Spectra SKLM Encryption

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

Simple Encryption Key Management for All Your Spectra 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 SKLM all your keys can be simply managed, securely protected, and used automatically across your library environment.

Central Management for Your Encryption Keys

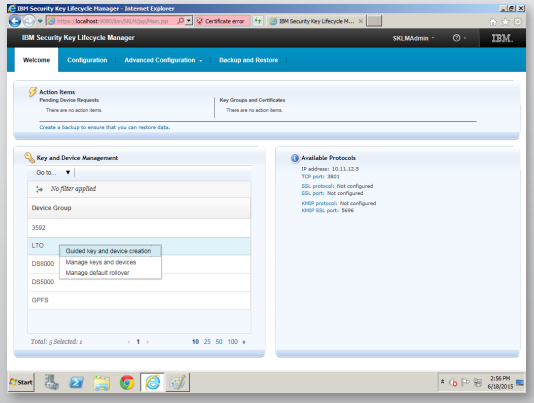
Spectra SKLM serves keys when called upon by a tape drive confirmed by the key server as a trusted recipient. This allows for keys to be centrally stored in a secure location. The architecture supports multiple protocols for key serving and manages certificates of authority as well as symmetric and asymmetric 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 SKLM can make the job easier. With Spectra SKLM, encryption keys used to encrypt the data to be deleted can be destroyed. The Spectra SKLM 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 SKLM 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 SKLM provides a FIPS operating mode to deliver an effortless validated encryption key management that is FIPS compliant.



Graphical User Interface Simplifies 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.

Toll Free: 303-449-6400 • 800-833-1132 • 6285 Lookout Road • Boulder, CO 80301 USA

SPECTRALOGIC.COM

Spectra SKLM Specifications

Specifications	Spectra SKLM
Server Hardware	• 4 GB RAM • 3.0 GHz processor (Windows or Linux) • 2-5 GB free disk space for SKLM • 512 MB free disk space for key store
SKLM Software	• Linux or Windows • SKLM Server • Websphere Application Server • DB2
Spectra Library Support	All TSeries Tape Libraries
Spectra Drive Support	• LTO-5, LTO-6, LTO-7, LTO-8, LTO-9 • IBM® TS1140/TS1150/TS1155/TS1160 Technology (within these Spectra libraries: TFinity, T950, T380)
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 SKLM instances ensuring continuous key management and data availability

Toll Free: 800-833-1132 • 303-449-6400 • 6285 Lookout Road • Boulder, CO 80301 USA

SPECTRALOGIC.COM