Ping Identity®

Ultimate Guide

# The Ultimate Use Case Guide for PingOne Recognize

A guide for organizations looking to add **biometric authentication** for their customers at the onboarding, access, and recovery steps for their customers, employees, and extended workforce.

# Table of Contents

# Introduction: Zero-Knowledge Biometrics for Trusted Journeys

Most authentication methods force a tradeoff between security, privacy, and user experience. They are insecure, costly, frustrating, or all three.

Whether it's a hard token, SMS OTP, call center, or password, none of these methods can prove that the person authenticating is the same genuine person who created the account. And most other biometrics, whether device-bound (Face ID) or cloud-based, either fall back to a guessable PIN or put users' biometric privacy at risk.

At the same time, the rise of deepfakes and AI-driven spoofing means any viable facial biometric solution also needs strong, passive liveness detection and protection against both presentation and injection attacks.

**Zero-Knowledge Biometrics** (ZKB) is Ping Identity's facial biometric authentication capability that forces no tradeoffs. It is an authentication technology that delivers the strongest security, privacy, and user experience with just one action.

Delivered via **PingOne Recognize**, ZKB proves, with a single look at any camera (desktop or mobile) that the person authenticating is the same person who created the account, without ever storing their biometric data in retrievable or reconstructable form.

It works across the user journey and across use cases: from a frontline worker logging in on a shared tablet to a banking customer with a new device recovering a lost account. With one glance at the camera, Zero-Knowledge Biometrics uses passive liveness to prove genuine identity assurance.

This guide shows how PingOne Recognize is used across key consumer and workforce journeys and how it underpins emerging **Verified Trust** flows across the wider identity security space - proving that the same person who created the account is present, while balancing security, privacy, and user experience.

# Customer Identity Use Case:

# Invisible Enrollment

PingOne Recognize is a third-party biometric authentication system. Like any other it requires an initial enrollment step. Although this is just a quick glance at the camera, it can still introduce friction.

To mitigate this, PingOne Recognize includes the market-leading **IDV Bridge** component that removes this manual biometric enrollment step. Instead, it **silently enrolls users into its system** using existing images taken during customer onboarding or HR system.

When a new user completes a facial-enabled enrollment or identity verification step, PingOne Recognize converts their face into a Zero-Knowledge Biometric profile and silently enrolls it in the background. Later, when they authenticate, there's no separate biometric setup step — just a single glance that includes passive liveness checks and deepfake-resistant anti-spoofing in under 300ms.

The same model works for existing populations: organizations can bulk-enroll users who have already completed IDV/KYC, or, in workforce scenarios, enroll employees directly from existing HR images. This transforms enrollment into a fully invisible, zero-friction experience for end users.

Like all of its parts, PingOne Recognize's enrollment is entirely privacy-preserving. It never stores biometric profiles in retrievable or reconstructable form, on the device or in the cloud, at enrollment or at any future authentication step. This is enabled by the innovative application of secure Multi-Party Computation (sMPC) to biometrics. For a deeper dive, see the solution overview or technical white paper.

## Business Value

### 1. Fraud & security

Authenticates against the originally verified person, not just the device, making it harder to exploit stolen credentials, OTPs, or social-engineering attacks. Certified liveness and injection-attack detection help block deepfakes and device-level spoofing.

### 2. User experience

No separate biometric enrollment step for most users — enrollment happens invisibly from existing verified images.

### 3. Cost & operational efficiency

Reduces re-KYC, SMS OTP, and help desk costs. Customers have seen multi-million-dollar annual savings by eliminating these steps at scale.

CUSTOMER STORY:

# Frictionless Biometric Onboarding at Scale

*"Enroll these low-quality customer images collected over the past decade into PingOne Recognize for future authentication."*

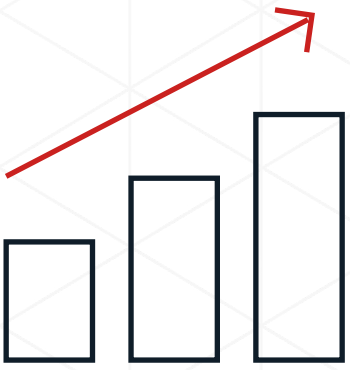
A major European wealth management and investment bank serving high-value clients relied on call centers to approve high-risk wire transfers and wanted to introduce Zero-Knowledge Biometric authentication.

Keeping the banking experience frictionless was critical, so instead of asking customers to enroll manually, the bank used the IDV Bridge to silently enroll its 400,000 users from historic ID images on file.

PingOne Recognize converted these verified images into Zero-Knowledge Biometric profiles and enrolled them in the background. This allowed call-center checks to be replaced with a single glance in around 300ms, while remaining privacy-preserving.

## Result:

Within the first month, the bank cut call-center authentication costs by about 90% and fraud costs by roughly 70%. Customers authenticated in milliseconds, their biometric data stayed private, stayed private — and enrollment had already been carried out on their behalf.



## Customer Identity Use Case:

# Passwordless Login and Step-Up Authentication

A European crypto investing app needed stronger authentication to meet MiCAR requirements in a target market. It was using local biometrics (such as Face ID or Android biometrics) to authenticate users — both at login and for step-up actions like changing account details or deleting an account.

However, these local checks were ultimately protected by the device PIN and had no link to the verified face captured during the original IDV process. That meant two things:

- They weren't strong enough for MiCAR, since anyone who knew the device PIN could enroll or pass local biometrics.
- They didn't truly prove that the person making high-risk changes was the same person who opened the account.

Plus, the crypto industry is one of the most privacy-conscious markets in the world, so any new technology introduced to strengthen security needed to function without centralizing or exposing biometric data.

By adopting **Zero-Knowledge Biometrics**, the app kept the experience similar to local facial biometrics — one look at the camera to log in or confirm an account change — but with crucial differences: the live face is now compared to the face verified at onboarding, not just the face enrolled on the device, and every glance runs passive liveness and deepfake-resistant presentation and injection-attack checks in the background.

## Business Value

### 1. Multi-factor by design

Authenticates the verified face and device, not just whoever can unlock the handset. Passive liveness and presentation/injection-attack detection make it significantly harder to use deepfakes or compromised devices as part of an account takeover.

### 2. Regulatory alignment

Moves from device-only, PIN-backed biometrics to an authentication model rooted in the verified identity used at IDV, supporting stronger, identity-centric assurance in line with MiCAR expectations.

### 3. User experience

Keeps the UX similar to local biometrics: users still just glance at the camera. No PINs, no extra prompts, and no new habits. The only change is that every check is now bound to the verified person, not just their device.

### 4. Privacy

Zero-Knowledge Biometrics ensures no biometric data or PII is ever stored in retrievable form, on device or in the cloud. This delivers stronger security without asking privacy-sensitive crypto users to trade away control over their biometric data.

Customer Identity Use Case:

# Payment Authentication & Self-Service Account Recovery

A **Tier-1 European bank** needed to cut the cost and fraud risk of both its payment authentication process and account recovery step, without weakening security or privacy. Payments depended on SMS OTPs and recovery on call centers:

• SMS OTPs were expensive and increasingly exposed to phishing and SIM-swap attacks.

• To recover accounts customers had to phone in, answer questions, and wait in queues to regain access.

Traditional centralized biometrics were off the table because storing biometric data in retrievable form conflicted with strict privacy standards. By deploying PingOne Recognize with Zero-Knowledge Biometrics, the bank introduced **self-service account recovery** secured with a single glance at the camera — without storing biometric data anywhere in retrievable or reconstructable form.

## Example Payment Flow

| Before PingOne Recognize | After PingOne Recognize |
|---|---|
| Customer starts a high-value payment in the app. | Customer starts the same payment and is prompted to **look at the camera once**. |
| Bank sends an SMS OTP; customer copies the code to approve. | In ~300ms, PingOne Recognize:<br>• Runs passive liveness and presentation/ injection-attack checks.<br>• Matches the live face to the Zero-Knowledge Biometric profile from the original KYC event and verifies the bound device. |
| SMS is costly, delays cause failed/ abandoned payments, and OTPs are exposed to phishing and SIM-swap. | If verified, the payment is approved instantly. No SMS, no codes, and no biometric data stored in retrievable or reconstructable form. |

# Example Recovery Flow

| Before PingOne Recognize | After PingOne Recognize |
|---|---|
| Customer loses access to the account and calls the helpdesk. | Customer starts recovery in the app or web portal. |
| Identity is checked via knowledge-based questions and SMS OTP. | They enter an identifier (username / email) and look at the camera once.<br>• Runs passive liveness checks to confirm a real person is present.<br>• Detects signs of presentation and injection attacks to help block deepfakes and compromised devices.<br>• Biometrics are transformed via sMPC into a Zero-Knowledge Biometric profile that ensures no biometric data is stored in retrievable or reconstructable form.<br>• Matched the transformed template to the one rooted in the originally verified identity captured during KYC.<br>• This is then paired with an additional factor as the device is not present, such as a PIN or password. |
| The process is slow, costly, and vulnerable to social engineering and OTP interception. | If verified, access is restored immediately — no call center, no SMS OTP. |

CUSTOMER STORY:

# Tier-1 European Bank Scales Recovery Without Call Centers

A leading Tier-1 European bank saw account recovery driving up call center costs and fraud risk. Locked-out users had to call, answer questions, and clear SMS OTP checks, creating friction for customers and opportunities for attackers.

After deploying PingOne Recognize for self-service biometric recovery, customers now restore access in seconds with a single glance at the camera, while Zero-Knowledge Biometrics ensured no biometric data was ever stored in retrievable form. Within the first year, the bank:

Saved **$4.1M** in call center and helpdesk costs.

Achieved a **79% reduction** in account takeover fraud.

Delivered an **80% reduction** in account recovery time.

The bank cut fraud, freed up operational capacity, and gave customers a faster, more intuitive recovery experience — all without compromising on privacy.

Workforce Identity Use Case:

# Passwordless Access on Shared Devices

In frontline and operational environments, such as manufacturing lines, retail stores, warehouses, and food production, employees often share terminals and can't carry smartphones or tokens on the floor. Passwords and hard tokens are slow, frequently shared, and expensive to manage.

PingOne Recognize brings Zero-Knowledge Biometrics to these shared devices, allowing employees to authenticate with one glance against their verified employment record instead of a shared PIN or badge - with passive liveness checks helping ensure there's a real person at the terminal, not just a photo or replay.

In these workforce/B2B scenarios, PingOne Recognize alone is **face-only** (not multi-factor by design), but still offers far stronger assurance than hard tokens, KBA, or local biometrics on shared machines, because it anchors identity to the original, verified employee image.

## How It Works

### 1. Invisible enrollment from HR records

• Existing HR photos are converted into Zero-Knowledge Biometric profiles and enrolled into PingOne Recognize in the background.

• No explicit biometric enrollment is required at the workstation; employees are "ready to authenticate" from day one.

### 2. One-glance access on shared terminals

• At the start of a shift or when accessing role-based apps (PoS, inventory, production control), an employee approaches any shared terminal.

• They enter or select a short identifier (username) and look at the camera once.

• PingOne Recognize authenticates their face against the employment image in under 300ms — including passive liveness checks — and grants access, without passwords, badges, or fobs.

### 3. Role-appropriate policies and step-up

• For higher-risk actions such as approving large orders, overriding quality controls, or accessing sensitive data, PingOne Recognize can be combined with additional factors or authorization logic.

• This keeps everyday access fast, while anchoring high-risk actions to a verified individual.

### 4. Verified workforce recovery

• When employees forget passwords or move to a new terminal, PingOne Recognize can be used to quickly re-establish access with a single glance instead of a helpdesk call, password reset, or token replacement.

Behind the scenes, the Zero-Knowledge Biometric profile contains no biometric data or PII and cannot be reverse-engineered, ensuring that workforce biometrics remain private even while being used across multiple shared devices.

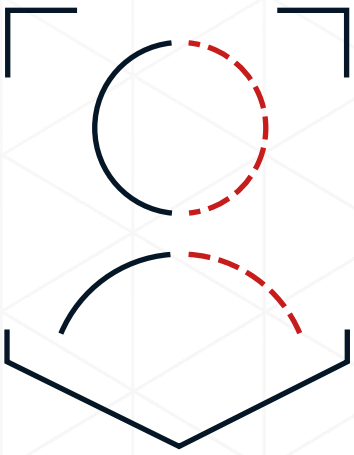
CUSTOMER STORY:

# US Food Product Supplier Secures Shared Terminals with One Glance

A US food product supplier needed to secure access for frontline workers rotating across shared terminals in their food production warehouse. Passwords and hard tokens were slowing teams down, being informally shared, and driving up helpdesk costs when lost or forgotten.

By deploying PingOne Recognize, the company bulk-enrolled employees from existing HR images using the IDV Bridge — invisible backend enrollment. Workers now authenticate on any shared terminal with a single glance, tied back to their verified employment record rather than a generic PIN or shared badge.

For routine access, Zero-Knowledge Biometrics replaced passwords and hard tokens; for higher-risk operations, Pingone Recognize is combined with existing access controls to apply additional checks where needed. The organization reduced helpdesk tickets related to login and token issues, improved shift start times, and strengthened accountability — all while keeping biometric data private and never stored in retrievable or reconstructable form.



#4349 | 04.26 | v01