

DSP 9000

Tactical Secure Voice Encryption System

Tactical-Level Voice Encryption

Protecting Radio Voice Channel Communications

Simple, Intuitive Operations
Rugged, Military Grade Design
Highly Reliable & Dependable



The parent product in the DSP 9000 family of tactical voice security products offers a cryptographically strong solution providing tactical-level voice encryption over narrowband voice channels. Front panel menu-selectable interface settings, configuration, and key management feature sets, support simple, intuitive reconfiguration for different HF, VHF, and UHF radios and landline audio channels. Excellent recovered voice quality is achieved over poor quality audio channel, including those often found on long range HF single sideband (HF-SSB) radio channels.

UNIVERSAL ENCRYPTOR SOLUTION – All products in the DSP 9000 family provide a common security solution adaptable to most voice radios in use today. The DSP 9000 allows a variety of fielded radio equipment to be seamlessly integrated with one common cryptographic system. The DSP 9000 can be rapidly reconfigured for situations where switching between radios with different audio level settings is required. Audio levels and other interface settings may be programmed either via front panel controls, or rapidly by loading a Configuration **SmartModule™** key fill device containing the desired interface setting (levels, impedances, PTT polarities, etc.) for each radio.

EASE OF USE – The DSP 9000 provides user-friendly controls along with both visual and audible user feedback. Day-to-day key management tasks are operationally simple, making the DSP 9000 a highly desirable addition to any military or governmental agency's voice communication systems. The Crypto Officer role at the Crypto Management System (CMS-9000) provides the ability to make all key management related decisions and selection. For example, a Crypto Officer can use the CMS to program and download the desired Local Key period (e.g. 12-hours, 24-hours, weekly, etc.). Keys are automatically self-managed by each DSP 9000 requiring no additional user involvement.

CRYPTOGRAPHY – The DSP 9000 cryptographically protects voice signals using two synergistic processes. The 1st process is the DSP 9000 Key Generator which produces a stream of secure, pseudorandom inputs to the 2nd voice processing stage.

- 1 - Four inputs seed the **DSP 9000™ Key Generator**: (a) one of the 800 locally-stored **Local Keys**, (b) the **Network Key**, (c) a pair of 256-Byte **System Key** look-up tables, and (d) a randomly-generated **Initialization Vector (IV)** created at each Sync Burst transmission. The key generator uses these four inputs to produce a continuous stream of pseudorandom outputs to the voice processor function.

- 2 - The DSP 9000's **Enhanced Domain Transform (EDT)™** voice processor function accepts the periodic inputs from the DSP 9000 Key Generator and digitally manipulates the incoming audio. It efficiently cryptographically-conceals the original plain text audio signal when encrypting and recovers the original plain text voice signal after decrypting.

REMOTE CONTROL – The RADIO connector on the DSP 9000 offers the necessary operational control lines, often needed for aircraft and shipborne installations where the DSP 9000 is necessarily placed some distance away from its operator. (TCC offers as a purchased option an aircraft compatible, DIN rail designed Remote Control Unit.)

AUTOMATED KEY MANAGEMENT – TCC's customized MS Windows™ based Crypto Management System (**CMS-9000**) key management support system allows the end-user to generate and autonomously manage their own keying materials. The 'CMS' uses a TCC **Security Vault™** that generates and stores keying materials in its anti-tamper protected enclosure. The CMS also programs interface and configuration settings onto SmartModules.

*** Features ***

High Grade Voice and Data Security

Interoperable with:

- ◇ DSP 9000HS (Secure Handset)
- ◇ DSP 9000-Implant (Embedded PCB)
- ◇ CSD 3324SE (via 'Commander's Net')

Exceptional Recovered Voice Quality

Available Configurations

- ◇ Half Duplex (HD)
- ◇ Full Duplex (FD)
 - ◇ A rear RADIO connector version is also available on both HD and FD versions
- ◇ Half Duplex / Radio Airborne (RA)
- ◇ Remote Control Unit
- ◇ TX Impedance Compensator Module

Menu-Driven Programming Features

- ◇ Key Management functions
- ◇ Configuration functions / settings
- ◇ Interface I/O levels & impedances

Selectable Synchronization Approaches

- ◇ Push-to-Talk (PTT) Sync
 - ◇ For non-restricted broadcast
- ◇ Manual Dual Sync
 - ◇ For two-way conversations
- ◇ Manual Single Sync (Half Duplex only)
 - ◇ For restricted (grouped) communication

Automated Key Management

- ◇ Local Key select configuration options
 - ◇ Automatically (user-selectable periods)
 - ◇ Manually (optional / menu command)
- ◇ Down-line Key Indexing (via Sync Burst)
 - ◇ Index points to one of 800 Local Keys

Highly Flexible Interface Range Settings

Highly Reliable Design

- ◇ Quality MIL-SPEC components
- ◇ Rugged Physical Design

DSP 9000

Voice Encryption System

For HF-SSB; VHF; & UHF Tactical
Voice Channel Radio Applications



Specifications

DSP 9000 Key Generator Design

Highly Non-Linear

DSP 9000 Key Generator Diversity

Local Keys (56-bits each)	7.20×10^{16}
Network Key (part 1: 8-bits)	2.56×10^2
System Key Tables (two x 256-Byte)	8.39×10^{79}
Initialization Vectors (16-bits each)	6.55×10^4
Total Key Generator Diversity	1.01×10^{104}

Internal Key Storage

Local Keys

Two independent Keybanks of 400 keys (800 total)

Stored in Battery-Backed, Anti-Tamper Protected RAM

Network Key (also in Battery-Backed RAM)

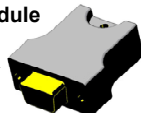
System Keys – maintained in an EPROM device

All keying materials are under end-customer's control and management

Key Fill Device Support

SmartModule-2K, each stores ½ Keybank
KFD-800C stores one Keybank

SmartModule



Enhanced Domain Transform (EDT)TM Processing

Cryptographically-Controlled

Three distinct DSP-based audio manipulations

Retains its original 3kHz audio channel bandwidth

Analog-encoded Data Security

Data mode supports up to 1,200bps modem data exchanges

Environmental & EMI/EMC

Operational Temp: -20°C to +70°C (Methods 502.2(P.II); 501.2(P.II))

Storage Temp: -40°C to +85°C (Methods 502.2(P.I); 501.2(P.I))

Humidity: MIL-STD-810D, Method 507.2 (Proc. II)

Vibration: MIL-STD-810D, Method 514.3 (Proc. I)

Shock: MIL-STD-810D, Method 516.3 (Proc. I)

EMI: MIL-STD-461C, (CE01/CE03/CS02/CS06/RE02/RS02)

MTBF

Exceeds 10,000 Hours (per MIL-STD-756)

Frequency Offset (HF-SSB)

Synchronization Recovery Range: ±120Hz

Frequency Reference / Control

Highly Accurate/Stable Crystal Oscillator

Continuous Secure Call Time: 40-minutes (typical)

Synchronization Method

Frequency Shift Keying: In-Band Sync Burst: 74-bits

PTT Sync (simplex / single path autonomous: broadcast)

Manual Dual Retrosync (two party, bi-directional)

Manual Single Sync (Shared Sync: broadcast)

Audio Channel Bandwidth Requirement (Minimum / Optimum)

400Hz to 2,500Hz (3dB) / 200Hz to 2,800Hz (3dB)

Red (Unencrypted Audio) Interfaces

HANDSET Connector (standard 5-pin / 6-pin MIL circular)

RADIO Connector (600 Balanced: 19-pin MIL circular)

Mic_Source_Select (menu set: 'RADIO' or 'HANDSET')

Range: -50dBm to +7dBm (selectable in 1dB steps)

Black (Encrypted Audio) Interface

RADIO Connector (600 Balanced: 19-pin MIL circular)

Range: -50dBm to +7dBm (selectable in 1dB steps)

Remote Control Interface (crypto status & operational controls)

RADIO Connector (via discrete 5V logic & PTT_In / PTT_Out)

Displays / Indicators

Front Panel Display, Cover Protected: 2-line by 16 character LCD

Audio Input Overdrive LED: services both Transmit / Receive paths

Key Management

Symmetric / Black (Encrypted) Manually Distributed Local Keys

Crypto Management System (**CMS-9000**) is available from TCC

Functional Design

Rugged, Heavy Gauge Extruded Aluminum Enclosure

Front Panel Latched Cover (protects LCD; keypad; and key fill port)

Anti-tamper: Network & Local Keys zeroized when case is opened

Standard 19" Rack Mountable with Optional Mounting Tray

DC Prime Power

9V - 32VDC

1-Watt (nominal) – Half Duplex

2-Watts (nominal) – Full Duplex

Voice Security over Severely Degraded Tactical Radio Channels

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.



NOTE
All specifications are subject to change without notification.

© Copyright 2010 by TCC
Document: DCN 92-1026

TCC Proprietary Information