Product Brief

THALES
Building a future we can all trust

CipherTrust Manager k160 Mk II

thalestct.com

THALES

Overview

The CipherTrust Manager k160 Mk II 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. Improving on the original k160, the Mk II is the ideal hardware platform to extend CipherTrust Data Security Platform's enterprise-grade capabilities from the core and cloud to the edge. CipherTrust k160's small form factor allows it to be easily deployed in any environment – from satellite offices to forward operating bases to mobile flyaway kits – while still providing the best-in-class security features customers are accustomed to finding in the CipherTrust product family.

CipherTrust k160 can be cryptographically rooted in either a FIPS 140 validated or high assurance token hardware security module (HSM). The token HSM operates as a secure root of trust by encrypting all sensitive objects (e.g. keys, certificates, etc.) in CipherTrust k160 with keys that are generated by and reside in the token HSM. The removable token HSM provides an easy-to-use method to support critical key management scenarios such as rapid key delivery disablement, key destruction, cryptographic erase, and time of use restrictions. The detachable token acts as a "kill switch" for access to mission-critical data, whether in a remote branch office or the most hazardous environment.

Rightsizing Cryptographic Key Management for the Edge

CipherTrust k160 Mk II extends the same pane of glass interface from the core and the cloud to the edge, reducing operational complexity and eliminating training overhead across teams. On its own or integrated into an enterprise-spanning CipherTrust key management solution, CipherTrust k160 seamlessly brings cryptographic key management where you need it.

Regardless of the specific use case, all CipherTrust k160 deployments benefit from the following characteristics of the CipherTrust k160 platform:

- Measuring only 7"x4.3"x1.65", the CipherTrust k160 Mk II is sized for 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.

Benefits

- Cost effective key management
- Large ecosystem of KMIP compliant endpoints
- Meets assurance requirements
- Removable token HSM
  - FIPS 140 Validated 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 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

CipherTrust k160 Mk II (Shown Actual Size)

THALES

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.
- **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 250,000 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 Mk II Dimensions: 7" x 4.3" x 1.65"
- Weight: 1.84 lbs
- Direct mount or 1U 19in. rack mount
- Thermal Storage: -40°C ~ 85°C
- Thermal Operation: -20°C ~ 65°C
- Storage Humidity: 0% ~ 90% relative humidity, non-condensing
- Operating Humidity: 0% ~ 90% relative humidity, non-condensing
- Vibration Testing: Random, 3 Grms, 5~500Hz
- Power: included 12V external power supply; locking DC power connector
- Web UI Management
- Serial and SSH command line
- KMIP and XML Key Management Protocols
- Two gigabit Ethernet interfaces
- 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

Contact us - For office location and contact information, please visit thalestct.com/contact-us