KEYNET Optical Manager

Centralized, trusted and user-friendly key & device management for the DSD 72B-SP optical network encryption family

The advanced KEYNET Optical Manager centrally and simply configures and manages a global network of TCC's DSD 72B-SP interoperable SONET/SDH encryption appliances. With an intuitive user interface and automated polling of alarms and logs, a network expert is not needed for trusted key and device management.

Centralized Management

TCC's DSD 72B-SP and DSD 72A-SP (STM) SONET/SDH encryption family are centrally deployed, configured and managed by TCC's advanced online KEYNET Optical Manager for network encryption and secure communications. Multiple layers of protection secure keys at every point in their life cycle without human intervention.

DSD 72B-SP Optical Encryption

The DSD 72B-SP SONET/SDH interoperable encryption family is available in rugged industrial, military and industrial variants. It provides strategic-level path encryption and secure communications of voice, data and video transmitted over fiber optic networks. Protocol agnostic and with automated KEYNET key and device management, DSD 72B-SP SONET/SDH encryption is a cost-effective, secure communications solution for global mission-critical networks.

Device and Key Management

KEYNET provides user-authenticated, role-based secure device management, as well as path configuration and monitoring that supports network policies (blocked, plain, secure). With an intuitive user interface and automated polls, alarms and logs, a network expert is not needed for trusted key and device management of a large network.

KEYNET provides end-user control over secret key generation functions and ensures that all virtual container (VC) data is processed in the assigned mode (secured, plain, blocked, unequipped, etc.). It also ensures that changes to VC endpoints (container re-routings) are efficiently managed. KEYNET's auditing of individual DSD 72B-SP SONET/SDH encryption devices allows role-based, authenticated users to confirm the configuration of all DSD 72B-SP SONET/SDH encryption devices, perform remote diagnostics, and manage each device's moment-to-moment virtual, logical connections.

Benefits

- Easy to use, centralized management platform
- Automated key and device management requires little human interaction
- Hardware-based security vault protects highly critical keys
- Multiple layers of protection
- User-authenticated device configuration and deployment for traceability
- Simple provisioning and management of security policies
- Intuitive user-friendly interface
- Network expert not needed to manage network security

Multiple Layers of Protection

KEYNET Optical Manager is comprised of an MS Windows® 7 based 19" rack mounted computer and an attached TCC Security Vault. The Security Vault communicates with its server via a dedicated Ethernet connection. The computer hosts the KEYNET server application (KSA) service. A KEYNET local client (KLC) application is also hosted on the computer, 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 DSD 72B-SP SONET/SDH encryptor over an IP network (e.g., the Internet, or private IP data network). KEYNET Lite-Optical is available for small networks.

Key Management Functionality

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

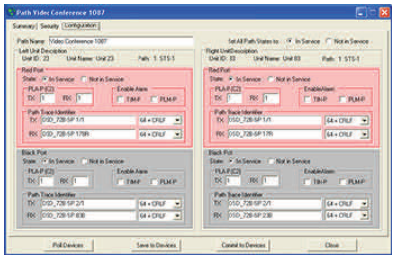
Device Management Functionality

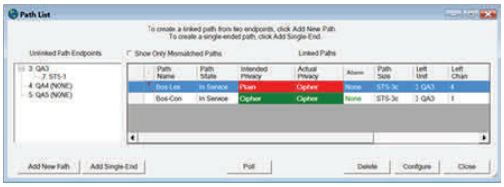
- Dynamically reassign VCs
- Set Security Levels of Individual VCs
  - Cipher/Block/Plain/Forced Plain
  - Unassigned/Unequipped
- Monitor critical functions
  - Per user-defined polling intervals
  - Retrieve security events (audits)
  - Monitor device logistical status
  - Record asynchronous events/traps
- Health of virtual containers
  - Section and path overhead data
- Inter-device communications links
  - Set path overhead IDCL channel(s)

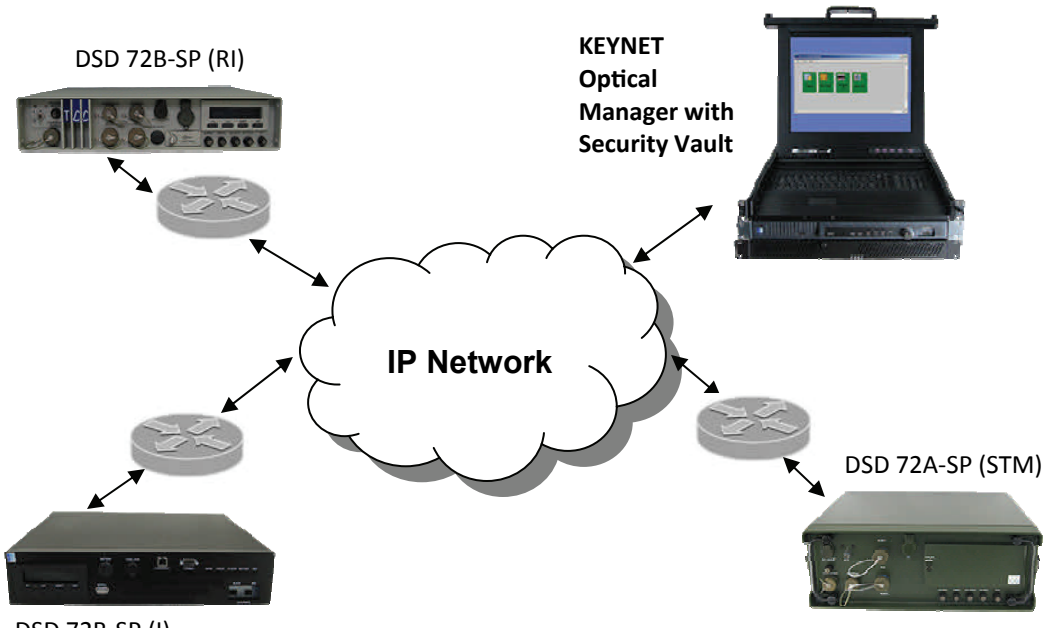
High-Level Security

Data Encryption Algorithm: AES-256

- Trusted secret key infrastructure
- All keys encrypted by Security Vault
- All management messages to/from KEYNET are encrypted
- All security relevant activities logged
- Logs retrieved by KEYNET
- Tamper-resistant enclosure; keys erased when enclosure is opened.







For more than 50 years, Technical Communications Corporation has specialized in superior-grade secure communications systems and customized solutions, supporting our CipherONE® best-in-class criteria, to protect highly sensitive voice, data and video transmitted over a wide range of networks. Government entities, military agencies and corporate enterprises in 115 countries have selected TCC's proven security to protect their communications.

Communicate in Confidence

TECHNICAL COMMUNICATIONS CORPORATION
100 Domino Drive, Concord, MA 01742 U.S.A.
+1-978-287-5100, Online request: www.tccsecure.com/sales
Fax: +1-978-371-1280, Web: www.tccsecure.com