Intesa
An IBM Company

Dall’acquisto dell’auto al finanziamento: il processo full digital di FCA bank

Self Onboarding

Torino, 22 maggio 2020

Documento sviluppato e concordato da Intesa con il cliente FCA Bank per candidatura Digital360 Awards

Intesa framework

Come sviluppiamo e implementiamo l'innovazione digitale:

CENTRI DI COMPETENZA

User Experience

Legal & Compliance

Biometrics

AI
Blockchain
IoT

salesforce DocuSign
Digital Signature

TECNOLOGIA

Microservices

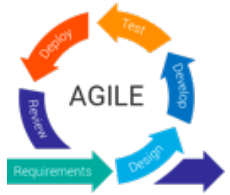
Kubernetes

Dockers

IBM Cloud

OPEN PLATFORM

METODOLOGIA



CO INNOVATE

FCA BANK

Composizione della piattaforma

Qualified Trusted Services

Identità Digitale

Autenticazione

Firma Elettronica

Archivio Legale

Governance

Internazionale

Configurabile

APIs

Evoluzione offerta

+

Blockchain

Artificial Intelligence

Analytics

Internet of Things

APIs/Microservizi

Self Onboarding – Descrizione

- Self Customer Onboarding supporta il processo di KYC di un nuovo cliente attraverso il rilascio di un'identità digitale che permette al cliente di interagire da remoto con la banca.

- La soluzione di Intesa è in grado di effettuare le seguenti attività:
- **Identificazione remota del cliente in modalità self**
- **Verifica di autenticità del documento d'identità**
- Controllo della **liveness**
- **Face recognition**
- **OCR** su documento d'identità

- Il risultato del processo KYC è l'identificazione sicura del cliente che può essere usata al fine di:
- **Rilascio di un certificato qualificato** valido per firmare digitalmente qualunque documento/contratto
- Rilascio di un certificato non qualificato per processi di firma elettronica avanzata

- L'attività di onboarding verrà registrata includendo la documentazione, pronta per la **conservazione a norma**. La soluzione è completamente personalizzabile, flessibile, compliant e totalmente integrabile con possibilità di welcome call e/o verifiche a posteriori

Self Onboarding – Punti di forza

Trasmissione di dati criptati

Dati acquisiti più velocemente

Totalmente compliant ai requisiti AGID e Banca d'Italia

Efficientamento delle attività di Back Office

Soluzione basata su micro-servizi

Processo totalmente personalizzabile

Combinazione di biometria, OCR e machine learning

FCA BANK

Contesto normativo – AML – V Direttiva

V direttiva 2018/843, Art. 13 c.1

Identificazione a distanza nella direttiva EU relativa alla prevenzione dell'uso del sistema finanziario a fini di riciclaggio o finanziamento del terrorismo

Ai fini della **lotta contro il riciclaggio di denaro e il finanziamento del terrorismo è essenziale identificare con precisione le persone fisiche** e giuridiche e verificarne i dati.
I più recenti sviluppi tecnici nel settore della digitalizzazione delle operazioni e dei pagamenti consentono una **identificazione** sicura elettronica o a **distanza.**

«Le misure di adeguata verifica della clientela consistono nelle attività seguenti: identificare il cliente e verificarne l'identità sulla base di documenti, dati o informazioni ottenuti da una fonte attendibile e indipendente, compresi, se disponibili, i mezzi di identificazione elettronica o i pertinenti servizi fiduciari di cui al regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio o altre procedure di identificazione a distanza o elettronica sicure, regolamentate, riconosciute, approvate o accettate dalle autorità nazionali competenti»

Contesto normativo – Banca d'Italia

Disposizioni in materia di adeguata verifica della clientela per il contrasto del riciclaggio e del finanziamento del terrorismo, presenti nel **provvedimento 30 Luglio 2019 Banca d'Italia**

Sezione VIII. Disposizioni specifiche in materia di operatività a distanza

Banca d'Italia, che ha il compito di individuare forme e modalità idonee all' acquisizione dei dati identificativi della Clientela, ritiene adeguata l'operatività a distanza tenendo conto dell'evoluzione delle tecniche oggi disponibili.
Per operatività a distanza si intende quella svolta senza la compresenza fisica.
Nei casi di operatività a distanza, la Banca o l'istituto finanziario:

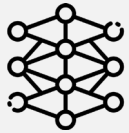
- Deve acquisire i dati identificativi del cliente e effettuarne il riscontro su una copia ottenuta in formato elettronico o con modalità analoghe di un valido documento di identità;
- Deve effettuare riscontri ulteriori sui dati acquisiti, secondo le modalità più opportune in relazione al rischio specifico (es. Welcome call).

Nel rispetto dell'approccio basato sul rischio, i destinatari possono utilizzare meccanismi di riscontro basati su soluzioni, tecnologiche innovative e affidabili (es., quelle che prevedono forme di riconoscimento biometrico), purché assistite da robusti presidi di sicurezza.

FCA Bank – Il processo di Self Onboarding

FCA Bank – Dettaglio processo Self Onboarding E2E (1/2)

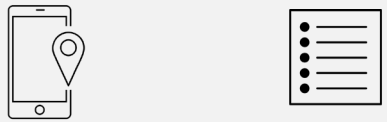
START

	Registrazione e Upload Documento (Web o App)	**OCR**	**Integrazione Anagrafica**	**Verifica Telefono/Mail**
Fattori chiave	▪ Inserimento dati personali e consenso al trattamento ▪ Upload documento ▪ Switch tra Web e App (tramite QR Code, link a cellulare, etc…)	▪ Riconoscimento tipologia documento tramite reti neurali ▪ Riconoscimento automatico dei dati tramite OCR e auto-compilazione maschera	▪ Integrazione eventuali informazioni mancanti ▪ Visualizzazione di una maschera con il riepilogo dei dati inseriti manualmente e riconosciuti dall'OCR	▪ Prima verifica contatti tramite OTP sms ▪ Successiva verifica contatti tramite OTP mail
Tecnologie	Reti neurali 	Motore OCR 	Motore OCR 	One Time Password 
Dettaglio	▪ L'upload del documento può avvenire da file in locale o tramite fotocamera		▪ Tra le informazioni mancanti: • Codice Fiscale • Dati di residenza/domicilio • ….	▪ L'OTP ricevuto viene inserito all'interno della maschera di navigazione, per confermare i contatti.

Il processo viene interamente registrato e tenuto in conservazione

FCA BANK

FCA Bank – Dettaglio processo Self Onboarding E2E (2/2)

	Verifica Documentale	Check Liveness	Face Matching	Firma Elettronica
Fattori chiave	▪ Verifiche di conformità del documento e accesso real-time a banche dati esterne ▪ Verifica incrociata di documentazione caricata ▪ Verifiche sul dispositivo (geolocalizzazione,..)	▪ Esecuzione di movimenti randomici con il volto	▪ Face matching tra selfie scattato dal soggetto e il documento caricato	▪ Firma elettronica della documentazione mediante OTP
Tecnologie	Geolocalizzazione Banche Dati 	Biometrics 	Biometrics 	One Time Password 
Dettaglio	▪ **Liste**: es. SCIPAFI, Watchlist, Blacklist, PEPs, Sanction List, Adverse Media Check ▪ **Check su documento**: detection, reference analysis, font usage & consistency, check MRZ, …	▪ I movimenti verranno comunicati in sequenza nella schermata e tramite l'audio del dispositivo.	▪ Il soggetto scatta una foto del volto e il software effettua il face matching tra il documento caricato e il selfie scattato tramite algoritmo biometrico.	▪ Il profilo di rischio del cliente è stato completato ▪ Il cliente può procedere alla firma della documentazione con firma elettronica

Il processo viene interamente registrato e tenuto in conservazione

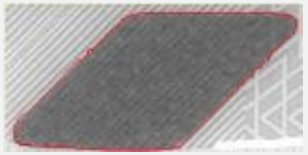
FCA BANK

Esempio di verifica documentale

Reference Analysis

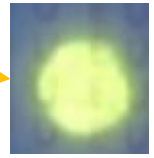
Image obtained

Referred Image



Consistency

Detection & Counting



Chip vs Card

Documenti supportati

- Tessera sanitaria
- Buste paga
- Ricevute presentazione dichiarazione dei redditi
- Carta d'identità Elettronica e Cartacea
- Patente
- Passaporto
- Codice Fiscale
- Permessi di soggiorno
- Visure Camerali
- ….

Possibili ulteriori check

- Human Face Detection
- Portrait Color
- Positioning & Integration
- Signature Know Font
- Font Usage & Consistency
- BIO/MRZ Data Comparison
- Verifiche su dispositivo utilizzato (manomissioni, coerenza con geolocalizzazione)
- Verifica incrociata di documentazione caricata (es. residenza)
- ….

FCA BANK