IDEMIA PUBLIC SECURITY



Identity Verification (IDV)

Confirm the real person behind every identity, from onboarding to account recovery.

Authentication alone cannot stop identity fraud

A synthetic identity approved at account opening. A contractor badged into a control room without anyone confirming who they are. A help-desk reset granted to a convincing deepfake. For banks and critical infrastructure operators, each of these hands an attacker trusted access, and none of them trips the controls built to protect the login. Identity has a lifecycle, and onboarding and recovery are where it is weakest. Without a verified person at the start, even the strongest authentication can end up protecting an impostor.

M

. .rppk. n n
. . .
- e -
- - - -
f - g

l l . . f .pnpu

31%

rise in U.S. new-account fraud victims in 2025

The sharpest increase of any fraud type, striking at the moment accounts are opened.

Javelin Strategy & Research, 2026 Identity Fraud Study

€7.1B+

in General Data Protection Regulation fines since 2018

Identity data is now a regulatory priority, with a measurable financial cost.

DLA Piper GDPR Fines and Data Breach Survey, January 2026

WHAT WE DO

s ((3sm 5((((((((((((((A
EEs ((((A ((((((((((A
A (A (((((((((((((

IDEMIA PUBLIC SECURITY

HOW IT WORKS

Four layers of protection in every verification

Every layer runs within one guided capture on any device, with assurance set to the risk of the transaction.

Document Capture & Authentication

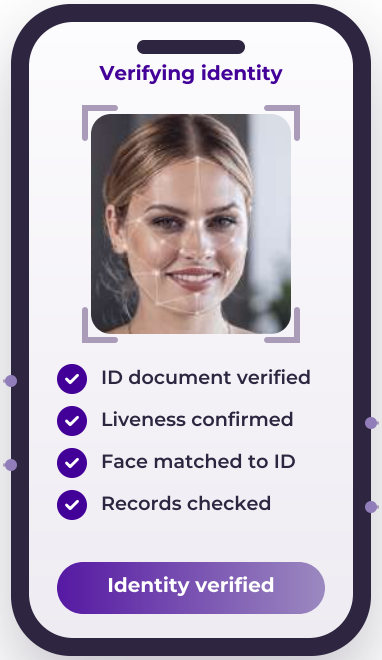
Captures and authenticates the identity document on web, iOS or Android.

- Guided auto-capture, plus NFC chip verification for ICAO documents
- Mobile ID verification
- Security features, template and data consistency checks across 4,500+ document types in 195+ countries

WHAT THE PERSON PROVIDES

Identity document or mobile ID

Live selfie



Face Capture & Liveness

Captures a selfie and proves a real, live person is present, in the same moment.

- Layered defenses: injection, presentation attack and deepfake detection, anti-replay and smartphone fingerprinting
- Met 100% of DHS RIVR presentation attack detection thresholds
- Certified ISO/IEC 30107-3 Level 2 (iBeta) and CEN/TS 18099 Substantial (BixeLab)

Face Verification

Matches the live face to the identity document portrait, or to a portrait on file.

- #1 for selfie-to-document matching accuracy in the DHS Remote Identity Validation Rally
- Face algorithms #1 for fairness in National Institute of Standards and Technology testing

Root of Trust & Third-Party Checks

Validates the identity against authoritative sources.

- Issuing agency records, including state motor vehicle agencies
- Telco data from mobile network operators
- Credit reporting attributes

WHAT YOU GET

One-time verification
Confidence score, assurance set to your risk

Reusable digital credential
Mobile ID and verifiable credentials

Basis for access credentials
Physical and digital access, smart cards, security keys

BUILT TO STANDARD

NIST 800-63 IAL2
Kantara approved

ISO 30107-3 Level 2
Certified liveness

SOC 2 Type II
Independent audit

BIPA & GDPR
740 ILCS 14 · EU 2016/679

IDEMIA PUBLIC SECURITY

WHERE IT IS USED

Use cases across customers and workforce

1 Account Opening
CONSUMER

Open accounts quickly, meet know your customer obligations and stop fraud at enrollment.

2 Workforce Onboarding
WORKFORCE

Verify employees, contractors and visitors before any badge, credential or system access is issued.

3 Account Recovery
CONSUMER · WORKFORCE

Replace knowledge questions and help-desk resets with self-service reverification.

4 Step-Up for High-Risk Actions
CONSUMER · WORKFORCE

Reverify the person before sensitive transactions or access to restricted assets.

5 Age Verification
CONSUMER

Automate age-restricted access checks that protect privacy and keep the experience smooth.

6 Periodic Compliance Checks
CONSUMER

Reverify existing customers when regulations require it, and stop account takeover fraud.

KEY BENEFITS

Confidence & Trust

- Deterministic fraud prevention, not probabilistic guesswork
- Kantara approved at NIST 800-63 Identity Assurance Level 2

Interoperability

- Native to the Microsoft Entra ID ecosystem
- OpenID Connect connector for fast integration
- v D ((((i s I mu ((Afi (i

Privacy

- User consent capture
- y ((((((
- No AI training on your customer data

ROOTED IN 50 YEARS OF LEGACY

Proven at scale

50+
Years of biometric innovation

45
State motor vehicle databases

-
-

0%
iBeta Presentation Attack Detection (PAD) error rate

Bring high-assurance Identity Verification to your organization

Connect with our team to discuss your use case, from account opening and employee onboarding, to age verification and account recovery.

Contact Us