thalestct.com

THALES

KeySecure for Government G460

Enterprise-level Centralized Cryptographic Key Management

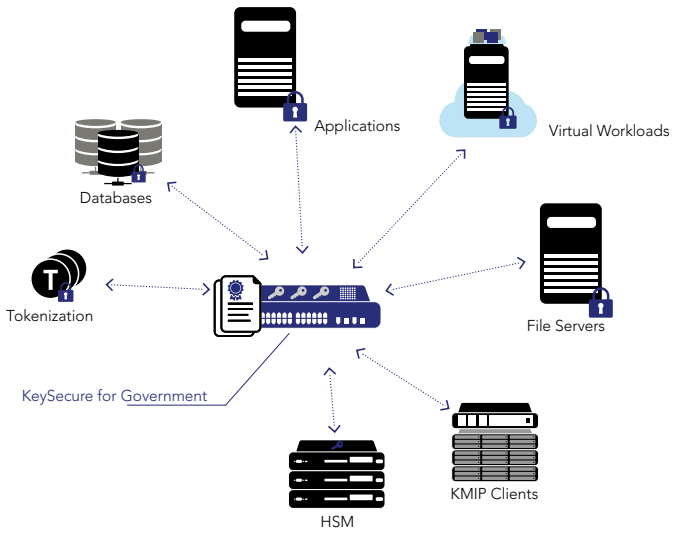
KeySecure for Government G460 (KeySecure G460) is a centralized cryptographic key management platform that supports a broad encryption ecosystem for the protection of sensitive data-at-rest across enterprise-level data centers. KeySecure G460 supports an embedded hardware root of trust utilizing a FIPS 140-2 Level 3 Luna for Government hardware security module.

Developed for U.S. Government use, KeySecure G460 is manufactured, sold, and supported in the U.S. exclusively by Thales Trusted Cyber Technologies (TCT)

KeySecure G460 Use Cases

KeySecure G460 protects and manages the cryptographic keys used in a wide variety of encryption solutions.

- **Backup Media:** Supports industry leading tape libraries, scalable backup and cloud archive solutions
- **Storage:** Supports leading storage platforms and cloud storage services
- **Data Encryption Solutions:** Provides encryption solutions for data in various formats – structured (such as databases) and unstructured (file level encryption, big data) – ensuring appropriate access to users requiring the information and IT teams providing infrastructure support
- **Applications:** Supports application level encryption via SafeNet ProtectApp and integrations from cloud application partners



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
- **Multiple Key Types.** Centrally manage Symmetric and 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.
- **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. Also, KeySecure G460 can utilize existing LDAP or AD directories to map administrative and key access for applications and end users.
- **High-Availability and Intelligent Key Sharing.** Deploy in flexible, high-availability configurations within an operations center and across geographically dispersed centers or service provider environments using 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 3rd party SIEM tools.
- **Next-Generation Storage and Archive Solution.** Simplify secure storage and efficiently scale data centers while reducing costs and complexity.
- **Cryptographic Erase.** Securely sanitize target media in compliance with NIST SP 800-88 Rev 1 by centrally managing key lifecycle.

Benefits

Single, centralized platform. for managing cryptographic content (keys and related data) and applications including the ability to perform high speed encryption/decryption operations

Use Case Expansion. Transform your key management appliance into a server that includes support for SafeNet encryption products

Simplify Compliance. Efficiently audit key management practices, save staff time, and simplify attainment of compliance mandates with efficient, centralized auditing of key management practices such as FIPS 140-2, PCI-DSS, HIPAA

Environment Independent Key Management. Key management policies and procedures are consistent

Risk Mitigation with Maximum Key Security. Tamper-proof hardware options supporting an embedded hardware root of trust with a FIPS 140-2 Level 3 Luna for Government hardware security module

Lower Total Cost of Ownership. Leverage a continuously growing list of 3rd party technologies leveraging SafeNet encryption products and the OASIS KMIP standard

Technical Specifications

Physical Characteristics

- Standard 1u 19" rack mount chassis
- Dimensions: 19" x 24" x 1.68" (482 mm x 610 mm x 42.8 mm)
- Weight: 30.42 lbs (13.8 kg)
- Input Voltage: 100-240 V, 50-60 Hz
- Power Consumption: 350 w
- Temperature: operating 50° F to 95° F (10° C to 35° C)
- Relative Humidity: 5% to 95% RH with 33° C (95° F) non-condensing

API Support

- Java, C/C++, .NET, XML open interface, KMIP standard

Network Management

- SNMP (v1, v2, and v3), NTP, URL health check, signed secure logs & syslog, automatic log rotation, secured encrypted and integrity checked backups and upgrades, extensive statistics

Appliance Administration

- Secure Web-based GUI, Command Line Interface

Authentication

- LDAP and Active Directory
- Common Access Card Authentication

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

3465 Box Hill Corporate Center Drive, Suite D, Abingdon, MD 21009 • 443-484-7070 • info@thalestct.com
thalestct.com