ensurity
A Step Ahead!

Ensurity Solutions
Passwordless & MFA Solutions

Multi-factor authentication has evolved as a best practice in the industry. The FIDO2 (Fast IDentity Online) standard represents a significant leap forward in this domain, offering robust, user-friendly authentication methods that transcend traditional passwords.

Ensurity offers 'ThinC-AUTH' series of hardware-based Security Keys, designed to work seamlessly with FIDO2 and Smart card protocols. The products are Microsoft and FIDO approved.

ThinC-AUTH Series

*ThinC-AUTH **Bio** is a Biometric Security Key.*

*ThinC-AUTH **BioPro** is a Biometric Multi-protocol (PIV and FIDO2) Security Key.*

*ThinC-AUTH **Touch** is a Touch-based multi-protocol (PIV and FIDO2) Security Key.*

Additionally, Ensurity offers a life-cycle management solution 'Asset Management System (AMS)' to deploy and manage the Security Keys, is becoming a critical requirement for many enterprises. The 'AMS' is a software server that can be deployed at enterprise's data center.

FIDO2 Key - features

- **Phishing-Resistant**: Unlike passwords, FIDO2 Security Keys are robust and phishing-resistant.
- **Scalable**: FIDO protocols are designed to be scalable and can be used by any website or application.
- **Faster, Simpler Sign-in**: Enables password-only logins to be replaced with secure and fast login experiences across all users' devices.
- **Cross Platform**: Works on all Operating System browsers. No Driver is needed.
- **Open Standards**: FIDO use standard public key cryptography techniques.
- **Reliable**: ThinC-AUTH Keys are always on and accessible – does not require a battery.
- **Easy to deploy**: Enterprise IT can deploy ThinC-AUTH Keys quickly. A single key can work out-of-the-box with hundreds of systems. This eliminates the need for costly integrations or additional devices for each system.
- No Battery and No Driver is required.

ThinC-AUTH • Biometric FIDO2 Security Key

- FIDO2-certified and Microsoft approved Security Key (available in USB Type-A interface).
- Embedded with CC EAL5+ certified Cryptographic Module.
- Designed & developed with 'Privacy & Security' as core.
- Built with state-of-the-art biometric 360° phishing-resistant and spoof-resistant capacitive touch sensor.
- Fingerprint minutiae templates obtained from sensor are encrypted, securely stored and confined to the device.
- Digital identity always remain private and protected by advanced encryption using certified crypto controller.
- Biometric Authentication support includes for FIDO U2F, FIDO2/WebAuthn, and OATH-TOTP.

Standard-edition vs Corporate-edition of "ThinC-AUTH' Security Keys

Standard Edition	Corporate Edition
End-user specific usability	Enterprise-specific usability
No Inventory management	Inventory is managed by AMS
PIN can be set by anyone, and PIN based (fallback to biometrics) authentication is enabled	PIN is controlled by AMS and is unknown to any user. PIN based authentication is disabled. User mandatorily authenticates with registered fingerprint.
Anyone can enroll fingerprints	Controlled environment to enroll the fingerprints via AMS
No control on number of Fingerprints for enrollment	Number of fingerprints for enrollment can be controlled through AMS portal
RESET can be set by anyone	Controlled environment to RESET the Keys via AMS

Support for TOTP/HOTP

- ThinC-AUTH Keys are programmable to add OATH-TOTP secrets. Supports SHA1, SHA256 and SHA512.
- TOTP codes are generated and displayed (in Ensurity TOTP desktop app) only against biometric authentication.
- Supports multi-profile TOTP secrets.

'ThinC-AUTH BioPro' • Multi-protocol Biometric Security Key

- FIDO2-certified and Microsoft approved Security Key (available in USB Type-A and Type-C interfaces).
- Embedded with FIPS 140-2 certified Cryptographic Module.
- The 'BioPro' variant supports Smart Card Authentication, means of verifying users into enterprise resources such as workstations, servers, applications, and network devices, in addition to the biometric authentication to the Security Key.
- Support for multi-cryptographic protocol authentication including FIDO U2F, FIDO2/WebAuthn, TOTP, and PIV (Personal Identity Verification) Smart Card, in addition to the biometric authentication.
- Uses X.509v3 certificate for biometric PIV authentication.
- 'Biometric authentication with Certificates' works on major OS including Microsoft Windows, Linux, macOS, and platforms including VPN, Remote Sessions, as well as leading browsers.
- Recommended for most secure work environment, such as government departments and financial institutes, as their workforce mostly is not allowed to use Smartphones for authentication.
- PIV Certificate can be generated from a Windows Certification Authority, a self-signed certificate, or import an existing certificate to the AUTH BioPro Key.

'ThinC-AUTH Touch' • Touch-based multi-protocol Security Key

- FIDO2-certified and Microsoft approved Security Key (Dual USB).
- Embedded with FIPS 140-2 certified Cryptographic Module.
- Support for multi-cryptographic protocol authentication including FIDO U2F, FIDO2/WebAuthn, TOTP, and PIV (Personal Identity Verification) Smart Card.
- Cost-efficient alternative to expensive readers.

'ThinC-AUTH Touch' • Touch-based multi-protocol Security Key

Standard Edition	Corporate Edition
• No Inventory management	• Inventory is managed by AMS
• PIN can be set by anyone	• PIN is controlled by AMS. PIN complexity can be defined by the Admin.
• RESET can be set by anyone	• Controlled environment to RESET the Keys via AMS

Life-cycle Management - AMS

- When Enterprises procure the Biometric FIDO2 Security Keys and plan to distribute to their users, it is recommended to have an inventory management tools to effectively manage the steps, viz. assigning Keys, enrolling fingerprints, and managing various attributes.
- Ensurity offers 'AMS' (Asset Management System) software platform for its' corporate-edition of Biometric Security Keys.

Why Ensurity's Security Keys? — Differentiators

- Ability to customize its' Biometric Security Keys to address specific requirements of enterprises in line with FIDO2 authentication standards.
  - Hide the PIN (unknown to User) / Disable PIN-Fallback
  - Restrict the Key for single Microsoft Account
  - Restrict the Number of Fingerprint Enrollment
  - Mandate Authentication with both 'PIN + Biometrics'
  - Link the User-Biometric Index to Credential
  - Validate the Security Key Serial Number for audit
  - Integrate Digital Signature within FIDO2 Security Key
  - Asset Management System (AMS) for AUTH Security Keys – a critical life-cycle management software for enterprise deployment needs.
  - Implement 'One User One PC One Key' functionality