Encryption and Secure Data Erasure

If a physical volume is encrypted, the TS7700 does not perform a physical overwrite of the data. The EK is shredded, which renders the encrypted data unrecoverable.

When compared to the normal or long erasure operation, EK shredding is much faster. Normal erasure is always used for non-encrypted tapes, and EK shredding is the default that is used for encrypted tapes. The first time an encrypted tape is erased, a normal erasure is performed, followed by an EK shredding. A TS7700 can be configured to perform a normal erasure with every data operation, but this function must be configured by an IBM SSR.

4.4.7 Planning for tape encryption in a TS7700T

The importance of data protection became increasingly apparent with news reports of security breaches, loss, and theft of personal and financial information, and government regulation. Encryption of the physical tapes that are used by a TS7700T helps control the risks of unauthorized data access without excessive security management burden or subsystem performance issues.

Encryption on the TS770T is controlled on a storage pool basis. SG and MC DFSMS constructs that are specified for logical tape volumes determine which physical volume pools are used for the primary and backup (if used) copies of the logical volumes. The storage pools, originally created for the management of physical media, were enhanced to include encryption characteristics.

The tape encryption solution in a TS7700T consists of the following components:

- The TS7700T tape encryption solution uses the IBM Security Key Lifecycle Manager (SKLM) or the IBM Security Key Lifecycle Manager for z/OS (ISKLM) as a central point from which all EK information is managed and served to the various subsystems.
- The TS1120, TS1130, TS1140, or TS1150 encryption-enabled tape drives are the other fundamental piece of TS7700T tape encryption that provide hardware that runs the cryptography function without reducing the data-transfer rate.
- The TS7700T provides the means to manage the use of encryption and the keys that are used on a storage-pool basis. It also acts as a proxy between the tape drives and the IBM Security Key Lifecycle Manager (SKLM) or IBM Security Key Lifecycle Manager for z/OS (ISKLM) by using Ethernet to communicate with the SKLM or ISKLM (or in-band through FICONs) to the tape drives. Encryption support is enabled with FC9900.

Rather than user-provided key labels per pool, the TS7700T can also support the use of default keys per pool. After a pool is defined to use the default key, the management of encryption parameters is run at the key manager. The tape encryption function in a TS7700T does not require any host software updates because the TS7700T controls all aspects of the encryption solution.

Although the feature for encryption support is client-installable, check with your IBM SSR for the prerequisites and related settings before you enable encryption on your TS7700T.

> **Tip:** Pool encryption settings are *disabled* by default.

Encryption key managers

The encryption key managers must be installed, configured, and operational before you install the encryption feature on the TS7700T.