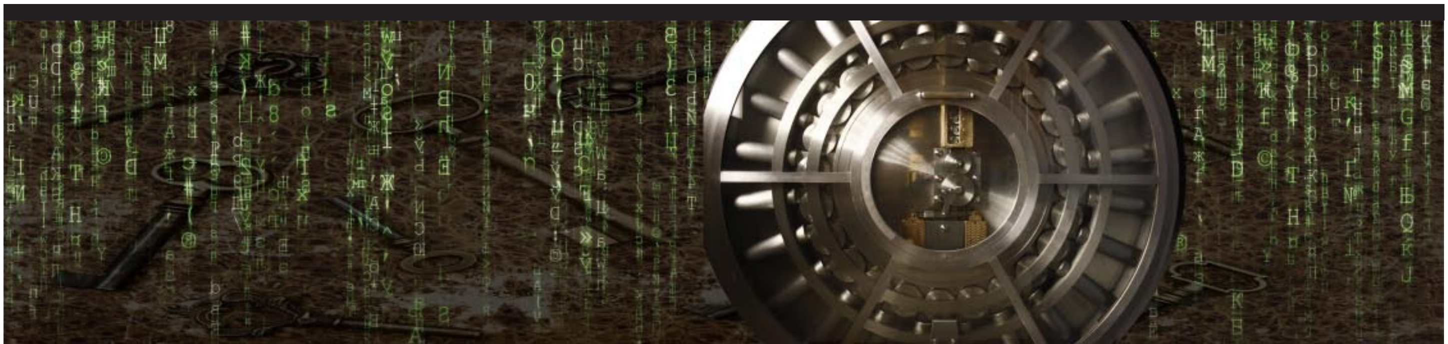
Engage Black•Vault HSM



Hardware Security Module

The **Black•Vault HSM** is a portable or embeddable Ethernet attached **H**ardware **S**ecurity **M**odule that combines a cryptographically advanced **HSM** with a Smart Card Reader and integrated touch screen display.

Independently Certified

The **Black•Vault HSM** is an independently certified standards based security module that performs key management and cryptographic operations for: application data, regulatory compliance and critical security systems employed by governments, PKI, enterprises...

Integrated Trust Path Authentication

An Integrated Touch Screen display with an intuitive menu provides administrators with a certified Trust Path for configuration and PIN entry.

Two-factor authentication and administrator roles with M of N prevents unauthorized access to critical security parameters.

Portable / Embeddable Form Factor

The compact "hard drive" form-factor and battery backed solid state key storage makes it possible to secure cryptographic keys in an HSM appliance that easily fits in a safe. The small form factor with Ethernet connection also supports mounting the **Black•Vault HSM** within application servers and other compact environments.

Military Grade Tamper Reactive

The Cryptographic Boundary is within Secure CPU's silicon. The Die Shield has dynamic fault detection with real time environmental and tamper detection circuitry.

- Achieves Level 3+ Tamper
- Eliminates Inadvertent Tamper
- Transport Safe

Benefits

- Overcomes Vulnerabilities of Soft Crypto
- Integrated Trusted Path Authentication
- Protects Intellectual Property
- Expedites Regulatory Compliance Audits
- Compact Size Fits in Safe Deposit Box
- Embeddable: Ethernet Attached
  - Hard Drive Form Factor
- Secure Key Management:
  - Generation, Storage, and Backup
- Protects Registration Authority keys
- Efficient offline root CA
- Code and Document Signing

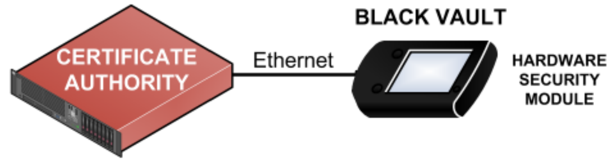
Features

- Solid State Design
- Certified Security Architecture
- Tamper Reactive Die Shield
- Suite B Accelerators
- Support for NIST ECC Curves
- Touch Screen Menu
- Secure Authentication/Access
- Role Based Multi factor authentication
- Backup through Key Cloning
- M of N per role

PUBLIC KEY INFRASTRUCTURE

Black•Vaults HSM are used by commercial and private certificate authorities (CAs) and registration authorities (RAs) to generate, store, and manage key pairs.

The **Black•Vault HSM** ensures that the Private key associated with a Certificate's public key is kept private. All cryptographic operations are executed within a 10 year battery backed semiconductor with a tamper reactive die shield.

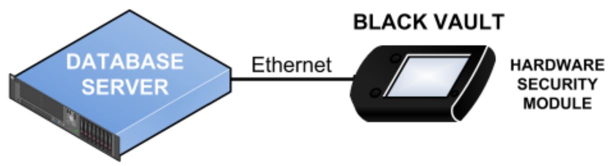


The **Black•Vault HSM** provides:

- Logical and physical protection
- Multi-factor user authorization
- Full audit and log traces
- Secure key backup

SECURING SENSITIVE AND SECRET DATA

Encrypting and Decrypting data using secret keys generated and retained within the **Black•Vault HSM** provides a certifiable level of assurance. Performing cryptographic operations in software within a general purpose operating system has proven exploits.



The vast majority of an enterprise's information is sensitive or secret and must be protected to prevent serious risk to operational continuity.

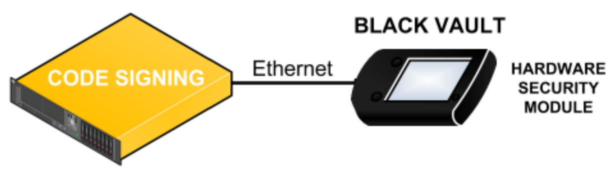
Employment of the **Black•Vault HSM** isolates and shields the critical security parameters and cryptographic operations.

CODE AND DOCUMENT SIGNING

Software Developers need to deliver Code, Patches, Scripts, and Libraries that are readily verifiable by installers as being authentic and unmodified. Similarly, electronic transfer and storage of documents increasingly requires that the validity of those documents can be ascertained.

Digital signatures provide a proven cryptographic process for code installers and document users to validate the authenticity of the publisher and content.

The critical security parameter of a code or document signing process is the private signing key. The theft of a private code or document signing key by a person or organization with malicious intent, could result in the introduction of attacks, malware, and corruption from what appears to be a "validated source".



Keys stored on on the same servers used for code development or document generation are susceptible to unauthorized access and compromise.

Generating and Storing the private code signing keys in the tamper-reactive, independently FIPS certified **Black•Vault HSM** hardware security module eliminates this organization crushing vulnerability.

Proven interoperability with:

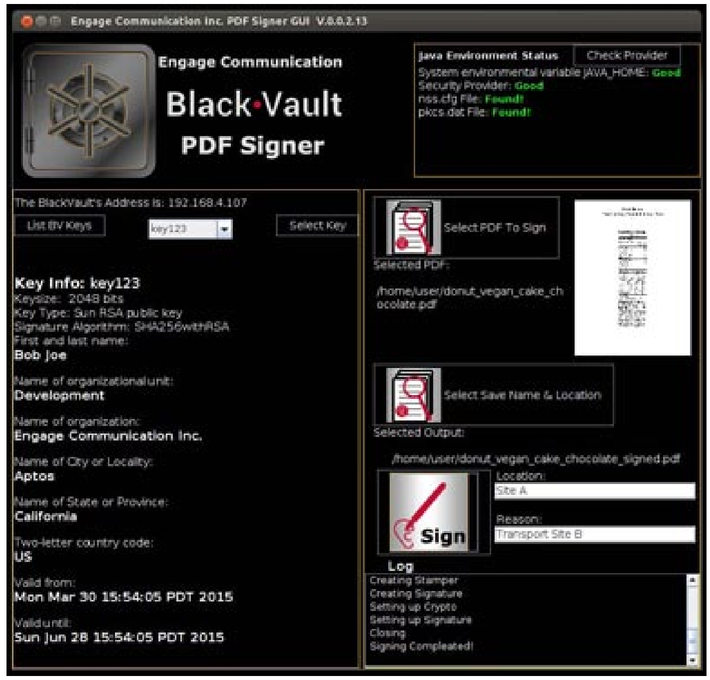
- Microsoft Authenticode
- Java Jarsigner
- Adobe Signature
- Eclipse

BlackVault Signer Applications: PDF, JAR and ZIP

Black•Vault Signer applications make code and document signing a well defined experience. The importance of and reliance on digital signatures is growing, and is critical in e-government, e-commerce, and e-banking domains. The security of private keys used in this process is equally important.

Black•Vault Signer makes this the signing process highly secure and easy to adopt for **PDF**, **Zip**, **JAR** and other document types. The **Signer** applications works with Windows and Linux.

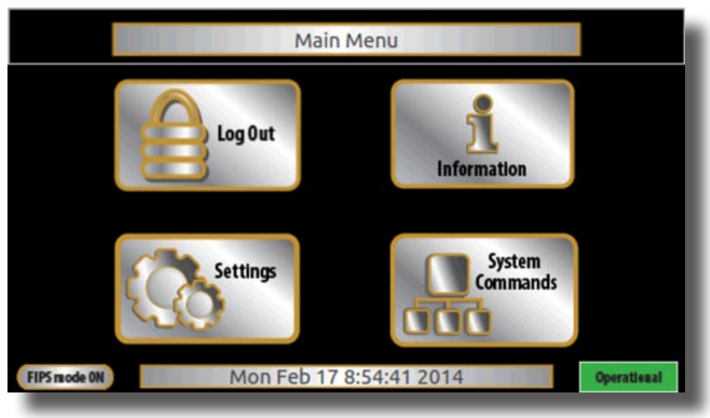
A single screen menu provides a comprehensive view of every selection required to sign. Status of the operational environment is provided to eliminate unexplained faults. The real time log provides detailed feedback.



MANAGEMENT

Black•Vault HSM utilizes a resistive touch LCD color display to provide an intuitive iconic user interface. A structured menu system facilitates straight forward configuration and management.

The user interface presents Crypto Officers with a sequence of dialog boxes that lead through a series of well-defined steps to initiate the HSM and provision cards and keys.

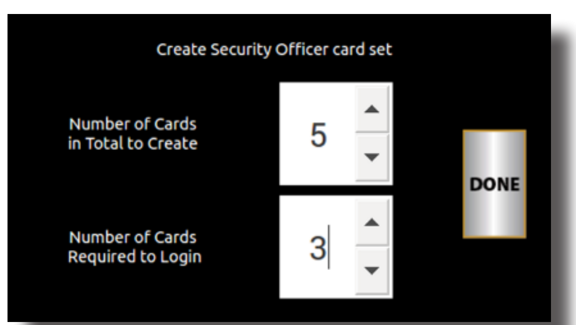


Integrated Smart Card Reader

The **Black•Vault HSM's** Smart Card reader connects to industry standard smart cards via PKCS#11 such as the industry leading Gemalto IDPrime .NET. Two-factor authentication (2FA) solutions secure Crypto Officer and Operator access with Digital Certificates (PKI).

Security Officer Card Creation

Straight forward setup of Security Officer(s) cards with "m of n" multifactor authentication.



Console Interface

An RS232 Console provides a connection to the Command Line interface.

Engage

Black·Vault HSM

Hardware Security Module

Technical Specifications

Supported Operating Systems
- Physical: Windows, Linux
- Virtual: VMware, Windows

Application Program Interfaces (APIs)
- PKCS#11, Java (JCE), Microsoft CAPI/CNG

Host Connectivity
- Ethernet 10/100 Copper; Optional SFP
- TLS

Cryptography
- Asymmetric public key algorithms:
  - RSA (1024, 2048, 4096, 8192),
  - Diffie-Hellman, DSA, ECDSA, ECDH
- Symmetric algorithm: AES 256
- Hash/message digest:
  SHA-1, SHA-2 (224, 256, 384, 512bit)
- Full Suite B implementation with
  Elliptic Curve Cryptography (ECC)
- Hardware Random Number Generator
  - NIST SP 800-90 compliant

Compliance
- Pending FIPS 140-2 Level 3+

Management and Monitoring
- Touch Screen Graphical User Interface
- Command Line Interface
- Syslog diagnostics support
- SNMPv3 Monitoring and Traps

Physical Characteristics
- Portable/Embeddable (Server Hard Drive Mechanics)
- Integrated Smart Card Reader
- Dimensions 102 x 153 x 26 mm (4 x 6 x 1in)
- Weight: 454g (1lb)
- Temperature: operating -10 to 60°C,
  storage -20 to 70°C
- Humidity: operating 10 to 90%
  storage 0 to 95%

Safety, and Environmental Compliance
- UL, CE, FCC • RoHS

Power
- DB9 Connector: Dual Hot Standby 5 to 30 VDC
- Power consumption: 4W

Engage • 9565 Soquel Drive, Aptos, CA 95003 • Tel: +1.831.688.1021 • 1.877.ENGAGE4 • www.engage-black.com