiche condizioni generali di contratto in cui è integrato.

Aruba PEC inoltre non sarà ritenuta responsabile il mancato o ritardato adempimento dei propri obblighi previsti ai sensi delle presenti condizioni causato da atti o eventi al di fuori del ragionevole controllo di Aruba PEC, tra cui ad esempio l'indisponibilità del Servizio dovuta a errori dell'utente, l'indisponibilità di piattaforme di terzi, errori causati da fornitori di API (o simili), problemi di rete o interruzioni.

5.7 Assessment of Remote Identity Proofing

Il processo di riconoscimento tramite *Remote Automatic Identity Proofing* è basato su quanto definito dal Regolamento Europeo eIDAS. La normativa e gli standard applicabili al servizio sono riportati di seguito:

- ETSI TS 119 461 - Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service components providing identity proofing of trust service subjects;
- ETSI EN 319 401 - General Policy Requirements for Trust Service Providers;
- ETSI EN 319 411 1/2 - Policy and security requirements for Trust Service Providers issuing certificates;
- Standard internazionali ISO/IEC, ad esempio ISO 27001;
- Regolamento (EU) 2016/679 – GDPR.

5.8 Contatti

Per tutte le informazioni che si ritenessero necessarie riguardo alle presenti condizioni o all'utilizzo del servizio di riconoscimento senza operatore, sono rese disponibili le seguenti modalità di contatto:

- Call center accessibile attraverso i canali del sito https://assistenza.aruba.it
- Invio di comunicazione all'indirizzo CPS-requests@ca.arubapec.it

5.9 Legge Applicabile

Le presenti Condizioni sono regolate ed interpretate in conformità alle leggi italiane e tutte le controversie sono deferite alla competenza del foro di Arezzo, salvo quanto diversamente disciplinato nelle specifiche condizioni di fornitura in cui il servizio è integrato.

5.10 Disposizioni finali

Aruba PEC può trasferire i propri diritti e i propri obblighi ai sensi dei presenti termini e condizioni a un'altra organizzazione, ciò non influirà sui diritti dell'utente o sui nostri obblighi ai sensi dei presenti termini e condizioni.

Il Richiedente può trasferire i propri diritti o obblighi ai sensi dei presenti termini e condizioni a un'altra persona solo previo accordo scritto. Una persona che non è parte di questi termini e condizioni non ha il diritto di far valere alcuno di questi termini e condizioni.

Se non insistiamo affinché l'utente esegua uno qualsiasi degli obblighi previsti dai presenti termini e condizioni, o se non facciamo valere i nostri diritti nei confronti del Richiedente, o se ritardiamo nel farlo, ciò non significa che abbiamo rinunciato ai nostri diritti nei confronti dell'utente e non significa che l'utente non sia tenuto a rispettare tali obblighi. Se rinunciamo a un'inadempienza da parte vostra, lo faremo solo per iscritto e ciò non significa che rinunceremo automaticamente a qualsiasi futura inadempienza da parte vostra.

Ciascuna delle condizioni contenute nei presenti termini e condizioni opera separatamente. Se un tribunale o un'autorità competente decidesse che una qualsiasi delle condizioni è illegale o inapplicabile, le altre condizioni rimarranno pienamente valide ed efficaci.

5.11 Clausole di rinvio

Per tutto quanto non disciplinato dai presenti termini e condizioni, si rimanda ai termini e alle condizioni specifiche di fornitura dei servizi in cui il Servizio è integrato.