thalestct.com

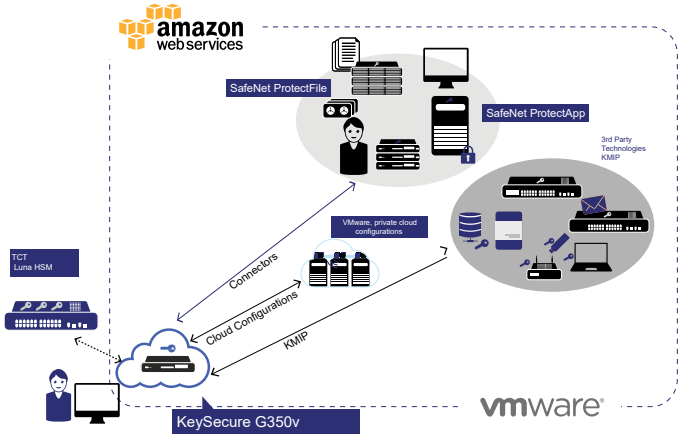
THALES

KeySecure for Government G350v

Centralized Cryptographic Key Management for Cloud & Virtual Environments

KeySecure for Government G350v (KeySecure G350v) is a hardened virtual cryptographic key management platform. It provides organizations with a secure, flexible alternative to hardware key management appliances. KeySecure G350v enables organizations to scale key management in private or public cloud infrastructures while eliminating the physical restraints and additional costs associated with hardware appliances.

KeySecure G350v is a FIPS 140-2 Level 1 validated hardened virtual appliance. It also supports a hardware root of trust utilizing a FIPS 140-2 Level 2 or 3 network-attached Luna for Government hardware security module or the Amazon CloudHSM service. Developed for U.S. Government use, KeySecure G350v is manufactured, sold, and supported in the U.S. exclusively by Thales Trusted Cyber Technologies (TCT).



Customer Controlled Key Management

KeySecure G350v allows organizations to protect and manage cryptographic keys and enforce access control across cloud infrastructures. It ensures that organizations maintain ownership of their cryptographic keys at all times so that their encrypted data remains protected and separated from the infrastructure host and other tenants.

KeySecure G350v Use Cases

KeySecure G350v manages and stores cryptographic keys for a wide variety of encryption solutions.

- Backup Media: Supports industry leading cloud archive solutions
- Storage: Supports leading 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 G350v 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.
- 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

Lower Administration Costs. Lower the cost of key management and encryption with centralized administration and automated operations

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

Security and Compliance for Cloud Environments. Take advantage of the lower costs of virtualized and cloud environments with flexible deployment options covering virtual environments such as VMware and AWS GovCloud, C2S and U.S. regions

Environment Independent Key Management. Key management policies and procedures are consistent whether deployed in a traditional data center, virtualized data center, cloud or a hybrid environment

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

Flexible Procurement Options. Scalable licensing and support models available through different procurement options via AWS Marketplace, IC Marketplace, or Thales Trusted Cyber Technologies

Supported Technologies

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