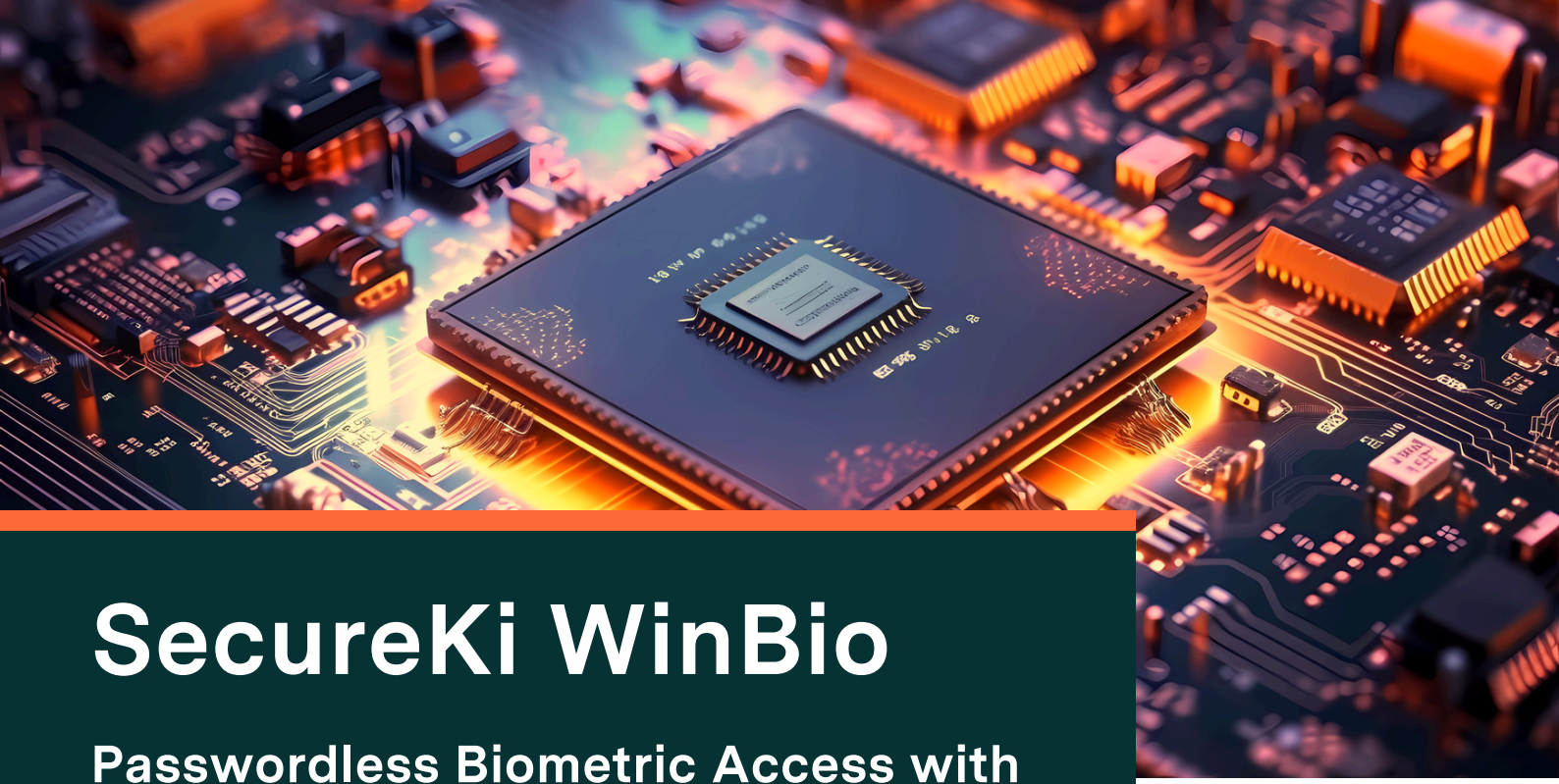
SECUREKI

WinBio

www.secureki.com



SecureKi WinBio

Passwordless Biometric Access with Built-In Credential Lifecycle Management

Overview

SecureKi WinBio, a secure, software-driven alternative to hardware-token passwordless solutions, transforms Windows desktop login by replacing traditional passwords with biometric authentication, automated password rotation, and mobile-based access control. Built on SecureKi's trusted identity and credential lifecycle platform, it allows users to log in instantly using fingerprint, finger-vein scanning, or face recognition with no password entry required.

Unlike hardware-token solutions that rely on USB keys, SecureKi WinBio uses a secure mobile app as the authentication engine, making passwordless access simpler, faster, and more scalable across the enterprise. It delivers FIDO2-level security without the cost and hassle of physical token management, while still supporting offline environments.

What makes SecureKi WinBio unique is its combination of passwordless biometric login with automated credential lifecycle management. This means IT teams can maintain full control over credential creation, rotation, and expiry without adding complexity for users.

The Challenge: Traditional Password Management

Many organizations continue to face password-related challenges that create risks and inefficiencies:

- Reused or weak passwords across multiple systems
- Forgotten passwords leading to frequent lockouts and costly helpdesk calls
- User fatigue from managing numerous complex credentials
- Password sharing in shared workstation environments
- Limited or no access in offline or remote locations

Key Features

Passwordless Biometric Login

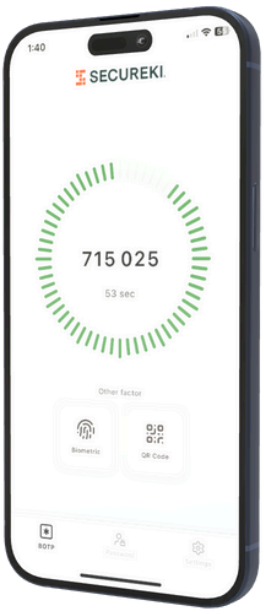
- Authenticate with fingerprint, finger-vein scanning, or face recognition
- Supports standard webcams (built-in or USB) without proprietary hardware
- Integrated with Windows Biometric Framework (WBF)
- Provides fast and secure access without typing passwords

Automated Password Rotation

- Rotates Active Directory or local user passwords at every login
- Enforces one-time-use credentials so users never need to know their own passwords
- Strengthens defense against credential theft and compromise

SecureKi Mobile App as Software Token

- Functions as a mobile-based smart authentication device
- Supports QR code login, fingerprint or face unlock for password retrieval, offline OTP/BOTP generation, and password expiry alerts with usage tracking

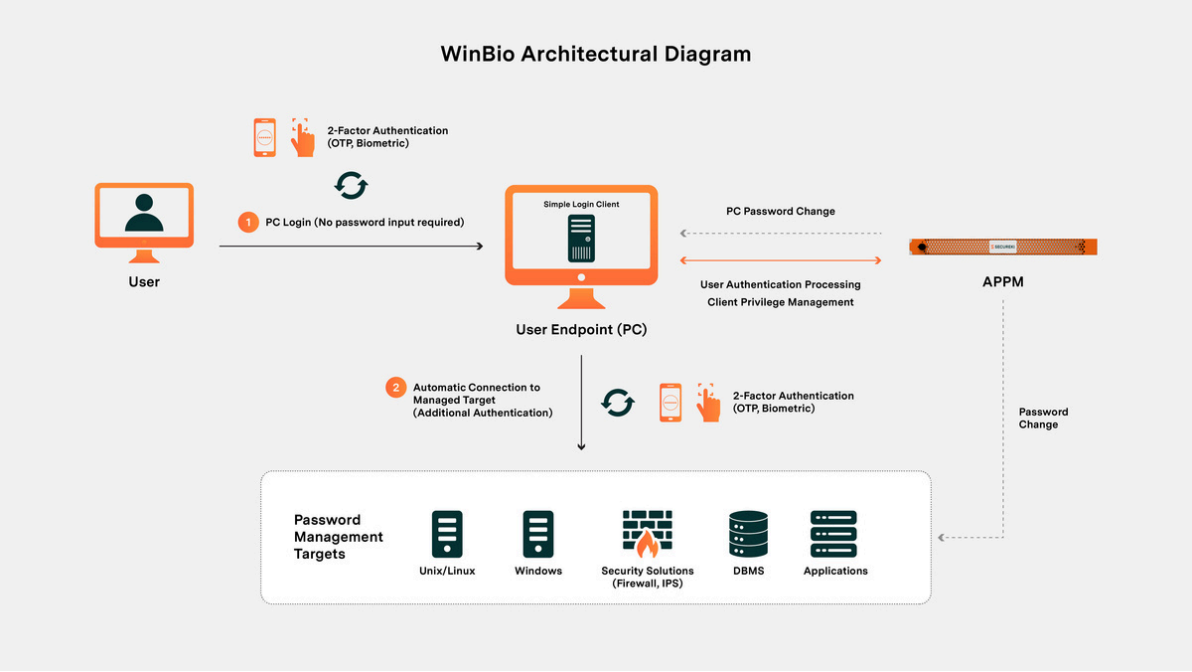


FIDO2-Level Passwordless Security

- Complies with FIDO2 standards to deliver phishing-resistant authentication
- Uses biometric and device-based verification
- Eliminates static credentials and replayable secrets

Policy and Access Control

- Fully integrated with the SecureKi Identity Security Suite
- Supports role-based access, workflow approvals, and credential expiry policies
- Provides centralized enforcement of login permissions, password retrieval rights, and OTP usage
- Delivers real-time audit logging of all authentication events
- Enables compliance with both internal policies and external regulatory standards



(SecureKi WinBio Architectural Diagram as shown above)

Use Case Scenarios

Healthcare & Shared Workstations

Overview: In hospitals and clinics, staff frequently share workstations to access electronic medical records and patient management systems. Fast and secure access is critical to avoid delays in patient care.

Challenge: Shared passwords lead to accountability gaps, while repeated password logins waste valuable time during emergencies. Compliance standards also require strict traceability of data access.

Solution: With SecureKi WinBio, doctors and nurses authenticate instantly with fingerprint or face recognition, ensuring every access attempt is tied to an individual identity. Password sharing is eliminated, access times are reduced, and full audit trails ensure regulatory compliance.

Financial Services & Regulatory Compliance

Overview: Banks and financial institutions must protect sensitive customer data and meet strict audit and compliance requirements.

Challenge: Traditional password systems are vulnerable to phishing, reuse, and credential theft, creating risk of non-compliance with FIDO2, ISO/IEC 27001, and NIST 800-63 standards.

Solution: SecureKi WinBio combines passwordless biometric login with automated password rotation, ensuring credentials are never reused or exposed. Staff access is fully logged, policies are enforced centrally, and regulatory compliance is maintained without adding burden to users or IT teams.

Manufacturing & Remote Operations

Overview: Factory operators, warehouse staff, and engineers often work in areas with limited or no internet connectivity. Systems still need to be secured, even when offline.

Challenge: Password resets are nearly impossible in disconnected environments, and shared terminals create security blind spots. Productivity drops when staff cannot log in quickly.

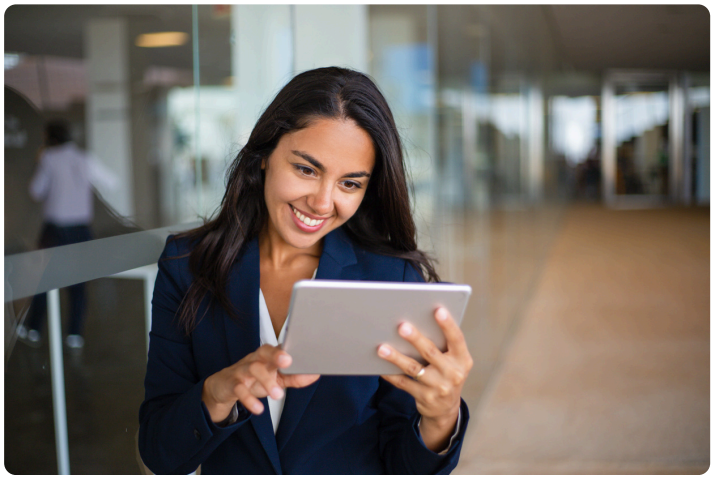
Solution: SecureKi WinBio's mobile app provides offline OTP/BOTP authentication, enabling secure access even in disconnected plants or offshore facilities. Once reconnected online, passwords are rotated automatically and tied to biometric identity, ensuring traceability without slowing operations.

Enterprise Workforce Productivity

Overview: Large enterprises face constant IT helpdesk tickets for forgotten or expired passwords. This reduces productivity and increases operational costs.

Challenge: Employees struggle with multiple complex credentials, leading to fatigue, lost time, and frustration. IT teams are overloaded with password reset requests.

Solution: SecureKi WinBio eliminates passwords from the login process entirely. Employees authenticate with biometrics, while the platform handles credential complexity and rotation in the background. This reduces helpdesk tickets, improves productivity, and creates a seamless user experience across the enterprise.



Emergency & Break-Glass Access

Overview: During emergencies, administrators or engineers may need immediate access to critical systems.

Challenge: Shared or static passwords create risk when multiple people have unmonitored access, and emergency situations often bypass normal security controls.

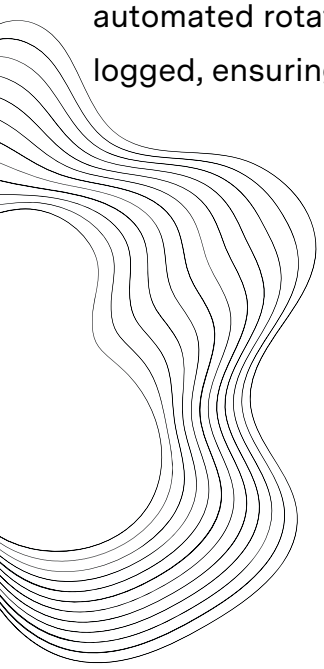
Solution: SecureKi WinBio provides controlled password retrieval through the SecureKi mobile app. Access is tied to biometric identity, logged in real time, and governed by policy. This ensures rapid emergency response while maintaining accountability and compliance.

Zero-Trust Security Model

Overview: Organizations adopting Zero Trust require strict identity verification, minimal privilege, and continuous audit across all users.

Challenge: Traditional password-based logins undermine Zero Trust by creating weak entry points that can be phished or shared.

Solution: SecureKi WinBio enforces biometric login, just-in-time credential issuance, and automated rotation as part of a Zero Trust approach. Every access attempt is verified and logged, ensuring users only have the minimum access they need, when they need it.



SecureKi Mobile App Highlights

Beyond desktop login, SecureKi WinBio extends its power through the SecureKi Mobile App. The app provides users with convenient, secure, and flexible ways to authenticate and manage credentials wherever they are — seamless, secure, and built for the modern workforce.

- Unlock with fingerprint or face recognition
- View rotated passwords with policy enforcement
- Scan QR code for desktop login
- Generate OTP/BOTP in offline environments

Comparison: Hardware Token vs SecureKi WinBio

Capability	Hardware-Token Solutions	SecureKi WinBio (Mobile-Based)
Passwordless Login (FIDO2)	✅ Yes	✅ Yes
Biometric Authentication	❌ No (PIN only)	✅ Fingerprint, finger-vein scanning and Face (via webcam)
Webcam Face Recognition	❌ Not supported	✅ Built-in or USB webcam

Capability	Hardware-Token Solutions	SecureKi WinBio (Mobile-Based)
QR Code Login	❌ Not typically supported	✅ Yes
Offline OTP/BOTP Support	✅ Yes	✅ Yes
Requires External Hardware	✅ Yes (USB/NFC key)	❌ No (Mobile App only)
Password Auto-Rotation	❌ Not included	✅ Included for AD and local accounts
Secure Password Retrieval	❌ Not available	✅ Controlled via mobile app
Access Policy & Audit Logs	✅ With integration	✅ Native with SecureKi Identity Suite
2-Step Login	❌ No	✅ Password + 2FA

Technical Specifications

- Supported OS: All Microsoft non-EOSL Windows platforms (Desktop and Server editions)
- Authentication Modes: Fingerprint, Face (via webcam), FIDO2, QR code, OTP/BOTP
- Integration Options: Active Directory, SecureKi Identity Security Suite, SecureKi Mobile App
- Deployment Models: Standalone deployment or integrated with SecureKi PAM Suite

Security and Compliance Benefits

In today's regulatory and threat landscape, compliance is no longer just a checkbox. It is a foundation for trust, resilience, and long-term business success. SecureKi WinBio helps organizations move beyond traditional password risks by aligning biometric authentication and automated credential management with global security frameworks. By embedding compliance into everyday user access, SecureKi WinBio ensures that enterprises can strengthen their security posture, meet regulatory obligations, and protect their reputation. All this without sacrificing user convenience.

- Eliminates password reuse and reduces phishing risks
- Supports Zero Trust, least privilege, and just-in-time access enforcement
- Provides accountability for shared and remote environments
- Complies with:
  - FIDO2
  - ISO/IEC 27001
  - NIST 800-63
  - GDPR

Identity Secured, Passwords Eliminated

SecureKi WinBio delivers the best of both worlds: the convenience of passwordless biometric login and the rigor of automated credential lifecycle management. By removing password risks, simplifying user access, and strengthening compliance, it helps organizations move toward a truly secure and scalable identity-first future.

Your privileged accounts deserve stronger protection. Let's talk about securing them today.

SecureKi Sdn Bhd (1143453-U)

Contact: info@secureki.com

www.secureki.com

Common Criteria Certified (EAL2)

The Common Criteria for Information Technology Security Evaluation (referred to as Common Criteria or CC) is an international standard (ISO/IEC 15408) for computer security certification. Common Criteria provides assurance that the process of specification, implementation, and evaluation of a computer security product has been conducted in a rigorous, standard, and repeatable manner at a level that is commensurate with the target environment for use.