

Keynet Optical Manager (KOM)

Release 1.0

High Security Key and Device Management

Remote Management of DSD 72B-SP SONET/SDH Devices

Offering strategically-strong AES-256 encrypted and authenticated messaging, the Keynet Optical Manager (KOM) provides remote key and device management for all fielded DSD 72B-SP optical data encryptors. Keynet securely performs scheduled device polling for up-to-the-minute device status.

Introduction

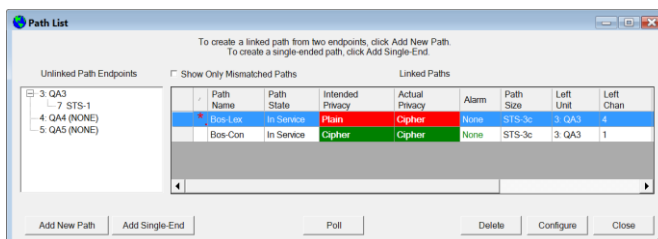
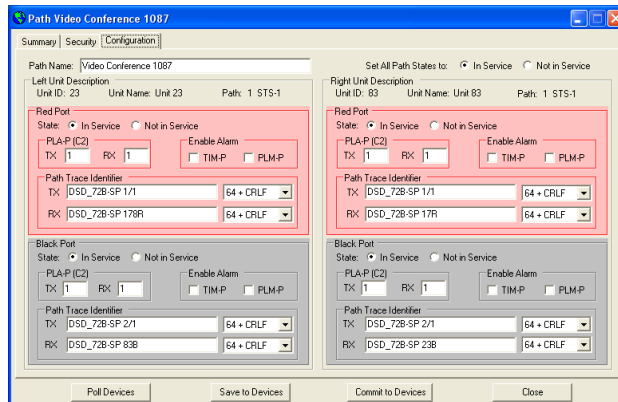
TCC released the **DSD 72B-SP** family of high-speed optical data encryptors in 2010 that are designed with strategically strong, AES-256 encryption algorithms, and supported by trusted key management architectures.

To provide support for the day-to-day management of '72B' devices, TCC has also released the **Keynet Optical Manager (KOM)**. KOM is designed to perform key and device management functions for all 72B encryptor products within a given customer's optical data network. This Keynet version is an evolutionary outgrowth from previous Keynet design that supports other TCC products. However, the new KOM version of Keynet expands its utility to fully support the substantial capabilities of the 72B product line.

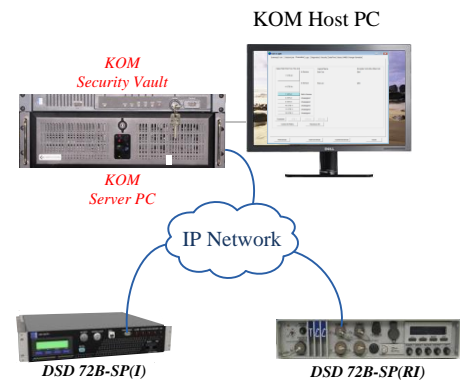
The KOM provides end-user control over secret key generation functions and ensures that all virtual containers (VCs) process their data in the assigned mode (secured, plain, blocked, unequipped, etc.). It also ensures that changes to VC endpoints (container re-routings) are managed with minimal downtime. The KOMs auditing of individual 72B devices allows remote-based, authenticated users to confirm the configuration of all 72B devices, perform remote diagnostics, and manage each device's moment-to-moment virtual, logical connections.

KOM (Release 1.0)

KOM release 1.0 is comprised of an MS Windows™ 7 based 19" rack mounted personal computer (PC) and an attached TCC **Security Vault**. The Security Vault communicates with its PC-based Server via a dedicated IP over Ethernet connection. The PC hosts the Keynet server application (KSA) service. A Keynet Local Client (KLC) application is also hosted on the PC, and communicates with the embedded KSA service. Using the KLC, the user logs onto and authenticates with the KSA. The Server also securely communicates with each fielded 72B device over an IP network (e.g., the Internet, or private IP data network). The initial release (1.0) of KOM offers a single client, single server workstation. Follow-on KOM releases (available as software upgrades) will seamlessly support multiple, fully-authenticated Keynet Remote Client (KRC) applications. This supports remote rerouting / remapping of optical data circuits connected to 72B devices by securely distributing keys in advance of the actual logical circuit cut-over.



Strategically Strong (AES-256) 72B Management Messaging



Keynet Optical Manager

*** Features ***

Key Management Functionality

- Centrally Managed by KOM Server
 - Scheduled key updates
 - Assigned optical paths
- Whenever required (on-demand)
 - Reassignment of fiber segments
 - Reroute of Virtual Containers (VCs)
 - Restoration due to fiber outages

Device Management Functionality

- Centrally Managed by KOM Server
 - Dynamically reassign VCs
 - Set Security Levels of Individual VCs
 - Cipher / Block / Plain / Forced Plain
 - Unassigned / Unequipped
- Monitor critical functions
 - Per user-defined polling intervals
 - Retrieve security events (Audits)
 - Monitor device logistical status
 - Record asynchronous events / traps
- Health of Virtual Containers
 - Section & Path overhead data
- Inter-Device Communications Links
 - Set path overhead IDCL channel(s)

High-Level Security

- Data Encryption Algorithm: AES-256
 - Trusted secret key infrastructure
 - All keys encrypted by Security Vault
 - All management messages to / from the KOM are encrypted
 - All security relevant activities logged
 - Logs retrieved by the KOM

Tamper-resistant enclosure

- Keys erased when enclosure is opened

