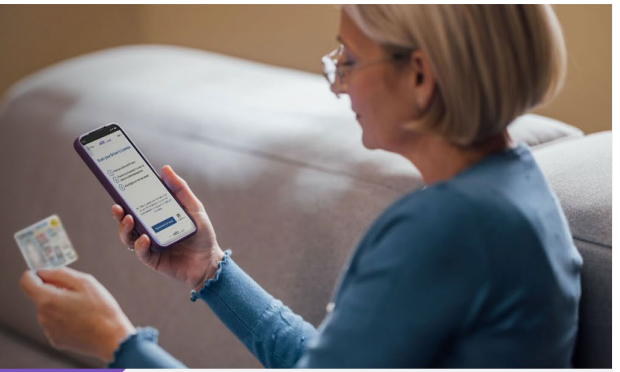


# Next-Gen Authentication Without Biometric Storage



## The Identity Challenge: Balancing Security & Privacy

With cyber threats and identity fraud on the rise, businesses need a **secure and frictionless way to verify identities**. Traditional authentication methods – passwords, one-time passcodes, and even stored biometric templates – introduce risks such as phishing, credential theft, and regulatory burdens.

Biometric authentication is highly secure, but users and regulators are increasingly concerned about **data privacy and storage risks**.

## Introducing PrivacyKey™

PrivacyKey™ replaces **stored biometric templates** with a cryptographic key pair, ensuring no biometric data is retained. Using a simple **selfie-based authentication process**, users securely verify their identity while maintaining **full privacy protection and regulatory compliance**.



### No biometric data storage

Eliminates risk of biometric theft



### Regulatory compliance

Meets GDPR, BIPA, CUBI, and other privacy laws



### User-friendly authentication

Seamless, frictionless access in under a second



### Phishing resistant

Prevents credential theft and unauthorized access

## How PrivacyKey™ Works

During onboarding, a selfie is used to create a public/private key pair. Only the public key is stored, and the private key is discarded. No keys or images are stored on the user's device, ensuring device-independence.

For each login, a new private key is generated using the user's face, matched with the stored public key through a digital signature, and then discarded after access is granted.

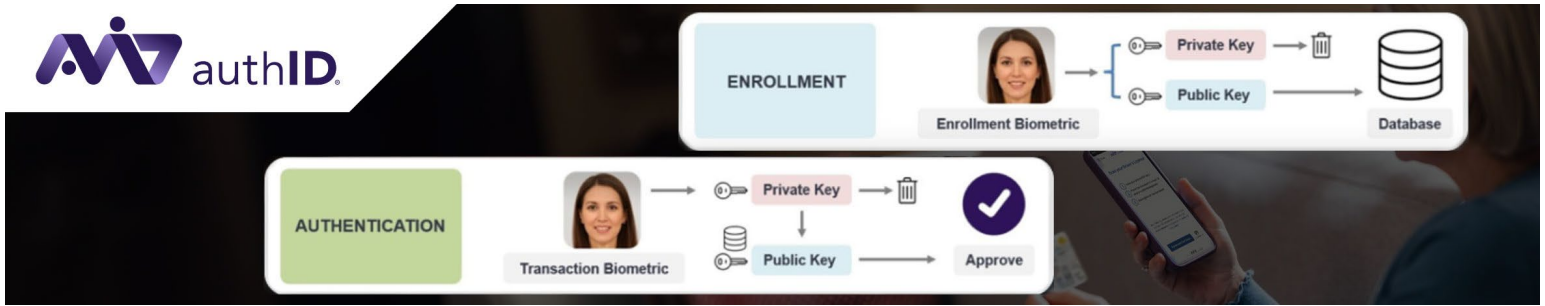
Our unique and patented technology allows authID to generate matching private keys with each new transaction.

## THE DEFINITIVE COMBINATION OF IDENTITY VERIFICATION AND PRIVACY PROTECTION

authID's **Proof™** solution enables users to establish their identity by verifying a government issued ID (e.g., driver's license, passport, or any of the 14,000+ supported documents worldwide) along with a selfie. Proof confirms the authenticity of the document, verifies the person presenting it, and links the two to create a **biometric root of trust**.

Our **Verified™** solution then allows users to seamlessly and securely authenticate using this trusted identity.

authID has never stored biometric data for matching, instead using an **encrypted hash**. With **PrivacyKey™**, even this hash is replaced by a **public/private key pair**, ensuring no biometric data is retained. This enhances compliance with **GDPR, BIPA, CUBI**, and other regulations while protecting users from digital threats.



## Key Benefits of PrivacyKey™

### Regulatory Compliance

- Independent **ISO-certified compliance** for biometric data protection
- Stored keys **cannot be reverse-engineered** into facial images or linked to personal data.
- Meets **GDPR, PSD2, CCPA, BIPA**, and other global privacy regulations

### Increased Security

- **Phishing-resistant authentication.** Private key cannot be compromised because it's not stored – your face is the key
- Eliminates vulnerabilities associated with passcodes, passkeys, PINS, intercepted SMS, and stored credentials
- PrivacyKeys can be rotated or revoked on demand or on a schedule to meet your security policy

### Reduced Liability

- No central database of biometric data, **minimizing cybersecurity risk**
- Reduces **regulatory exposure, liability, and insurance costs**

### Streamlined User Experience

- **Intuitive interface** for fast, seamless authentication
- **1 in 1 billion accuracy** prevents duplicates while allowing instant access
- **Authentication in under a second**, faster than one-time passcodes or authenticator apps

### Multi-Faceted Authentication

- **1:1 matching** for seamless authentication
- **1:N identification** for scalable identity verification, enter by face, or pay by face
- **Offline authentication** via SOK, allowing secure access without an internet connection

### Privacy-Preserving

- Authentication is performed **without storing any biometric or sensitive data**

## PrivacyKey™: Designed for Every Industry



### Financial Services & Banking

Secure high-value transactions and account logins



### Government & Public Sector

Enable secure citizen authentication while ensuring privacy



### Gaming Industry

Future of Privacy Keys in Gaming Security



### Healthcare & Insurance

Protect patient records without storing sensitive biometrics



### Workforce & Enterprise Access

Continuous identity assurance for employees



### Hospitality Industry

Securely elevate the guest experience