L'INTERAZIONE CREA VALORE

DOCUMENTO PUBBLICO

Identity Proofing Practise Statement TocToc

Via Alessandro Dudan, 00143 Rome (RM), Italy

Indice

1. Introduzione 4
2. Gestione della Policy 8
3. Casi d'Uso di Identity Proofing per persona fisica 11
4. Sicurezza 34
5. Conclusioni 38
ALLEGATI 39
Allegato A - Persona legale e Persona naturale che rappresenta Persona legale 40

Data	7 nov 2025
Versione	1.1
Classificazione	PUBBLICO
Oggetto	Identity Proofing Practise Statement (IPPS): descrizione dei processi operativi e delle procedure tecniche implementate per eseguire i servizi di identity proofing

1. Introduzione

1.1 Scopo del documento

Il presente Identity Proofing Practise Statement (IPPS) descrive le pratiche operative e le procedure adottate da TocToc per fornire un servizio di identity proofing conforme ai requisiti di:

- ETSI TS 119 461
- ETSI EN 319 401
- Regolamento UE 910/2014 (eIDAS) e successive modifiche e integrazioni come da Regolamento UE 1183/2024 (eIDAS2)
- Regolamento di Esecuzione UE 2022/1502
- Regolamento Generale sulla Protezione dei Dati (GDPR)
- Direttiva (UE) 2022/2555 (NIS2)
- Regolamento (UE) 2024/1689 (IA ACT)

I servizi di TocToc sono progettati per garantire processi sicuri e affidabili di autenticazione dell'identità degli utenti. I servizi di verifica dell'identità degli utenti da remoto sono erogati attraverso la Piattaforma AIO TocToc, certificata per gli standard ISO 27001:2022, ISO 9001:2015, ISO 27017:2015, ISO 27018:2019.

1.2 Ambito di Applicazione

TocToc agisce come Identity Proofing Service Provider (IPSP) per conto di TSP o QTSP e sotto la loro responsabilità, fornendo servizi di identity proofing in qualità di Responsabile o Sub-Responsabile per il trattamento dei dati. Il servizio di identity proofing si intende come una componente di un servizio fiduciario.

Il presente IPPS si applica ai processi di identity proofing, come descritti al Capitolo 3, offerti da TocToc, agli strumenti e alle tecnologie utilizzate e al personale e ai sistemi coinvolti nella verifica dell'identità degli utenti.

Per i servizi di verifica dell'identità erogati da TocToc, il richiedente può essere una persona naturale, una persona giuridica, o una persona naturale che rappresenta una persona giuridica.

1.3 Scenari di rischio nel perimetro dell'Identity Proofing

1.3.1 Minacce Generali

I processi di verifica dell'identità da remoto implementati da TocToc sono esposti a una serie di minacce, in particolare legate alla frode e al furto di identità, tra cui:

1. Personificazione:
    a. Utilizzo non autorizzato di dati personali per impersonare un altro soggetto
    b. Tentativo di eludere sistemi di face matching o liveness con immagini/video artefatti o mediante l'uso di maschere siliconiche.
2. Evidenze falsificate o manomesse:
    a. Processo compromesso da evidenze di bassa qualità in termini di illuminazione o risoluzione video
    b. Utilizzo di documenti d'identità falsi, contraffatti o alterati
    c. Tentativo di eludere sistemi di face matching o liveness con immagini/video artefatti o mediante l'uso di maschere siliconiche.
    d. Processo compromesso da evidenze scadute, revocate, o riportate come smarrite o rubate
3. Compromissione dei canali di comunicazione:
    a. Manipolazione dei sistemi di cattura delle immagini
    b. Intercettazione o alterazione dei dati scambiati durante il processo di verifica remota
4. Collusione interna o esterna:
    a. Coinvolgimento di operatori e/o utenti nella frode.

1.3.2 Gestione degli scenari di rischio

TocToc adotta un approccio sistemico e proattivo alla gestione delle minacce relative al furto di identità, alla frode e all'abuso del processo di identificazione. Le minacce vengono analizzate e valutate fin dalle fasi di progettazione del servizio di identity proofing, secondo i principi di **security by design** e **risk-based approach**, in linea con quanto previsto dagli standard ETSI applicabili.

Le misure di mitigazione sono integrate nei processi organizzativi e tecnici, e vengono riviste regolarmente attraverso esercitazioni, aggiornamenti tecnologici e audit interni, al fine di garantire la resilienza del sistema rispetto al mutare del panorama delle minacce.

1.4 Il Processo di Identity Proofing

Il processo di verifica dell'identità consiste nel verificare con il grado di certezza richiesto che l'identità di un Richiedente sia corretta.

Gli attori del processo di identificazione sono:

- Il **SP** (Service Provider, **TrustSP**, **QualifiedTSP**) o **Cliente** di TocToc che richiede la verifica dell'identità e che riceve l'esito della verifica;
- L'**IPSP** (Identity Proofing Service Provider - TocToc) che effettua la verifica per conto del SP;
- Il **Richiedente** (**Utente** finale di norma cliente dei clienti di TocToc) come persona fisica, persona giuridica o persona fisica che rappresenta una persona giuridica, la cui identità deve essere verificata.
- Il **Registration Officer** (Operatore di verifica dell'identità) incaricato dal TSP che svolge le attività manuali di verifica dell'identità.

Le fasi del processo di verifica dell'identità sono le seguenti:

1. **Iniziazione**: il Richiedente accede alla piattaforma, per il processo di identificazione, su invito ricevuto a mezzo email dal Cliente oppure dalla Piattaforma stessa o ancora tramite redirezione automatica dal portale o sito del Cliente e sceglie la modalità di identificazione. In questa fase TocToc mette a disposizione una soluzione tecnica che consente l'esposizione dell'informativa privacy e dei termini e condizioni e la raccolta del consenso del Richiedente ove necessario. Si specifica che è responsabilità del Cliente fornire l'informativa privacy e i termini e condizioni del servizio e ottenere il consenso del Richiedente per il trattamento dei dati coerentemente con i servizi effettuati mediante TocToc.
2. **Collezione di evidenze e attributi**: il Richiedente fornisce le evidenze necessarie per l'identificazione. Queste evidenze possono includere documenti ufficiali, video, immagini o altri attributi identificativi come data o luogo di nascita. Le evidenze e gli attributi richiesti per la verifica dell'identità possono variare e sono concordati volta per

volta con il Cliente rispettando il principio della minimizzazione dei dati. Viene comunque considerato come set minimo di attributi da richiedere al Richiedente: [nome, cognome, data di nascita, codice fiscale]. I documenti di riconoscimento di norma accettati nei processi di identity proofing per persona fisica sono: Carta di Identità, CIE, Patente di guida, in corso di validità e rilasciati dallo Stato Italiano, e Passaporti internazionali in corso di validità. A seconda delle esigenze del Cliente e dei requisiti di legge applicabili, è possibile irrobustire la verifica dell'identità collezionando e verificando attributi ed evidenze supplementari, solo dopo valutazione da parte di TocToc delle richieste di business e relativi requisiti di legge.

3. **Validazione di evidenze e attributi**: le evidenze e gli attributi vengono validati per verificarne l'integrità e l'autenticità. Il controllo sulla validità dei documenti è effettuato manualmente o con l'ausilio di strumenti automatizzati, mentre la protezione contro documenti rubati o smarriti è supportata dall'interrogazione di fonti autoritative di informazioni sui documenti (CRIMNET/SCIPAFI).
4. **Associazione all'Utente**: in questa fase le evidenze e gli attributi raccolti e verificati vengono associati all'utente creando un legame tra l'identità virtuale dell'utente e i dati reali che lo identificano. La validazione delle evidenze e l'associazione all'utente, svolte dal Registration Officer, seguono flussi specifici di attività e di controlli (checklist) condivisi volta per volta con il SP. Al primo controllo non rispettato nel flusso di videoriconoscimento, il processo si ferma dando vita a un KO ripetibile o definitivo. I processi di identity proofing TocToc, anche quando supportati da strumenti automatici, sono sempre sottoposti a validazione finale di un Registration Officer.
5. **Emissione del risultato**: una volta completato il processo di validazione e associazione, il sistema emette il risultato dell'identity proofing. Se positivo, l'utente può procedere con l'accesso al servizio per cui è stato effettuato l'identity proofing, altrimenti l'utente viene notificato del fallimento e in caso di KO ripetibile viene richiesto di ripetere il processo.

2. Gestione della Policy

2.1 L'Organizzazione

TocToc srl (http://www.toctoc.me) è una tech company italiana che dal 2014 agevola la digitalizzazione delle aziende, di ogni dimensione e settore. Sviluppiamo soluzioni e servizi digitali per aiutare le imprese e la pubblica amministrazione a crescere e a migliorare i loro processi e l'erogazione dei propri servizi.

2.2 La Piattaforma AIO

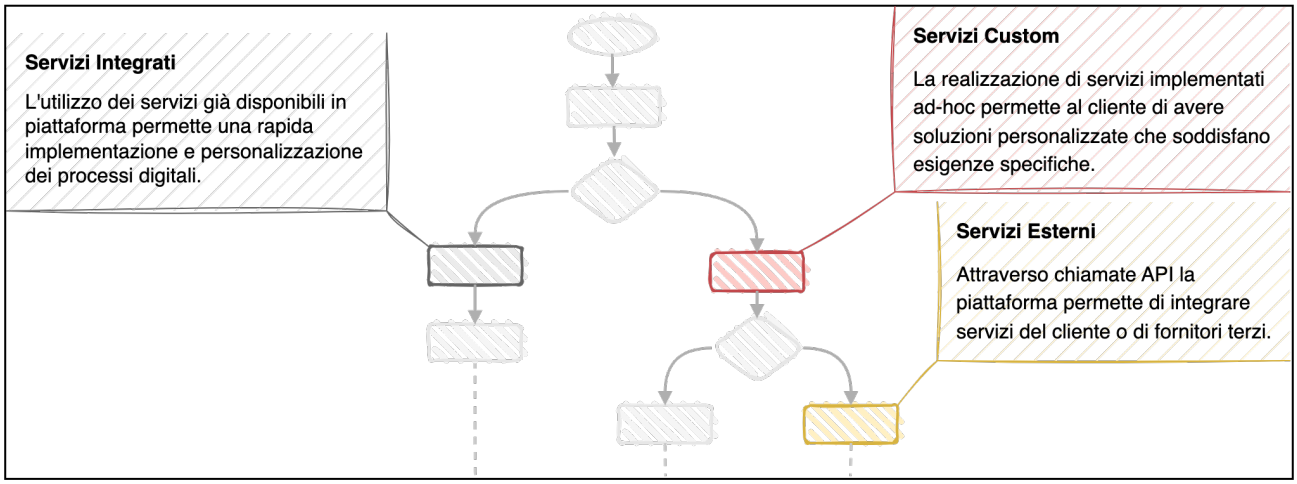
La soluzione permette di digitalizzare e dematerializzare i processi aziendali, include funzionalità come l'automazione dei flussi di lavoro, la gestione dei documenti elettronici, l'interazione e la collaborazione online, oltre che l'integrazione con i servizi esterni.

La gestione del workflow, che è il core della piattaforma, è basata sul modello di macchina a stati e consente di creare processi digitali personalizzati correlando singoli servizi tra loro.

Avviato un processo digitale si generano eventi, di sistema o interattivi, che possono essere configurati in modo sincrono o asincrono e eseguiti in serie o in parallelo.

L'ingegneria del software lowcode / nocode rende il sistema altamente flessibile, l'utilizzo e la configurazione di ogni singolo servizio favorisce la manutenzione, l'aggiornamento e l'evoluzione nel tempo del processo digitale implementato.

La piattaforma è dotata dei principali servizi utili all'automazione dei processi e alla trasformazione digitale, permette di implementare moduli personalizzati per soddisfare esigenze specifiche, è predisposta per l'integrazione con i sistemi esterni, dei Clienti o di fornitori terzi.



2.2 Dati di Contatto

TocToc s.r.l.
Via Alessandro Dudan, 7
00143 Roma (RM)
PIVA 12925931003
toctoc@pec.aruba.it[1]

2.3 Pubblicazione dell'Identity Proofing Practise Statement

La versione più aggiornata dell'IPPS approvata dal management è disponibile sul sito http://www.toctoc.me

Il presente documento viene revisionato con cadenza almeno annuale e comunque a ogni cambiamento significativo.

2.4 Certificazioni e Qualifiche

- UNI EN ISO 9001:2015[2]
- ISO /IEC 27001:2022[3]
- ISO /IEC 27017[4]
- ISO /IEC 27018[5]
- QUALIFICAZIONE ACN[6], da parte dell'Agenzia per la Cybersicurezza Nazionale (ACN), dei servizi cloud SaaS offerti dalla soluzione TocToc All-In-One (AIO) per le Pubbliche Amministrazioni, per il livello di qualificazione QC1 (ID Scheda: SA-4823).
- SOGGETTO AGGREGATORE SPID e CIE: a seguito della stipula con AgID della Convenzione per servizi Privati, emanata con Determinazione n. 0017962 del 20/09/2022, e per servizi Pubblici, con Determinazione n. 0022523 del 07/12/2022. TocToc è inoltre Soggetto Aggregatore privato Entra con CIE riconosciuto dalla Federazione entra con CIE e dal Ministero dell'Interno dal 09/11/2023. I Soggetti

1. mailto:toctoc@pec.aruba.it
2. https://www.toctoc.me/wp-content/uploads/2024/07/Cert.-CSQA-Toc-Toc_9001_2024.pdf
3. https://www.toctoc.me/wp-content/uploads/2024/07/Cert.-CSQA-Toc-Toc_27001_2024.pdf
4. https://www.toctoc.me/wp-content/uploads/2024/07/Cert.-CSQA-Toc-Toc_27017_2024.pdf
5. https://www.toctoc.me/wp-content/uploads/2024/07/Cert.-CSQA-Toc-Toc_27018_2024.pdf
6. https://www.toctoc.me/wp-content/uploads/2024/08/Qualificazione_ACN_servizi_Cloud_TocToc_Srl_per_le_PA.pdf

aggregatori offrono a terzi la possibilità di rendere accessibile tramite SPID e CIE i rispettivi servizi online.

- ADERENTE INDIRETTO SCIPAFI: TocToc S.r.l. è autorizzata ad erogare il servizio SCIPAFI esclusivamente su apposita delega di aderenti diretti, come definiti dall'articolo 1, comma 1, lettera a), del Decreto del Ministro dell'economia e delle finanze 19 maggio 2014, n. 95.

2.5 Termini e Condizioni

I termini e le condizioni applicabili nei confronti dei Clienti di TocToc per i servizi di verifica dell'identità da remoto sono regolati nelle Condizioni Generali di Contratto della Piattaforma AIO attraverso la quale sono erogati i servizi. Nel caso di identificazione tramite mezzi di identificazione elettronica, i termini e le condizioni sono regolati anche nell'Accordo di Servizio SPIDGO.

I termini e condizioni applicabili all' Utente in veste di Richiedente del processo di identity proofing sono regolati dalle specifiche "Termini e Condizioni per il Servizio di Verifica dell'Identità da Remoto".

2.6 Terminazione del Servizio

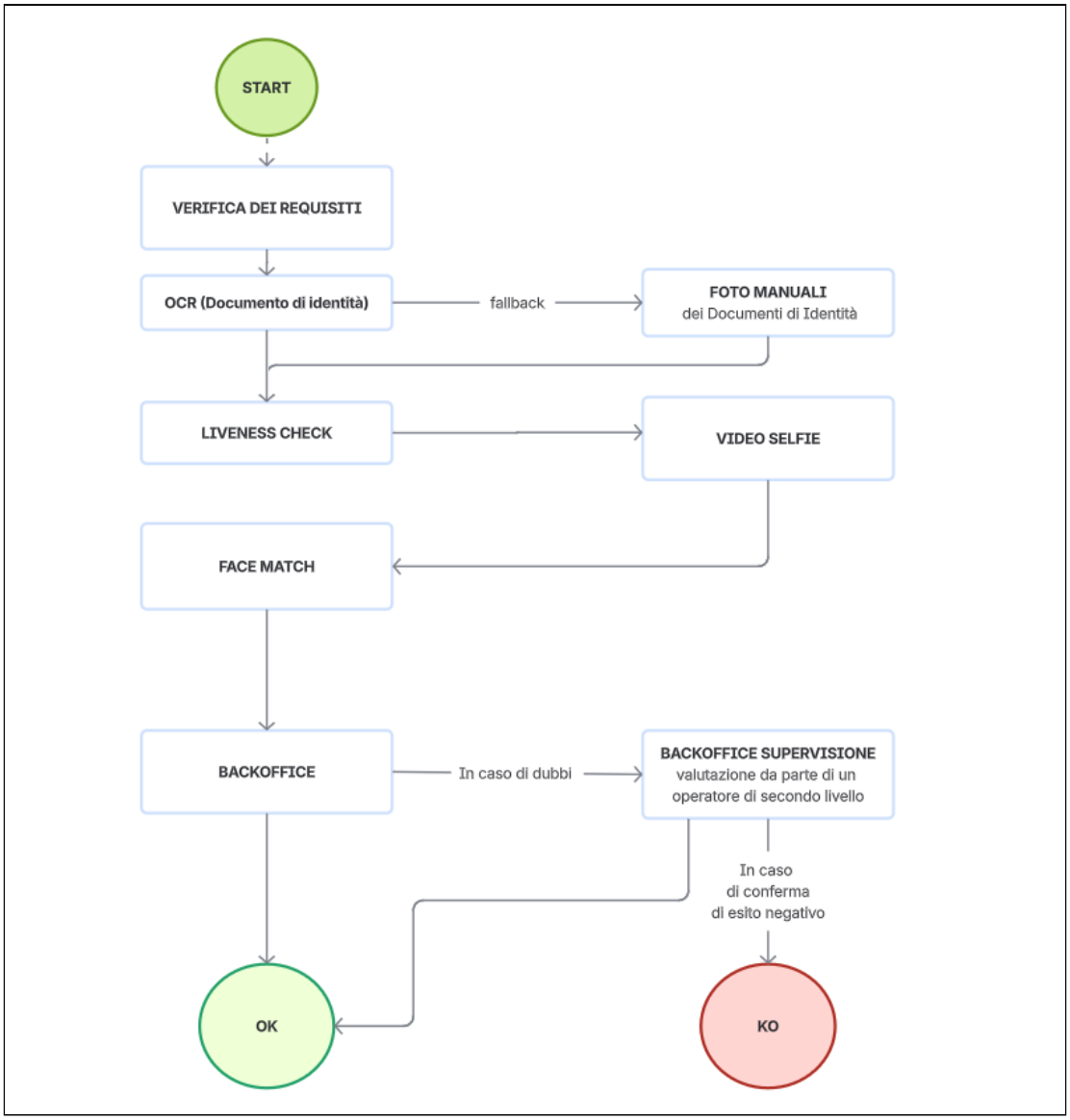
La cessazione del servizio di identity proofing può avvenire per decisione unilaterale di TocToc, su richiesta del Cliente, per cause di forza maggiore o in seguito alla cessazione dell'accordo contrattuale tra le parti. Le modalità attraverso le quali avviene la cessazione del servizio e le attività ad essa correlate come, a titolo esemplificativo e non esaustivo: notifica e comunicazione per la cessazione, gestione dei dati personali e delle evidenze dei processi, assistenza per transizione a un altro fornitore, sono definite volta per volta in sede contrattuale con il Cliente.

Le modalità di interruzione e terminazione del processo di identity proofing per l'Utente sono descritte in "Termini e Condizioni per il Servizio di Verifica dell'Identità da Remoto".

3. Casi d'Uso di Identity Proofing per persona fisica

3.1 Processo non supervisionato da remoto (Unattended)

Utilizzo di un documento di identità fisico in un contesto remoto non presidiato, in cui il richiedente presenta un documento di identità in una sessione remota senza supervisione umana.



Flusso Unattended

3.1.1 “TocToc Selfie”

Operazione ibrida con convalida e associazione al richiedente effettuate in un secondo momento tramite una combinazione di analisi automatizzata e operazioni manuali del Registration Officer.

Presenza del richiedente	Operazione	Clausola dell’ETSI 119 461	Documento di identità	Validazione delle evidenze	Associazione al richiedente	LoIP
Da remoto non supervisionata	Ibrida	9.2.3.3	Fisico	Manuale e automatica	Manuale e automatica	Extended

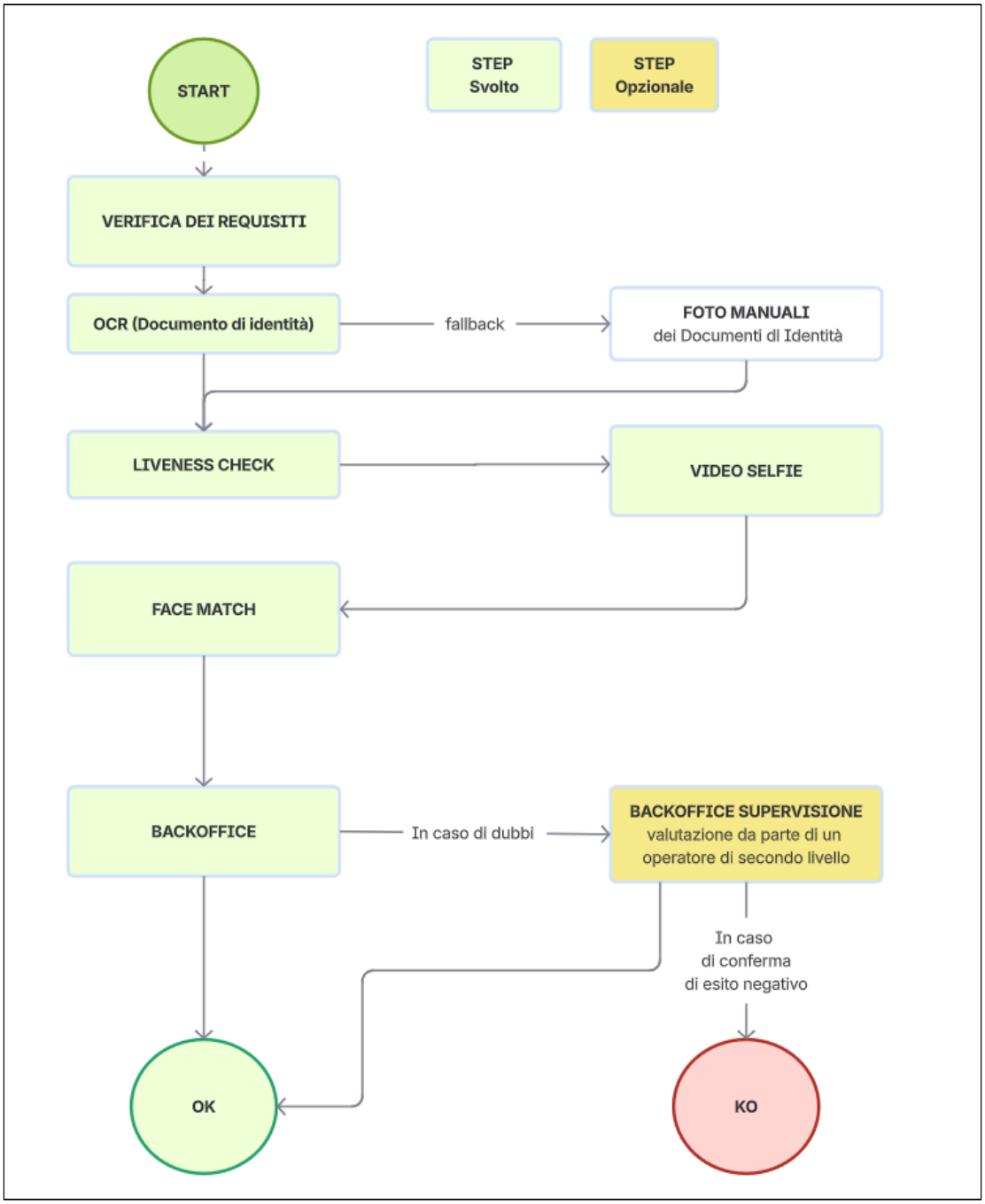
Il processo “**TocToc Selfie**” offre un esperienza molto semplice e consiste in una procedura guidata che l'utente segue in autonomia dove viene invitato a registrare un video che includa il proprio volto e il documento di identificazione. Durante la procedura guidata, l'utente può essere invitato a svolgere un’azione randomica, pronunciare una frase o a fornire altre informazioni per confermare la propria identità e/o le proprie intenzioni. Le operazioni di verifica dell’identità vengono effettuate in un secondo momento dal Registration Officer.

- Acquisizione delle evidenze: l’utente segue una procedura guidata in autonomia dove viene invitato a registrare un video che includa il proprio volto e il documento di identificazione.
- Verifica delle evidenze: diversi strumenti effettuano la validazione del documento o del video registrato per ridurre i tentativi di frode e assistere il Registration Officer per la verifica finale:
  - OCR: riconosce la tipologia del documento e ne estrae il testo per effettuare i controlli di coerenza interna;
  - Liveness Detection: con tecnologie passive di liveness check e con tecniche attive di verifica della vitalità del Richiedente.
- Associazione al richiedente: Il Registration Officer è assistito dallo strumento automatizzato di face matching e dalle tecniche di Analisi Morfologica per effettuare il confronto tra il volto dell’utente sul documento e il volto dell’utente presente a video.

- Decisione finale: il Registration Officer supportato dagli strumenti automatizzati sancisce l'esito dell'identificazione.

Qualora il Registration Officer rilevasse qualche anomalia o avesse dubbi nel validare la pratica può rimettere la stessa al Supervisore con una nota aggiuntiva.

E' previsto vi possa essere un ulteriore step di processo per la convalida definitiva, svolto da un operatore di secondo livello/supervisore sia per un controllo a campione che in caso di dubbi da parte del Registration Officer. In tale circostanza, è possibile svolgere ulteriori controlli, se previsti dallo specifico processo concordato con il TSP o con il Cliente.



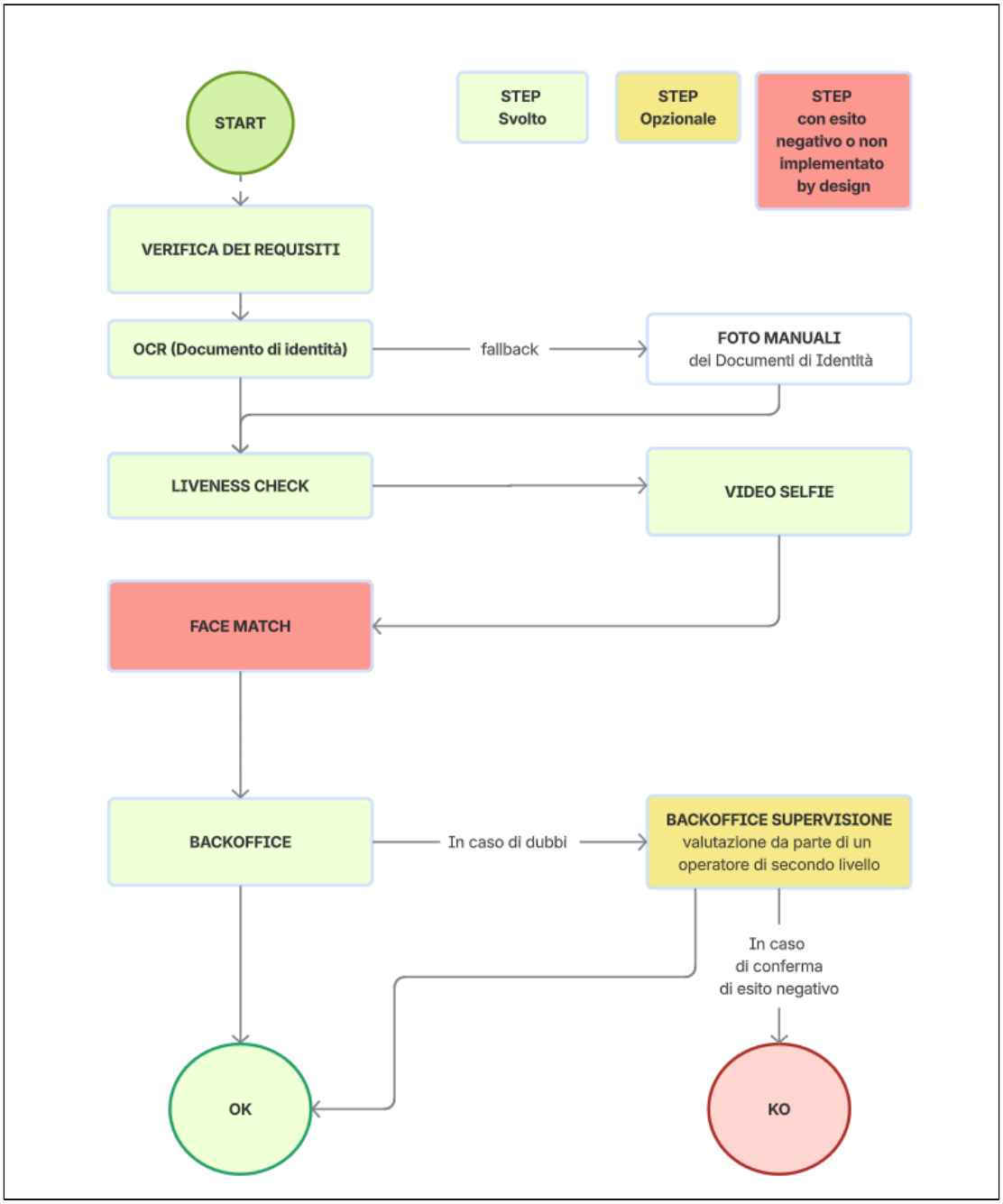
TocToc Selfie

3.1.1.1 “TocToc Selfie” - Variante A

Operazione ibrida con convalida e associazione al richiedente effettuate in un secondo momento tramite una combinazione di analisi automatizzata e operazioni manuali del Registration Officer.

Presenza del richiedente	Operazione	Clausola dell’ETSI 119 461	Documento di identità	Validazione delle evidenze	Associazione al richiedente	LoIP
Da remoto non supervisionata	Ibrida	9.2.3.3	Fisico	Manuale e automatica	Manuale	Baseline

In caso di esito negativo della tecnologia di face matching, l’associazione al richiedente viene effettuata esclusivamente in modalità manuale dal Registration Officer. Fatti salvi l’esito positivo o l’implementazione by design nel processo di almeno uno strumento automatizzato di verifica delle evidenze, tale fase continuerà ad essere svolta in modalità ibrida.



TocToc Selfie - Variante A

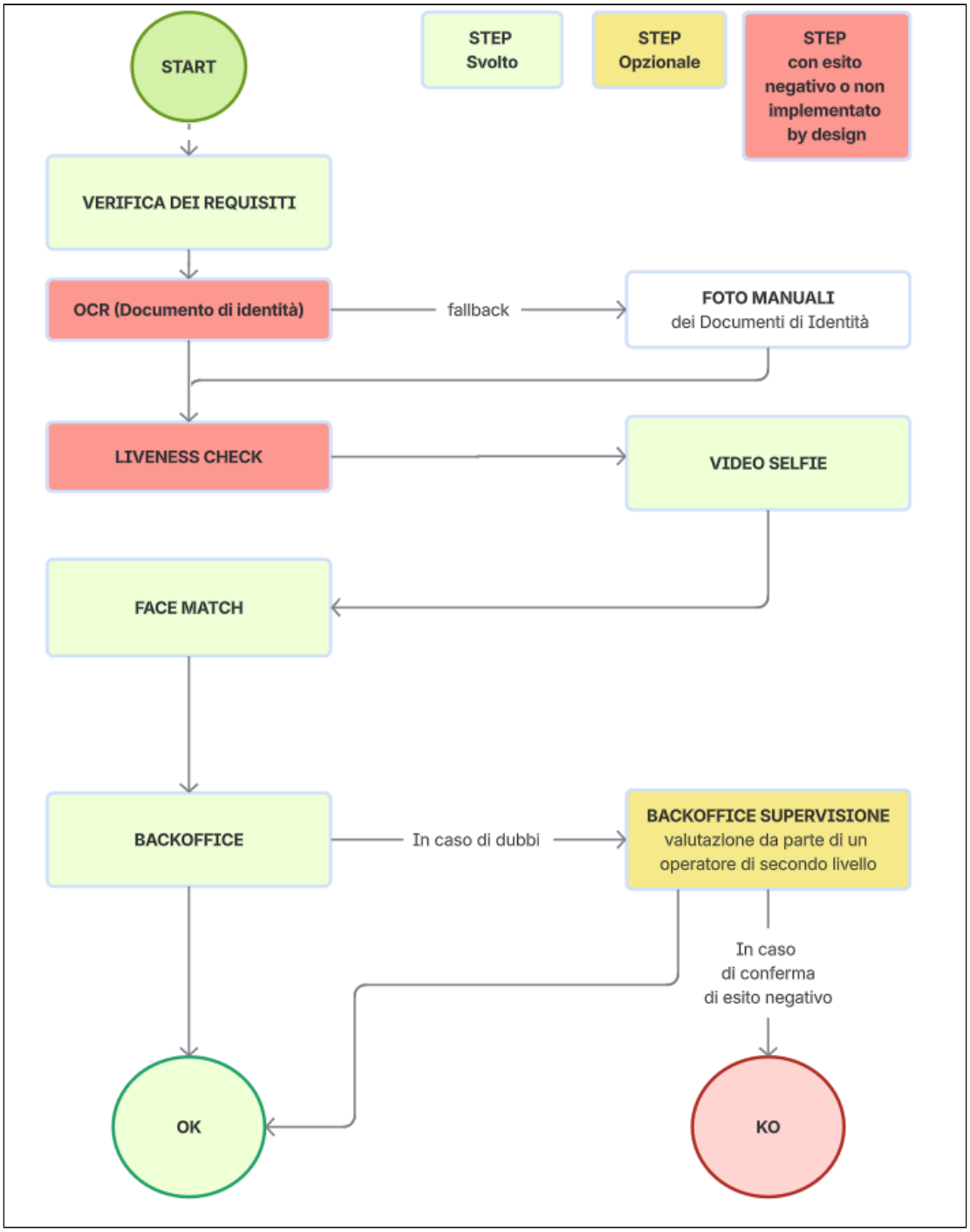
3.1.1.2 “TocToc Selfie” - Variante B

Operazione manuale con convalida e associazione al richiedente effettuate manualmente in un secondo momento dal Registration Officer.

Presenza del richiedente	Operazione	Clausola dell'ETSI 119 461	Documento di identità	Validazione delle evidenze	Associazione al richiedente	LoIP
Da remoto non supervisionata	Manuale	9.2.3.2	Fisico	Manuale	Manuale	Baseline

In caso di esito negativo o mancata implementazione by design di tecnologie di face matching e di tutti gli strumenti automatici per la verifica delle evidenze, le operazioni di verifica delle evidenze e di associazione al richiedente saranno svolte manualmente dal Registration Officer.

Occorre specificare che di norma, a seguito di diversi tentativi errati effettuati da uno stesso utente in modalità non supervisionate, è possibile dare il via a un meccanismo di fallback passando alla modalità sincrona con operatore.



TocToc Selfie - Variante B

3.2 Processo supervisionato da remoto (attended)

Utilizzo di un documento d'identità fisico in un contesto remoto assistito, dove il richiedente presenta un documento d'identità in una sessione remota e comunica in tempo reale con un Registration Officer.

3.2.1 “TocToc con Operatore”

Funzionamento ibrido manuale e automatizzato con convalida e vincolo al richiedente effettuato in tempo reale tramite una combinazione di analisi automatizzata e operazioni manuali del Registration Officer.

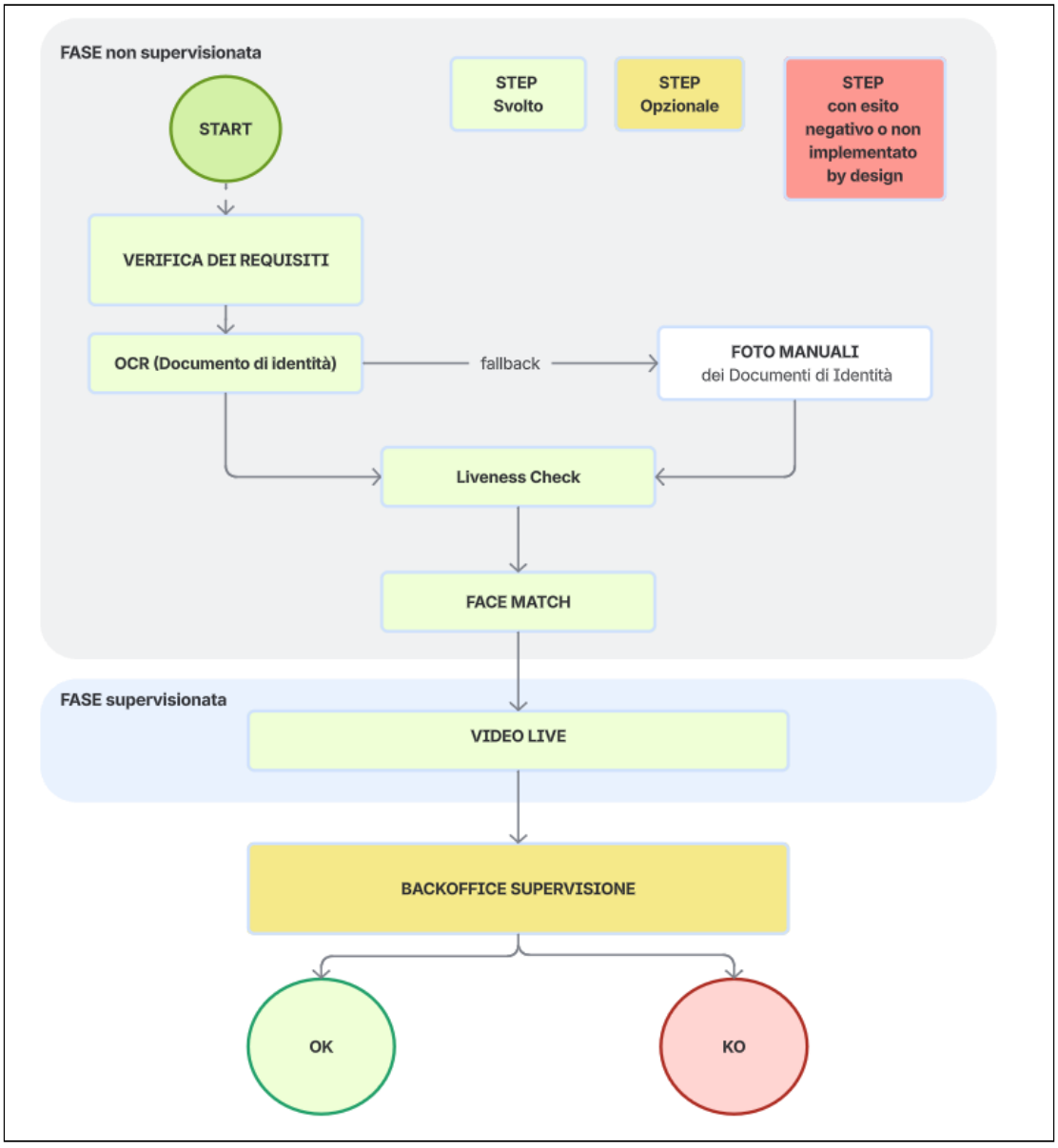
Presenza del richiedente	Operazione	Clausola dell’ETSI 119 461	Documento di identità	Validazione delle evidenze	Associazione al richiedente	LoIP
Da remoto supervisionata	Ibrida	9.2.2.3	Fisico	Manuale e automatica	Manuale e automatica	Extended

Il processo “**TocToc con Operatore**” prevede che l'utente venga invitato preliminarmente a scattare foto al fronte e al retro del proprio documento di identità, utilizzando la webcam del proprio dispositivo, in un processo guidato preliminare alla video chiamata con il Registration Officer. Il Registration Officer, durante la video chiamata, seguendo una specifica checklist di passaggi predefiniti, verifica la validità e l'autenticità dei documenti e dei dati raccolti ed effettua l’associazione dell’utente ai dati acquisiti. Questo processo riduce i tempi e i costi associati alla verifica dell'identità dei clienti rispetto ai metodi tradizionali de visu, offrendo un'esperienza utente semplice e assistita. Questa modalità di identificazione può essere personalizzata dal cliente grazie a una serie di opzioni, tra cui l’utilizzo di calendari che definiscono le fasce orarie di presidio del servizio, la gestione delle code e del routing.

Di seguito la descrizione delle fasi del processo:

- Acquisizione delle evidenze: l’utente viene invitato a fornire le proprie informazioni personali e a mostrare i propri documenti d'identità utilizzando la webcam del dispositivo.

- Verifica delle evidenze: diversi strumenti supportano il Registration Officer nella validazione dei documenti di identità o delle evidenze video per ridurre i tentativi di frode:
    - OCR: riconosce la tipologia del documento e ne estrae il testo per effettuare i controlli di coerenza interna;
    - Liveness Detection: con tecnologie passive di liveness check e con tecniche attive di verifica della vitalità del Richiedente.
- Associazione al richiedente: Il Registration Officer è assistito dallo strumento automatizzato di face matching e dalle tecniche di Analisi Morfologica per effettuare il confronto tra il volto dell'utente sul documento e il volto dell'utente presente a video in tempo reale.
- Decisione finale: la pratica di videoriconoscimento è assistita passo passo da uno script che suggerisce all'operatore cosa dire e una frase di "uscita" qualora qualsiasi controllo del processo dovesse fallire o dovesse riscontrare difficoltà. Il Registration Officer, supportato dagli strumenti automatizzati, sancisce l'esito dell'identificazione. E' previsto vi possa essere un ulteriore step di processo per la convalida definitiva, svolto da un operatore di secondo livello/supervisore sia per un controllo a campione che in caso di dubbi da parte del Registration Officer. In tale circostanza, è possibile svolgere ulteriori controlli, se previsti dallo specifico processo concordato con il TSP o con il Cliente.



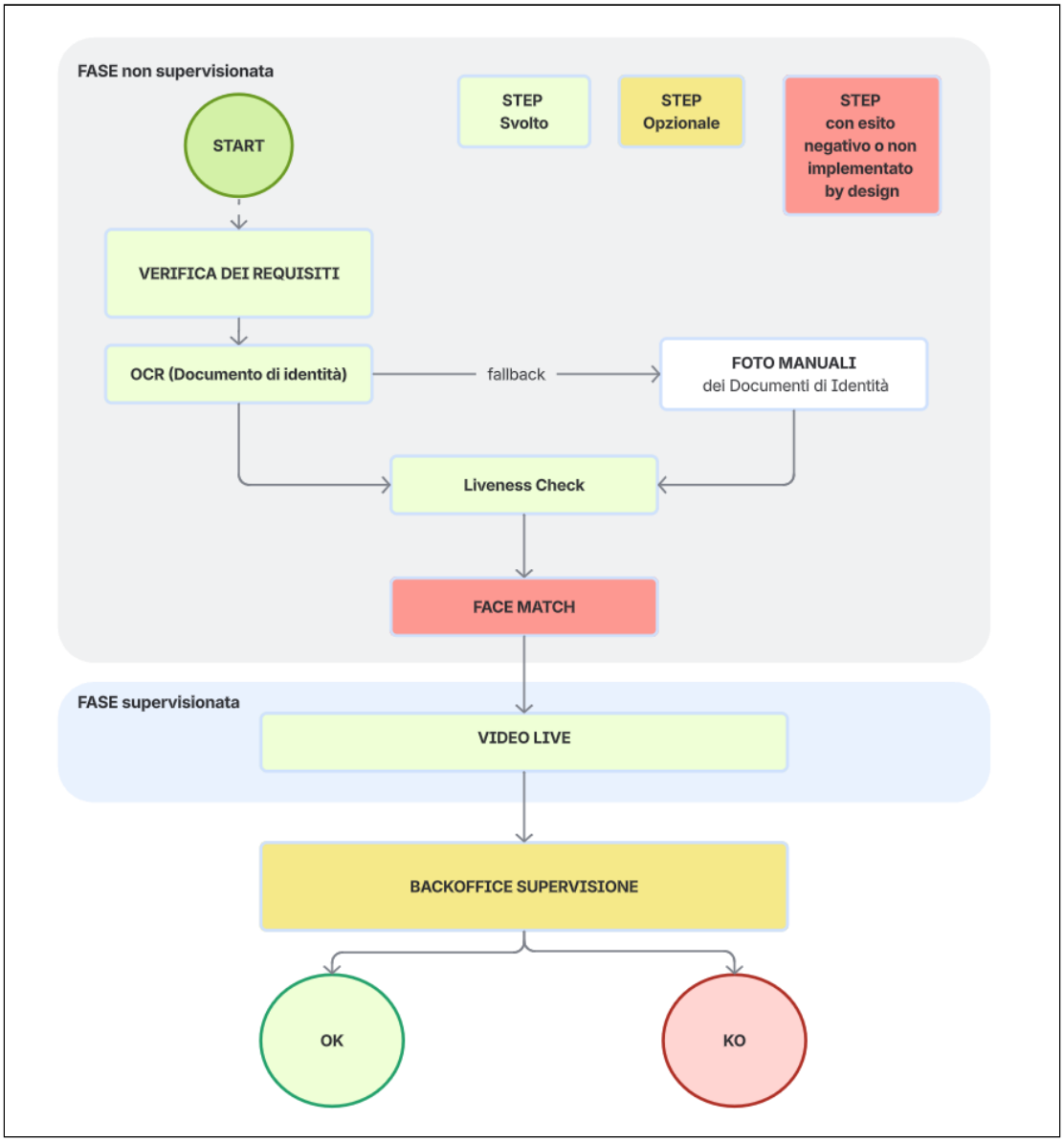
TocToc con Operatore

3.2.1.1 “TocToc con Operatore” - Variante A

Funzionamento ibrido manuale e automatizzato con convalida e vincolo al richiedente effettuato in tempo reale tramite una combinazione di analisi automatizzata e operazioni manuali del Registration Officer.

Presenza del richiedente	Operazione	Clausola dell'ETSI 119 461	Documento di identità	Validazione delle evidenze	Associazione al richiedente	LoIP
Da remoto supervisionata	Ibrida	9.2.2.3	Fisico	Manuale e automatica	Manuale	Extended

In caso di esito negativo o mancata implementazione by design della tecnologia di face matching, l'associazione al richiedente viene effettuata esclusivamente in modalità manuale dal Registration Officer. Fatti salvi l'esito positivo o l'implementazione by design nel processo di almeno uno strumento automatizzato di verifica delle evidenze, tale fase continuerà ad essere svolta in modalità ibrida.



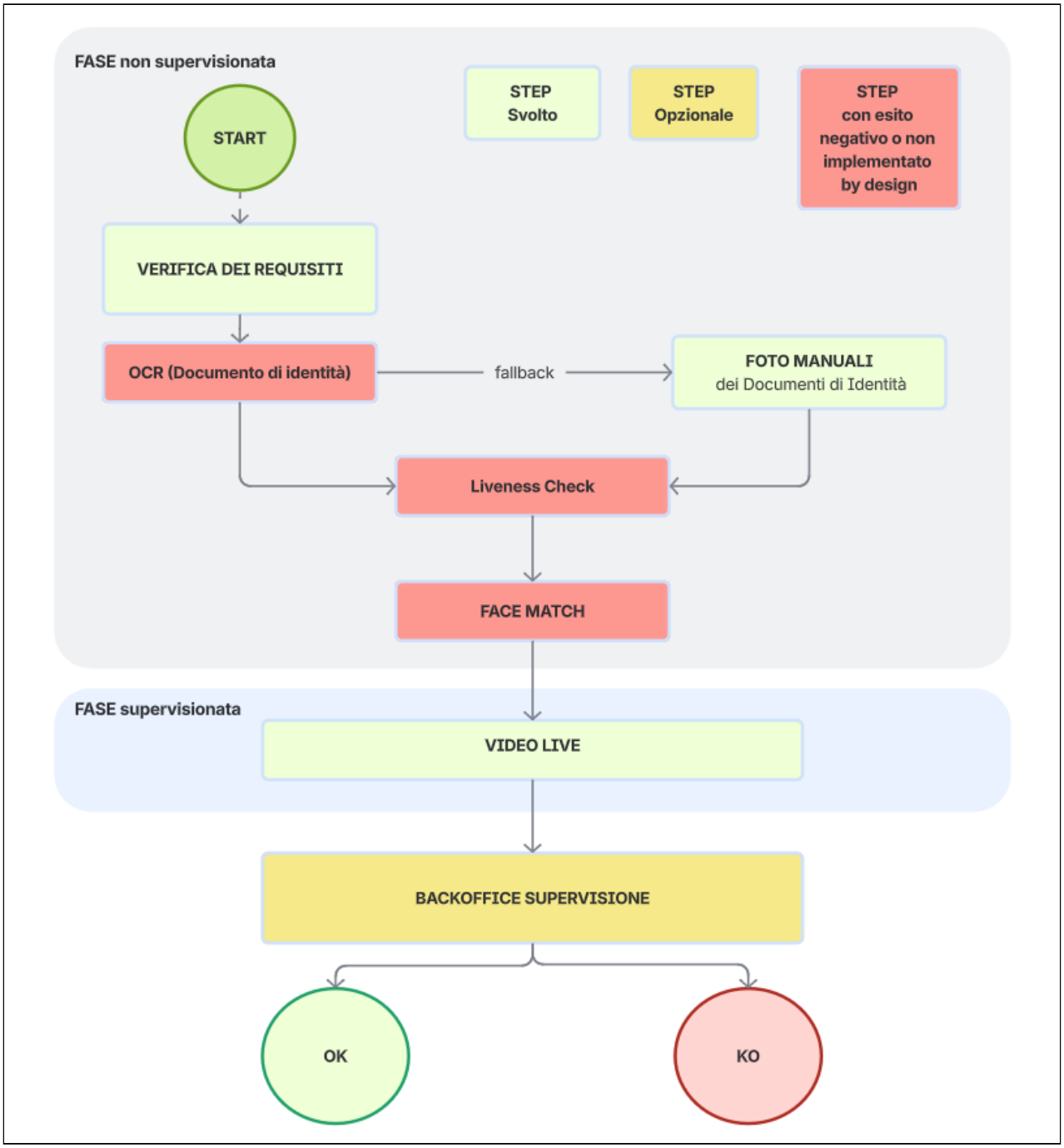
TocToc con Operatore - Variante A

3.2.1.2 “TocToc con Operatore” - Variante B

Operazione manuale con convalida e associazione al richiedente effettuate manualmente in tempo reale dal Registration Officer.

Presenza del richiedente	Operazione	Clausola dell'ETSI 119 461	Documento di identità	Validazione delle evidenze	Associazione al richiedente	LoIP
Da remoto supervisionata	Manuale	9.2.2.2	Fisico	Manuale	Manuale	Baseline

In caso di esito negativo o mancata implementazione by design di tecnologie di face matching e di tutti gli strumenti automatici per la verifica delle evidenze, le operazioni di verifica delle evidenze e di associazione al richiedente saranno svolte manualmente dal Registration Officer.



TocToc con Operatore - Variante B

3.3 Utilizzo di mezzi di identificazione elettronica (eID means)

3.3.1 “TocToc SPIDGO”

La soluzione “**SPIDGO**” fornisce la struttura tecnologica necessaria per esporre in modo semplice e immediato i servizi in rete tramite l’autenticazione con SPID e supporta le principali incombenze amministrative di adesione al circuito SPID – AgID / Entra con CIE – MinInt. Con la soluzione SpidGO, TocToc svolge, quindi, il ruolo di intermediario amministrativo e tecnologico tra i Service Provider (SP aggregati) e gli Identity Provider (IdP) agevolando l’ingresso, nelle federazioni SPID/CIE, di tutte le aziende che espongono servizi attraverso un portale di Single-Sign-On (SSO) e che desiderano rendere accessibili alla propria clientela anche attraverso l’autenticazione SPID/CIE.

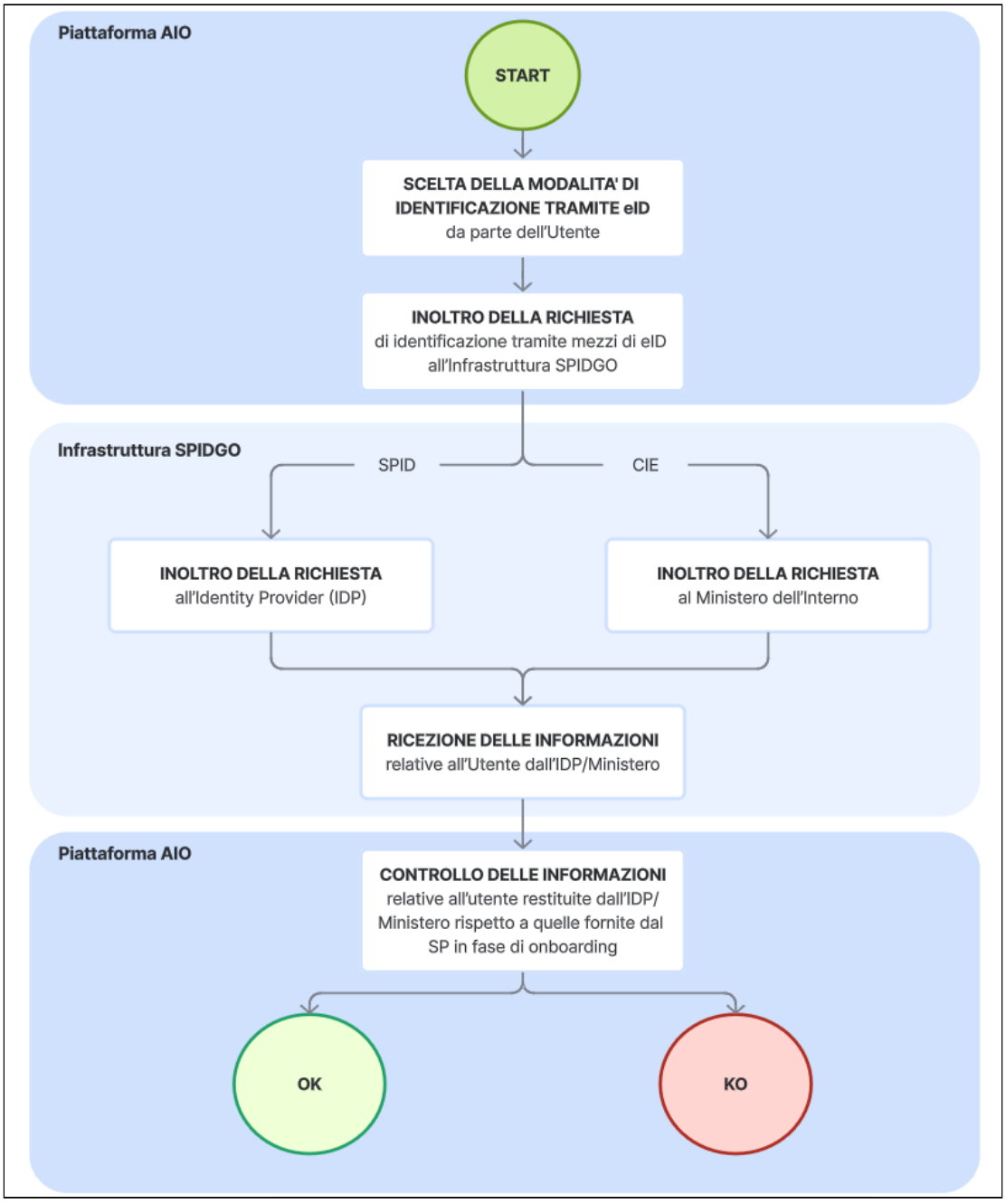
Per potersi autenticare mediante un mezzo di identificazione elettronica, è richiesto che l’eID utilizzato sia conforme almeno al livello di garanzia *substantial*. Questo significa che sono accettati esclusivamente SPID o CIE con un livello di sicurezza pari o superiore al livello 2.

Con SPIDGO l’utente si identifica da remoto, in modo sicuro e veloce, attraverso la login tramite SPID (Sistema Pubblico di Identità Digitale) o lo schema “Entra con CIE” (Carta d'Identità Elettronica). Queste modalità di autenticazione prevedono che:

1. L'utente acceda in Piattaforma AIO online attraverso il portale del Service Provider e selezioni l'opzione di login tramite mezzi di eID.
2. L’utente venga reindirizzato a una pagina di autenticazione sicura, dove potrà effettuare il login tramite il proprio Identity Provider SPID o la propria CIE.
3. Il sistema riceva i dati dell’utente e, se tutto corrisponde, ne consenta l’utilizzo durante la prosecuzione del processo digitale.

La verifica dell’identità quindi è totalmente automatizzata, e viene controllato automaticamente anche che il codice fiscale restituito come attributo dell’identificazione corrisponda al codice fiscale fornito dall’utente in fase di onboarding.

Presenza del richiedente	Operazione	Clausola dell'ETSI 119 461	Mezzo di Identificazione Elettronica	Validazione delle evidenze	Associazione al richiedente	LoIP
Non specificato ma tramite mezzi di identificazione elettronica	Automatica	9.2.4	Entra con CIE SPID	Automatica	Automatica	Baseline (se SPID/CIE Liv.2) Extended (se con SPID/CIE Liv.3)



TocToc SPIDGO

3.4. Matrice dei Processi TocToc

La piattaforma TocToc AIO dispone di audit trail per ogni decisione e registra quale modalità è stata utilizzata per verificare l'identità.

Presenza del richiedente	Operazione	Processo TocToc	Documento di identità	Validazione delle evidenze	Associazione al richiedente	LoIP
Da remoto supervisionata	Manuale	Con Operatore - Variante B	Fisico	Manuale	Manuale	Baseline
	Ibrida	Con Operatore - Variante A	Fisico	Manuale e automatica	Manuale	Extended
	Ibrida	Con Operatore	Fisico	Manuale e automatica	Manuale e automatica	Extended
Da remoto non supervisionata	Manuale	Selfie - Variante B	Fisico	Manuale	Manuale	Baseline
	Ibrida	Selfie - Variante A	Fisico	Manuale e automatica	Manuale	Baseline
	Ibrida	Selfie	Fisico	Manuale e automatica	Manuale e automatica	Extended
Tramite mezzo di identificazione elettronica	Automatica	SpidGo	N.A. “Login SPID” “Entra con CIE”	Automatica	Automatica	Baseline/ Extended

3.5 Irrobustimento dei processi di Identity Proofing

Qualunque sia il flusso di attività svolte, su base opzionale è possibile irrobustire l’identity proofing con moduli aggiuntivi antifrode da concordare volta per volta con il Cliente.

- **SCIPAFI (implementato)**: l’integrazione con il Sistema di Cooperazione Interforze per la Prevenzione delle Frodi Identitarie (SCIPAFI) permette di interrogare, nel rispetto

delle finalità antifrode e dei principi di proporzionalità e minimizzazione, le banche dati della pubblica amministrazione (es. ANPR, codice fiscale, anagrafe tributaria) per contrastare l'uso di identità fittizie o rubate.
- **CRIMNET (implementato)**: il controllo del numero del documento di identità nell'archivio dei documenti rubati e/o smarriti consiste nell'interrogare il database messo a disposizione della Polizia di Stato generando, come evidenza, lo step nel file di audit.

3.6 Codifica dei caratteri e normalizzazione degli attributi

Tutti i dati anagrafici acquisiti e gestiti nel corso del processo di identity proofing sono trattati utilizzando il set di caratteri **UTF-8** (Unicode Transformation Format – 8 bit), in conformità alle buone prassi internazionali per l'interoperabilità e la rappresentazione corretta di caratteri speciali, accenti, simboli e lettere di alfabeti estesi.

La codifica UTF-8 è applicata a:

- dati acquisiti tramite moduli digitali o interfacce utente;
- dati estratti tramite OCR dai documenti d'identità;
- evidenze e record salvati nei sistemi di log, nei report e nelle basi dati;
- esportazioni e scambi dati verso i Clienti o altri soggetti autorizzati.

Durante il processo di verifica e validazione anagrafica, possono emergere differenze nei dati identificativi dell'utente, legate a:

- errori di battitura o trascrizione, soprattutto nei dati OCR;
- presenza di nomi o cognomi doppi non sempre coerenti tra documento e dichiarazione dell'utente o dalle informazioni derivanti da fonti esterne;
- uso o assenza di accenti, caratteri speciali o segni diacritici;
- forme abbreviate, inversioni o variazioni grafiche (es. "Di Giovanni" vs "Digiovanni").

Tali difformità vengono gestite, in backoffice dai Registration Officer, secondo logiche di tolleranza controllata concordate caso per caso con il Cliente, sulla base degli specifici requisiti del servizio richiesto.

3.7 Parti interessate e responsabilità

Parte Interessata	Descrizione	Responsabilità	Aspettative e Relazione con il Servizio
Cliente (Service Provider)	Organizzazione che richiede l'esecuzione del processo di identity proofing per abilitare i propri utenti finali all'accesso a un servizio.	Definisce i requisiti del processo, riceve l'esito dell'identificazione, fornisce informativa e base giuridica al trattamento dei dati, mantiene la relazione contrattuale con l'utente finale.	Fornitura di un processo conforme, tracciabile, auditabile e adattabile ai propri flussi di onboarding e accesso digitale.
Utente (Soggetto da identificare)	Persona fisica che si sottopone al processo di identificazione per accedere a un servizio online.	Fornisce dati veritieri, segue le istruzioni, collabora all'identificazione; accetta termini del servizio e privacy policy.	Accesso agevole, chiaro e sicuro al servizio richiesto tramite un processo trasparente e tutelato.
Ministero dell'Interno / CIE (Entra con CIE)	Autorità che gestisce l'infrastruttura di autenticazione tramite Carta d'Identità Elettronica (CIE).	Eroga e certifica il sistema di autenticazione tramite CIE; garantisce affidabilità, disponibilità e sicurezza del sistema.	Interoperabilità e corretto utilizzo dell'infrastruttura di autenticazione da parte del TSP, secondo i protocolli ufficiali.
AgID (SPID)	Agenzia per l'Italia Digitale, responsabile del sistema pubblico di identità digitale.	Vigila sulla corretta integrazione con SPID; fornisce specifiche tecniche e regolamentari.	Conformità del servizio all'ecosistema SPID, anche in termini di sicurezza, trasparenza e auditabilità.
Identity Provider (per SPID)	Entità accreditate presso AgID che gestiscono l'autenticazione SPID.	Eseguono l'autenticazione SPID su richiesta del nostro sistema tramite SPID Proxy o SPID SSO.	Utilizzo corretto del protocollo SPID, mantenimento dell'identità federata, tracciabilità delle richieste.
Amazon Rekognition	Servizio cloud utilizzato per operazioni automatizzate per rendere più sicura l'identificazione remota.	Fornisce capacità computazionale e algoritmi di intelligenza artificiale per confronti biometrici. È integrato tramite API.	Corretta configurazione e uso del servizio in modo conforme alla normativa privacy e sicurezza delle informazioni.

Parte Interessata	Descrizione	Responsabilità	Aspettative e Relazione con il Servizio
Regula Forensic	Fornitore di tecnologia OCR per l'estrazione automatica dei dati dai documenti d'identità.	Eroga funzionalità di lettura e validazione dei documenti. I modelli sono integrati via SDK/API.	Precisione, affidabilità ed efficienza nella lettura dei dati anagrafici e documentali.
ODR – Officer di Registrazione	Personale interno o incaricato, addetto alla verifica manuale delle evidenze (nei processi asincroni) o alla conduzione diretta del processo (nei processi sincroni).	Convalida i dati acquisiti e le evidenze biometriche/documentali; determina l'esito dell'identificazione; opera secondo policy interne e audit trail tracciato.	Processi di verifica standardizzati, tracciabili e conformi a quanto definito nelle procedure interne e nel presente IPPS.
DPO (Responsabile della Protezione dei Dati)	Figura designata ai sensi del GDPR.	Sorveglia la conformità al GDPR, valuta impatti privacy (DPIA), supporta nella gestione dei diritti degli interessati.	Garanzia del rispetto dei principi di liceità, minimizzazione, accountability e tutela dei dati trattati durante l'identificazione.
Fornitori infrastrutturali	Provider di servizi tecnologici sottostanti	Erogano servizi infrastrutturali su cui poggiano i servizi.	Continuità operativa, protezione dei dati, SLA adeguati. Oggetto di due diligence e valutazione terze parti.
ACN (Agenzia per la Cybersicurezza Nazionale)	Autorità italiana competente per la supervisione dei servizi cloud fiduciari e qualificati.	Controlla e qualifica i servizi digitali secondo regolamenti specifici.	Ricezione tempestiva di notifiche di sicurezza, auditabilità, rispetto dei criteri di qualifica.
Autorità Giudiziaria o Forze dell'Ordine	Autorità competenti per indagini penali o attività giudiziarie connesse alla verifica dell'identità degli utenti o all'uso fraudolento del servizio.	Possono richiedere, nei limiti di legge, l'accesso a dati e registrazioni rilevanti ai fini investigativi o probatori.	Ricevere collaborazione nei termini previsti dalla normativa vigente salvaguardando la riservatezza e l'integrità del sistema.

Parte Interessata	Descrizione	Responsabilità	Aspettative e Relazione con il Servizio
Garante per la Protezione dei Dati Personali	Autorità nazionale di controllo per il rispetto della normativa sulla protezione dei dati personali (GDPR e Codice Privacy).	Può effettuare verifiche, ispezioni e richiedere documentazione relativa ai trattamenti svolti, compresi quelli connessi ai processi di identity proofing.	Garantire trasparenza, responsabilizzazione (accountability), disponibilità della documentazione e cooperazione in caso di richieste o procedimenti ispettivi.

Tutte le terze parti tecnologiche sono soggette a valutazione dei rischi, clausole contrattuali di sicurezza, e revisione periodica delle performance e dei livelli di servizio.

Gli ODR sono formati secondo procedure interne conformi a ETSI TS 119 461, inclusi aspetti di imparzialità, tracciabilità delle decisioni e segregazione dei ruoli.

4. Sicurezza

4.1 Sicurezza del processo

- **Tracciabilità e Notifica** all'operatore: Ciò vuol dire che al Registration Officer viene sempre notificato quando uno step di processo o un controllo specifico previsto ha dato esito negativo, affinché operi verifiche più approfondite anche attraverso l'esercizio di una checklist che si aggiorna dinamicamente in relazione agli esiti dei moduli precedenti.
- **Formazione dei Registration Officer**: i processi di identity proofing sono definiti e riassunti in un documento specifico che descrive puntualmente il flusso delle attività e i controlli da effettuare. Inoltre è stato realizzato un "Manuale di Analisi Morfologica" per fornire un approccio sistematico alla verifica dell'identità di un utente da remoto e per ridurre gli errori nelle operazioni manuali, e un "Manuale sui principali documenti di riconoscimento vigenti", consultando la fonte autoritativa del PRADO.
- **Controllo degli accessi e privilegi**: l'accesso ai dati personali è permesso solamente agli amministratori del tenant del Cliente TocToc. I Registration Officer hanno accesso esclusivamente alle informazioni relative alle pratiche da effettuare e solamente per il tempo necessario a sancirne un esito.
- **Casualità nell'assegnazione delle pratiche**: la singola pratica di identity proofing viene assegnata casualmente tra i Registration Officer in servizio.
- **OCR**: il servizio consente agli utenti di acquisire le foto dei propri documenti di identità, ad esempio la carta d'identità o il passaporto, utilizzando la webcam del proprio dispositivo in modo da poterle utilizzare per la verificare della propria identità. Il sistema offre inoltre funzionalità di riconoscimento automatico dei documenti (OCR), che consentono di verificare che i documenti di identità siano formalmente validi e che soddisfino i requisiti necessari. Questo significa che il sistema è in grado di analizzare automaticamente le immagini acquisite e di estrarre informazioni come nome, data di nascita, numero di documento e altri dettagli importanti, oltre che effettuare controlli anticontraffazione basandosi su tecniche visuali. L'estrazione automatica dei dati, grazie anche al modulo MRZ e BARCODE, garantisce maggiore precisione e affidabilità riducendo di molto la possibilità di

errori umani durante la digitazione dei dati rendendo il processo di verifica dell'identità ancora più veloce e affidabile.
Per fare questo la piattaforma integra i servizi di Regula Forensic, azienda impegnata da oltre 30 anni nell'affinare tecnologie e soluzioni in grado di automatizzare i processi relativi alla verifica e all'esame dei documenti di identità nel mondo.

- **Verifica dei documenti di identità rubati o smarriti**: l'aggiunta di moduli come Crimnet e SCIPAFI, permette di verificare in tempo reale la validità dei documenti di identità, identificando se sono stati segnalati come scaduti, rubati o smarriti. Questa integrazione garantisce una maggiore sicurezza nei processi che richiedono l'identificazione, riducendo il rischio di utilizzo di documenti non validi o compromessi. Inoltre, questo servizio ottimizza l'efficienza operativa, consentendo verifiche affidabili e conformità normativa.
- **Audit Trail e log**: ogni passo del processo di identificazione viene registrato e monitorato per garantire trasparenza e tracciabilità.

4.1.1 Verifica biometrica e rilevamento di vitalità

Il processo di riconoscimento dell'identità integra funzionalità automatizzate di **face matching** e di **liveness detection**, basate sul servizio **Amazon Rekognition**. Queste funzionalità sono impiegate per:

- Verificare la corrispondenza biometrica tra il volto dell'utente e la fotografia contenuta nel documento d'identità,
- Rilevare ed escludere tentativi di attacco tramite presentazione (PAD – Presentation Attack Detection).

4.1.1.1 Face Liveness

Amazon Rekognition Face Liveness impiega tecniche attive e passive di PAD per rilevare ed evitare attacchi come:

- Foto stampate o su schermo,
- Riproduzioni video,
- Maschere 3D (silicone, lattice, contornate),

- Contenuti generati artificialmente (deepfake, animazioni 3D).

Il servizio è stato sottoposto a test indipendenti da parte di **iBeta**, laboratorio accreditato NIST, in conformità alla norma **ISO/IEC 30107-3**. I test di livello 1 e 2 hanno valutato l'efficacia del sistema contro diversi tipi di attacchi.

I risultati dei test condotti da iBeta su Amazon Rekognition Face Liveness sono i seguenti:

Parametro	Descrizione	Valore rilevato (confidence threshold ≥ 50)
True Rejection Rate (TRR)	percentuale di attacchi correttamente respinti dal sistema di liveness.	**100%**
True Acceptance Rate (TAR)	percentuale di utenti legittimi correttamente accettati dal sistema di liveness.	**100%**

Parametro	Descrizione	Valore rilevato (confidence threshold ≥ 50)
APCER (Attack Presentation Classification Error Rate)	Percentuale di attacchi accettati erroneamente come validi	**0%**
BPCER (Bona Fide Presentation Classification Error Rate)	Percentuale di utenti legittimi respinti erroneamente	**0%**

4.1.1.2 Face Matching

Amazon Rekognition è stato sottoposto a una valutazione indipendente da parte di iBeta, laboratorio accreditato NIST, mediante l'utilizzo di un dataset per la verifica dell'identità contenente immagini suddivise in sei gruppi demografici distinti secondo criteri di tonalità della pelle e genere.

L'analisi ha evidenziato quanto segue:

Parametro	Descrizione	Valore minimo osservato tra i 6 gruppi (soglia di similarità impostata = 95)
True Match Rate (TMR)	Percentuale di coppie di immagini appartenenti alla stessa persona correttamente riconosciute come corrispondenti dal sistema.	99,97185%
True Non-Match Rate (TNMR)	Percentuale di coppie di immagini appartenenti a persone diverse correttamente identificate come non corrispondenti dal sistema.	99,99988%
Parametro	**Descrizione**	**Valore minimo osservato tra i 6 gruppi (soglia di similarità impostata = 95)**
False Rejection Rate (FRR)	Percentuale di coppie di immagini della stessa persona che il sistema non riconosce come corrispondenti (cioè falsi negativi).	0,02815%
False Acceptance Rate (FAR)	Percentuale di coppie di immagini di persone diverse che il sistema identifica erroneamente come corrispondenti (cioè falsi positivi).	0,00012%

Tali risultati dimostrano che il sistema mantiene un'elevata affidabilità e accuratezza senza variazioni significative in funzione del gruppo demografico.

4.2 Sicurezza della Piattaforma, del Servizio e dei dati trattati

La sicurezza è garantita attraverso un approccio olistico che integra misure tecniche, organizzative e operative volte a tutelare la riservatezza, l'integrità e la disponibilità delle informazioni. Tali misure comprendono la sicurezza delle infrastrutture, la protezione applicativa, la gestione dei privilegi e degli accessi, il monitoraggio continuo, la sicurezza dei processi e la formazione del personale. Una descrizione dettagliata delle misure implementate è disponibile nel *Whitepaper sulla Sicurezza*[7], che costituisce parte integrante della documentazione di conformità e disponibile nella sua versione sempre aggiornata.

7. https://www.toctoc.me/white-paper-sulla-sicurezza/

5. Conclusioni

TocToc si impegna a garantire l'erogazione di servizi di identity proofing in conformità ai regolamenti e agli standard di cui al paragrafo 1.1, e a mantenere la riservatezza, l'integrità e la disponibilità dei dati e delle informazioni relativi a suddetti processi, nonché a garantire i diritti degli utenti relativamente ai propri dati in conformità con il GDPR.

ALLEGATI

Allegato A - Persona legale e Persona naturale che rappresenta Persona legale

Allegato A - Persona legale e Persona naturale che rappresenta Persona legale

Questo documento descrive le modalità attraverso cui TocToc eroga il proprio servizio di verifica dell'identità per persona legale (9.3 del TS 119 461), e per persona naturale che rappresenta una persona legale (9.4 del TS 119 461), conformemente ai requisiti di:

- ETSI TS 119 461
- ETSI EN 319 401
- Regolamento UE 910/2014 (eIDAS) e successive modifiche e integrazioni come da Regolamento UE 1183/2024 (eIDAS2)
- Regolamento di Esecuzione UE 2022/1502
- Regolamento Generale sulla Protezione dei Dati (GDPR)

A.1 - Verifica dell'identità della persona legale e della persona naturale che rappresenta la persona legale

A.1.1 Iniziazione

Viene ricevuta dalla Piattaforma una richiesta di identificazione per registrazione o accesso a un servizio digitale per conto di una persona legale. Si specifica che è necessario che il Richiedente sia una persona naturale munita di necessari poteri di rappresentanza nei confronti della persona legale per la quale intende avanzare la richiesta di identificazione. La coerenza e la sussistenza di tali poteri è oggetto di verifica del presente processo di identificazione.

A.1.2 Raccolta di attributi ed evidenze

Per la **persona legale**, gli attributi necessariamente richiesti per l'identificazione sono: paese di registrazione, denominazione dell'azienda, forma societaria, codice unico identificativo (Partita IVA).

Per la **persona naturale che agisce per conto della persona legale**, gli attributi e le evidenze necessariamente richiesti, sono definiti e raccolti come descritto al Capitolo 3 dell'Identity Proofing Practice Statement.

La raccolta di attributi avviene su **input diretto** del Richiedente tramite la compilazione di campi strutturati relativi agli attributi identificativi obbligatori come sopra definito, o **attraverso l'integrazione** con i sistemi del Cliente.

A.1.3 Validazione di attributi ed evidenze

Per la **persona legale,** viene verificata la correttezza degli attributi raccolti dall'interrogazione di OPENAPI (una soluzione SaaS che aggrega e valida dati da fonti autorevoli in tempo reale), verificando l'esistenza legale dell'impresa e che la stessa non risulti in stato di fallimento o liquidazione o in altra condizione che la renda non attiva, secondo quanto stabilito dal Regolamento 2022/1502.

La validazione di evidenze e attributi per persona naturale che agisce per conto della persona legale, viene effettuata come descritto al Capitolo 3 dell'Identity Proofing Practice Statement.

A.1.4 Associazione al Richiedente

Si conferma il collegamento tra le evidenze raccolte e la persona legale oggetto dell'identificazione, confrontando i dati presentati in fase di onboarding e i dati restituiti da OPENAPI.

L'associazione al Richiedente per la persona naturale che agisce per conto della persona legale, è descritta al Capitolo 3 dell'Identity Proofing Practice Statement.

Infine, si verifica che la persona naturale che ha presentato richiesta di identificazione per conto della persona legale abbia i necessari poteri di rappresentanza. Il servizio Company Full di OPENAPI permette di verificare se il codice fiscale del Richiedente, fornito in onboarding, compare tra i codici fiscali dei rappresentanti legali dell'impresa nelle fonti autoritative.

A.1.5 Emissione dell'esito

Una volta completato il processo di validazione e associazione, il sistema emette il risultato dell'identity proofing. Se positivo, al Richiedente viene concesso l'accesso al servizio per cui è stato effettuato l'identity proofing, altrimenti il Richiedente viene notificato del fallimento e in caso di KO ripetibile viene richiesto di ripetere il processo.

Il livello di identity proofing (LoIP) garantito dai processi TocToc per persona legale, è extended.

Il livello di identity proofing (LoIP) garantito dai processi TocToc per persona naturale che agisce per conto di una persona legale, eredita il LoIP raggiunto dal processo di identity

proofing per persona naturale, come descritto al Cap. 4 dell'Identity Proofing Practice Statement.