ENGAGE BLACK

Black•Vault CA

Certificate Authority with integrated HSM

The **Black•Vault CA** is a **Certificate Authority** with an integrated **Hardware Security Module** that simplifies and secures the implementation and operation of PKI infrastructures. Ready to deploy purpose built FIPS level 3 CA appliance that performs:

- X.509 certificate generation
- CSR and CRL processing
- OCSP and EST servers
- Key generation & management

The **Black•Vault CA** is deployed as a root or subordinate CA and is effective in online and offline PKI applications including:

- VPNs, TLS
- Industrial Internet of Things (IIoT)
- Web Services
- Code & Document Signing
- Secure Email
- NSA Commercial Solutions for Classified

The **Black•Vault CA** securely boots up as a secure certificate authority server running inside of a tamper reactive cryptographic boundary. All cryptographic functions, including private / public key generation and certificate signing are performed inside FIPS Level 3 protected hardware.

The cryptographic algorithms are also FIPS certified and use a sophisticated NIST hardware random number generator to ensure key entropy. Private keys are never in the clear; including key backups where keys are encrypted.

Military Grade Tamper Reactive

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

Benefits

- CA Appliance
  - Eliminates Complex Software Installation
- Out of Box Ultimate Level of Security
  - Integrated HSM with truly Private Keys
- 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

Features

- Secure Boot
- Solid State Design
- Certified Security Architecture
- Tamper Reactive Die Shield
- Suite B Accelerators
- Support for NIST ECC Curves
- Secure Authentication/Access
- Enrollment over Secure Transport
- High Availability

BlackVault CA Operation

Black•Vault CA cryptographic operations are performed in accordance with the FIPS mandates of the Computer Security Division of the National Institute of Standards and Technology.

Secure Boot uses a One Time Factory Programmed key to ensure that only code signed by Engage Black's private key is executed.

Critical Security Parameters, such as a certificate's private key, are encrypted by an inaccessible Master key that is zeroized upon tamper.

Secure and Effective Management
Management interface is accessed by an authenticated and encrypted Secure Socket Shell channel. Operation is partitioned by privilege into security relevant functions that are Administrator, Auditor and Operator role based.

Elliptic Curve Cryptography
ECC is mandated by government Security Agencies around the world. **ECC**'s computational efficiency benefits resource-constrained devices such as those used for **IoT**.

Enrollment over Secure Transport
EST is a certificate management protocol that utilizes Certificate Management over Cryptographic Message Syntax (CMC) over a secure transport. **EST** profiles certificate enrollment for PKI clients and supports elliptic curve cryptography (**ECC**).

Certificate Signing Requests
Certificate Signing Request are input from **EST** clients, as files or copied and pasted by an administrator's computer.

Certificate Distribution
Devices can obtain certificates through **EST,** Secure File Transfer, USB and Copy & Paste.

Validation Authority
Certificate validation is provide through Certificate Revocation Lists (CRL) that are available on an internal or remote HTTPS server or accessed with the Online Certificate Status Protocol (OCSP).

Real-Time Audits
Cryptographically protected Real-Time Audits of the configuration & operation provides Security Administrators with the information needed to discover anomalous activity or failure of critical functions.

Backup
There are 2 methods to backup certificate information: **Cloning** and **S**ecure **F**ile **T**ransfer.

High Availability
Real Time Cloning with redundant load sharing and power.

Industrial Rated Hardware
Solid State design with -20 to +60 Centigrade operating temperature range.

Industrial Internet of Things PKI CA

Black•Vault CA specifically targets **Industrial IoT's** security need for secure identity authentication.

Establishing the foundation of trust that **IIoT** systems, devices, applications, and users need to safely interact and exchange sensitive data.

Specifically the **Black•Vault CA's** support for **ECC** and **EST** enables IIoT devices to readily achieve Certificate based authentication.

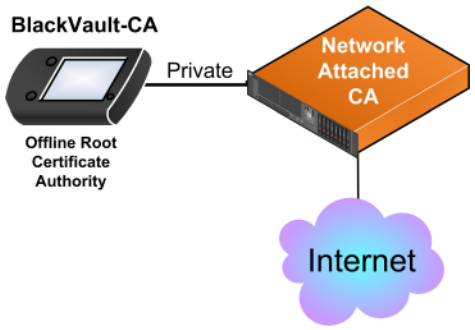
Secure identity authentication for:

NERC CIP, IEC 62351, SSL, TLS, HTTPS

Offline Root Certificate Authority

Security conscious organizations that run internal PKIs operate their root CA offline. **Black•Vault CA** is ideally suited to be the Offline Root CA for public and private PKI infrastructure.

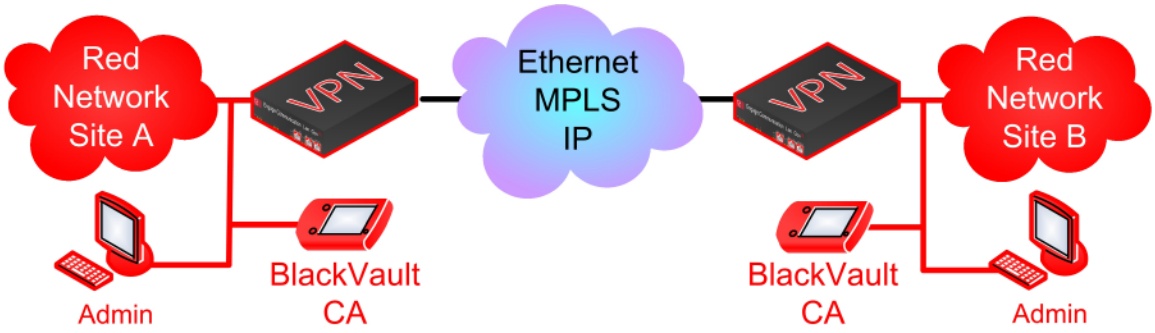
- Security of the Private Key
  - Tamper Reactive Die Shield
- Ultra Advanced Cryptography
  - Elliptical Curves
- 7 Year Battery Backed Store
- Fits in a Safe



VPN Authentication

The **Black•Vault CA** Certificate Authority facilitates secure connection establishment between VPN gateways by providing an X.509 authentication method to validate identities. Easy to use and highly secure, the BlackVault CA removes all excuses for not running secure Virtual Private Networks.

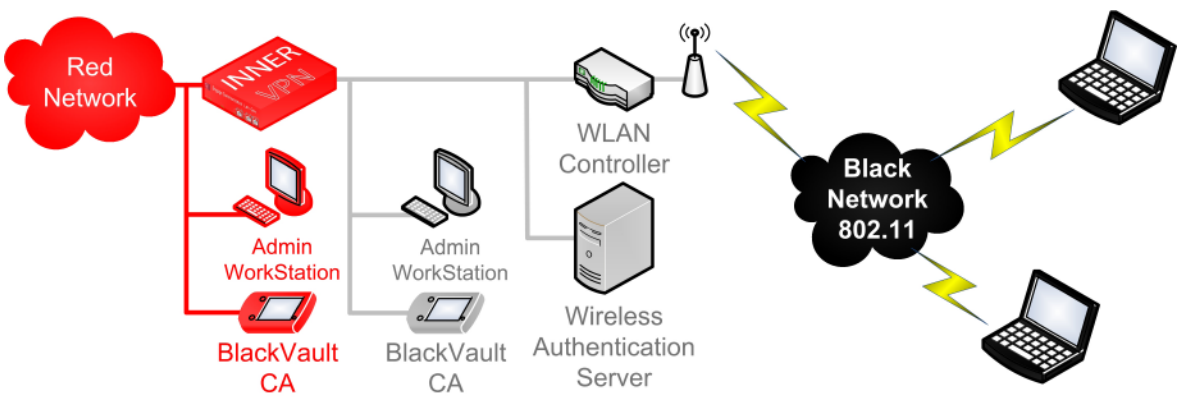
VPN gateway Certificate Signing Requests are input by a command line copy and paste method or via the Simple Certificate Enrollment Protocol. Certificate Revocation List are retrieved by VPN gateways using Online Certificate Status Protocol (OCSP).



Wired Virtual Private Network

Commercial Solutions for Classified (CSfC)

The Government's CSfC program creates profiles for a layered combination of commercially available solutions to construct classified networks using **VPNs**. One of the key components of this network is the Certificate Authority. The **Black•Vault CA** with Suite B cryptography, advanced HSM functionality and intuitive controls improves the security of **CSfC** networks while simplifying their operation and minimizing their footprint.



CSfC Campus IEEE 802.11 Wireless Local Area Network

ENGAGE BLACK

Black·Vault CA

Certificate Authority with integrated HSM

Technical Specifications

Cryptography

- Asymmetric public key algorithms:
  - RSA (2048, 3072, 4096)
  - ECDH, ECDSA
- Symmetric algorithm: AES 128, 192, 256 bit
- Hash/message digest:
  SHA-2 (256, 384, 512bit)
- Full Suite B implementation with
  Elliptic Curve Cryptography (ECC)
  EC curves P-256, P-384, P-521

Protocols

- SSH, TLS
- EST: Enrollment over Secure Transport
- X.509: Certificate Revocation Lists (CRLs)
- OCSP: Online Certificate Status Protocol

Hardware

- Hardware True Random Number Generator
- NIST SP 800-90 compliant DRBG
- Secure Boot Loader: PKI Authentication
- Memory Encryption And Integrity Check
- Real-Time Clock
- Ethernet 10/100 Copper or Optional SFP Fiber
- USB 2.0 Host
- Console: RS232 (RJ45)
- Tamper: Mechanical, Die-Shield, Temp & Voltage

Exchange Formats

With Key:

- Personal Information Exchange
  PKCS #12
- Base-64 (PEM) with password
  PKCS #8

Without Key:

- DER encoded (.CER)
- Base-64 (PEM) encoded (.PEM)
- Cryptographic Message Syntax Standard
  PKCS #7 (.P7B)

Management and Monitoring

- Menu Driven VT100 CLI (SSH)
- Syslog diagnostics support
- SNMPv3 Monitoring and Traps

Physical Characteristics

- Portable (Server Hard Drive Mechanics)
  Wall and Din Rail Mounting
- Dimensions 102 x 153 x 26 mm (4 x 6 x 1in)
- Weight: 454 grams; 1 pound
- Temperature: operating -20 to 60°C,
- Humidity: operating 10 to 90%
  storage 0 to 95%

Safety & Environmental Compliance

- UL, CE, FCC • RoHS

Power

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