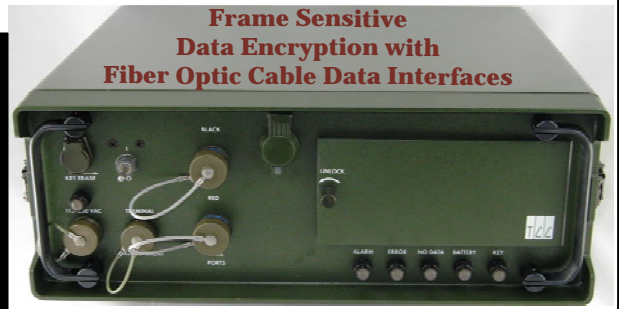


TCC DSD 72A-SP(STM)

STM-4 (622.08Mbps)
STM-1 (155.52Mbps)
Data Encryptor

**High-Level
Data Encryption**
**Protecting Enterprise &
Governmental Data
Communications**



DSD 72A-SP(STM)

The **DSD 72A-SP(STM)** SONET/SDH data encryptor is TCC's latest offering in a long line of ruggedized data security devices, designed to reliably operate in the harshest of operational environments. Like all of the TCC encryption products in the 'DSD' line, the **DSD 72A-SP(STM)** provides **strategic level data protection** with trusted, user-friendly, key and device management. The product's protocol sensitive path encryption approach provides **end-to-end virtual container (VC-n)** encryption and handling that allows unrestricted network routing of virtual containers with no plaintext network exposure of the path encrypted payload.

Data bandwidth demands continue to increase for both military and governmental communications. Mission critical information, including voice, streaming video, data telemetry, and general purpose data like email and file transfers, must be protected from interception and exploitation. Wide area networks (WANs) transport broadband, high-speed data at rates exceeding 622Mbps. Conventional broadband radio solutions cannot easily handle these data bandwidths, driving the demand for fiber optic networks (FONs). These higher bandwidth networks rely on data routing within the WAN. Most commercial fiber optic data encryptors take the easy, concatenated data approach that encrypts the entire optical payload. However, the **DSD 72A-SP(STM)** encrypts individual Virtual Container payloads leaving each container's Path Overhead (POH) unencrypted, thus permitting Add / Drop Multiplexers (ADMs) and Digital Cross Connects (DXCs) within the FON to route individual virtual containers without decrypting any payload to obtain POH data.

Security Threat

Even non-networked FON lines are vulnerable to eavesdropping. Many users lease commercial FON circuits as part of their network infrastructure, exposing data at network repeaters, ADMs, and switches. Even if these network elements are under the control of the user, FON lines themselves can be tapped anywhere along the path. The risk is magnified by the high volume of the data passing over these links, making the FON infrastructure an attractive point of the network for an adversary to attack. It is critical that these data links be protected in an end-to-end manner.

The Solution

The **DSD 72A-SP(STM)** SONET/SDH data security device is designed to fully counter the threat to fiber optic data communications. The exploitation vulnerability is effectively eliminated by the combined use of its AES-256 encryption algorithm and its SHA-256 Secure Hash Algorithm based authentication. The design also allows an efficient means of incorporating a national encryption algorithm in place of AES-256. All data encryptions is accomplished end-to-end; user payload is never exposed within the FON.

In addition to operating at either 622.08Mbps, or 155.52Mbps when so configured, the **DSD 72A-SP(STM)** is a "layer 2" encryption device, fully supporting the SONET/SDH standards and preserving all framing structures. Each virtual container (VC) is separately encrypted. The encrypted VCs are totally unaffected by network topology.

The **DSD 72A-SP(STM)** is a ruggedized, rack-mountable device meeting MIL-SPEC standards, and is designed to operated reliably in challenging environmental conditions. Wherever deployed in a remote location or in a controlled office environment, the **DSD 72A-SP(STM)** is designed with durability, reliability, and ease-of-use in mind making it perfectly suited for government and military security applications. It is also 100% backwards compatible with both the **DSD 72B-SP(RI)** and the **DSD 72B-SP(I)** products.

*** Features ***

Network Compatibility

- Supports both SDH STM-4 & STM-1 and SONET OC-12 & OC-3 protocols
- Compatible with transmission over both fiber optic cable and microwave RF
- Handles SONET/SDH Regenerator; Multiplexer, & Path Overhead Data
- Adaptable network configuration (STM-4)
 - One VC-4-4c payload
 - Up to four 'VC-4' payloads
 - Up to twelve 'VC-3' payloads
 - Or a mix of 'VC-3' & 'VC-4' payloads
- Accommodates Add/Drop Multiplexer and Digital Cross-Connect elements within the fiber optic network
- Data need not be decrypted to be routed within the optical data network

Security

- AES-256 algorithm, or (optionally) a National co-developed crypto algorithm
- Secret Key Management infrastructure
- Encrypted device management messages
- SHA-256 integrity and authentication
- Controlled menu access
- Comprehensive audit logs

High Reliability

- Rugged MIL-SPEC components
- High Reliability Power Supply options:
 - Universal AC power supply - or -
 - +24VDC power supply - or -
 - 48VDC power supply
- Extensive Built-In-Test (BIT)
- Remotely executed BIT capability
- Modular design for rapid repairs
- Tamper-resistant enclosure, physical lock

DSD 72A-SP(STM)

SONET / SDH
622.08Mbps (or 155.52Mbps)
Encrypted Data Protection

Designed to meet ITU-T SDH Standards

Designed to meet ANSI SONET Standards



Interfaces

- Optical Transceivers for each Line I/O Interface
 - STM-4 (OC-12) @ 622.08Mbps Optical
 - STM-1 (OC-3) @ 155.52Mbps Optical
- Radio Transceiver (Electrical) Interface
 - ITU-T G.703 STM-1/ES1 (§15) @ 155.52Mbps Electrical

Device Management

- At the Local Device, or Remotely Controlled (via *Keynet 3™*)
- Encrypted and Authenticated Device Management Messages
- Key Changes handled without Traffic Interruption

End-To-End Encryption Options

- 1) AES-256 - standard
- 2) National Algorithm(s) via co-development - optional

Key Management Options *

- 1) Symmetric Key with Secure Key Management Infrastructure
- 2) Symmetric Key using Manually Distributed Key Approach

* All options offer SHA-256 Integrity and Authentication *

Functional Design

- Ruggedized enclosure with MIL-SPEC components
 - 20°C to +55°C (Operational Temperature)
- Prime Power Options:
 - 100VAC to 240VAC / 50Hz, 60Hz, & 400Hz
 - + 24VDC
 - 48VDC
- Standard 19" Rack Mountable
- High Reliability under adverse environmental conditions
- Extensive Built-In-Test capability
- Access Control and Anti-Tamper design

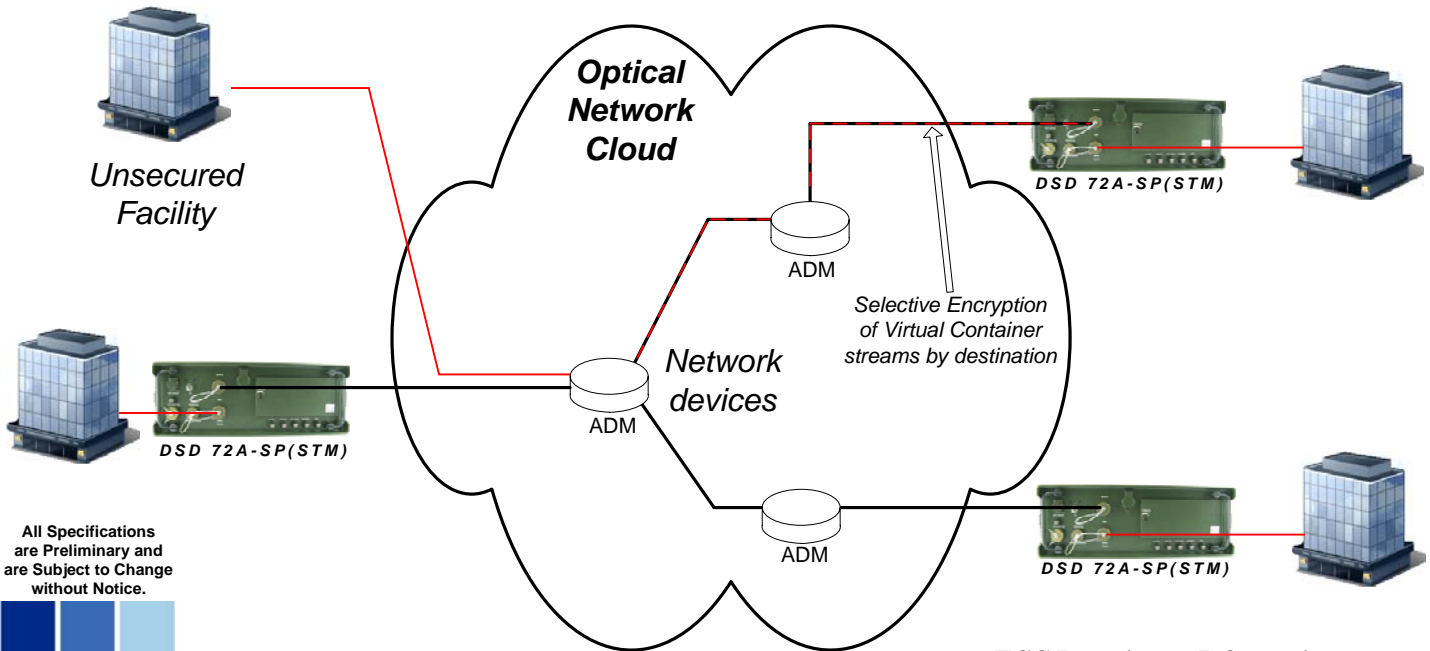
specifications

Standards-Compliant
Fiber Optic Interfaces

Network

- Supports both SONET and SDH protocols
- Transparent handling of SONET/SDH section & path headers
- Adaptable payload configurations
 - 1 x VC-4-4c (concatenated payload)
 - 1 x VC-4 and 9 VC-3s
 - 2 x VC-4s and 6 x VC-3s
 - 3 x VC-4s and 3 x VC3s
 - 4 x VC-4s
- Accommodates Add/Drop Multiplexer elements occurring anywhere in the network path ... without any exposure of unencrypted data payloads

STM-4 / OC-12 Intelligent Frame-Sensitive Encryption



All Specifications are Preliminary and are Subject to Change without Notice.



TCC Proprietary Information

Technical Communications Corporation
100 Domino Drive
Concord, Massachusetts, USA 01742-2892