Lesson 6: Digital Identity and Authentication

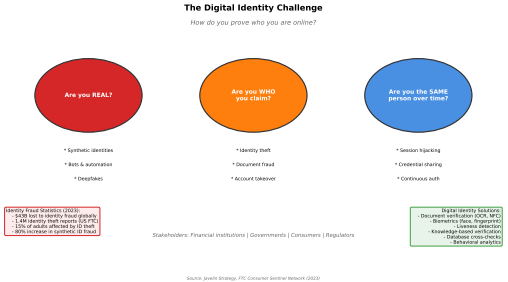
Module 1: FinTech Fundamentals

Digital Finance

Digital Identity Challenge

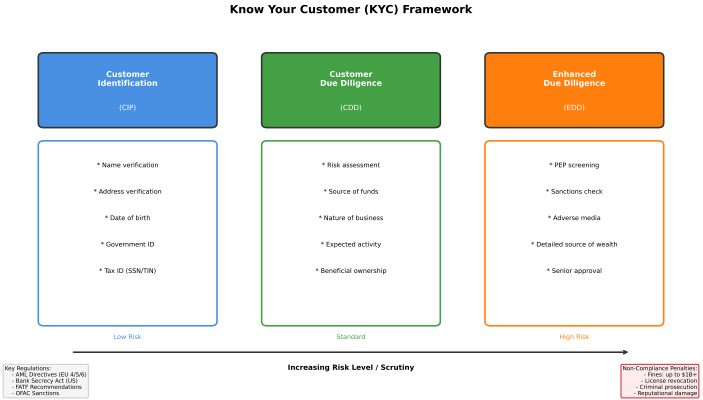
Identity Verification Problem

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



1.7 billion adults remain unbanked—identity verification is the primary barrier to financial inclusion.

KYC Regulatory Requirements

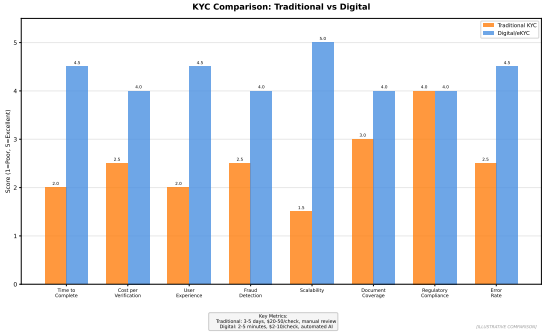


KYC is legally mandated for all financial institutions—FATF, AMLD, and BSA set global standards.

Traditional vs Digital KYC

Process Comparison

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

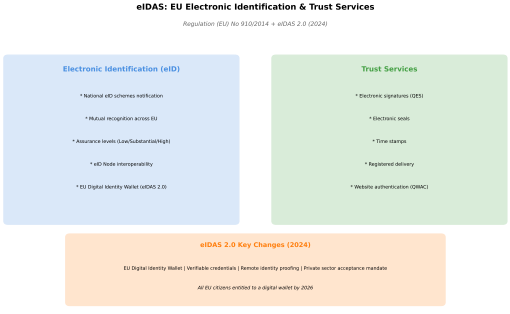


Digital KYC reduces verification time from 7-14 days to 5-10 minutes—at 90% lower cost.

eIDAS Framework

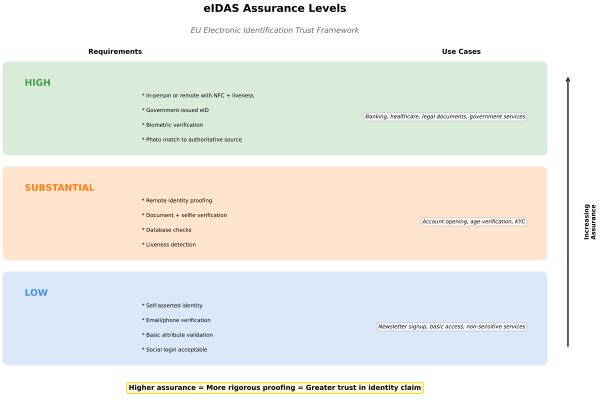
EU Digital Identity

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



eIDAS enables cross-border electronic identity recognition across all 27 EU member states.

eIDAS Assurance Levels

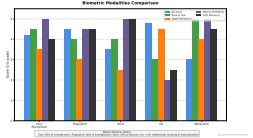


Three assurance levels (Low/Substantial/High)—High requires in-person or equivalent verification.

Biometric Authentication

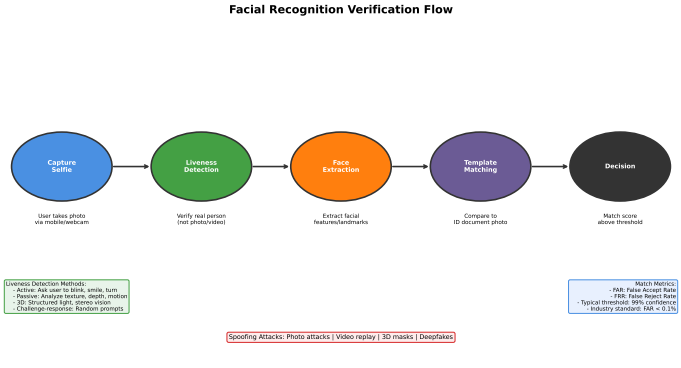
Modalities

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



Iris scanning achieves 99.99% accuracy—face recognition (99.5%) is preferred for mobile UX.

Facial Recognition Flow

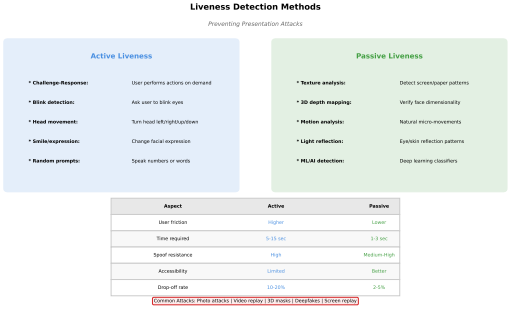


Face capture to match takes 2-3 seconds—AI extracts 128+ facial landmarks for comparison.

Liveness Detection

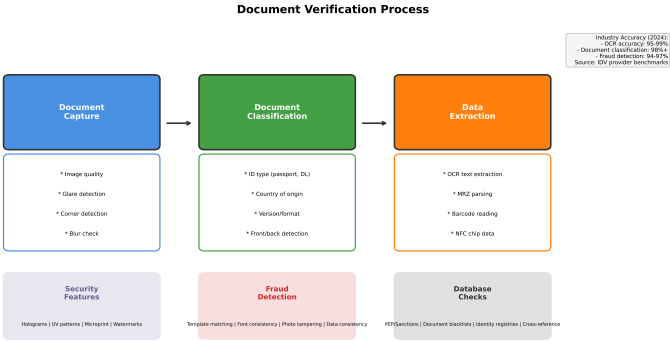
Anti-Spoofing

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



Liveness detection prevents photo/video spoofing—3D depth sensing defeats deepfake attacks.

Document Verification Technology



AI detects document tampering by analyzing holograms, microprinting, and UV security features.

OCR and NFC Chip Reading

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)

1. Image Capture	Camera captures document
2. Pre-processing	Deskew, noise reduction
3. Text Detection	Locate text regions
4. Character Recognition	ML-based text extraction
5. MRZ Parsing	Machine Readable Zone decode
6. Validation	Check digit verification

NFC (Near Field Communication)

1. Chip Detection	Phone detects NFC chip
2. BAC/PACE Auth	Authenticate with MRZ data
3. Data Read	Extract chip data groups
4. Active Auth	Verify chip authenticity
5. Passive Auth	Validate digital signatures
6. Clone Detection	Verify chip is original

Metric	OCR	NFC
Accuracy	95-99%	100%
Security	Medium	Very High
User effort	Take photo	Tap phone
Device req.	Camera	NFC-enabled
Tampering detect	Limited	Cryptographic

Best Practice: Combine OCR + NFC for maximum security and accuracy

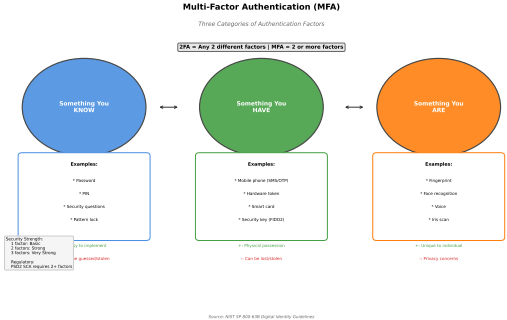
Sources: ICAO 9303 (Machine Readable Travel Documents), ePassport specifications

NFC chip reading provides cryptographic proof—data signed by issuing authority cannot be forged.

Multi-Factor Authentication (MFA)

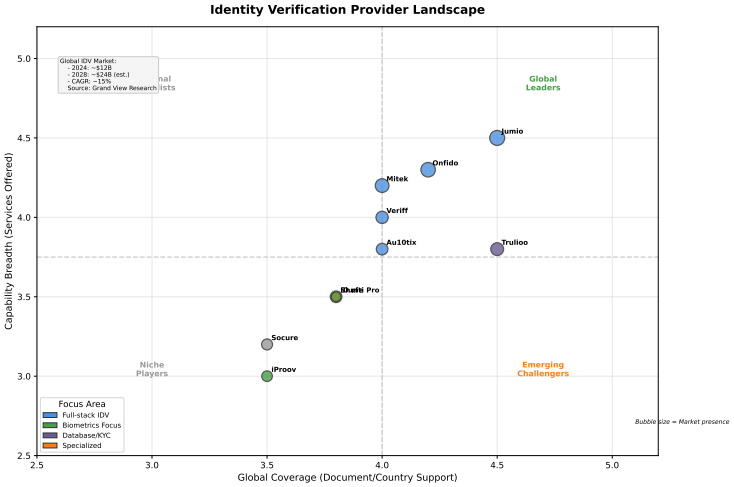
Authentication Factors

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



MFA combining 2+ factors reduces account takeover fraud by 99.9%—now standard for banking.

Identity Verification Providers

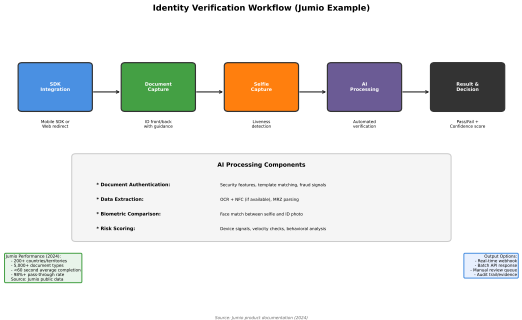


Jumio, Onfido, and Trulioo lead the $15B IDV market—consolidation accelerating via M&A.

Jumio Case Study

AI-Powered KYC

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

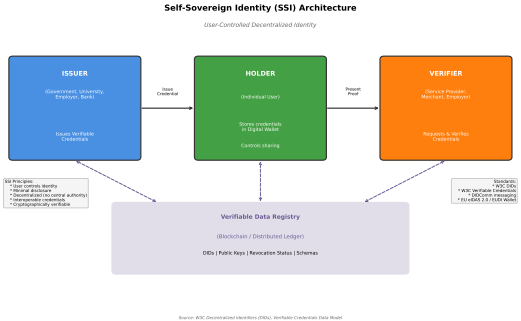


Jumio processed 1B+ verifications—95% automation rate with 5-minute average completion.

Self-Sovereign Identity (SSI)

Decentralized Model

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

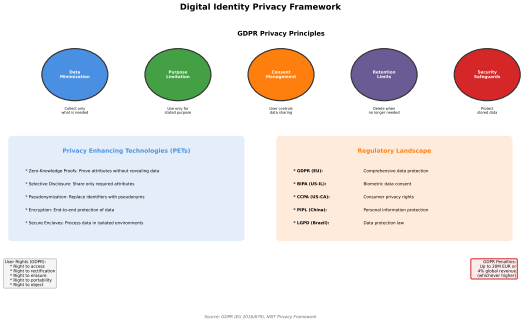


SSI gives users control over their credentials—verify age without revealing birthdate.

Privacy Concerns

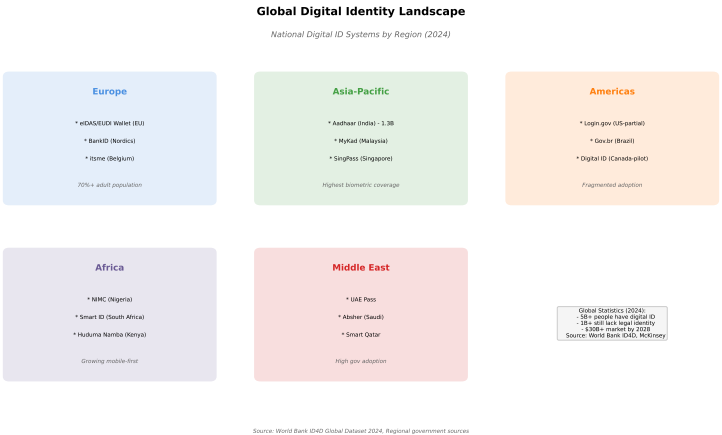
Data Protection

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



GDPR requires data minimization and right to erasure—biometric templates are sensitive personal data.

Global Identity Programs

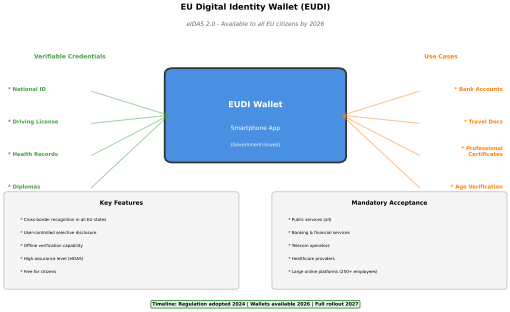


India's Aadhaar (1.4B), Estonia's e-ID, and Singapore's Singpass lead global digital ID adoption.

Future: Digital Wallets

EU Digital Identity Wallet

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



EU Digital Identity Wallet mandated by 2026—every EU citizen will have government-issued mobile ID.

Key Takeaways

- **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

Digital identity is the foundation of financial inclusion—secure verification enables trusted services.