TKLM Encryption

For organizations with more complex and robust requirements, Spectra TKLM Encryption Key Management is time tested and proven across enterprise level customers requiring the highest standard of encryption security. With Spectra TKLM you can deploy a clean, simple key management solution that meets the complex requirements your organization faces. Spectra TKLM is a robust encryption key manager that delivers a unified key management strategy to streamline your encryption implementation.

Simple Encryption Key Management for All Your Libraries

Not all encryption keys are created or used equally. Each key may have its own lifecycle and usage pattern. The more encryption keys you have the more complex your management becomes. This is especially true when you have more than one tape library involved. With Spectra TKLM all your keys can be simply managed, securely protected, and used automatically across your library environment.

Central Management for Your Encryption Keys

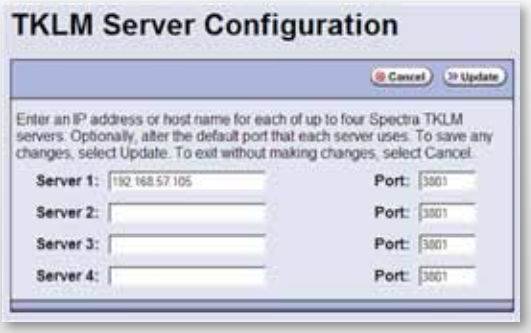
Spectra TKLM serves keys when called upon by a tape drive confirmed by the key server as a trusted recipient. This allows for keys to be centrally stored in a secure location. The architecture supports multiple protocols for key serving and manages certificates of authority as well as symmetric and asymmetric keys. As a result, users can centrally create, import, distribute, back up, archive, destroy, audit and manage the full lifecycle of keys from a single point whether their environment is distributed or not.

Data Protection and Destruction Made Easy

Regulations increasingly specify how long data can be retained. After that point, many organizations are required to dispose of it. Getting rid of stored, unencrypted data is difficult, but encryption with Spectra TKLM can make the job easier. With Spectra TKLM, encryption keys used to encrypt the data to be deleted can be destroyed. The Spectra TKLM audit trail verifies the key's destruction ensuring that data is unreadable and reliably destroyed to meet your organization's compliance requirements.

Authentication and Strong Security

Spectra TKLM provides strong authentication between the key manager and the tape drives it serves by checking the validity of the drive in its drive table and further ensuring that it is authenticated via the certificate authority. Once authenticated, a session key is generated to initiate a secure communication session between the key server and the drive. The encryption key is then itself encrypted and transmitted over the secure link. Spectra TKLM provides a FIPS operating mode to deliver an effortless validated encryption key management that is FIPS compliant.



Graphical User Interfaces Simplify Configuration and Management

The web-based GUI provides an easy-to-use interface to simplify key management configurations and tasks. Administrators can easily create key stores, assign keys and certificates, and manage the lifecycle of each key from a central console. The GUI also provides easy management of key retention, key and device groupings, and policy sets for retention, compliance and legal discovery purposes.

(P) 303.449.6400 • 800.833.1132 • (F) 303.939.8844 • (A) 6285 Lookout Road • Boulder, CO 80301 USA

TKLM Specifications

Specifications	Spectra TKLM
Server Hardware	• 4 GB RAM • 3.0 GHz processor • 1-5 GB free disk space for TKLM • 400 MB free disk space for key store
TKLM Software	• Linux or Windows • TKLM Server • Websphere Application Server • DB2
Spectra Library Support	All T-Series Tape Libraries
Spectra Drive Support	• LTO-5/LTO-6 (IBM) • TS1140 Technology (T-Finity Only)
Management Interface	• GUI • CLI
Federal Information Processing Standard (FIPS)	Optional configuration setting for FIPS mode
Key Management Interoperability Protocol (KMIP)	Conforms to Key Management Interoperability Standard (OASIS)
Key Quantity	• Key per tape capability • 1,000,000+ keys
Scalability	Manage multiple libraries and / or locations from a single pane of glass
Key & Certificate Management	• Monitor and manage full range of encryption keys and certificate authority status as well as associated metadata • Secure third-party key exchange
Security	• RBAC • Key, Device, and User Grouping (Segregation) • Audit Trail • Key Destruction
Redundancy	Backup and failover to multiple TKLM instances ensuring continuous key management and data availability