

Biometric Identity Verification

Create real trust at every customer interaction

Highlights

Entrust biometric identity verification solutions can help you build connected experiences across the customer journey without compromising on security against account takeover attacks, deepfakes, and beyond.

You can establish a trusted biometric tied to a verified ID at account opening and unlock the full power of the user journey at high-risk moments such as password reset – without compromising on fraud prevention.

Higher conversion rates

Our award-winning user experience (UX) design matches to a previously verified identity document, resulting in some Entrust customers seeing a 40% increase in conversions.

Increased user trust

Secure biometric-led identity verification (IDV) and authentication as part of the UX drives higher trust compared with businesses not using these approaches today.

Fewer fraud attacks

Combining identity document verification with AI-powered biometrics helps prevent up to 50% more fraud than traditional document verification methods.

Key Features and Benefits

Global coverage

Verifies ID types from 195 countries, supporting the IDs your customers are using daily.

Real-time results

Award-winning, AI-powered technology validates facial biometrics in seconds.

Prevents deepfakes

Certified against PAD Level 2 liveness standards to stop the smartest fraud.

Single API integration

Seamlessly integrate Entrust's trusted biometric authentication via one powerful API.

Patented fraud detection

Blends recognized metadata and visual fraud solutions with ID-specific AI features.

Flexible no-code identity journeys

Build your ideal identity experience with no code and deploy in minutes.



With Entrust, we can really trust the customers signing up for our services, unlocking a host of benefits later in the customer lifecycle.

FERNANDO PLAZ, HEAD OF PRODUCT, MACH

Why Entrust?

No need to choose between fraud prevention and the user experience.

User Experience	Performance	Privacy
Seamlessly enable access by connecting a user's identity at onboarding to that same identity at potential high-risk moments.	95% of biometrics matched and verified in less than 3 seconds.	Privacy-preserving facial biometric capture backed by 256-bit SSL encryption.
Active anti-bias AI reduces false rejections for a superior UX, no matter where a user is from.	AI-powered document verification detects up to 50% more fraud than traditional methods such as database matching.	Data policies and retention defined by you, with local or Entrust-hosted storage.
Enrich the identity profile with award-winning ID verification and database signals by Entrust and curated third parties.	Supported by Fraud Lab, our team of experts work 24/7 to keep you two steps ahead of leading GenAI attacks.	

See why Entrust was named a Leader in the [Gartner® Magic Quadrant™ for Identity Verification](#)