Trusted Cyber Technologies

THALES
Building a future we can all trust

CipherTrust k160

Centralize and simplify data security policies and key management at the edge

Overview

CipherTrust k160 is a compact cryptographic key management platform that protects and manages cryptographic keys and associated policies used to encrypt the most sensitive data-at-rest. This cost-effective solution is ideal for small to medium sized deployments commonly found in small offices, remote sites, and tactical environments. CipherTrust k160's small form factor allows it to be easily deployed in any environment while still providing the best in class security features customers are accustomed to finding in the CipherTrust product family.

CipherTrust k160 includes a FIPS 140-2 certified token or a high assurance cryptographic token as its hardware root of trust. The token hardware security module (HSM) operates as a secure root of trust by encrypting all sensitive objects (e.g. keys, certificates, etc.) in CipherTrust Manager with keys that are generated by, and reside in, the token HSM. The removable token HSM provides an easy to use method to support common key management scenarios such as rapid key delivery disablement, key destruction, cryptographic erase, and time of use restrictions. By simply removing the detachable token you can keep mission-critical data safe, whether in the most hazardous environment or a remote branch office.

Rightsizing Cryptographic Key Management for the Edge

Originally developed for the tactical market segment, the CipherTrust k160 has evolved into a cost-effective key management solution that is well suited for many small to medium size deployments of encrypting endpoints (e.g. storage arrays, virtual machines, file servers, etc.). Regardless of the specific use case, all CipherTrust k160 deployments benefit from the following characteristics of the CipherTrust k160 platform:

- Measuring only 6.5"x4.0"x1.5", the CipherTrust k160 fits well in space-constrained environments in which the customer has low size, weight, and power (SWaP) needs.
- CipherTrust k160 is easy to operate by someone with basic computer skills.
- Removable token HSM to quickly disable key delivery.

CipherTrust k160 (Shown Actual Size)

Benefits

- Cost effective key management
- Large ecosystem of KMIP compliant endpoints
- Meets assurance requirements
- Removable token HSM
- FIPS 140-2 Certified Token
- High Assurance Token
- Rapid key destruction
- Cryptographic erase
- Small form factor
- Multiple mounting options
- Manufactured, sold, and supported exclusively in the United States by Thales Trusted Cyber Technologies (TCT)

Common CipherTrust k160 Deployments

CipherTrust k160 can be used in conjunction with the CipherTrust k470, k570, k170v, and k470v models as part of an enterprise-wide key management strategy. With common security features, user interfaces, and reporting mechanisms across the entire CipherTrust product family, agencies can leverage their investment in training, security evaluations, and compliance procedures to deploy core-level cryptographic key management capabilities to the edge using the CipherTrust k160. CipherTrust k160 is commonly deployed as a cost-effective solution in the following environments:

- Small data storage deployments
- Branch and remote offices
- Tactical deployments including forward deployed environments, forward operating bases, mobile command centers, forward mission operations
- Disaster recovery centers
- Remote, lights-out, non-managed facilities
- Lab or proof of concept deployment

Highlighted Capabilities

- **Removable Token HSM**: The token HSM is a secure root of trust for key generation, secure key storage, and encryption/decryption. Removal of the token provides a rapid means to block key delivery to the cryptographic endpoint
- **Full Key Lifecycle Management and Automated Operations**: CipherTrust k160 simplifies management of encryption keys across their entire lifecycle, including secure key generation, backup/restore, clustering, deactivation, and deletion. It makes automated, policy-driven operations easy to perform, and generates alarms for events of interest.
- **Centralized Administration and Access Control**: Unifies key management operations with role-based access control and provides full audit log review. Authenticates and authorizes administrators and key users using existing AD and LDAP credentials.
- **Secrets Management**: Provides the ability to create and manage secret and opaque objects for usage on the platform.
- **Multi-tenancy Support**: Provides capabilities required to create multiple domains with separation of duties to support large organizations with distributed locations or multiple companies hosted by Managed Service Providers (MSP).
- **Developer Friendly REST APIs**: Offers new REST interfaces, in addition to KMIP and NAE-XML APIs, allows customers to remotely generate and manage keys as well as off-load cryptographic operations from clients to the CipherTrust k160 appliance.
- **Flexible HA Clustering and Intelligent Key Sharing**: Provide the option of clustering physical and / or virtual appliances together to assure high availability as well as increased encryption transaction throughput.
- **Robust Auditing and Reporting:** Includes tracking of all key state changes, administrator access, and policy changes in multiple log formats (RFC-5424, CEF, LEEF) for easy integration with SIEM tools. In addition, customers can generate pre-configured/customizable email alerts. Audit trails are securely stored and signed for non-repudiation.
- **Diverse Encryption Use Cases:** CipherTrust k160 supports a comprehensive set of encryption use cases through Thales TCT CipherTrust data protection connectors and an ecosystem of partners.
- **Maximum Capacity** of 10,000 symmetric keys can be stored on CipherTrust k160 (with a maximum of 100 keys using concurrent connections.)
- **Mounting Options:** CipherTrust k160 includes mounting brackets which allow it to be directly attached to most any shelf, cabinet, or wall. Thales TCT also offers a custom 1U shelf to mount the CipherTrust k160 in a standard 19" rack (each shelf can house up to two k160s).

Technical Specifications

Physical Characteristics

- CipherTrust k160 Dimensions: 6.5" x 4.0" x 1.5"
- Weight: 1.2 lbs.
- Direct mount or 1U 19in. rack mount
- Thermal Storage: -30°C ~ 80°C
- Thermal Operation: -30 ~ 65°C
- Storage Humidity: 5 ~ 95% @ 40C
- Operating Humidity: 0% ~ 90% relative humidity
- Vibration Testing: Random, 1Grm, 5~500Hz
- Power: included external power supply; locking DC power connector
- Power Range: input 120-240V AC, 1.5A, 50-60Hz; output 12V DC, 40W

Interfaces

- Web UI Management
- Serial and SSH command line
- KMIP and XML Key Management Protocols
- 1G Ethernet interface
- Integrated Token HSM connection

About Thales Trusted Cyber Technologies

Thales Trusted Cyber Technologies, a business area of Thales Defense & Security, Inc., is a trusted, U.S. provider of cybersecurity solutions dedicated to U.S. Government. We protect the government's most vital data from the core to the cloud to the edge with a unified approach to data protection. Our solutions reduce the risks associated with the most critical attack vectors and address the government's most stringent encryption, key management, and access control requirements.

For more information, visit www.thalestct.com