

SafeBoot® FOR USB Phantom

Secure USB Flash Storage & Token Services



SAFEBOOT® FOR USB PHANTOM IS SECURE USB FLASH STORAGE THAT INCORPORATES BUILT-IN USER ACCESS CONTROL AND STRONG DATA ENCRYPTION – ENSURING THAT SENSITIVE DATA REMAINS SECURE WHEREVER IT TRAVELS. IT ALSO PROVIDES BOTH PERSONAL AND CORPORATE CREDENTIAL PROTECTION AND VALIDATION, ENSURING THAT IDENTITIES REMAIN SECURE.

In today's organizations, mission-critical data travels freely across networked environments and the Internet, and it is stored and accessed on a variety of devices, including USB flash storage. The storage capacity of these devices has grown enormously, even while their physical size has become smaller. This makes them highly portable and capable of storing a wide variety of mission-critical information. However, reduced size makes these devices easier to lose, and a higher storage capacity increases the potential amount of data at risk for unauthorized access if a device is lost or stolen.

STRONG, MULTI-USER ACCESS CONTROL

SafeBoot for USB Phantom supports multiple users – each with their own secure partition. A password and/or fingerprint will unlock SafeBoot for USB Phantom and grant the user access to their data. A maximum number of password or biometric authentication retries may be set to counter a brute-force attack. SafeBoot for USB Phantom may even be shared with others without compromising each other's sensitive information. By using an optional "public" area on the device, sharing information with colleagues, partners, friends and family can be achieved without the need to share the entire file structure.

POWERFUL, TRANSPARENT ENCRYPTION

USB (Phantom uses AES-256 to encrypt all data stored on USB flash devices. The encryption and decryption processes are transparent to the user and are performed "on-the-fly," with virtually no performance loss. Like all SafeBoot products, no end-user training is required.

PORTABLE SECURITY TOKEN SERVICE (PSTS) SUPPORT

SafeBoot for USB Phantom is a state-of-the-art, Portable Security Token Service (PSTS) for WS-Trust. USB Phantom is capable of issuing SAML tokens for an unlimited number of bindings to Target Services.

CRYPTOGRAPHIC SERVICES

SafeBoot for USB Phantom offers a host of general-purpose, industry standard, cryptographic services, including random number generation, key generation with internal or external entropy, symmetric encryption / decryption (AES), asymmetric signing, verification, encryption and decryption (RSA), One Time Password (OATH HOTP), secure hash (SHA-1 and SHA-256) and compliance with industry standards such as X9.31, PKCS #1 and SAML 1.1.



DRIVERLESS & "ZERO-FOOTPRINT" TECHNOLOGY

Maximum flexibility is provided through "zero-footprint" technology. SafeBoot for USB Phantom provides security independent of the operating system environment. USB Phantom does not require software installation nor administrator rights – all that is required is an accessible USB port.



SECURE CENTRAL RECOVERY

If a user forgets a password or leaves the organization, information can still be retrieved from USB sticks from the SafeBoot for USB line.



SafeBoot does not use one password as a backdoor. Instead, it uses unique, centrally-stored passwords accessible only by IT security administrators.

SAFEBOOT® PORT CONTROL COMPATIBILITY

In combination with SafeBoot® Port Control™, data leakage is a thing of the past. Now it is possible to granularly block any type of device except the fully secured USB storage device, SafeBoot for USB. Users do not have control over the security policies that are set centrally by SafeBoot security administrators within the company.



SAFEBOOT FOR USB PHANTOM BENEFITS

- Secure USB data storage/transport
- Secure token services
- Helps organization to comply with regulatory data security mandates such as Sarbanes-Oxley, HIPAA, Basel II
- Eliminates costs associated with USB/data disposal

SAFEBOOT FOR USB PHANTOM FEATURES

- Strong multi-user access control
- Authentication via password and/or fingerprint
- Powerful AES-256 encryption
- Driverless & “zero-footprint” for true portability.
- PSTS (Portable Security Token Service) support
- Encrypts data on-the-fly and is transparent, requiring no end-user training
- Optional public area for sharing non-encrypted information
- Secure recovery mechanisms
- SafeBoot Management Center for USB integration
- SafeBoot Port Control compatibility
- FIPS140-2 certification
- Worldwide support network, including 24/7 support

SPECIFICATIONS SUMMARY

(VISIT WWW.SAFEBOOT.COM FOR MORE INFORMATION)

Interface

- Instant Plug & Play operation
- USB 1.1, 2.0
- USB bus power (no external power needed)

System Requirements

- Windows 2000, Windows 2003, Windows XP®, MAC, Linux

General Purpose Cryptographic Services

- One time password generation compliant with OATH HOTP algorithm
- SHA-1 and SHA-256 hash algorithms
- Keyed-Hash Message Authentication Code (HMAC)
- RSA key generation (X9.31 and PKCS #1)
- 1024/2048/3072 bit RSA Key sizes
- RSA Signature and Verification (X9.31 and PKCS #1)
- RSA Encryption/Decryption (PKCS #1)

Portable Security Token Service (PSTS) Capabilities

- WS-Trust profile support using SAML 1.1
- Supports Microsoft InfoCard

Storage

- Ranges from 128 MB to more than 2 GB

Regulatory

- EMC, FCC, CE
- FIPS140-2

Warranty

- Limited, one-year warranty (return to point of purchase)

CERTIFIED, AWARD-WINNING TECHNOLOGY

With approximately three million users, SafeBoot has the largest installed base of any device and data security solution. SafeBoot has achieved consecutive 4- or 5-star ratings from SC Magazine, as well as the SC Magazine Reader Trust Award for Best Encryption Product. SafeBoot holds several certifications, including FIPS 140-2 and Common Criteria EAL-4, ensuring that SafeBoot solutions employ true strong encryption and secure key management. The solution is widely used by organizations worldwide, including banks, insurance companies, consultancy firms, governmental bodies, and health care organizations.

