Engage

Black•Vault CYNR

Cypher Signing Appliance with integrated HSM

The **Black•Vault CYNR** is a code and document signing appliance with an integrated cryptographically advanced **H**ardware **S**ecurity **M**odule, Smart Card Reader, Host USB and resistive Touch Screen Display.

The **Black•Vault CYNR's HSM** creates, securely stores and controls the keys used for cypher signing. The Private key associated with the **CYNR's** public key is contained within the FIPS Level 3+ tamper reactive cryptographic boundary of the integrated **HSM**. Secure Key Backup with "M of N" authentication ensures secure Restoration of the Keys.

Circle of Trust

The built-in touch screen display, smart card reader and secure boot eliminates the risk from intermediary software or devices. An intuitive on-screen interface provides step by step guidance with a certified Trust Path for configuration, PIN entry and signing operations.

M of N Login with 2-Factor Identification

The **Black•Vault CYNR** can be readily configured to require a quorum of trusted individuals with unique "M of N" 2-Factor Authenticated Smart Cards to be present to authorize signing of code or documents. This ensures that no single individual can represent the enterprise and release reputation damaging code or documents.

Purpose-Built

Secure installation and configuration of a general purpose operating system based Signer application combined with a Hardware Security Module is very complex and time consuming. The **Black•Vault CYNR** securely boots up as a Cypher Signing Appliance connected to its cryptographically advanced internal **HSM**.

Benefits

- Cypher Signing Appliance
  - Eliminates Complex Software Installation
- Out of Box Ultimate Level of Security
  - Integrated HSM with truly Private Keys
- Controls key use for code signing
- Overcomes Vulnerabilities of Soft Crypto
- Integrated Trusted Path Authentication
- Protects Intellectual Property
- Expedites Regulatory Compliance Audits
- Compact Size Fits in Safe Deposit Box
  - Hard Drive Form Factor
- Secure Key Management:
  - Generation, Storage, and Backup

Features

- Secure Boot
- Solid State Design
- 10 Year Battery
- 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 Cloning
- M of N per role

CODE SIGNING

Maintaining the security of the private code signing key is of critical importance to the developer and the end user. If a developer leaves their keystore and passwords in an unsecured location such that a third-party could find and use them, a developers authoring identity and the trust of their customers is compromised.

Injecting malicious code into legitimate applications is a powerful tool available to cyber attackers. The third-party could sign and distribute apps that maliciously replace your authentic apps with ones that corrupt, steal user data, attack other apps or the system itself.

It is increasingly important to ensure private keys associated with these digital signatures are secure for an extended period of time. An Android Developer's private key is required for signing all future versions of their app. Updates to their existing app requires the original code signing key.

Black•Vault CYNR, with a 10 year battery backed key store, makes App signing a highly secure and easy to implement solution for JAVA and Android apps.

DOCUMENT SIGNING

Digital signatures play an ever increasing role in authenticating and verifying the integrity of documents and files used in legal, financial, real estate and in other cases where it is important to detect forgery or tampering. A valid digital signature gives a recipient reason to believe that the document was created by a known sender.

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 a very high level of security with a digital signature process that is both easy to implement and use for PDF and Zip files.

QUORUM

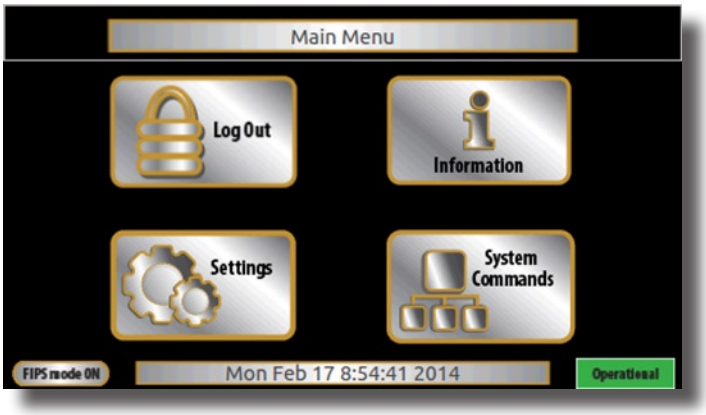
The **Black•Vault CYNR's** Smart Card interface with 2-Factor "m of n" authentication makes the establishment of a Quorum for code or document signing inherently straight forward.

in order to conduct a signing, the required minimum number of members of the organization must have physically logged in.

This ensures that no single individual is able to represent the organization. The fate of a company is not dependent upon the disposition of one person.

OPERATION

Black•Vault CYNR utilizes a resistive touch LCD color display to provide an intuitive iconic user interface. Operation is partitioned by privilege into security relevant functions that are Crypto Officer and Operator role based.



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.

A structured menu system facilitates straight forward:

- Key Generation: Private / Public Key Pair
- Certificate Signing Requests
- Importation of Root signed Certificate
- Selection of Signing Key
- Selection of file to be signed
  - Hash Validation of Selected File
- Destination of Signed file

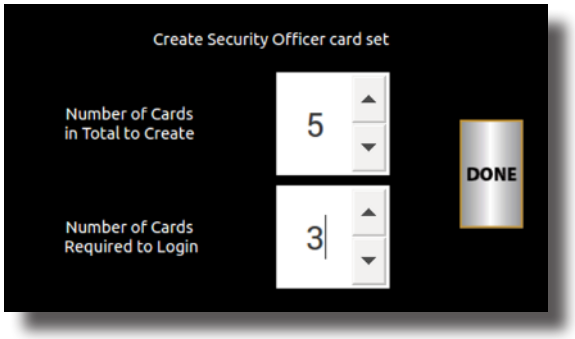
Autonomous and Network Attached modes of operation are supported. In autonomous operational mode all operations are performed via the touch screen GUI interface with files being transferred via a USB Flash Drive.

Standardized Certificate Signing Request are encoded as a file that provides a Certificate Authority with the public key along with the information that identifies the company. CSRs are sent to an attached USB drive or to a Network Attached folder.

Real-Time Audits of the configuration and operation provide Security Administrators with the necessary information to discover anomalous activity or failure of critical functions.

Security Officer Card Creation

Straight forward setup of Security Officers cards with "m of n" multifactor authentication.



Integrated Smart Card Reader

The **Black•Vault'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).

Engage

Black·Vault CYNR

Cypher Signing Appliance with integrated HSM

Technical Specifications

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

Compliance

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

Management and Monitoring

- Touch Screen Graphical User Interface

Physical Characteristics

- Portable (Server Hard Drive Mechanics)
- 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 & Environmental Compliance

- UL, CE, FCC • RoHS

Power

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