Phoenix SecureKey™

Datasheet

PC Protection Rooted in Firmware

Phoenix SecureKey combines firmware-enforced protection with a physical authentication device (pass key) to provide resilient firmware anti-intrusion security for Windows-based PCs. Computers are protected against unauthorized access as Phoenix SecureKey allows operating system start and login only when an authentication device has been detected and validated. Smartphones, USB thumb drives, BLE and FIDO compliant devices can all be used with SecureKey, while custom pass key devices can also be employed. FIDO compliant devices incorporating cryptographic techniques against spoofing and fake copies of the device provide a more secure method for passwordless physical presence and user identity authentication. Additionally, Bluetooth RSSI (Received Signal Strength Indicator) allows configuration of pass key proximity settings for device discovery and connection.

PC Protection

- Extra authentication layer prevents booting the PC with only a login password
- Cryptography and Bluetooth/FIDO protocols defend against using a fake copy of the pass key
- Configurable to support single or multiple pass keys for single or multi-factor authentication without needing a password
- User-authenticated recovery available via cryptographically secured unique or common passcodes
- Registered pass key devices enable physical presence protection, while FIDO biometric devices provide additional user identity authentication
- User configurable Bluetooth proximity controls via RSSI

Key Components

- UEFI firmware feature: start/wake the PC using security features at the firmware level
- Pass key: physical USB drive, Bluetooth, or FIDO compliant device registered with the firmware to start or wake the PC

Use Cases

- Corporate: safeguard PCs from unauthorized access
- Education: control student access to school PCs
- Parental Controls: manage child access to any PC
- Personal Security: protect data if the PC is lost or stolen

Easy to Use

- No special hardware required—a standard USB key, Bluetooth, or FIDO compliant device can be registered as a pass key device
- Firmware will not allow Windows to start from power-on or hibernation without a pass key device
- Protects at the firmware level for single or multi-factor authentication using multiple pass keys without needing a password
- Single sign-on (SSO) authentication for Windows 10 enhances the user-experience by logging into Windows on behalf of the user without needing a password
- Passcode protection ensures easy recovery if a pass key is lost or stolen
- Configurable time-out setting shuts down the PC if a pass key device is not present, saving battery life

Secure

- Prevents intrusion using a stolen Windows login password because the firmware will not load the operating system or allow login if the pass key device or recovery passcode cannot be authenticated
- Cryptographic technology is used to authenticate the pass key and protect the passcode data stored in the PC hardware
- Rolling code algorithms and security standards incorporated in the Bluetooth and FIDO specifications prevent intrusion attempts with a fake copy of the pass key
- Registered pass key devices enable physical presence protection, while FIDO biometric devices provide additional user identity authentication
- Bluetooth RSSI controls allow users to configure proximity limits

Easy Recovery with Backup Passcode

- Users register either unique or common passcodes to recover the system should the pass key become lost or stolen

Want to learn more about Phoenix SecureKey?

Send us an email at sales@phoenix.com

phoenix® technologies