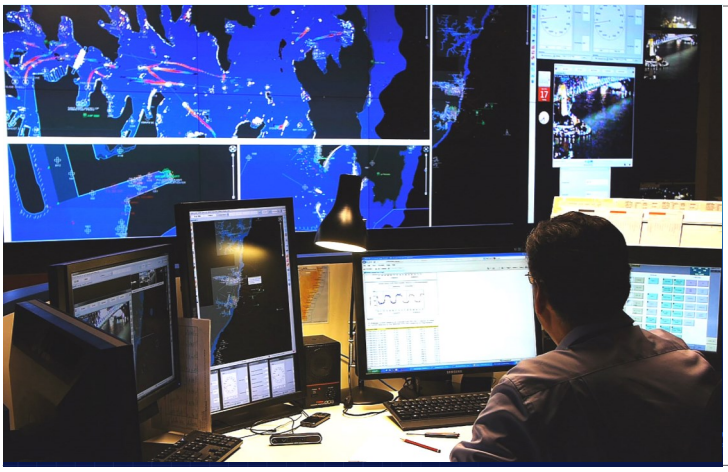
DSD 72A-SP Military Bulk Encryption System



Strategic-level data encryption protecting mission-critical military and government communications in the most demanding environments

The DSD 72A-SP military bulk encryption system provides strategic-level cryptographic security for data signals in demanding environments. Critical applications such as missile control and firing units; broadband data networks; command, control, communications, computer and intelligence networks(C4I), and many others are protected today by the DSD 72A-SP.

Protecting Critical Applications

Securing full duplex data links at rates from 64Kbps to 34.368Mbps and higher, the DSD 72A-SP reliably delivers strategic-level security in very demanding environments for critical applications such as:

- Strategic communications backbone
- Tactical C4I data links
- Missile defense networks
- Air defense fire unit systems

Modular, Adaptable Design

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. The units are trusted for their cryptographic strength. TCC continuously evolves and advances the DSD 72A-SP to meet current-day customer requirements.

Customized Algorithms

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

encryption algorithms. Customized algorithms are cooperatively developed by a joint team of cryptographic experts from both the end-customer and TCC. The DSD 72A-SP's cryptographic hardware architecture incorporates flexible field programmable gate arrays (FPGAs), supporting efficient implementation of data encryption algorithms.

Proven, Highly Reliable Design

The DSD 72A-SP has a long history of demonstrated reliability with over 2,200 units deployed worldwide. Tested to meet and exceed stringent MIL-STD-810 environmental requirements, it seamlessly integrates into tactical mobile shelters, missile launch platforms and fixed communications facilities. With two supported cryptographic synchronization modes, long cycle and cipher feedback, the DSD 72A-SP stays online in high-link error and jamming environments.

Benefits

- Strategic-level data protection
- TCC SNARK or another custom-defined national algorithm
- Demonstrated cryptographic strength
- Proven reliability in demanding, harsh environments
- Support for multiple electrical interfaces and link protocols
- Ease of management with automated key selection, centralized (or peer to peer) device management and autonomous operation

Crypto Management System for centralized key generation/storage and device management

Operational Simplicity

The DSD 72A-SP's simple device operation and automated key management streamline network operations. An installed DSD 72A-SP can operate autonomously on a data network for many months or years with no maintenance or operator action required. Using a large Local Key storage area (battery-backed memory) along with automated key changes, crypto support personnel typically perform key load operations at most once a year.

Key Management System

SNARK-based DSD 72A-SP units' primary 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 (traffic encrypting 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' authenticated user interface provides differentiation of role-based privileges minimizing the exposure of sensitive key material.

Technical Specifications

Cryptography

◊ SNARK 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 (baseline SNARK *implementation*)

◊ 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

◊ Key Fill Device: SmartModule-64K
- Holds one (or both) Keybank(s) of Local Keys

Device Management

CMS-72A
- ◊ Remote Device Management (via RS-232/Centralized CMS)
- ◊ IP Network-Based Device Management, optional (via IP over Ethernet)
- ◊ 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)

Size and Weight

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

Environmental and EMI

Operational Temperature: -20ºC to +70ºC
Storage Temperature: -40ºC to +85ºC
Humidity: 95% (240-hours) MIL-STD-810 Method 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

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

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

Feature Highlights

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

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