THALES

KeySecure for Government G160

Centralized Cryptographic Key Management Platform for Tactical Environments

KeySecure G160 (Shown Actual Size)

KeySecure for Government G160 (KeySecure G160) 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. KeySecure G160'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 KeySecure for Government product family.

KeySecure G160 includes a FIPS 140-2 Level 3 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 KeySecure 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 Field

Originally developed for the tactical market segment, the G160 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 KeySecure G160 deployments benefit from the following characteristics of the G160 platform:

- Measuring only 6.5"x4.0"x1.5", the G160 fits well in space-constrained environments in which the customer has low size, weight, and power (SWaP) needs.
- G160 is easy to operate by someone with basic computer skills.
- Removable token HSM to quickly disable key delivery.
- Broad partner ecosystem. KeySecure is proven interoperable with industry's leading vendors in the storage (NetApp, Tintri, HPE, Dell EMC, Cohesity, etc.), virtualization (VMware, AWS, etc.), hyper-converged infrastructure (Nutanix, Klas Telecom, etc.), file encryption (Windows, Linux), and application encryption (Enveil, MarkLogic, etc.) markets.

Benefits

- Cost effective key management
- Large ecosystem of KMIP compliant endpoints
- Meets assurance requirements
- Removable token HSM
  - FIPS 140-2 Level 3 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 KeySecure G160 Deployments

KeySecure G160 can be used in conjunction with the KeySecure G460 and G350v models as part of an enterprise-wide key management strategy. With common security features, user interfaces, and reporting mechanisms across the entire KeySecure for Government product family, customers can leverage their investment in training, security evaluations, and compliance procedures to deploy core-level cryptographic key management capabilities to the edge using the KeySecure G160. The G160 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 deployments

Highlighted Capabilities

- **Heterogeneous Key Management.** Manage keys for SafeNet encryption products as well as a large variety of third-party encryption solutions through an industry standard interface.
- **Key Types.** Centrally manage symmetric keys, asymmetric keys, secret data, and X.509 certificates along with associated policies.
- **Full Lifecycle Key Support and Automated Operations.** Simplify the management of encryption keys across the entire lifecycle including secure key generation, storage and backup, key distribution, deactivation and deletion. Automated, policy driven operations simplify key expiry and rotation tasks.
- **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.
- **Centralized Administration of Granular Access, Authorization Controls and Separation of Duties**. Unify key management operations across multiple encryption deployments and products, while ensuring administrators are restricted to roles defined for their scope of responsibilities, from a centralized management console.
- **High-Availability.** Deploy in high-availability configurations locally or across geographically dispersed locations in an active-active mode of clustering.
- **Auditing and Logging.** Detailed logging and audit tracking of all key state changes, administrator access and policy changes. Audit trails are securely stored and signed for non-repudiation and can be consumed by leading third-party SIEM tools.
- **Cryptographic Erase.** Securely sanitize target media by centrally managing key lifecycle in compliance with NIST SP 800-88 Rev 1
- **Mounting Options.** KeySecure G160 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 G160 in a standard 19" rack (each shelf can house up to two G160s).
- **Extensible Security Platform.** State of the art platform with room for future adaptability via software upgrades.

Technical Specifications

Physical Characteristics

- G160 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

Audit and Logging

- SNMP
- Syslog
- Secure log files
- Integration with 3rd party SIEM tools

About Thales Trusted Cyber Technologies

Thales Trusted Cyber Technologies, a business area of Thales Defense & Security, Inc., protects the most vital data from the core to the cloud to the field. We serve as a trusted, U.S. based source for cyber security solutions for the U.S. Federal Government. Our solutions enable agencies to deploy a holistic data protection ecosystem where data and cryptographic keys are secured and managed, and access and distribution are controlled.

Contact Us: For more information, visit www.thalestct.com