

DSD 72A-SP

Bulk Data Link Encryptor

Strategic-Level Data Encryption

Protecting Classified Government Data Communications



Securing full duplex data links at rates from 64kbps to 34.368Mbps and higher, the *DSD 72A-SP* data encryption system reliably delivers strategic-level security in very demanding environments. *DSD 72A-SP* units are in service around the world being in various critical data applications including missile control and firing units; broadband data networks; command, control, computer, and intelligence (C4I) networks; and many other high profile applications. Generally viewed as one of the most versatile encryption products in the world, the *DSD 72A-SP* has been deployed with a variety of different encryption algorithms and a broad range of standards based interface configurations. These units are trusted for their demonstrated reliability as well as for their cryptographic strength.

The *DSD 72A-SP* Data Encryption System provides strategic-level data security for military and top-level governmental applications. Its evolving design is inspired by specified customer requirements; TCC continuously evolves and advances the *DSD 72A-SP* product's design to meet those requirements.

Modular, Adaptable Design

In addition to the baseline SNARK™ cryptographic algorithm, the *DSD-72A-SP*'s highly adaptable, modular architecture promotes efficient development and validation of customized national algorithms. Customized algorithms are cooperatively-developed by a team of cryptographic experts from the customer and TCC. The *DSD 72A-SP*'s cryptographic hardware architecture incorporates flexible field programmable gate arrays (FPGAs), supporting efficient implementations of data encryption algorithms as well as custom key and device management approaches.

Proven, Highly Reliable Design

The *DSD 72A-SP* has been designed to, and tested to operate in harsh environmental conditions. The *DSD 72A-SP* has a long history of demonstrated reliability with over 2,200 units deployed worldwide. Built to meet and exceed stringent MIL-STD-810 environmental requirements, it seamlessly integrates into tactical mobile shelters, missile launch platforms, and fixed communications facilities.

Operational Simplicity

The *DSD 72A-SP*'s simple device operation and automated key management streamline network operations. Designed for operational simplicity, an installed *DSD 72A-SP* can operated autonomously on a data network for many months or years with no maintenance or operator action required. Large Local Key storage and automated key change minimize requirements for authorized personnel to perform key load operations; typically once a year or less.

Key Management System

SNARK-based *DSD 72A-SP* units' keys are generated and loaded into the SmartModule key fill device using the Crypto Management System (CMS-72A). The CMS-72A uses an anti-tamper protected Security Vault™ to generate and store Local Keys. The Local Keys are encrypted and securely stored in a 'SmartModule™' key fill device for distribution to the target *DSD 72A-SP* device. The CMS-72A supports black key distribution securing the Local Keys from compromise during transport in SmartModule key fill devices. The CMS's authenticated user interface provides differentiation of role-based privileges minimizing the exposure of sensitive key material.

*** Features ***

Typical Applications

- ◇ Strategic Communications Backbone
- ◇ Tactical C4I Communications Links
- ◇ Long-Range Missile Defense Networks
- ◇ Air Defense Fire Unit Commo Systems

Network Compatibility

- Supports Multiple Interfaces & Protocols
- ◇ ITU-T CEPT E1; CEPT E2; CEPT E3
- ◇ ANSI T1
- ◇ Eurocom D/1 Multi-rate
- ◇ E1; E2; Eurocom D/1 'Triple Interface'
- ◇ ATACS Multi-rate
- ◇ D/1 – ATACS Hybrid, Multi-rate
- ◇ TIA-/EIA-422 Multi-rate
- ◇ TRITAC Multi-rate

Encryption Options

- Encryption Engine Options
- ◇ SNARK (128-bit key)
- ◇ National Algorithms (various sizes)

Key Management

- Approaches
- ◇ Manually Distributed Secret Key
Key Fill Devices (Black Key)
- ◇ Crypto Management System (CMS)
Vault-Based Local Key Generation
and Key Storage
- Key Fill Device service port

Device Management

- ◇ Pier-to-Pier (In-Band)
via 'High Speed Command Link'
- ◇ Centralized CMS to each *DSD 72A-SP*
Out-of-Band Communications
Ethernet (IP) or RS-232

DSD 72A-SP

High Speed Bulk Encryptor

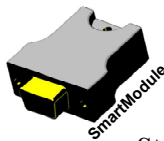
specifications

Cryptography

- ◇ *SNARK*TM Non-Linear Key Stream Generator (standard)
 - 128-bit Traffic Encryption Key
 - ◇ Dual Keybanks (400 keys each x 2 = 800 keys total)
- Supported Crypto Synchronization Modes
 - ◇ Long Cycle (64-bit IV) Mode
 - ◇ Cipher Feedback Mode (Self-Synchronizing)
- ◇ National Algorithm(s)
 - ◇ Co-Developed by Customer and TCC Cryptographers
 - ◇ Traffic Key Lengths: Customer Specified (≥128-bits)
 - ◇ Algorithm Operational Mode: Customer Specified
 - ◇ Supported Synchronization Mode(s): Customer Specified

Key Management (*SNARK*)

- ◇ Key Fill Device: *SmartModule-64K*TM
 - Holds one (or both) Keybank(s) of Local Keys
- ◇ Manually Distributed Secret Key
 - Local Keys: 120-bits each (times 800 keys per device)
 - Network Key: 8-bits
- ◇ Black Key Distribution
 - Encrypted keys stored in SmartModule key fill device



Device Management

- 'CMS-72A'
- Remote Device Management (via RS-232/Centralized CMS)
- Local Unit Device Management (via Front Panel menus or via Pre-configured SmartModule)

Full Duplex Interface Options (Unit Configuration Specific)

- G.703 CEPT E3 (E31) (34.368Mbps) Bulk, Single Rate
- G.703 CEPT E2 (E22) (8.448Mbps) Bulk, Single Rate
- G.703 CEPT E1 (E12) (2.048Mbps) Bulk, Single Rate
- ANSI T1 (E11) (1.544Mbps) Bulk, Single Rate
- EIA-422 (64kbps – 8.192Mbps; 8.448Mbps) Bulk
- TRITAC (256; 288; 512; 576; 1,024; 1,152; 2,048; 2,304kbps)
- ATACS (256; 512; 1,024kbps) Bulk
- D/1 (Mux) – ATACS (Radio) (256; 512; 1,024kbps) Bulk
- Eurocom D/1 (256; 512; 1,024; 2,048kbps) Bulk; Autobaud
- Triple Interface (selectable Eurocom D/1; CEPT E1; & CEPT E2)

Environmental and EMI

- Operational Temperature: -20°C to +70°C
- Storage Temperature: -40°C to +85°C
- Humidity: 95% (240-hours) MIL-STD-810 Meth 507.2; Proc III
- Rain: MIL-STD-810 Method 506.2; Proc I
- Transit Drop: MIL-STD-810 Method 516
- Shock: MIL-STD-810 Method 516.3; Proc I
- Vibration: MIL-STD-810 Method 514.3; Proc I
- Altitude: MIL-STD-810 Method 500.2; Proc II
- EMI: MIL-STD-461A – CS02; CS06; RS03

Size and Weight

- 15.3cm high / 43.2cm wide / 35.6cm deep
- 11.4kg (25lbs) maximum

Primary Power

- High Reliability Internal Power Supply Options
 - AC-Option
 - 85V to 264VAC Universal / 47 – 440Hz
 - DC-Option
 - 24VDC or 48VDC ± 20%
- Power Consumption
 - 20-Watts (maximum)

Standard 19" Rack Mountable

Comprehensive Built-In-Test capability

Physical (Key/Lock) Access Controls

- MedicoTM Case Lock (with Anti-Tamper Key Erase)
- Medico Lock actuated Menu Access control



Bulk Data High Speed Link Encryptor

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

Commitment to Quality

As an ISO 9001 certified company, TCC designs, manufactures and supports high-grade secure communications systems that protect highly sensitive information transmitted over a wide range of data, voice and fax networks. Over 2,000 government/military agencies, financial institutions, telecom carriers and other multinational corporations worldwide rely on TCC to protect their communications networks.



© Copyright 2010 by TCC
Document: DCN 94-1069

TCC Proprietary Information

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