Lesson 6: Digital Identity and Authentication
Module 1: FinTech Fundamentals

Digital Finance
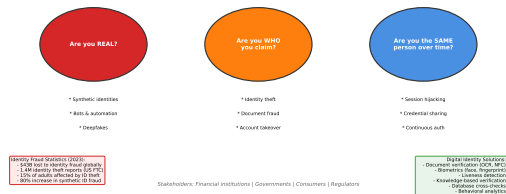
Identity Verification Problem

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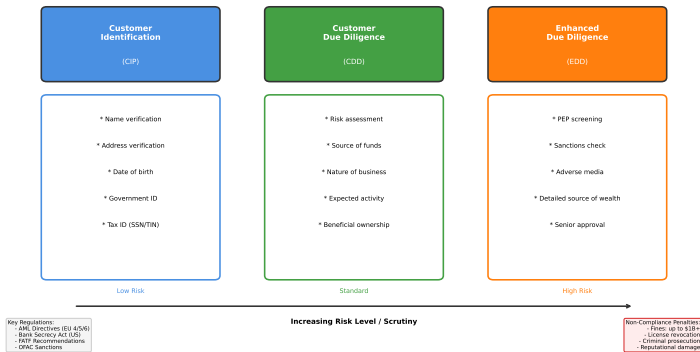
The Digital Identity Challenge

How do you prove who you are online?

Are you REAL?

Are you WHO you claim?

Are you the SAME person over time?

- Synthetic identities
- Bots & automation
- Deepfakes

- Identity theft
- Document fraud
- Account takeover

- Session hijacking
- Credential sharing
- Continuous auth

Identity Fraud Statistics (2023):
- $43B lost to identity fraud globally
- 1.4M identity theft reports (US FTC)
- 15% of adults affected by ID theft
- 80% increase in synthetic ID fraud

Stakeholders: Financial institutions | Governments | Consumers | Regulators

Digital Identity Solutions:
- Document verification (OCR, NFC)
- Biometrics (face, fingerprint)
- Liveness detection
- Knowledge-based verification
- Database cross-checks
- Behavioral analytics

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

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

Know Your Customer (KYC) Framework

Customer Identification (CIP)	Customer Due Diligence (CDD)	Enhanced Due Diligence (EDD)
* Name verification	* Risk assessment	* PEP screening
* Address verification	* Source of funds	* Sanctions check
* Date of birth	* Nature of business	* Adverse media
* Government ID	* Expected activity	* Detailed source of wealth
* Tax ID (SSN/TIN)	* Beneficial ownership	* Senior approval
Low Risk	Standard	High Risk

Increasing Risk Level / Scrutiny

Key Regulations:
- AML Directives (EU 4/5/6)
- Bank Secrecy Act (US)
- FATF Recommendations
- OFAC Sanctions

Non-Compliance Penalties:
- Fines: up to $1B+
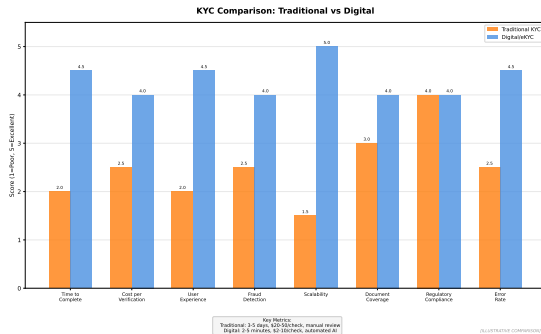- License revocation
- Criminal prosecution
- Reputational damage

Source: FATF Guidelines, AML regulatory frameworks

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%

KYC Comparison: Traditional vs Digital

Key Metrics:
Traditional: 3-5 days, $20-50/check, manual review
Digital: 2-5 minutes, $2-10/check, automated AI

(ILLUSTRATIVE COMPARISON)

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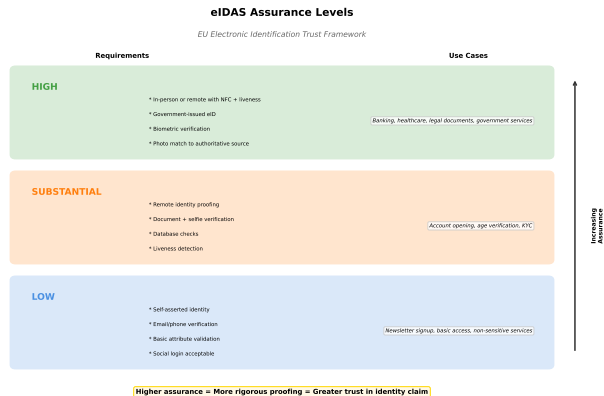
eIDAS Framework

EU Digital Identity

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

eIDAS: 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 (QWAC)

eIDAS 2.0 Key Changes (2024)

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

All EU citizens entitled to a digital wallet by 2026

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

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

eIDAS Assurance Levels

EU Electronic Identification Trust Framework

Requirements		Use Cases

HIGH
* In-person or remote with NFC + liveness
* Government-issued eID
* Biometric verification
* Photo match to authoritative source

Banking, healthcare, legal documents, government services

SUBSTANTIAL
* Remote identity proofing
* Document + selfie verification
* Database checks
* Liveness detection

Account opening, age verification, KYC

LOW
* Self-asserted identity
* Email/phone verification
* Basic attribute validation
* Social login acceptable

Newsletter signup, basic access, non-sensitive services

Increasing Assurance ↑

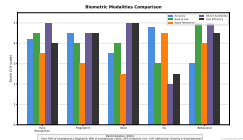**Higher assurance = More rigorous proofing = Greater trust in identity claim**

Source: EU Regulation 910/2014, Implementing Regulation 2015/1502

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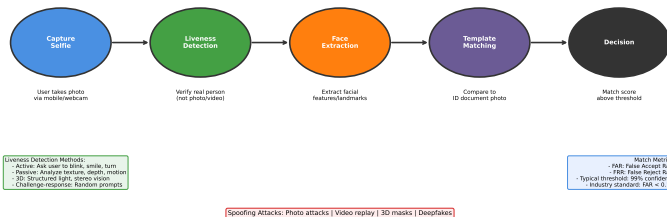
Biometric Authentication

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 Verification Flow

Capture Selfie	Liveness Detection	Face Extraction	Template Matching	Decision
User takes photo via mobile/webcam	Verify real person (not photo/video)	Extract facial features/landmarks	Compare to ID document photo	Match score above threshold

Liveness Detection Methods:
- Active: Ask user to blink, smile, turn
- Passive: Analyze texture, depth, motion
- 3D: Structured light, stereo vision
- Challenge-response: Random prompts

Match Metrics:
- FAR: False Accept Rate
- FRR: False Reject Rate
- Typical threshold: 99% confidence
- Industry standard: FAR < 0.1%

Spoofing Attacks: Photo attacks | Video replay | 3D masks | Deepfakes

[CONCEPTUAL PROCESS 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

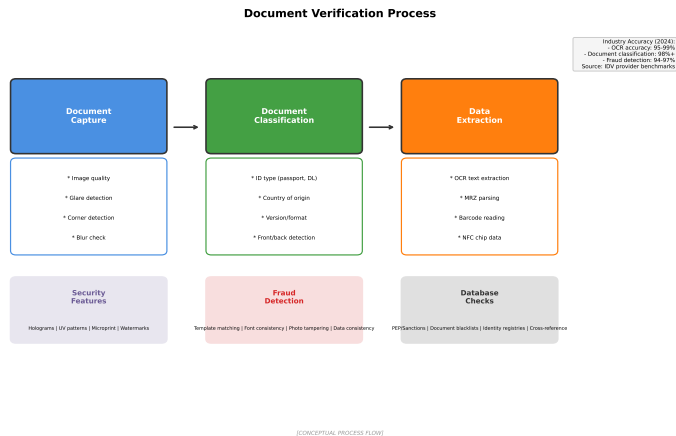**Liveness Detection Methods**

Preventing Presentation Attacks

Active Liveness	
* **Challenge-Response:**	User performs actions on demand
* **Blink detection:**	Ask user to blink eyes
* **Head movement:**	Turn head left/right/up/down
* **Smile/expression:**	Change facial expression
* **Random prompts:**	Speak numbers or words

Passive Liveness	
* **Texture analysis:**	Detect screen/paper patterns
* **3D depth mapping:**	Verify face dimensionality
* **Motion analysis:**	Natural micro-movements
* **Light reflection:**	Eye/skin reflection patterns
* **ML/AI detection:**	Deep learning classifiers

Aspect	Active	Passive
User friction	Higher	Lower
Time required	3-15 sec	1-3 sec
Spoof resistance	High	Medium-High
Accessibility	Limited	Better
Drop-off rate	10-25%	2-5%

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

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

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

Document Verification Technology

Document Verification Process

Industry Accuracy (2024):
- OCR accuracy: 95-99%
- Document classification: 98%+
- Fraud detection: 94-97%
Source: IDV provider benchmarks

Document Capture	Document Classification	Data Extraction
* Image quality	* ID type (passport, DL)	* OCR text extraction
* Glare detection	* Country of origin	* MRZ parsing
* Corner detection	* Version/format	* Barcode reading
* Blur check	* Front/back detection	* NFC chip data

Security Features	Fraud Detection	Database Checks
Holograms	UV patterns	Microprint	Watermarks	Template matching	Font consistency	Photo tampering	Data consistency	PEP/Sanctions	Document blacklists	Identity registries	Cross-reference

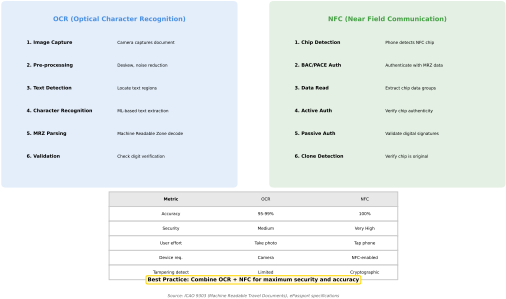*[CONCEPTUAL PROCESS FLOW]*

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
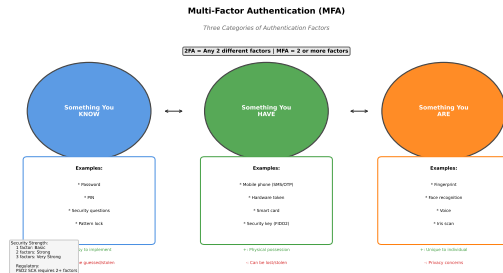
Document Data Extraction: OCR vs NFC

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

Source: 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)
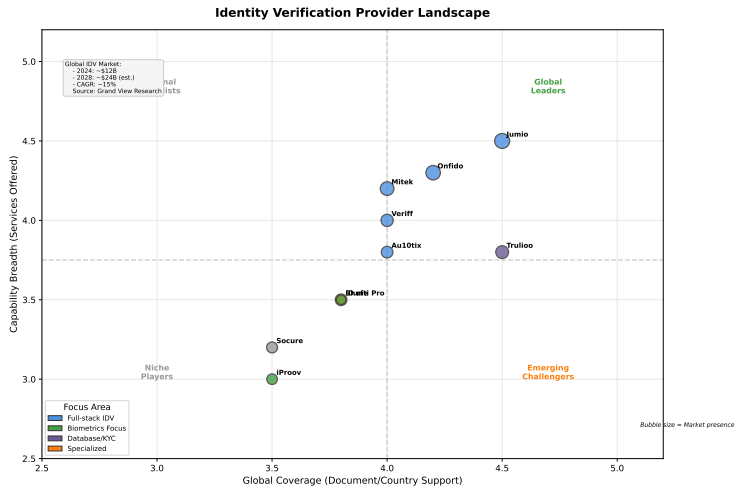
Authentication Factors

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

Multi-Factor Authentication (MFA)

Three Categories of Authentication Factors

2FA = Any 2 different factors | MFA = 2 or more factors

Something You KNOW

Examples:
- Password
- PIN
- Security questions
- Pattern lock

Something You HAVE

Examples:
- Mobile phone (SMS/OTP)
- Hardware token
- Smart card
- Security key (FIDO2)

+ Physical possession

− Can be lost/stolen

Something You ARE

Examples:
- Fingerprint
- Face recognition
- Voice
- Iris scan

+ Unique to individual

− Privacy concerns

Security Strength:
1 Factor: Basic
2 factors: Strong
3 factors: Very Strong

Regulatory:
PSD2 SCA requires 2+ factors

Source: NIST SP 800-63B Digital Identity Guidelines

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

Identity Verification Provider Landscape

Global IDV Market:
- 2024: ~$12B
- 2028: ~$24B (est.)
- CAGR: ~15%
Source: Grand View Research

Capability Breadth (Services Offered)

Global Coverage (Document/Country Support)

Global Leaders

Jumio
Onfido
Mitek
Veriff
Au10tix
Trulioo
iDenfy / Persona Pro

Socure
iProov

Niche Players

Emerging Challengers

Bubble size = Market presence

Focus Area
- Full-stack IDV
- Biometrics Focus
- Database/KYC
- Specialized

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

Identity Verification Workflow (Jumio Example)

| SDK Integration | Document Capture | Selfie Capture | AI Processing | Result & Decision |

Mobile SDK or Web redirect · ID feedback with guidance · Liveness detection · Automated verification · Pass/Fail + Confidence score

AI Processing Components

Document Authentication:	Security features, template matching, fraud signals
Data Extraction:	OCR + NFC (if available), MRZ parsing
Biometric Comparison:	Face match between selfie and ID photo
Risk Scoring:	Device signals, velocity checks, behavioral analysis

Jumio Performance (2024):
- 200+ countries/territories
- 5,000+ document types
- >95 second average completion
- NFC+ pass-through rate
Source: Jumio public data

Output Options:
- Real-time webhook
- REST API response
- Manual review queue
- Audit trail/evidence
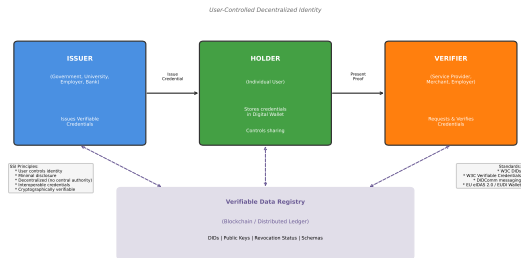
Source: Jumio product documentation (2024)

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
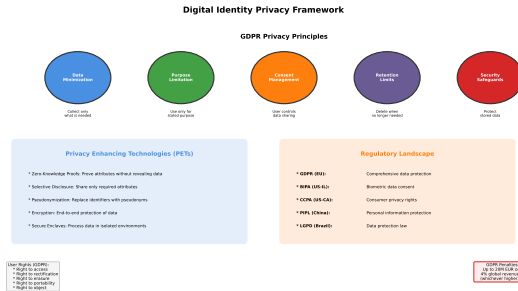
Self-Sovereign Identity (SSI) Architecture

User-Controlled Decentralized Identity

ISSUER	HOLDER	VERIFIER
(Government, University, Employer, Bank)	(Individual User)	(Service Provider, Merchant, Employer)
Issues Verifiable Credentials	Stores credentials in Digital Wallet	Requests & Verifies Credentials
	Controls sharing	

Issue Credential → Present Proof →

SSI Principles
* User controls identity
* Minimal disclosure
* Decentralized (no central authority)
* Interoperable credentials
* Cryptographically verifiable

Standards:
* W3C DIDs
* W3C Verifiable Credentials
* DIDComm messaging
* EU eIDAS 2.0 / EUDI Wallet

Verifiable Data Registry

(Blockchain / Distributed Ledger)

DIDs | Public Keys | Revocation Status | Schemas

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

---

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

Data Protection

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

Digital Identity Privacy Framework

GDPR Privacy Principles

Data Minimization	Purpose Limitation	Consent Management	Retention Limits	Security Safeguards
Collect only what is needed	Use only for stated purpose	User controls data sharing	Delete when no longer needed	Protect stored data

Privacy Enhancing Technologies (PETs)

* Zero-Knowledge Proofs: Prove attributes without revealing data
* Selective Disclosure: Share only required attributes
* Pseudonymization: Replace identifiers with pseudonyms
* Encryption: End-to-end protection of data
* Secure Enclaves: Process data in isolated environments

Regulatory Landscape

* **GDPR (EU):** Comprehensive data protection
* **BIPA (US-IL):** Biometric data consent
* **CCPA (US-CA):** Consumer privacy rights
* **PIPL (China):** Personal information protection
* **LGPD (Brazil):** Data protection law

User Rights (GDPR):
* Right to access
* Right to rectification
* Right to erasure
* Right to portability
* Right to object

GDPR Penalties:
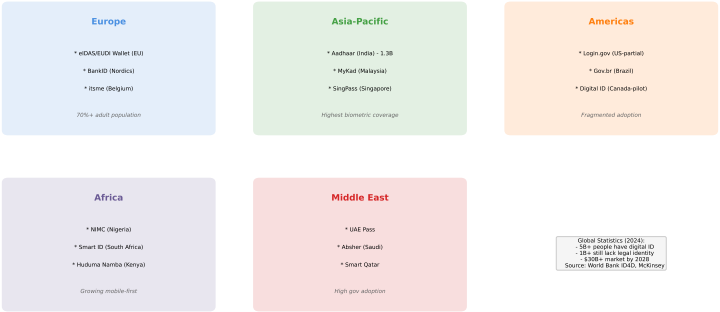Up to 20M EUR or 4% global revenue (whichever higher)

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

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

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
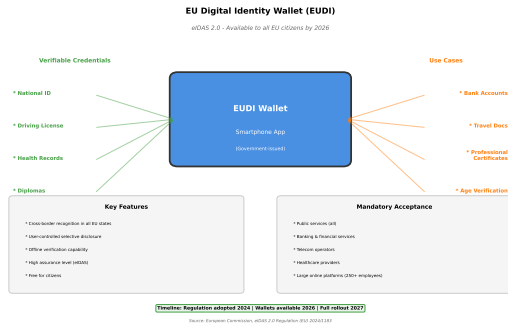Source: World Bank ID4D, McKinsey

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

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 (EUDI)

eIDAS 2.0 - Available to all EU citizens by 2026

Verifiable Credentials

- National ID
- Driving License
- Health Records
- Diplomas

EUDI Wallet

Smartphone App

(Government-issued)

Use Cases

- Bank Accounts
- Travel Docs
- Professional Certificates
- Age Verification

Key Features

- Cross-border recognition in all EU states
- User-controlled selective disclosure
- Offline verification capability
- High assurance level (eIDAS)
- Free for citizens

Mandatory Acceptance

- Public services (all)
- Banking & financial services
- Telecom operators
- Healthcare providers
- Large online platforms (250+ employees)

Timeline: Regulation adopted 2024 | Wallets available 2026 | Full rollout 2027

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

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.