ENGAGE BLACK Black•Vault HSM·TSA

Timestamp Authority - Hardware Security Module

The **Black•Vault HSM**·TSA is an Ethernet attached Hardware Security Module that combines a cryptographically advanced **HSM** with **creation and authenticity of timestamps**.

Independently Certified

The **Black•Vault HSM**·TSA 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...

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**·TSA 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 active tamper detection circuitry.

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

Secure Timestamping

The **Black•Vault HSM**·TSA ensures the tamper proof creation and authenticity of the timestamped data for many applications. Verify at all times, if the timestamped data matches the exact same form at the point in time it was logged by the timestamp.

Benefits

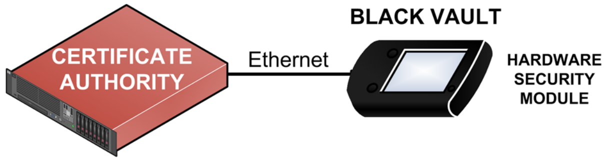
- Overcomes Vulnerabilities of Soft Crypto
- Protects Intellectual Property
- Expedites Regulatory Compliance Audits
- Compact Size Fits in Safe Deposit Box
- Embeddable: Ethernet Attached
  - Hard Drive Form Factor
- Secure Key Management:
  - Generation, Storage, and Backup
- Protects Registration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

Features

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

PUBLIC KEY INFRASTRUCTURE

The **Black•Vault HSM**.TSA is used by commercial and private Certificate Authorities (CAs) and registration authorities (RAs) to generate, store, and manage key pairs.



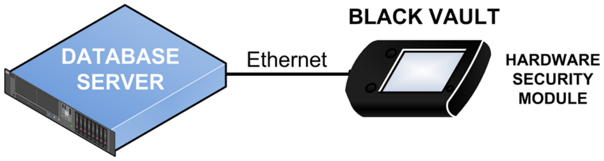
The **Black•Vault HSM**.TSA ensures that the Private key associated with a Certificate's public key is kept private. All cryptographic operations are executed within a 7 year battery backed semiconductor with a tamper reactive die shield.

The **Black•Vault HSM**.TSA 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**.TSA 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 B**Black•Vault HSM**.TSA isolates and shields the critical security parameters and cryptographic operations.

CODE AND DOCUMENT SIGNING with TIMESTAMPING

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".

The **Black•Vault HSM**.TSA as a Timestamp Authority provides authenticity to the existence of a document or data at a specific point in time.

Keys stored 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.TSA hardware security module is a best practice for maximum security.

The TSA Server and the HSM PKCS#11 API have independent logins creating isolated access to their Signing Keys adding another layer of protection.

Proven interoperability with::

- Microsoft Authenticode
- Java Jarsigner
- Adobe Signature
- Eclipse

MANAGEMENT

Black•Vault HSM$^{\cdot\text{TSA}}$ utilizes 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

Black•Vault HSM$^{\cdot\text{TSA}}$ Smart Card reader connects to industry standard smart cards via PKCS#11

Two-factor authentication (2FA) solutions secure Crypto Officer and Operator access.

BV•Tool

Powerful, easy to use, **PKCS#11 CLI** tool able to perform many different cryptographic operations that works on Windows and Linux both physical and virtualized. Some of the functions are:

Key Management

- Create Keys
- Delete Keys
- Key Import/Export Wrap/Unwrap

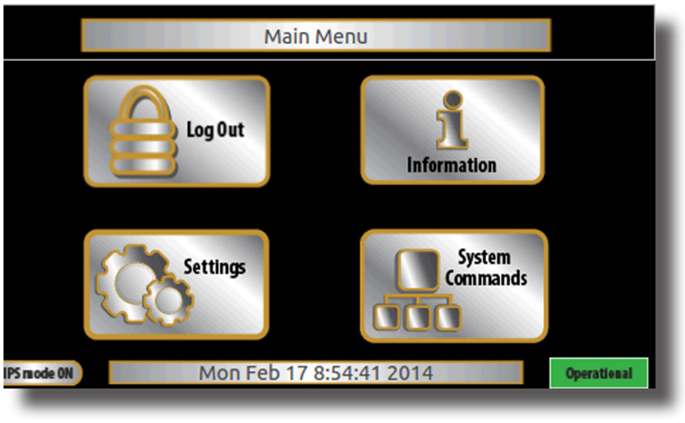
Create Certificates

- CSRs
- Certificates
- Self-Signed Certificates

As well as...

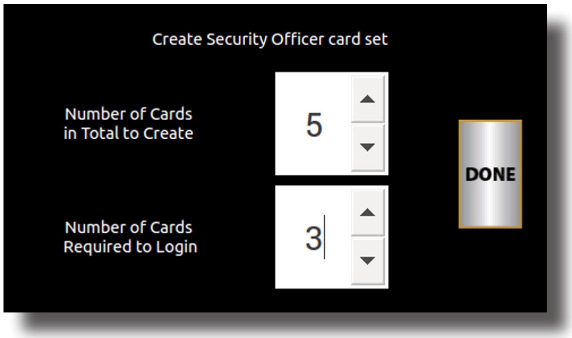
- Sign/Verify Files
- Encrypt/Decrypt Files

Able to utilize AES, RSA EC, and DSA key types. Sign using various hashes including but not limited to SHA256, SHA384, and SHA512.



Security Officer Card Creation

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



Create Security Officer card set

Number of Cards in Total to Create 5

Number of Cards Required to Login 3

SDK comes with purchase of an **HSM** designed to help you integrate your application with the BlackVault through its **PKCS#11** interface

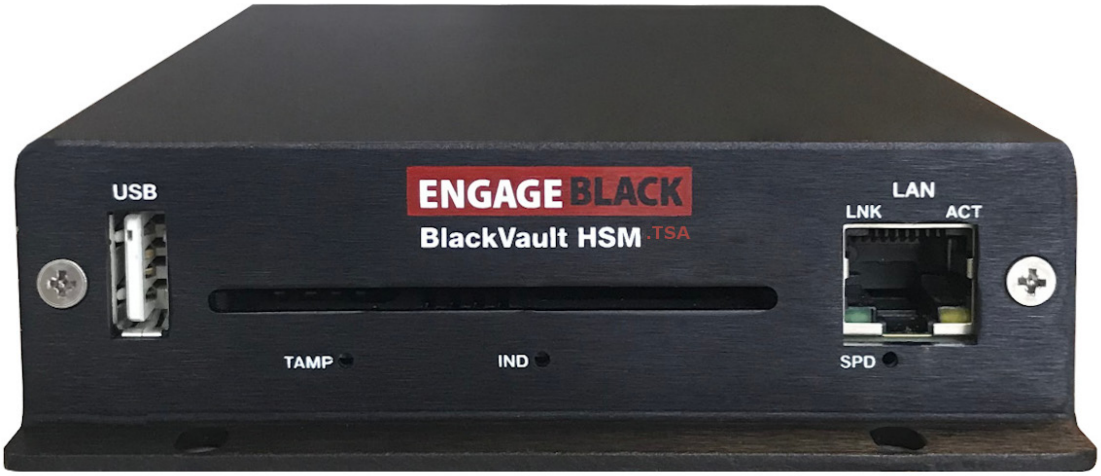
- Includes example code of Python and C++

Simple easy to use integration guides with stepby step walkthroughs to get you up and running with a variety of applications including:

- Authenticode
- Eclipse
- Android Dev Studio
- Java
- Microsoft Active Directory Certificate Services

ENGAGE BLACK Black·Vault HSM·TSA

Timestamp Authority - Hardware Security Module



Technical Specifications

Supported Operating Systems

- Physical: Windows, Linux
- VMWare: Windows and Linux

Interfaces

- PKCS#11, Java (JCE), Microsoft Authenticode CNG
- RFC 3161 timestamp protocol
- PKCS#10 and PKCS#7 for request and import of TimestampServer certificates
- NTP Network Time Protocol for synchronization of TimestampServer with external time server

Host Connectivity

- Ethernet 10/100 Copper; Opcional SFP
- TLS

Fields of application

- Document management and archiving systems
- Long-term archiving solutions
- Electronic tender platforms
- Electronic contracts

Cryptography

- Asymmetric public key algorithms:
  - RSA (1024, 2048, 4096)
  - Diffie-Hellman ECDH, DSA, ECDSA
- Symmetric algorithm: AES 128, 192, 256
- Hash/message digest:
  SHA-1, SHA-2 (224, 256, 384, 512bit)
- Implementación completa de Suite B con Criptografía de curva elíptica (ECC)
- NIST SP 800-90 complaciente DRBG

Certification

- HSM FIPS 140-2 Level 3

Management and Monitoring

- Graphical User Interface
- Remote Management
- Command Line Interface
- Syslog diagnostics support

Physical Characteristics

- Portable/Embeddable (Server Hard Drive Mechanics)
- Integrated Smart Card Reader
- Bloqueo de retención de tarjetainteligente
- 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