

## Lesson 6: Digital Identity and Authentication

### Module 1: FinTech Fundamentals

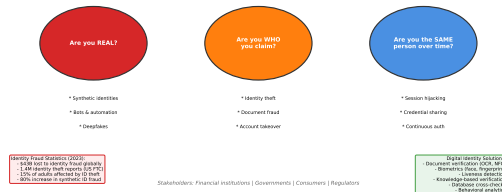
Digital Finance

## Identity Verification Problem

- 1.7B unbanked adults
- Lack of identity documents
- Fraud losses: **\$5.8B** (2023)
- Remote onboarding need

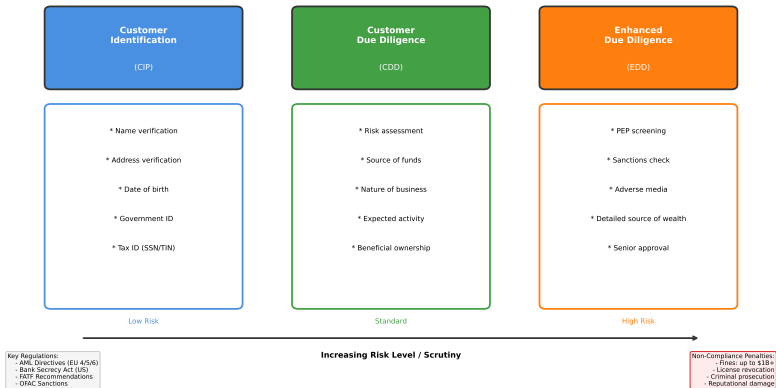
## The Digital Identity Challenge

How do you prove who you are online?



Source: Javelin Strategy, FTC Consumer Sentinel Network (2023)

## Know Your Customer (KYC) Framework

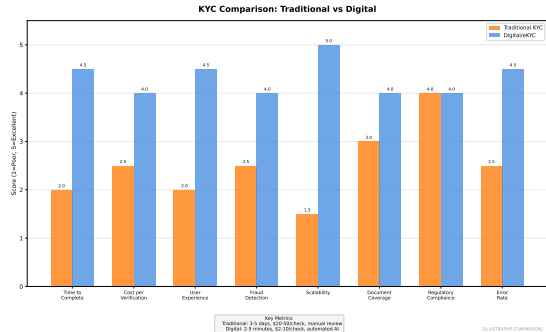


Source: FATF Guidelines, AML regulatory frameworks

# Traditional vs Digital KYC

## Process Comparison

- Traditional: 7-14 days
- Digital: 5-10 minutes
- Cost: **\$60 vs \$5**
- Drop-off: 40% vs 15%



## EU Digital Identity

- Electronic ID recognition
- Trust services regulation
- Cross-border validity
- Three assurance levels

### eIDAS: EU Electronic Identification & Trust Services

Regulation (EU) No 910/2014 + eIDAS 2.0 (2024)

#### Electronic Identification (eID)

- \* National eID schemes notification
- \* Mutual recognition across EU
- \* Assurance levels (Low/Substantial/High)
- \* eID Node interoperability
- \* EU Digital Identity Wallet (eIDAS 2.0)

#### Trust Services

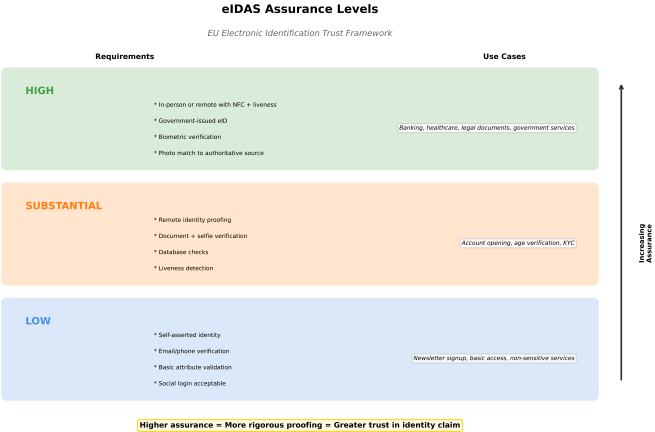
- \* Electronic signatures (QES)
- \* Electronic seals
- \* Time stamps
- \* Registered delivery
- \* Website authentication (QRNC)

#### eIDAS 2.0 Key Changes (2024)

EU Digital Identity Wallet | Verifiable credentials | Remote identity proofing | Private sector acceptance mandate

All EU citizens enrolled to a digital wallet by 2026

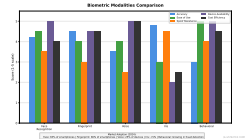
Source: EU Regulation 910/2014, eIDAS 2.0 (2024)



Source: EU Regulation 910/2014, Implementing Regulation 2015/2502

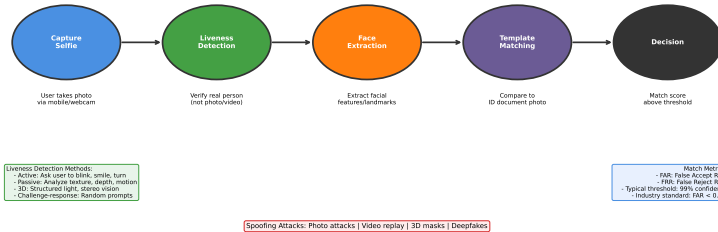
## Modalities

- Fingerprint: 99.8% accuracy
- Face recognition: 99.5%
- Iris scan: 99.99%
- Voice: 95% accuracy



Source: [Unreadable]

## Facial Recognition Verification Flow



[CONCEPTUAL PROCESS FLOW]



## Anti-Spoofing

- Active: User actions
- Passive: Texture analysis
- 3D depth sensing
- Challenge-response

### Liveness Detection Methods

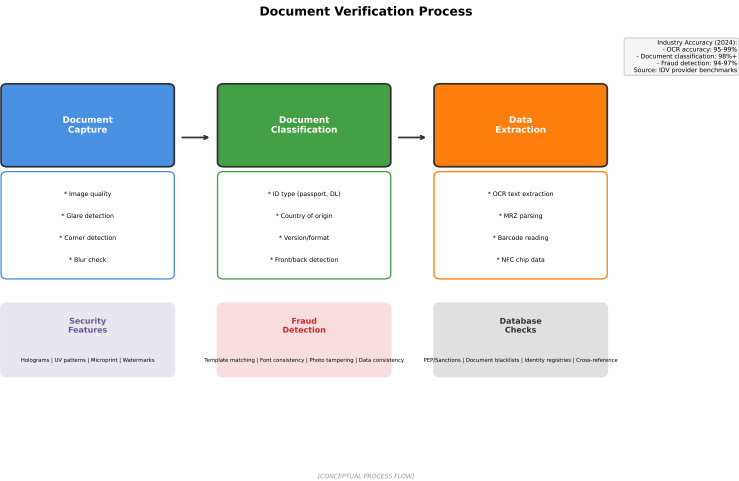
Preventing Presentation Attacks



Aspect	Active	Passive
User friction	Higher	Lower
Time required	5-15 sec	1-3 sec
Spoof resistance	High	Medium-High
Accessibility	Limited	Better
Drop off rate	10-20%	2-5%

Common Attacks: Photo attacks | Video replay | 3D masks | Displays | Screen replay

Source: Industry liveness detection standards (ISO/IEC 30107)



## Automated Extraction

- Optical character recognition
- Machine-readable zone (MRZ)
- NFC chip data (ePassports)
- Security features check

## Document Data Extraction: OCR vs NFC

OCR (Optical Character Recognition)		NFC (Near Field Communication)	
1. Image Capture	Camera captures document	1. Chip Detection	Phone detects NFC chip
2. Pre-processing	Denoise, noise reduction	2. BAC/PACE Auth	Authenticate with MRZ data
3. Text Detection	Locate text regions	3. Data Read	Extract chip data groups
4. Character Recognition	ML-based text extraction	4. Active Auth	Verify chip authenticity
5. MRZ Parsing	Machine Readable Zone decode	5. Passive Auth	Validate digital signatures
6. Validation	Check digit verification	6. Clone Detection	Verify chip is original

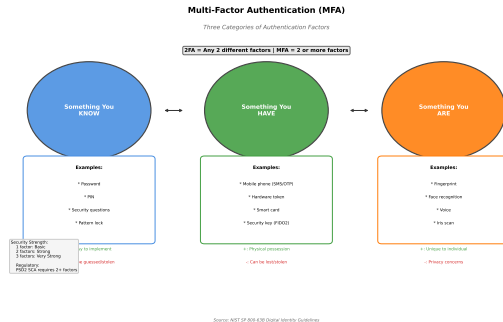
Metric	OCR	NFC
Accuracy	85-90%	100%
Security	Medium	Very High
User effort	Take photo	Tap phone
Device req.	Camera	NFC-enabled
Scalability	High	Low
Best Practice	Combine OCR + NFC for maximum security and accuracy	

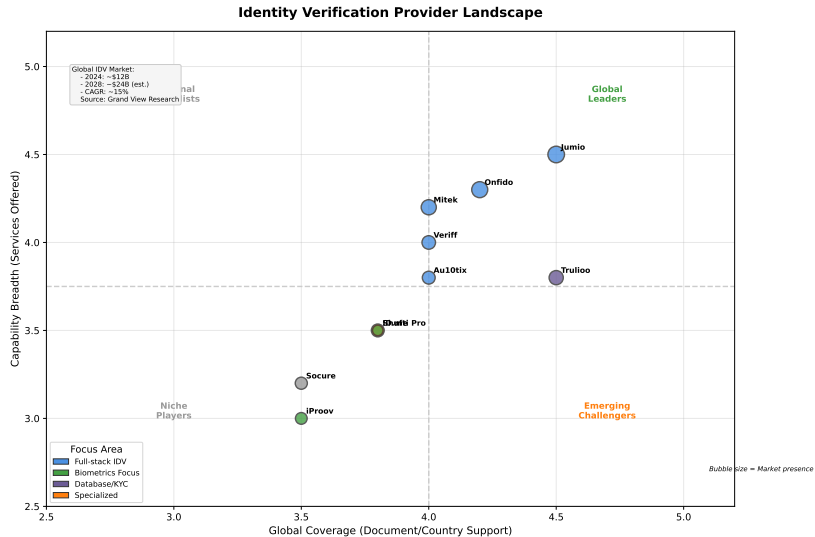
Source: ICAO 9303 Machine Readable Travel Documents, ePassport specifications

# Multi-Factor Authentication (MFA)

## Authentication Factors

- Knowledge: Password/PIN
- Possession: OTP token
- Inherence: Biometric
- Reduces fraud 99.9%

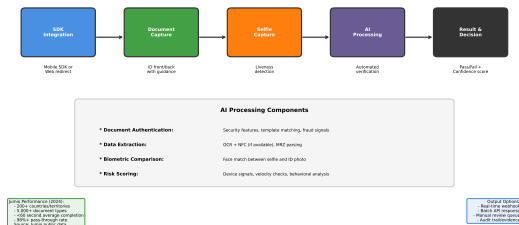




## AI-Powered KYC

- 1B+ verifications
- 5 minute verification
- 95% automation rate
- 200+ countries

### Identity Verification Workflow (Jumio Example)

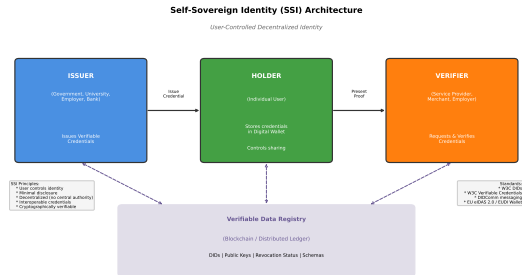


Source: Jumio product documentation (2024)

# Self-Sovereign Identity (SSI)

## Decentralized Model

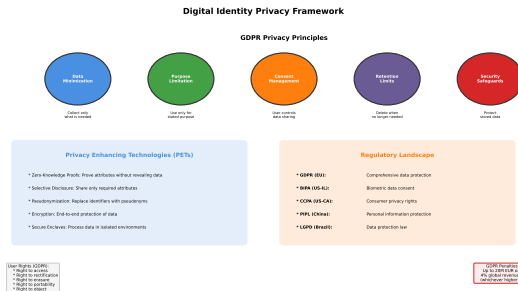
- User controls credentials
- Blockchain-based
- Verifiable credentials
- Privacy-preserving



Source: W3C Decentralized Identifiers (DIDs), Verifiable Credentials Data Model

## Data Protection

- GDPR compliance
- Biometric template storage
- Data minimization
- Right to erasure



Source: GDPR (EU) 2016/679, NIST Privacy Framework



## Global Digital Identity Landscape

National Digital ID Systems by Region (2024)

### Europe

- \* eIDAS/EUDI Wallet (EU)
- \* BankID (Nordics)
- \* Itsme (Belgium)

70%+ adult population

### Asia-Pacific

- \* Aadhaar (India) - 1.3B
- \* MyKad (Malaysia)
- \* SingPass (Singapore)

Highest biometric coverage

### Americas

- \* Login.gov (US-partial)
- \* Gov.br (Brazil)
- \* Digital ID (Canada-pilot)

Fragmented adoption

### Africa

- \* NIMC (Nigeria)
- \* Smart ID (South Africa)
- \* Huduma Namba (Kenya)

Growing mobile-first

### Middle East

- \* UAE Pass
- \* Absher (Saudi)
- \* Smart Qatar

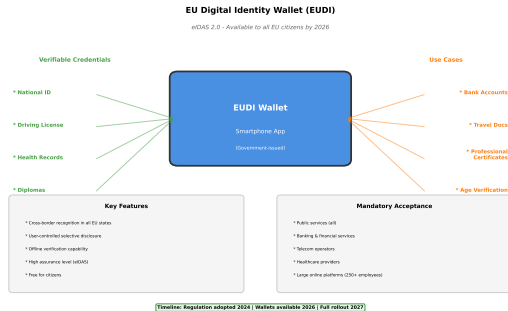
High gov adoption

Global Statistics (2024):  
- 5B+ people have digital ID  
- 1B+ still lack legal identity  
- \$30B+ market by 2028  
Source: World Bank ID4D, McKinsey

Source: World Bank ID4D Global Dataset 2024, Regional government sources

## EU Digital Identity Wallet

- eIDAS 2.0 mandate
- 2026 rollout target
- Universal EU acceptance
- Private sector integration



Source: European Commission, eIDAS 2.0 Regulation (EU) 2024/1183

- **KYC:** Digital verification reduces cost 90% and time 95%
- **eIDAS:** EU framework for cross-border identity
- **Biometrics:** Face + liveness detection standard approach
- **MFA:** Multi-factor prevents 99.9% of fraud
- **Future:** Self-sovereign identity and digital wallets