

Aruba PEC S.p.A.

Descrizione Piattaforma IDS e processi di Identity Proofing

Versione: 1.0

Data aggiornamento: 29.09.2026

Classificazione documento: Pubblico

VERSIONE	DATA	CHANGELOG
1.0	29/09/2026	Prima emissione

SOMMARIO

1	INTRODUZIONE E AMMINISTRAZIONE	3
1.1	Quadro generale	3
1.2	Amministrazione del documento.....	3
1.2.1	Versione del documento e organizzazione responsabile.....	3
1.2.2	Soggetti responsabili dell'approvazione	4
1.3	Definizioni.....	4
2	PIATTAFORMA IDS.....	6
2.1	Piattaforma IDS - Introduzione	6
2.1.1	Attori e responsabilità operative	6
2.1.2	Architettura e configurazione.....	6
2.1.3	Integrazione applicativa, API e interfacce.....	7
2.1.4	Interfacce e strumenti.....	7
2.1.5	Processo generale di identificazione	7
2.1.6	Evidenze, conservazione e retention.....	7
2.1.7	Documenti di identità accettati e attributi raccolti.....	8
2.1.8	Trattamento dati biometrici e utilizzo di AI	8
3	DESCRIZIONE DELLE MODALITÀ DI IDENTIFICAZIONE	8
3.1	Modalità di identificazione con LoA High – LoIP Extended	8
3.1.1	DVO+ - identificazione video assistita di tipo ibrido	8
3.1.2	RAIP e S-RAIP - identificazione non assistita di tipo automatico e ibrido.....	10
3.1.3	Identificazione mediante CieID.....	15
3.1.4	Identificazione mediante TS-CNS	17
3.1.5	Identificazione mediante utilizzo di firma elettronica qualificata.....	19
3.2	Altri metodi di identificazione supportati.....	21
3.2.1	DVO - identificazione video assistita	21
3.2.2	Identificazione mediante credenziali SPID di livello 2.....	23
4	MISURE DI SICUREZZA	26
4.1	Principali Standard di Riferimento	26
4.1.1	ISO/IEC 27001 e ISO/IEC 27002	26
4.1.2	ISO 27005.....	26
4.2	Framework adottato per la gestione della Sicurezza delle Informazioni	27
4.2.1	GOVERN.....	28
4.2.2	IDENTIFY.....	28
4.2.3	PROTECT.....	28
4.2.4	DETECT.....	28
4.2.5	RESPOND.....	28
4.2.6	RECOVER.....	28
	APPENDICE 1 – TECNOLOGIE IN OUTSOURCING	29

1 INTRODUZIONE E AMMINISTRAZIONE

1.1 Quadro generale

Aruba PEC S.p.A. (Aruba PEC) mette a disposizione dei propri Clienti la piattaforma IDS e le relative componenti tecnologiche per lo svolgimento dei processi di identificazione descritti nel presente documento.

I processi di verifica dell'identità gestiti mediante IDS sono utilizzati dal Cliente per le proprie finalità, in funzione della modalità di identificazione utilizzata e della normativa applicabile, anche per il rilascio di servizi fiduciari del Cliente, l'attivazione di servizi digitali e ulteriori finalità previste dalla normativa nazionale, europea o di settore.

Il presente documento descrive la piattaforma IDS e i processi di identificazione da essa supportati, di seguito denominati anche “**Servizi di Identity Proofing**”, messi a disposizione del Cliente in modalità stand-alone. In tale ambito Aruba PEC opera esclusivamente quale fornitore della soluzione tecnologica utilizzata dal Cliente per le proprie finalità di identificazione.

I riferimenti al Regolamento (UE) n. 910/2014 – eIDAS (versione vigente) ed allo Standard ETSI TS 119 461 v. 2.1.1 - *Policy and security requirements for trust service components providing identity proofing of trust service subject* riguardano le caratteristiche dei processi descritti e il relativo contesto di utilizzo da parte del Cliente.

1.2 Amministrazione del documento

1.2.1 Versione del documento e organizzazione responsabile

La versione del presente documento è indicata nella prima pagina. Il documento è stato redatto, pubblicato e aggiornato da Aruba PEC S.p.A.

I dati dell'organizzazione sono i seguenti:

Dato	Descrizione
Organizzazione	Aruba PEC S.p.A.
Sede legale	Via San Clemente n. 53 – 24036 Ponte San Pietro (BG)
Partita IVA	01879020517
Numero REA	BG - 445886
Sito web	www.aruba.it

1.2.2 Soggetti responsabili dell'approvazione

Prima della sua adozione, il presente documento viene esaminato e validato internamente dalle unità aziendali preposte alla conformità normativa e ai profili giuridici, nonché dalle strutture incaricate della gestione operativa del servizio.

1.3 Definizioni

Termine	Definizione
APCER	<i>Attack Presentation Classification Error Rate</i> . Per maggiori dettagli vedasi standard ETSI TS 119 461.
Associazione al Richiedente	Parte del processo di riconoscimento che verifica che il Richiedente sia la persona 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	<i>Bonafide Presentation Classification Error Rate</i> . Per maggiori dettagli vedasi standard ETSI TS 119 461.
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.
Cliente	È la persona giuridica cliente di Aruba PEC che si avvale della piattaforma IDS e dei processi di identificazione per le proprie finalità.
Contesto di verifica dell'identità	Requisiti esterni che influenzano il processo di verifica dell'identità, dovuti alle finalità della verifica dell'identità, ai relativi requisiti normativi e alle conseguenti restrizioni sulla raccolta degli attributi e delle prove, nonché sul processo di verifica dell'identità stesso.
Documento di identità	Documento fisico o digitale rilasciato da una fonte autorevole e attestante l'identità del Richiedente.
Documento di identità digitale	Documento di identità rilasciato in formato <i>machine-processable</i> , firmato digitalmente dall'Ente Emittitore e 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 in un passaporto.
Documento di identità fisico	Documento di identità emesso in forma fisica e in modalità <i>human-readable</i> .
DVO	Acronimo, stante per "De Visu Online", di specifico processo di identificazione con operatore connesso da remoto con il Richiedente.
Evidenza autorevole	Evidenza che attesta alcuni attributi del Richiedente, gestita da una fonte autorevole.
Extended LoIP	<i>Level of Identity Proofing (LoIP)</i> che raggiunge un elevato livello di affidabilità, basato sul soddisfacimento dei requisiti minimi di buona pratica per il processo di

	identificazione. Tale livello è considerato idoneo per l'identificazione ai fini del rilascio di certificati qualificati e attestazioni elettroniche qualificate di attributi ai sensi del Regolamento eIDAS. Per ulteriori informazioni si rimanda anche alla norma ETSI TS 119 461.
Fonte autorevole	Qualsiasi fonte, indipendentemente dalla sua forma, sulla quale si possa fare affidamento per fornire dati, informazioni e/o prove accurate che possano essere utilizzate per dimostrare gli attributi del Richiedente.
IDS	Acronimo, stante per "IDentification Service", piattaforma utilizzata per gestire ed orchestrare i processi di identity proofing di cui al presente documento.
Liveness detection	Tecnica di misura e 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.
Mezzi di identificazione elettronica	Un'unità materiale e/o immateriale contenente dati di identificazione personale e utilizzata per l'autenticazione per un servizio online.
NFC	Near Field Communication - tecnologia di comunicazione wireless a corto raggio che consente lo scambio di dati tra dispositivi molto vicini.
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.
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.
Richiedente	La persona fisica sottoposta a identificazione per le finalità del Cliente mediante i mezzi messi a disposizione da Aruba PEC. Il Richiedente può rappresentare una persona giuridica.
Sessione di identificazione	Singola sessione di identificazione in cui al Richiedente viene chiesto di eseguire alcune attività per fornire e convalidare la propria identità.
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 PIATTAFORMA IDS

2.1 Piattaforma IDS - Introduzione

IDS - Identification Service è una piattaforma SaaS multi-tenant progettata per l'integrazione di processi di identificazione di persone fisiche in flussi applicativi. L'integrazione avviene principalmente mediante API esposte attraverso una API Management Platform; l'esperienza del Richiedente finale può essere erogata tramite front-end whitelabel IDS oppure, per i metodi compatibili, tramite un front-end realizzato dal Cliente e integrato via API.

I processi gestiti da IDS sono differenziati in base alla modalità di interazione con il Richiedente cui il Cliente ha un rapporto diretto, al grado di automazione, alla natura dell'evidenza autorevole impiegata e alla presenza o meno di una supervisione umana. La piattaforma orchestra il ciclo di vita della pratica e integra servizi propri e provider esterni, mantenendo il collegamento tra dati iniziali, esecuzione del metodo, controlli di coerenza, esito ed evidenze.

2.1.1 Attori e responsabilità operative

Cliente / System Integrator	Integra IDS nei propri sistemi, crea la pratica, indica dati e metodi ammessi, riceve notifiche ed esito e recupera le evidenze secondo la configurazione concordata.
Richiedente	Persona fisica sottoposta al processo di identificazione mediante uno dei metodi abilitati.
Operatori	Gestiscono piattaforma e tenant; eseguono i DVO e, ove configurato, la verifica manuale delle pratiche e delle evidenze.
Piattaforma IDS	Orchestra avvio, esecuzione, stato, controlli di coerenza, generazione/associazione delle evidenze e notifiche.
Provider esterni	Erogano i componenti o i metodi di identificazione integrati da IDS.

2.1.2 Architettura e configurazione

La piattaforma è configurata secondo un modello multi-tenant. Per ciascun tenant possono essere definiti elementi grafici, URL dedicati, metodi disponibili e fasi opzionali dei workflow.

La retention può essere differenziata per metodo, con criteri più restrittivi per i processi che trattano dati biometrici.

Le caratteristiche principali della piattaforma possono essere riassunte come segue:

- personalizzazione di loghi, colori, etichette e testi dell'interfaccia;
- abilitazione selettiva dei metodi di identificazione;
- configurazione degli step opzionali e delle tempistiche operative;
- regole di retention differenziate a livello di tenant e metodo.

2.1.3 Integrazione applicativa, API e interfacce

La creazione della pratica avviene tramite API, le quali consentono la creazione, la consultazione dello stato e il recupero delle evidenze, l'annullamento e, nei limiti consentiti dallo stato, l'aggiornamento della pratica.

Gli eventi sono notificati al Cliente/System Integrator tramite webhook verso endpoint configurati. L'API Management Platform rende disponibili catalogo, documentazione tecnica, sottoscrizioni, gestione applicazioni e credenziali, test e analytics tecniche.

Per definite classi di processo (attualmente per RAIP e S-RAIP, v. capitolo successivo) è disponibile un SDK web e mobile (iOS e Android) che consente al Cliente di realizzare l'interfaccia mantenendo la piattaforma IDS quale backend di orchestrazione. Il flusso web non consente l'uso della funzionalità NFC.

2.1.4 Interfacce e strumenti

Interfaccia	Attori	Funzione principale
Developer Portal	Cliente / System Integrator	Catalogo e documentazione API, sottoscrizioni, applicazioni/credenziali e analytics.
Front-end IDS	Richiedente	Scelta del metodo ed esecuzione del riconoscimento.
Backoffice IDS	Operatori	Tenant, workflow, tempi e monitoraggio pratiche.
Pannello di validazione	Operatori	Esecuzione processi di visu, DVO, verifica S-RAIP e decisione sulle pratiche.

2.1.5 Processo generale di identificazione

Il ciclo ordinario, ricorrente per tutti i metodi di identificazione attualmente esistenti, è ricondotto alle fasi seguenti, coerenti nell'impostazione con il modello ETSI TS 119-461:

- **Avvio del processo di identificazione:** il Richiedente riceve le informazioni preliminari sul processo di identificazione che deve affrontare.
- **Raccolta dei dati:** il Richiedente fornisce gli attributi e le evidenze richiesti per l'identificazione.
- **Validazione:** vengono eseguiti i controlli previsti su dati, documenti, certificati, evidenze elettroniche o biometriche.
- **Associazione dei dati al Richiedente:** l'evidenza (o evidenze) validata viene collegata al Richiedente, mediante gli strumenti previsti per ciascun metodo di identificazione (v. capitolo successivo).
- **Rilascio del risultato di identificazione:** viene prodotto l'esito di avvenuta identificazione, corredato delle ulteriori evidenze ottenute durante il processo.

IDS può eseguire inoltre controlli di coerenza tra i dati ricevuti in sede di registrazione dal Richiedente e quelli ottenuti dallo specifico metodo.

2.1.6 Evidenze, conservazione e retention

Le evidenze generate durante il processo di identificazione vengono gestite da IDS secondo le modalità previste dal processo e dalla configurazione del servizio concordata con il Cliente.

2.1.7 Documenti di identità accettati e attributi raccolti

I documenti di identità accettati e gli attributi oggetto di raccolta sono definiti in relazione alle caratteristiche dello specifico processo, alle relative finalità proprie del Cliente e ai requisiti tecnici delle modalità di identificazione utilizzate.

2.1.8 Trattamento dati biometrici e utilizzo di AI

Alcune tipologie di processo di identificazione descritte nel prossimo capitolo (DVO+, RAIP, S-RAIP) si avvalgono di sistemi di intelligenza artificiale, senza che i dati personali dei Richiedenti siano utilizzati per l'addestramento dei relativi modelli.

I dati biometrici sono trattati esclusivamente per le verifiche di identificazione e cancellati una volta completato il loro utilizzo, senza essere ulteriormente conservati.

3 DESCRIZIONE DELLE MODALITÀ DI IDENTIFICAZIONE

I processi descritti nei prossimi paragrafi sono classificati in funzione del livello di affidabilità del processo di identificazione, del livello di garanzia associato alle evidenze o ai mezzi di identificazione utilizzati e del contesto normativo applicabile.

I processi descritti sono utilizzati per le finalità del Cliente, che possono comprendere l'emissione di propri servizi fiduciari o finalità diverse da quelle di certificazione.

Ai fini dell'erogazione di servizi fiduciari del Cliente, qualificati e non qualificati, le modalità di identificazione illustrate nel presente documento possono essere utilizzate nel rispetto della normativa applicabile e in funzione del livello di garanzia o di sicurezza previsto per lo specifico servizio.

Per livello Baseline/Substantial si intende un grado significativo di affidabilità dell'identificazione; il livello Extended/High prevede requisiti e controlli più rigorosi, volti a garantire il più elevato grado di affidabilità e protezione da frodi d'identità, secondo i rispettivi quadri di riferimento eIDAS ed ETSI 119-461.

3.1 Modalità di identificazione con LoA High – LoIP Extended

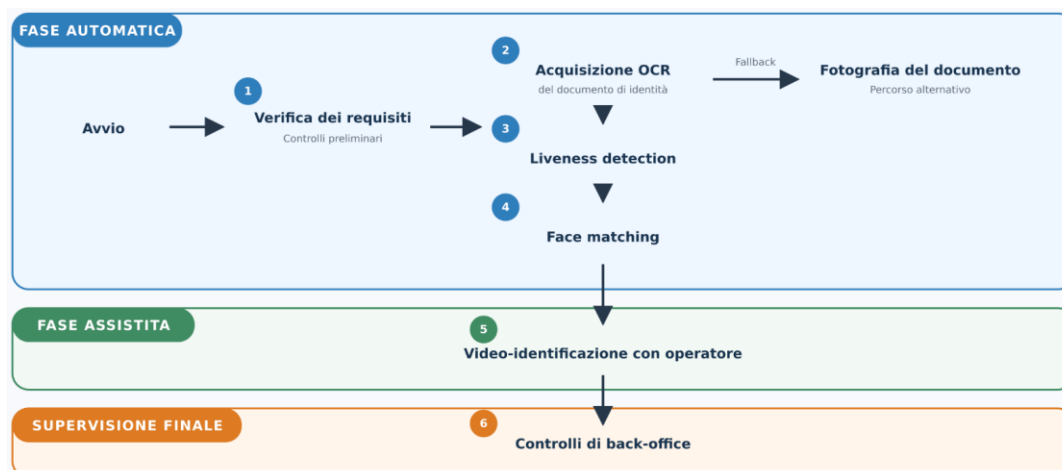
3.1.1 DVO+ - identificazione video assistita di tipo ibrido

DVO+ è un processo di identificazione remota “de visu” basato su una sessione video in tempo reale con operatore, preceduta da una fase preliminare non supervisionata nella quale i controlli automatici sull'evidenza raccolta supportano l'operatore, rafforzando il processo.

Modalità	Remote attended con pre-fase automatizzata e controlli biometrici (ETSI 119-461, C.3.4)
-----------------	---

Livello dichiarato	Extended (High)
Controlli indicati	OCR, validazione documento, liveness detection, controlli di antispoofing, face matching, operatore; backoffice opzionale

Il flusso end-to-end può essere riassunto come da diagramma di seguito riportato:



Il Richiedente è guidato attraverso un processo che fornisce un'esperienza di identificazione assistita da un operatore, composta dalle seguenti fasi:

Inizializzazione del processo

Verifica preliminare dei requisiti: verifica dei requisiti tecnici del dispositivo e della connessione Internet, al fine di assicurare lo svolgimento di una sessione di identificazione che garantisca un'acquisizione delle evidenze di elevata qualità e adeguati livelli di sicurezza informatica.

Raccolta dei dati e dell'evidenza; Pre-convalida del documento di identità

Acquisizione OCR del documento di identità:

- Il Richiedente acquisisce le immagini del documento d'identità mediante l'interfaccia guidata resa disponibile da Aruba.
- La componente OCR estrae automaticamente i dati presenti nella zona di ispezione visiva (VIZ) e nella zona a lettura ottica (MRZ), ove disponibile.
- In funzione del documento, vengono acquisiti dati anagrafici, codice fiscale, nazionalità, residenza, estremi, validità e luogo o Paese di emissione. Per il contesto italiano, se il Richiedente utilizza la propria carta di identità elettronica, la raccolta della tessera sanitaria non è necessaria.
- Il sistema effettua una pre-convalida dei dati e dell'evidenza raccolti, verificandone l'autenticità e la validità.

Collegamento preliminare dell'evidenza al Richiedente

Liveness detection: il sistema verifica che l'identificazione sia effettuata da una persona reale e non costituisca un tentativo di alterazione o falsificazione mediante tecniche quali photo morphing, deepfake, utilizzo di maschere o strumenti analoghi.

- Il servizio assiste il Soggetto nell'acquisizione dell'immagine del volto, fornendo indicazioni in tempo reale per assicurare il corretto posizionamento del viso e adeguate condizioni di illuminazione e qualità dell'immagine.
- Durante l'acquisizione, il sistema rileva e analizza il volto in tempo reale ai fini dell'esecuzione dei successivi controlli biometrici.

Face matching: il sistema effettua un confronto automatico tra il volto del richiedente e quello raffigurato nel documento di identità, a supporto dell'operatore nelle successive fasi del processo.

Convalida finale dei dati e dell'evidenza; Collegamento finale dell'evidenza al Richiedente

Sessione video con un operatore video: l'operatore conduce la video-identificazione attenendosi a un'apposita procedura e ad una checklist interna.

Controlli di back-office (eventuali, a seconda della configurazione del processo): un operatore riesamina tutte le evidenze raccolte e il processo di identificazione nel suo complesso, secondo rigorose procedure interne e con il supporto di punteggi attribuiti mediante controlli automatici.

- **Accettazione o rifiuto della sessione di video-identificazione:** sulla base degli esiti dei controlli di back-office, l'operatore decide se approvare o rifiutare la sessione.

Emissione di proof of evidence

A seguito del positivo completamento dell'identificazione viene generato un pacchetto probatorio che comprende:

- la registrazione audio-video,
- le immagini dei documenti di identità,
- le immagini acquisite durante la liveness detection,
- l'audit trail contenente gli esiti dei controlli effettuati. L'audit trail include inoltre le impronte informatiche dei singoli file prodotti.

La documentazione è cifrata mediante una chiave pubblica generata da Aruba.

3.1.2 RAIP e S-RAIP - identificazione non assistita di tipo automatico e ibrido

Aruba PEC mette a disposizione due modalità di verifica automatica dell'identità da remoto: il Remote Automatic Identity Proofing (RAIP), interamente automatizzato, e il Supervised Remote Automatic Identity Proofing (S-RAIP), che integra una supervisione umana in specifiche fasi del processo.

Entrambe le modalità di identificazione possono essere utilizzate ai fini dell'erogazione di servizi fiduciari del Cliente, anche qualificati, e si articolano nelle seguenti fasi: inizializzazione, raccolta dei dati e dell'evidenza, validazione, associazione dell'evidenza al Richiedente ed emissione del risultato di avvenuta identificazione.

Le differenze tra i due processi consistono di tre macro-elementi:

	RAIP	S-RAIP
Modalità	Interamente automatizzata	Automatizzata con supervisione umana
Intervento umano	Non previsto	Limitato alla validazione e all'associazione al Richiedente
Evidenze aggiuntive	Esiti dei controlli automatici	Esito della supervisione

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 practice* di settore. Aruba PEC definisce e mantiene inoltre livelli obiettivo di prestazione per le metriche PAD, con riferimento agli scenari PAD dal Livello 1 al Livello 3 e al Livello 5 (injection).

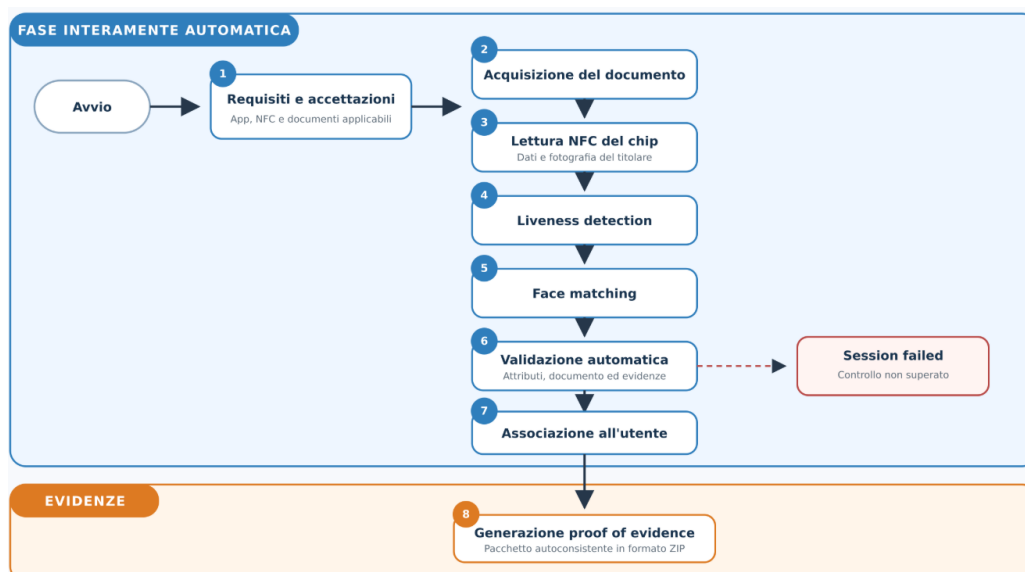
Il sistema di Injection Attack Detection utilizzato da Aruba ha superato una valutazione equivalente al livello High di CEN/TS 18099. Inoltre è stato valutato conformemente a ISO/IEC 19795-1 e 19795-2 su oltre un milione di confronti, ottenendo FMR dello 0,005%, FNMR del 2,21% e FTA dello 0%.

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.

3.1.2.1 RAIP - Remote Automatic Identity Proofing

Modalità	Remote unattended, con operazioni automatiche (ETSI 119-461, C.3.4)
Livello	Extended (High)
Controlli	NFC, validazione documento, liveness detection, controlli di antispoofing, face matching

Il flusso end-to-end può essere riassunto come da diagramma di seguito riportato:



Inizializzazione

Prima dell'avvio, al Richiedente vengono mostrati i contenuti definiti con il Cliente in funzione delle finalità di identificazione da quest'ultimo determinate.

Il processo richiede l'utilizzo di uno smartphone abilitato alla lettura NFC e di un documento conforme allo standard ICAO 9303 tra quelli ammessi da Aruba PEC nel manuale operativo dedicato al processo specifico, denominato "MODAP_A_31_SPS". Alla data di redazione del presente documento sono utilizzabili la Carta d'Identità Elettronica e il passaporto elettronico italiani.

Raccolta degli attributi e delle evidenze

Il processo guida il Richiedente nell'acquisizione delle evidenze necessarie e raccoglie:

- le immagini del fronte e del retro del documento;
- i dati e la fotografia contenuti nel chip del documento;
- i metadati identificativi e temporali della sessione;
- gli eventuali alert generati dai controlli.

Al termine della trasmissione ai sistemi Aruba, i dati relativi all'identificazione sono eliminati dal dispositivo mobile. Eventuali errori nella raccolta o nel trasferimento delle evidenze determinano il fallimento della sessione.

Nel caso di rappresentanti di persone giuridiche, è possibile acquisire ulteriori attributi mediante l'interrogazione di registri attendibili. Qualora le informazioni non siano disponibili, il Richiedente può essere invitato a produrre documenti o attestazioni comprovanti i propri poteri di rappresentanza.

Validazione

I sistemi Aruba verificano che il documento rientri tra quelli ammessi e ne controllano autenticità e validità. I dati acquisiti mediante lettura NFC sono confrontati con quelli dichiarati dal Richiedente; viene inoltre verificata la validità della firma elettronica apposta dall'Ente emittitore nel documento digitale. In presenza di caratteri diacritici, il confronto è effettuato applicando le regole di traslitterazione previste dallo standard ICAO 9303.

Associazione dell'evidenza al Richiedente

La componente automatica esegue inoltre:

- la **liveness detection**, per verificare che il campione biometrico provenga da una persona reale presente durante la sessione. In tale fase sono acquisite le immagini del volto del Richiedente;
- il **face matching**, mediante confronto tra il volto del Richiedente, la fotografia presente nel chip e quella riportata sul documento fisico.

La presenza di difformità, la rilevazione di possibili attacchi o il mancato raggiungimento delle soglie di affidabilità previste determinano la conclusione negativa della sessione. Le verifiche e le decisioni sono elaborate nei Data Center Aruba e non nell'App installata sul dispositivo del Richiedente.

Associazione ed emissione della proof of evidence

Le evidenze raccolte e validate sono associate al Richiedente mediante la generazione di una proof of evidence unica e autoconsistente, costituita da un pacchetto in formato ZIP. Il pacchetto comprende almeno:

- le immagini del volto acquisite durante la *liveness detection*;
- la fotografia estratta dal chip del documento;
- le immagini del documento di identità;
- i dati acquisiti mediante lettura NFC;
- i metadati della sessione, inclusi identificativo, data, ora e durata;
- il report complessivo della sessione e gli esiti dei singoli controlli.

Per i rappresentanti di persone giuridiche sono incluse anche le evidenze relative alla persona giuridica e ai poteri di rappresentanza.

3.1.2.2 S-RAIP - Supervised Remote Automatic Identity Proofing

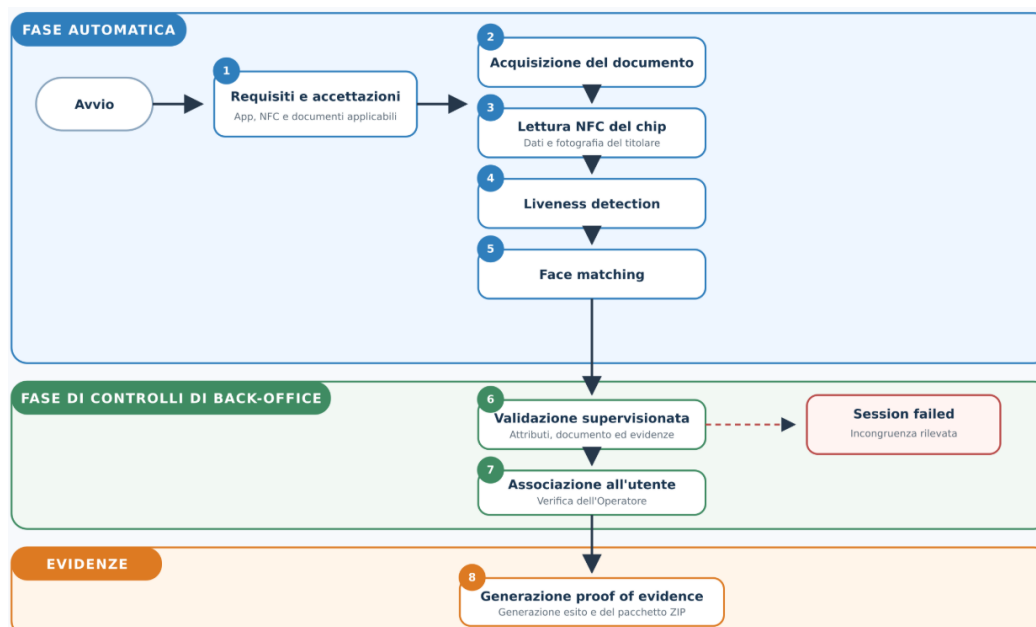
Il S-RAIP utilizza le medesime modalità di inizializzazione, acquisizione dei dati e raccolta delle evidenze previste per il RAIP.

Modalità	Remote unattended ibrido, con operazioni manuali e automatiche (ETSI 119-461, C.3.4)
Livello	Extended (High)

Controlli

NFC, validazione documento, liveness detection, controlli di antispoofing, face matching; backoffice

Il flusso end-to-end può essere riassunto come da diagramma di seguito riportato:



Inizializzazione e raccolta delle evidenze

Il Richiedente utilizza, come per il processo RAIP sopra descritto, un dispositivo abilitato alla lettura NFC e uno dei documenti conformi allo standard ICAO 9303 ammessi da Aruba PEC nel manuale operativo dedicato al processo specifico, denominato “MODAP_A_31_SPS”.

Prima dell'avvio, al Richiedente vengono mostrati i contenuti definiti con il Cliente in funzione delle finalità di identificazione da quest'ultimo determinate.

Validazione preliminare automatica

I sistemi Aruba verificano che il documento rientri tra quelli ammessi e ne controllano autenticità e validità. I dati acquisiti mediante lettura NFC sono confrontati con quelli dichiarati dal Richiedente; viene inoltre verificata la validità della firma elettronica apposta dall'Ente emittitore nel documento digitale. In presenza di caratteri diacritici, il confronto è effettuato applicando le regole di traslitterazione previste dallo standard ICAO 9303.

Associazione dell'evidenza al Richiedente

La componente automatica esegue inoltre:

- la **liveness detection**, per verificare che il campione biometrico provenga da una persona reale presente durante la sessione. In tale fase sono acquisite le immagini del volto del Richiedente;

- il **face matching**, mediante confronto tra il volto del Richiedente, la fotografia presente nel chip e quella riportata sul documento fisico.

La presenza di difformità, la rilevazione di possibili attacchi o il mancato raggiungimento delle soglie di affidabilità previste determinano la conclusione negativa della sessione. Le verifiche e le decisioni sono elaborate nei Data Center Aruba e non nell'App installata sul dispositivo del Richiedente.

Convalida finale dei dati e dell'evidenza; Collegamento finale dell'evidenza al Richiedente

Le evidenze e i risultati dei controlli sono successivamente riesaminati in back-office da un operatore. L'Operatore svolge le verifiche nel rispetto delle procedure interne e mediante strumenti informatici dedicati, che consentono di esaminare i documenti, confrontare le immagini del volto e ingrandire i dettagli rilevanti.

La supervisione è limitata alla validazione delle evidenze e alla loro corretta associazione al Richiedente; l'inizializzazione, la raccolta dei dati e la produzione del pacchetto probatorio rimangono automatizzate. Qualsiasi incongruenza o incoerenza rilevata dall'operatore comporta il rifiuto della sessione.

Nel caso di rappresentanti di persone giuridiche, la supervisione può comprendere anche l'esame degli attributi acquisiti dai registri attendibili e della documentazione prodotta per dimostrare i poteri di rappresentanza.

Emissione della proof of evidence

Il S-RAIP produce un pacchetto probatorio in formato .zip contenente le medesime evidenze previste per il RAIP, descritte al sottoparagrafo precedente.

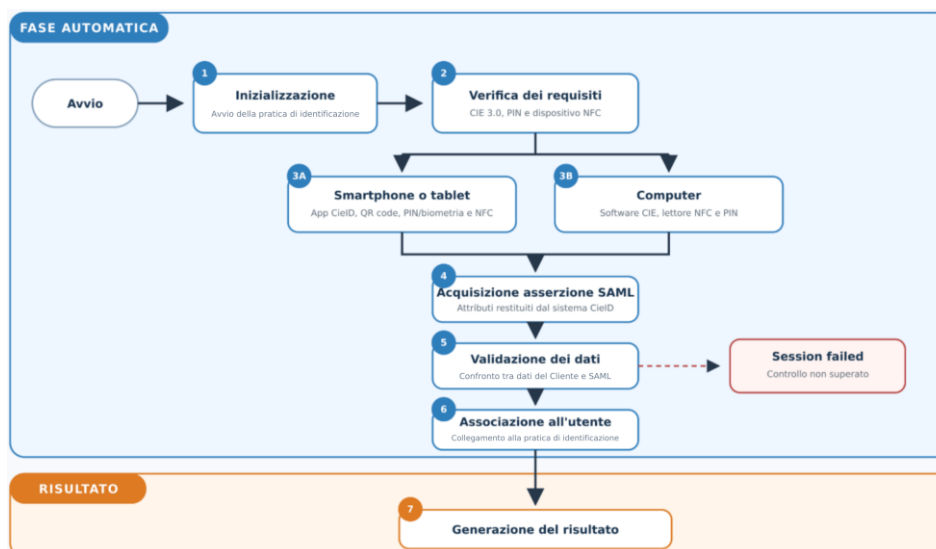
L'esito delle attività svolte dall'operatore e i relativi log sono gestiti secondo le modalità previste dal processo e dalla configurazione del servizio.

3.1.3 Identificazione mediante Cield

Il processo consente di verificare a distanza l'identità del Richiedente mediante autenticazione con Carta d'Identità Elettronica. La CIE costituisce un mezzo di identificazione elettronica notificato ai sensi del Regolamento eIDAS con livello di garanzia elevato. Il processo non richiede l'intervento di un operatore.

Modalità	Identificazione con sistema di identità digitale notificato di livello 3 (ETSI 119-461, C.3.2)
Livello	Extended (High)
Controlli	Verifica evidenza di avvenuta autenticazione

Il flusso end-to-end può essere riassunto come da diagramma di seguito riportato:



Inizializzazione

Prima dell'autenticazione, IDS verifica o comunica la disponibilità dei requisiti necessari:

- CIE versione 3.0 valida e attiva;
- PIN della Carta d'Identità Elettronica;
- smartphone o tablet dotato di NFC e App CielD installata e configurata dal Richiedente; oppure
- computer dotato di software CIE e lettore contactless NFC/RFID.

Raccolta dei dati e delle evidenze

L'autenticazione può essere effettuata attraverso due percorsi alternativi.

Nel caso di utilizzo di smartphone o tablet, il Richiedente inserisce il numero seriale della CIE, accede all'App CielD e scansiona il QR code visualizzato. L'autenticazione prosegue mediante inserimento delle ultime quattro cifre del PIN oppure, se precedentemente configurato nell'App, mediante il sistema biometrico disponibile sul dispositivo. Il Richiedente avvicina quindi la CIE al sensore NFC e completa le operazioni indicate, compresa la generazione del codice richiesto dall'interfaccia.

Nel caso di utilizzo del **computer**, il Richiedente installa e configura il software CIE, collega il lettore contactless, avvicina la Carta al dispositivo e inserisce le ultime quattro cifre del PIN.

A seguito dell'autenticazione, il sistema CielD restituisce un'asserzione SAML contenente gli attributi identificativi del Richiedente. Il processo non prevede pertanto l'acquisizione autonoma, da parte di Aruba, delle immagini del documento o di campioni biometrici destinati al riconoscimento facciale.

Validazione dei dati e delle evidenze

IDS verifica la coerenza tra i dati di registrazione trasmessi dal sistema chiamante e gli attributi contenuti nell'asserzione SAML restituita dal sistema CielD. Il set di attributi oggetto di verifica dipende dal processo e dalle specifiche concordate con il Cliente.

Il processo può proseguire soltanto se l'autenticazione con CielD è completata correttamente e i dati acquisiti risultano coerenti con quelli associati alla richiesta del servizio.

Associazione dei dati e dell'evidenza al Richiedente

In caso di esito positivo, l'asserzione SAML e gli attributi validati sono associati al Richiedente e alla relativa richiesta. Tale associazione consente di collegare in modo univoco l'identità attestata dal sistema CielD ai dati precedentemente raccolti.

Emissione della proof of evidence

L'evidenza dell'identificazione è generata in formato idoneo alla conservazione, corredata dall'asserzione SAML CielD e dagli ulteriori elementi previsti dal servizio.

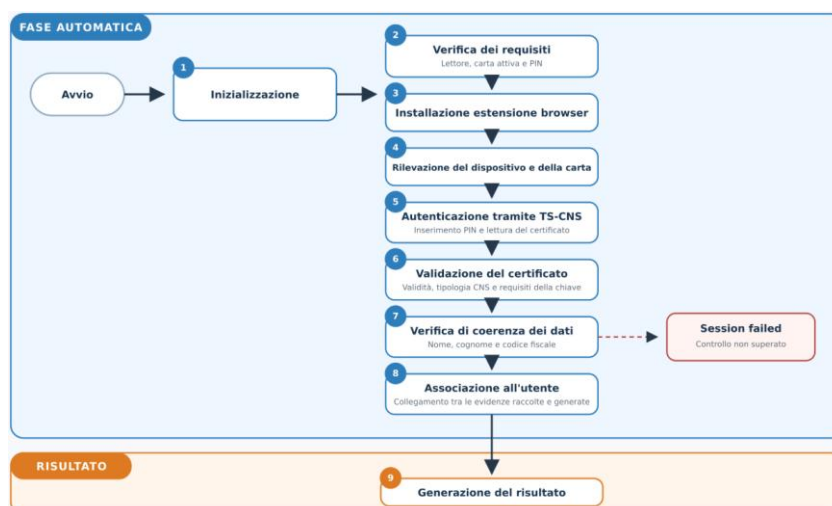
L'evidenza è gestita da IDS secondo le modalità previste dal processo e dalla configurazione del servizio concordata con il Cliente.

3.1.4 Identificazione mediante TS-CNS

Il processo consente l'identificazione automatica del Richiedente mediante il certificato di autenticazione contenuto in una Tessera Sanitaria con funzionalità CNS attiva o in una Carta Nazionale dei Servizi.

Modalità	Identificazione con sistema di identità digitale notificato di livello 3 (ETSI 119-461, no use case specifico)
Livello	Extended (High)
Controlli	Verifica certificato e credenziali CNS

Il flusso end-to-end può essere riassunto come da diagramma di seguito riportato:



Inizializzazione

Il Richiedente seleziona il metodo TS-CNS sulla piattaforma IDS e avvia il processo.

Le attività preliminari, le informative e le eventuali accettazioni sono definite in funzione del servizio del Cliente e delle modalità di integrazione concordate.

Il sistema informa il Richiedente dei requisiti necessari:

- lettore di smart card collegato al computer;
- TS-CNS o CNS attiva;
- PIN associato alla carta;
- estensione browser necessaria per interagire con il dispositivo.

Raccolta dei dati e delle evidenze

Il Richiedente installa, ove necessario, l'estensione browser richiesta. Il sistema rileva il lettore e la carta inserita, quindi richiede l'immissione del PIN.

A seguito dell'autenticazione, IDS acquisisce dal certificato CNS i dati identificativi del titolare necessari al processo (il set dei dati dipende dal processo e dalle specifiche concordate con il Cliente). Il PIN è utilizzato esclusivamente per consentire l'operazione sulla carta e non costituisce un dato identificativo acquisito da IDS.

Validazione dei dati e delle evidenze

IDS verifica automaticamente:

- che il certificato sia valido e non scaduto;
- che si tratti di un certificato riconducibile a una carta CNS;
- che la chiave crittografica soddisfi i requisiti tecnici previsti dalla normativa applicabile;

- che gli attributi identificativi estratti dal certificato siano coerenti con i dati ricevuti dal sistema chiamante.

L'identificazione è completata esclusivamente in caso di esito positivo di tutti i controlli. L'assenza del dispositivo, l'inserimento di un PIN non valido, l'inidoneità del certificato o la mancata corrispondenza dei dati determinano il mancato completamento della sessione.

Associazione dei dati e dell'evidenza al Richiedente

I dati estratti dal certificato e i risultati dei controlli vengono associati al Richiedente e alla relativa richiesta. La corrispondenza di nome, cognome e codice fiscale consente di collegare l'identità attestata dalla TS-CNS o CNS ai dati già presenti nel sistema chiamante.

Emissione della proof of evidence

L'evidenza di identificazione è gestita da IDS secondo le modalità previste dal processo e dalla configurazione del servizio concordata con il Cliente.

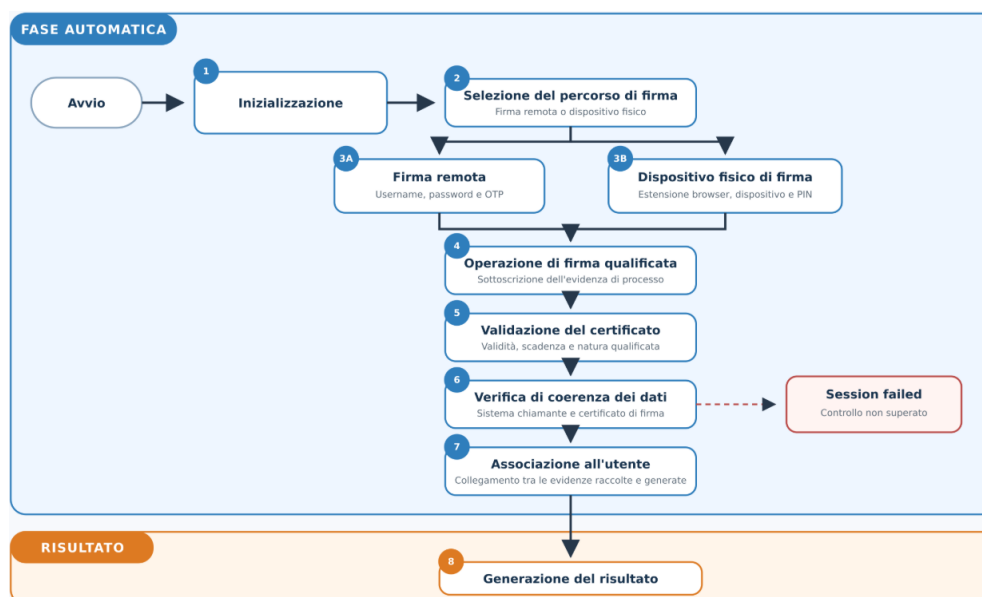
3.1.5 Identificazione mediante utilizzo di firma elettronica qualificata

Il processo consente di identificare il Richiedente mediante un certificato di firma elettronica qualificata rilasciato da un prestatore di servizi fiduciari qualificato. Il metodo si fonda sull'associazione tra il titolare e il certificato utilizzato per sottoscrivere l'evidenza prevista dal processo.

Il processo può essere completato mediante firma qualificata remota oppure mediante firma qualificata locale installata su un dispositivo fisico, quale una smart card o un token crittografico.

Modalità	Identificazione con sistema di identità digitale notificato di livello 3 (ETSI 119-461, C.3.3)
Livello	Extended (High)
Controlli	Verifica certificato e corretta esecuzione firma

Il flusso end-to-end può essere riassunto come da diagramma di seguito riportato:



Inizializzazione

Le attività preliminari, le informative, le accettazioni e il documento da sottoscrivere sono definiti in funzione del servizio e delle modalità di integrazione concordate.

Raccolta dei dati e delle evidenze

Il sistema presenta i requisiti necessari in base al percorso selezionato.

Firma remota. Il Richiedente utilizza le credenziali del servizio di firma — username e password — e il codice OTP generato mediante uno dei canali abilitati. IDS acquisisce il certificato associato alla firma e i dati identificativi in esso contenuti.

Firma locale. Il Richiedente dispone di una firma qualificata locale installata su dispositivo fisico collegato al computer e del relativo PIN. Ove necessario, installa l'estensione browser richiesta; il sistema rileva quindi il dispositivo e consente l'esecuzione dell'operazione di firma.

In entrambi i percorsi il Richiedente sottoscrive, mediante firma qualificata, il documento o l'evidenza prevista dal processo.

Validazione dei dati e delle evidenze

IDS verifica automaticamente:

- la validità e la scadenza del certificato;
- la natura qualificata del certificato e della firma;
- la corretta esecuzione dell'operazione di firma;

- la coerenza tra i dati ricevuti dal sistema chiamante e quelli contenuti nel certificato. Il set di attributi oggetto di verifica dipende dal processo e dalle specifiche concordate con il Cliente.

L'identificazione è completata con successo soltanto se tutti i controlli tecnici e di coerenza previsti sul certificato del Richiedente risultano superati. In caso contrario, la sessione si conclude con esito negativo.

Associazione dei dati e dell'evidenza al Richiedente

I dati estratti dal certificato, il documento sottoscritto e i risultati delle verifiche vengono associati univocamente al Richiedente e alla relativa richiesta. La corrispondenza dei dati identificativi consente di collegare in maniera univoca l'identità attestata dal certificato alle informazioni ricevute dal sistema chiamante.

Emissione della proof of evidence

L'esito e le evidenze generate sono messi a disposizione del Cliente secondo le modalità di integrazione concordate. L'eventuale documento sottoscritto è quello definito dal Cliente per il proprio servizio. La conservazione è gestita dal Cliente o tramite il servizio da questo individuato, salvo che sia contrattualmente previsto l'utilizzo della conservazione Aruba. L'eventuale comunicazione al Richiedente e l'attivazione del servizio sono gestite dal Cliente, ove previste.

3.2 Altri metodi di identificazione supportati

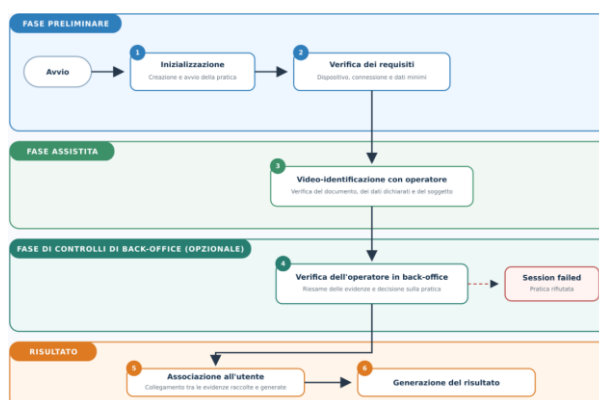
3.2.1 DVO - identificazione video assistita

Il DVO è un metodo di identificazione remota assistita, basato su una sessione video in tempo reale tra il Richiedente e un operatore di riconoscimento. Il processo è implementato per soddisfare il livello di garanzia Substantial e può essere utilizzato tramite IDS anche come servizio autonomo di identity proofing, indipendente dall'emissione di certificati o di altri servizi fiduciari.

A differenza del DVO+, il DVO non prevede una fase preliminare composta da acquisizione OCR del documento, liveness detection e face matching. La verifica dell'identità è effettuata principalmente dall'operatore durante la sessione video con il Richiedente.

Modalità	Remote attended
Controlli	Verifica manuale dell'identità e del documento del Richiedente

Il flusso end-to-end può essere riassunto come da diagramma di seguito riportato:



Inizializzazione

Il Cliente crea la pratica tramite API, trasmettendo a IDS i dati identificativi del Richiedente.

Prima dell'avvio della sessione vengono verificati i requisiti tecnici del dispositivo e della connessione internet e sono acquisiti i dati minimi necessari alla gestione della pratica.

Raccolta dei dati e delle evidenze

Il Richiedente accede alla sessione video in diretta con un operatore e presenta il documento di identità richiesto. Nel corso della sessione sono raccolti i dati dichiarati dal Richiedente e le evidenze previste dalla procedura interna di video-identificazione.

Durante questa fase avviene una composizione completa delle evidenze mostrate dal Richiedente. La sessione viene inoltre registrata integralmente e documentata mediante immagini, metadati e log applicativi.

Validazione dei dati e delle evidenze

L'operatore conduce la video-identificazione applicando una procedura dedicata. In particolare, è possibile verificare:

- la corrispondenza tra il Richiedente collegato e il documento esibito;
- la coerenza dei dati dichiarati con quelli riportati sul documento;
- la leggibilità, validità e apparente integrità del documento;
- il comportamento e le interazioni del Richiedente durante la sessione;
- il corretto completamento delle attività previste dalla procedura.

IDS può inoltre effettuare controlli di coerenza tra i dati forniti dal Cliente e/o dal Richiedente in precedenza e quelli acquisiti durante l'identificazione. Tali controlli riguardano tipicamente nome, cognome e codice fiscale e possono essere configurati in funzione delle esigenze del Cliente.

È possibile prevedere una successiva fase di controlli di back-office. Quando configurata, un secondo operatore riesamina le evidenze della sessione, applica i controlli interni e approva o rifiuta la pratica, registrando le motivazioni della decisione. In assenza di supervisione, l'esito deriva dalla sessione condotta dall'operatore.

Associazione dei dati e dell'evidenza al Richiedente

IDS associa alla pratica del Richiedente i dati raccolti, le evidenze della sessione, l'esito della video-identificazione e, ove prevista, la decisione dell'operatore di back-office.

L'associazione è effettuata utilizzando i riferimenti della pratica e i dati identificativi trasmessi dal Cliente, in modo da garantire la riconducibilità dell'esito allo specifico Richiedente.

Emissione della proof of evidence

A seguito della conclusione del processo di identity proofing, viene rilasciato un risultato di avvenuta identificazione.

A seguito del positivo completamento dell'identificazione viene generato un pacchetto probatorio che comprende:

- la registrazione video,
- le immagini dei documenti di identità,
- l'audit trail contenente gli esiti dei controlli effettuati. L'audit trail include inoltre le impronte informatiche dei singoli file prodotti.

La documentazione generata è protetta mediante tecniche crittografiche sicure dai sistemi di Aruba.

Al termine del processo IDS genera un esito positivo o negativo e aggiorna lo stato della pratica. Il Cliente riceve la notifica dell'esito mediante webhook e può consultare lo stato e recuperare le evidenze attraverso le API disponibili.

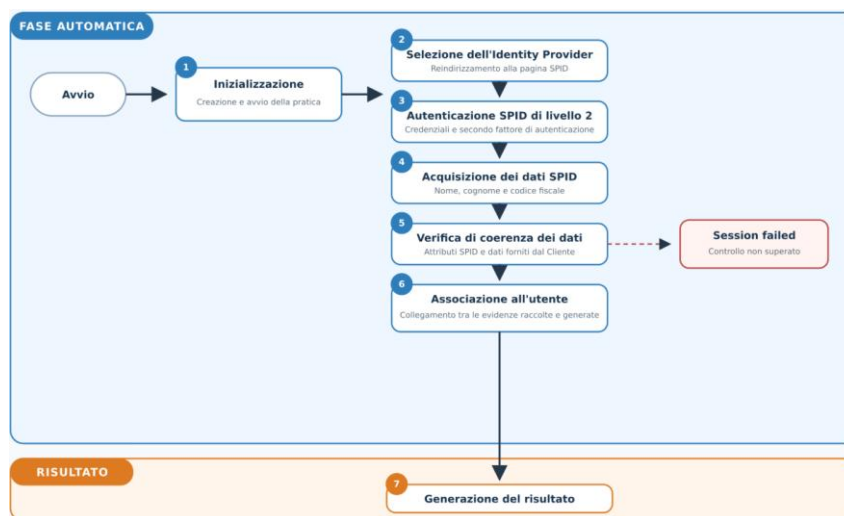
Le evidenze sono rese disponibili al Cliente e gestite secondo le modalità previste dalla configurazione del servizio e dagli accordi contrattuali applicabili, anche con riferimento alla loro eventuale conservazione.

3.2.2 Identificazione mediante credenziali SPID di livello 2

SPID è un metodo di identificazione automatica basato sull'autenticazione mediante un'identità SPID di livello 2, progettato per raggiungere un livello di sicurezza "substantial". Il metodo è destinato agli utenti possessori di un'identità SPID e consente a IDS di utilizzare gli attributi restituiti dall'Identity Provider come base per l'identificazione.

Modalità	Identificazione con sistema di identità digitale notificato di livello 2
Controlli	Verifica evidenza di avvenuta autenticazione

Il flusso end-to-end può essere riassunto come da diagramma di seguito riportato:



Inizializzazione

Il Cliente crea la pratica mediante API, trasmettendo a IDS i dati della persona da identificare e indicando SPID tra i metodi utilizzabili.

Il Richiedente viene indirizzato al front-end IDS oppure all'interfaccia realizzata dal Cliente e integrata con IDS, dove avvia il processo di identificazione.

Raccolta dei dati e delle evidenze

Il Richiedente viene reindirizzato alla pagina di autenticazione SPID e seleziona il proprio Identity Provider.

L'autenticazione viene effettuata con SPID di livello 2, mediante le credenziali rilasciate dall'Identity Provider e un secondo fattore di autenticazione, quale ad esempio un codice OTP generato dall'applicazione dell'IdP.

A seguito dell'autenticazione, IDS acquisisce gli attributi identificativi restituiti dall'Identity Provider.

Validazione dei dati e delle evidenze

IDS verifica il corretto completamento dell'autenticazione e confronta eventualmente gli attributi SPID con i dati comunicati dal Cliente in fase di creazione della pratica.

I controlli di coerenza, quando presenti, riguardano tipicamente nome, cognome e codice fiscale. Il Cliente può configurare i controlli da applicare in funzione delle proprie esigenze operative.

La pratica può proseguire esclusivamente se l'autenticazione è completata con successo e i dati confrontati risultano coerenti. In caso contrario, il processo si conclude con esito negativo.

Associazione dei dati e dell'evidenza al Richiedente

Gli attributi SPID, l'esito dell'autenticazione e le evidenze tecniche generate vengono associati alla pratica e al Richiedente mediante i relativi identificativi.

Emissione della proof of evidence

Al termine del processo IDS genera l'esito dell'identificazione e aggiorna lo stato della pratica. Il Cliente viene informato mediante webhook e può consultare lo stato e recuperare le evidenze attraverso le API della piattaforma.

Le evidenze sono rese disponibili al Cliente e gestite secondo le modalità previste dalla configurazione del servizio e dagli accordi contrattuali applicabili, anche con riferimento alla loro eventuale conservazione.

Dopo il download o l'invio in conservazione, i dati presenti su IDS vengono eliminati secondo le policy di data retention configurate.

4 MISURE DI SICUREZZA

Aruba PEC utilizza sistemi affidabili e adotta misure di sicurezza basate su standard e best practice riconosciuti a livello europeo e internazionale. Il proprio Sistema di Gestione della Sicurezza delle Informazioni (SGSI) è conforme e certificato secondo lo standard ISO/IEC 27001.

Di seguito sono descritti i principali standard e framework adottati per la gestione della Sicurezza delle Informazioni.

4.1 Principali Standard di Riferimento

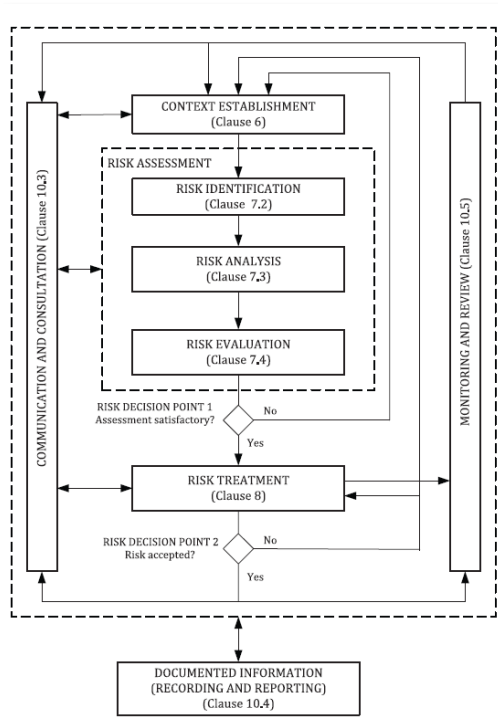
4.1.1 ISO/IEC 27001 e ISO/IEC 27002

La ISO/IEC 27001 definisce i requisiti per l'istituzione, l'attuazione, il mantenimento e il miglioramento continuo di un Sistema di Gestione della Sicurezza delle Informazioni (SGSI), supportando l'identificazione e la gestione dei rischi che possono incidere sulla riservatezza, integrità e disponibilità delle informazioni.

La ISO/IEC 27002 fornisce linee guida per l'implementazione dei controlli di sicurezza delle informazioni, con riferimento agli aspetti organizzativi, procedurali e tecnologici. Tali controlli supportano, ma non sostituiscono, le attività di valutazione e trattamento del rischio.

4.1.2 ISO 27005

La ISO/IEC 27005 fornisce linee guida per la gestione del rischio relativo alla Sicurezza delle Informazioni, a supporto dei principi e dei requisiti previsti dalla ISO/IEC 27001 e in coerenza con l'approccio generale alla gestione del rischio definito dalla ISO 31000.



ISO/IEC 27005: Processo di Gestione del Rischio per la Sicurezza delle Informazioni

4.2 Framework adottato per la gestione della Sicurezza delle Informazioni

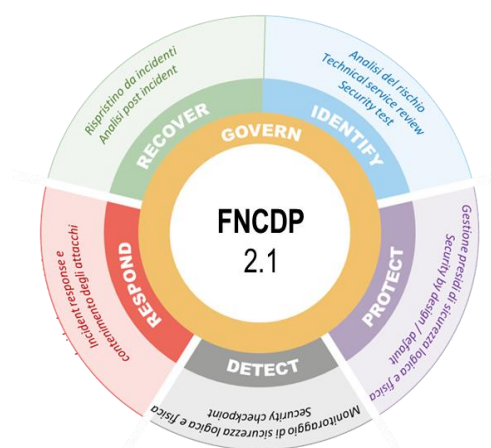
La Sicurezza delle Informazioni della **Piattaforma di Identificazione** è gestita facendo riferimento al **Framework Nazionale per la Cybersecurity e la Data Protection (FNCDP) – Edizione 2025 v2.1**, sviluppato dal Centro di Ricerca CIS della Sapienza Università di Roma e dal Laboratorio Nazionale di Cybersecurity del CINI, con il supporto dell'Agenzia per la Cybersicurezza Nazionale (ACN).

Il Framework supporta la gestione dei rischi di cybersecurity e protezione dei dati attraverso l'integrazione degli aspetti organizzativi, procedurali, tecnologici e normativi. Nell'ambito della Piattaforma di Identificazione è utilizzato a supporto della gestione del rischio, della definizione e del monitoraggio delle misure di sicurezza e del miglioramento continuo della postura di sicurezza.

Il Framework si articola nelle seguenti sei Funzioni:

- **Govern (GV):** definizione delle strategie di cybersecurity, delle politiche, dei ruoli, delle responsabilità e dei processi di governo del rischio;
- **Identify (ID):** identificazione degli asset, dei processi, delle dipendenze e dei rischi rilevanti;
- **Protect (PR):** adozione delle misure organizzative, fisiche e tecniche necessarie alla protezione delle informazioni e dei servizi;
- **Detect (DE):** monitoraggio e rilevazione tempestiva di eventi anomali, vulnerabilità e incidenti di sicurezza;
- **Respond (RS):** gestione, contenimento e mitigazione degli incidenti di sicurezza, incluse le relative attività di comunicazione;
- **Recover (RC):** ripristino dei servizi e delle capacità operative e adozione di misure finalizzate al miglioramento della resilienza.

L'adozione del Framework supporta un approccio strutturato alla cybersecurity, alla resilienza operativa, alla continuità dei servizi e alla conformità ai requisiti applicabili.



Framework adottato per la gestione della Sicurezza delle Informazioni

4.2.1 GOVERN

La funzione GOVERN definisce il sistema di governo della cybersecurity e della gestione del rischio informatico, incluse strategie, politiche, ruoli, responsabilità e attività di miglioramento continuo.

4.2.2 IDENTIFY

La funzione IDENTIFY supporta l'identificazione degli asset informativi, delle infrastrutture, dei processi, delle dipendenze e dei rischi rilevanti per la Piattaforma di Identificazione, consentendo di definire le priorità di protezione e le misure di trattamento del rischio.

4.2.3 PROTECT

La funzione PROTECT comprende le misure organizzative, fisiche e logiche adottate per proteggere informazioni e servizi, incluse la gestione degli accessi, la protezione dei dati, la sensibilizzazione del personale e i controlli tecnici di sicurezza.

4.2.4 DETECT

La funzione DETECT comprende le attività di monitoraggio e rilevazione finalizzate a identificare tempestivamente eventi anomali, vulnerabilità e incidenti di sicurezza che possano interessare la Piattaforma di Identificazione.

4.2.5 RESPOND

La funzione RESPOND comprende le attività necessarie per gestire, analizzare, contenere e mitigare gli incidenti di sicurezza e i relativi impatti sulla Piattaforma di Identificazione.

4.2.6 RECOVER

La funzione RECOVER comprende le attività necessarie al ripristino dei servizi e delle capacità operative a seguito di un incidente di sicurezza, nonché le misure finalizzate al miglioramento della resilienza organizzativa e tecnologica.

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

APPENDICE 1 – TECNOLOGIE IN OUTSOURCING

Per alcuni componenti legati ai processi, Aruba PEC si affida alle tecnologie fornite dai seguenti fornitori:

- **FACETEC, INC.**

Disponibile al seguente link: <https://www.facetec.com/>.

FaceTec è il fornitore delle componenti biometriche utilizzate da Aruba PEC on-premise nell'ambito dei processi di identificazione remota automatizzata, incluse le funzionalità di riconoscimento facciale, confronto biometrico e liveness detection, finalizzate a verificare la corrispondenza del Richiedente con il documento di identità e la sua effettiva presenza durante il processo.

La tecnologia FaceTec è stata sottoposta a test e valutazioni indipendenti con riferimento, tra gli altri, agli standard ISO/IEC 30107-3 per la Presentation Attack Detection e ISO/IEC 19795-2 per le prestazioni dei sistemi biometrici. I relativi report, test e certificazioni sono disponibili al seguente link: <https://dev.facetec.com/studies-reports-tests-certifications>.

- **TOCTOC S.r.l.**

Disponibile al seguente link: <https://www.toctoc.me>.

TocToc è un fornitore di piattaforma tecnologica di cui Aruba PEC in modalità SaaS si avvale per lo svolgimento dei processi di identificazione a distanza, sia in modalità supervisionata mediante operatore sia in modalità automatizzata. La piattaforma supporta la raccolta e la verifica dei documenti e delle informazioni del Richiedente, l'esecuzione dei controlli previsti e la produzione delle evidenze relative al processo di identificazione. I data center del fornitore sono collocati in UE.

I processi di Identity Proofing di TocToc sono conformi allo standard ETSI TS 119 461. TocToc ha inoltre conseguito le certificazioni ISO 9001, ISO/IEC 27001, ISO/IEC 27017 e ISO/IEC 27018.

Le informazioni sulle certificazioni e sugli standard adottati sono disponibili sul [sito di TocToc](#).