BlackVault *Hardware Security Platform*

SECURE

TRUSTED

INTUITIVE

Engage

Cryptographic Appliances with Integrated
Level 3+ Hardware Security Module

The **BlackVault** hardware security platform keeps cryptographic material safe and secure, while providing application specific appliances that greatly simplify incorporation of Hardware Security Module (HSM) functionality into Certificate Authority, Registration Authority, Code Signing, Document Signing and other Public Key Infrastructure (PKI) applications. It also supports existing HSM applications using traditional APIs and can incorporate custom functionality.

SECURE

Integrated Layer 3+ Tamper Reactive HSM secures cryptographic material from physical and environmental tamper

SECURE

Advanced cryptographic algorithms include Suite B, Elliptic Curve Cryptography (ECC) along with traditional algorithm and hash / message authentication support

SECURE

Secure Boot ensures that the operating system and application code is root signed

TRUSTED

Built-in touch screen display and smart card reader allow direct authentication at the BlackVault, removing the risk of compromise by intermediate parties, software or devices

TRUSTED

M of N authentication and key backup partitioning ensure multi-person authentication prior to administrative modifications to the BlackVault, or key backup distribution

TRUSTED

NIST compliant Random Number Generator (RNG) and FIPS “certified” cryptographic algorithms

INTUITIVE

Integrated touch screen with easy to use GUI simplifies setup and operation

INTUITIVE

Securely boots as application specific appliance, avoiding complexities of traditional OS / HSM installation and configuration

INTUITIVE

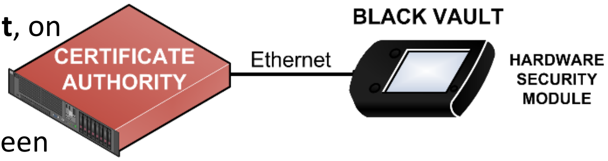
Supports PKCS#11 and CAPI/CNG APIs for use with existing HSM applications

BlackVault - Hardware Security Module (HSM)

In HSM mode, the **Black•Vault** hardware security platform functions as a traditional HSM, with unique functionality that makes authentication, security and ease of use paramount. It's compact form factor allows for easy placement on a desktop, server hard drive slot, or in a safe for off-line applications. A battery life of over 10 years and robust transport characteristics, mean the **Black•Vault** can easily be moved to different locations without risk of loss or compromise of cryptographic material. Ideal for enterprise and cloud companion applications the BlackVault supports both networked and stand-alone operation.

Public Key Infrastructure (PKI)

CA and RA functions are at risk when PKI private keys are managed by general purpose OS / servers. The **Black•Vault**, on the other hand, securely stores keys in a tamper reactive semiconductor die-shield and allows multi-factor authentication with a single trust path. A built-in touch screen display and support of major crypto-APIs make integrating **Black•Vault** a familiar process.

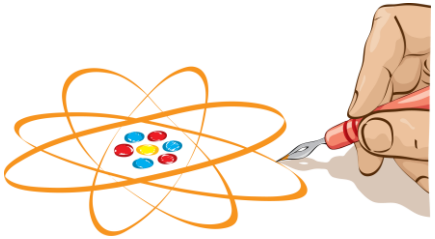


Code Signing

Injecting malicious code into legitimate applications is a powerful tool available to cyber attackers. It is increasingly important to ensure private keys associated with these digital signatures are secure. **Black•Vault** uses proven cryptographic processes to support Microsoft Authenticode (CAPI / CNG) and PKCS#11 based Java, Linux and other code signing environments

Document Signing

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** makes this process highly secure and easy to adopt for PDF, ZIP, JAR and other document types.



Data at Rest

Generation, management and protection of cryptographic keys used to encrypt database files is crucial. **Black•Vault** ensures these keys are not only secure, but also available when needed.

BlackVault CYNR – Code Signing Appliance

The **Black•Vault CYNR** is a “plug-n-play” code signing appliance that allows software developers to easily digitally sign and timestamp their software. Digital signatures can be self-signed or tied to a standard chain of trust. Developers can sign code locally at the **CYNR** by using its USB port to insert the code, and touch screen display to operate the signing process. Alternatively, networked code signing is also supported via the **CYNR’s** secure Ethernet port and integrated client application. All cryptographic material and signatures are stored within the **Black•Vault CYNR** highly secure HSM.

Increased Security

The **Black•Vault CYNR** enables publishers concerned about the risk of spyware, malware, etc. being introduced into their code, to incorporate Hardware Security Module (HSM) protection into their code signing process; without the complexities of installing and operating general purpose Operating Systems and HSMs. Private keys are secure in a Level 3+ tamper reactive cryptographic boundary.

Smart Card Reader with 2-Factor “m of n” authentication makes the establishment of Quorums inherently straight forward.

Easy to Use

With the **Black•Vault CYNR**, highly secure code signing within a powerful HSM can be up and running in minutes. The **CYNR** powers up in Code Signing mode and once authenticated, allows all signature information to be entered via its integrated touch screen display. Signing code is as simple as inserting a USB stick with the code on it and performing a few quick steps on the touch screen display. Of course, the **Black•Vault CYNR** can also be connected to the network for centralized code signing applications.

BlackVault CYNR – Document Signing Appliance

The **Black•Vault CYNR** brings a new level of security and simplicity to document signing by integrating document signing applications and Hardware Security Module (HSM) protection into a unified solution. From a user friendly client interface simply select the file to be signed, create the public / private key pair (or select a previously existing key) and click sign. The digital signature, along with its public key and certificate are included in the file in the appropriate document format. Behind the scenes the integrated HSM creates, stores, and logs private key and digital signature information in a highly secure Level 3+ tamper reactive device.

Increased Security

Digital signatures play an ever increasing role in authenticating and verifying the integrity of documents and files used in legal, financial, real estate, code archiving, and other transactions. With the growing sophistication of cyber attackers, ease of forging electronic signatures, and concern of internal fraud, organizations must put appropriate security measures in place. The **Black•Vault CYNR** provides this high level of security with a digital signature process that is both easy to implement and use.

PDF Signing

The **Black•Vault CYNR** allows **PDF** documents to be securely signed and certified using an intuitive client application that automatically incorporates HSM private key management and storage functionality. Digital signature transactions are logged and available through the **Black•Vault CYNR** management console. Time stamping of transactions can also be selected.

JAR / ZIP Signing

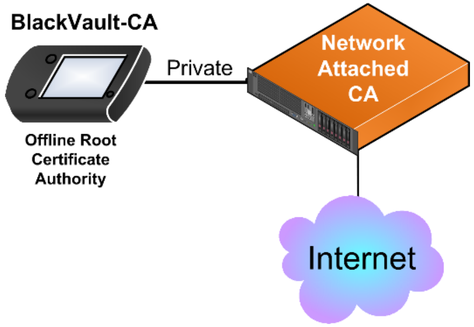
Black•Vault CYNR makes it easy to incorporate higher security for private keys and certificates associated with **ZIP** and Java Archive (**JAR**) signing. An easy to use client application seamlessly integrates HSM functionality into the process, ensuring cryptographic material is only created and processed within a protected environment. Signing transactions are logged to ensure traceability for audit and forensic purposes.

BlackVault CA – Certificate Authority Appliance

The **Black•Vault CA** is an integrated Certificate Authority appliance that can be configured as a root CA generating its own self-signed certificate, or a subordinate CA with a chain of trust to the root CA. It generates certificates for a variety of Public Key Infrastructure (PKI) applications and publishes a Certificate Revocation List (CRL). The BlackVault CA provides an integrated CRL Distribution Point (CDP) whose location is included in the certificate, and supports the Online Certificate Status Protocol (OCSP) to respond to specific certificate revocation status requests.

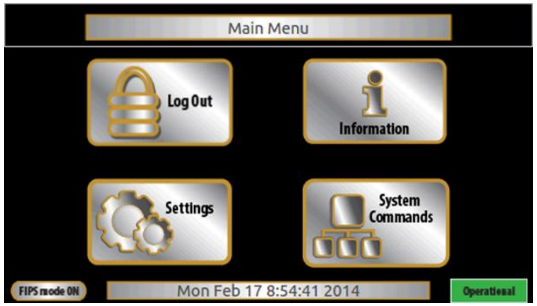
Increased Security

With the **Black•Vault CA**, enterprise, utility, government and other security stakeholders can now easily introduce Hardware Security Module (HSM) protection into their PKI infrastructure. The growing sophistication of cyber criminals makes protecting certificate generation, storage and management a top priority. **Black•Vault CA** performs all CA functions inside a tamper reactive HSM with sophisticated multi-factor authentication.



Easy to Use

The **Black•Vault CA** is “purpose-built” for Certificate Authority applications. Unlike general purpose OSs and stand-alone HSMs, the **Black•Vault CA** powers on in CA mode automatically linking all CA functionality to its highly secure, Level 3+ HSM. A built-in touch screen display and smart card reader enable authentication and setup directly at the HSM.



Online / Offline

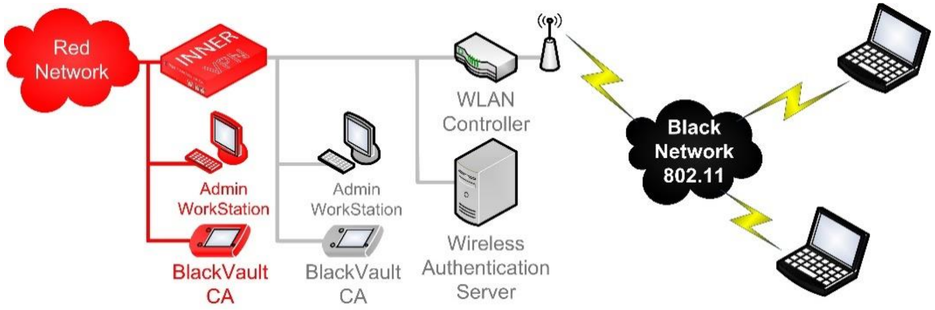
Black•Vault CA is ideal for both online and offline CA operations. It can be network attached, via its secure Ethernet port, responding to certificate and CRL requests in real time. Or it can perform CA functions offline using its USB port. The **Black•Vault CA** can even be powered down and stored in another location or safe, taking advantage of its 10 year battery life.

BlackVault - Commercial Solutions for Classified (CSfC)

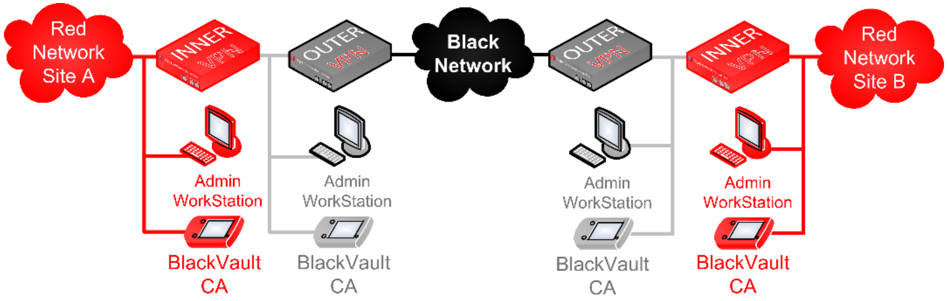
To assist with the rapid adoption of new technologies for National Security Services (NSS) applications, the U.S. Government is creating "Capability Packages" that provides reference architectures and configuration information to construct layered security solutions with commercial equipment. Certificate Authority (CA) functionality is a key element in these architectures and the **Black•Vault CA** appliance provide increased security and protection while simplifying operational procedures when compared to software / server based CAs. The **Black•Vault's S**uite B and elliptical curve cryptography, Level 3+ tamper reactive support, silicon-based cryptographic boundary, compact form factor, and built-in 10 year battery are effective for both online and offline CA applications.

BlackVault CA - CSfC

The **Black•Vault CA** appliance securely boots into CA mode avoiding the complicated setup process typically associated with HSMs and general purpose OS CAs. Once up, authentication can be performed directly at the **Black•Vault CA** using its integrated smart card reader and touch screen display. Self-signed or root trust certificates are generated, Certificate Revocation Lists (CRLs) maintained and distributed, and logs of all activities kept.



CSfC Campus IEEE 802.11 Wireless Local Area Network



Independently Managed Virtual Private Network

SECURE TRUSTED INTUITIVE

BlackVault *Hardware Security Platform*

Cryptography

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

Protocols

- SSH, SFTP, FTP, TLS

Hardware

- Hardware True Random Number Generator
  - NIST SP 800-90 compliant
- Secure Boot Loader: Public Key Authentication
- Memory Encryption And Integrity Check
- Real-Time Clock
- Resistive Touch Color TFT
- Smart Card Reader: ISO 7816
- Ethernet 10/100 Copper or Optional SFP Fiber
- USB 2.0 Host and Device
- Dual Hot Standby 5 to 30 VDC • 4 Watts

Compliance

- Pending FIPS 140-2 Level 3+
- Tamper: Mechanical, Die-Shield, Temp & Voltage

Physical Characteristics

- Portable (Server Hard Drive Mechanics)
- Dimensions 102 x 153 x 26 mm (4 x 6 x 1in)
- Weight: 454g (1lb)

Engage

1.877.ENGAGE4 • +1.831.688.1021
9565 Soquel Drive • Aptos, Ca 95003
sales@engageinc.com • www.engage-black.com