

# AuthTron Security Key



FIDO2 Strong Authentication  
(FIDO2 & U2F)



Turnkey solution



Built-in Crypto Engine



Key Management  
Interface

# 81% of cyberattacks result from passwords

Many attempts to establish seemingly unnecessary procedure, which is usually labeled as “red tape” in governmental entities or enterprises, are in large part to place trust and ensure accountability. In case something unexpected or violations occur, there is someone to be blamed and held accountable. The situation gets even worse in the digital world. Digital bits are invisible. We do not know whether malicious contents sneak in under the cloak of legitimacy. In this regard, we use accounts and passwords, SMS, policies and others to confirm identities. Verification is doubtlessly required, but as there are more and more accounts and passwords to memorize and nastier cyber and phishing attacks, enforcing harsher password policies resembles a hamster on a wheel. A report even shows passwords are the root of 81% of breaches (Verizon Data Breach Investigations Report, 2017). Despite strong passwords, managing passwords itself is problematic and may lead to leakage. Only by thinking beyond the frame can we devise a way of letting usability and security go hand in hand.

## Paradigm Shift in Root-of-Trust

With passwords jeopardizing productivity and security, a paradigm shift toward the PKC-based (public key cryptography) trust anchor has occurred. We no longer place trust in passwords. Rather, we place trust in cryptography; we place trust in a private key securely stored in a secure environment and never leaving its physical secure boundary. In 2021, WiSECURE Technologies joined FIDO (Fast Identity Online) Alliance, becoming a member of FIDO Japan and FIDO Taiwan. WiSECURE then collaborates with leading service providers to deliver FIDO authentication solutions. From clouds to ends, WiSECURE’s mission is to rescue governmental entities and enterprises from the threats of phishing and impersonation.

## WiSECURE AuthTron™ - Turnkey Solution

WiSECURE AuthTron™ security key is U2F and FIDO2 L2 certified, supporting password-less and multi-factor authentication. With AuthTron™ turnkey solution covering RP server, FIDO server, hardware security module (HSM) and issuance and management mechanism, WiSECURE aims to satisfy enterprise-level requirements for supervision, secure maintenance and device authorization and control. The same model has been implemented by Google with issues of data leakage and illegal access resolved. WiSECURE also provides crypto-based customization service, adding other cryptographic functions for data encryption, transaction signature, blockchain applications and so on.

You can use AuthTron™ security key to log into MicroSoft, Google, Amazon, Dropbox, etc.

Why should passwords be eliminated?

- Weak spot causing breach
- Painstaking management

From “password” to “cryptography”



AuthTron™ Features

- Enterprise orientation
- Password-less and multi-factor
- Built-in cryptographic functions





## Specification

---

Supported Applications	<ul style="list-style-type: none"><li>• FIDO2 Authenticator</li><li>• Hardware Cryptographic Module</li></ul>
Key Management Functions	<ul style="list-style-type: none"><li>• Multiple Application Key Domains (Up to 8 applications / Up to 128 keys per application)</li><li>• Support ECC (NIST P-256, P-384, P-521, Brainpool 512), RSA (2048) keys</li></ul>
Authentication Features	<ul style="list-style-type: none"><li>• Security policy for limited password attempts (FIDO only)</li><li>• Touch pattern for user presence (FIDO only)</li></ul>
Crypto Algorithms and Services	<ul style="list-style-type: none"><li>• ECDSA / ECMQV / EdDSA / RSA</li><li>• ECDH / ECIES</li><li>• HMAC-SHA2 / HMAC-SHA3</li><li>• SHA2 / SHA3 (Host Software Library)</li><li>• Key Wrapping and Unwrapping</li><li>• PBKDF</li><li>• Random Number Generation<ul style="list-style-type: none"><li>– DRBG with TRNG as seed</li></ul></li></ul>
Cryptographic API	<ul style="list-style-type: none"><li>• PKCS#11</li><li>• Native API</li></ul>
Interface	<ul style="list-style-type: none"><li>• USB 2.0</li></ul>
Certification	<ul style="list-style-type: none"><li>• FIDO2 level 1, level2 and U2F level 1</li><li>• CC EAL5+ certified security chip</li><li>• CE</li><li>• FCC</li><li>• RoHS</li></ul>

## Advantages of WiSECURE FIDO2 Solution



### Comprehensive Product Portfolio

With crypto modules applied to clouds and ends, WiSECURE is also engaged in deployment and consulting, expecting to help customers clarify potential risks in specific use cases so as to constitute the most cost-efficient solution.



### Crypto Implementation and ODM Service

From low-level crypto functions to hardware development, WiSECURE builds security products from the grounds up and also provides ODM service for customers requesting branded security keys.



### Cognition-based User Presence

WiSECURE adopts patented "cognition-based user presence", which reaches the biometrics security level without the need to access users' sensitive biometric information.

---

## FIDO2 Strong Authentication Solution Heightened Data Protection

Centering on cryptography, WiSECURE is devoted to protection of customers' valuable data. Built on FIDO2 certified AuthTron™ security key and CryptoAir® encryption engine, the data protection solution FileAegis® has been launched to protect and securely share data. Employing FileAegis® ensures

### **You can trust your data are secure**

Data on premises are encrypted in case of internal and external attacks or human errors

### **You can trust co-workers' data are safe**

FIDO2 authentication cracks unauthorized access and enforces audit logging of action

Additional signing mechanisms can also be supplemented

### **You can trust customers' data are sealed**

Leakage of customers' personal information may bring about massive legal fines

FileAegis® protects data at rest and in transit from malware, man-in-the-middle attack and unauthorized access. FIDO2 authentication framework enables least privilege management and audit logging to enforce enterprise security policy.

To know more about our solution or FIDO2 application, please contact us.

<https://www.wisecure-tech.com/contact/>

+886-2-29343166