TCC Proprietary Information

DSP 9000HS

Tactical Secure Voice Tactical Handset Encryption System

* *

Tactical-Level Voice Encryption

Protecting Radio Voice Channel Communications

* *

This self-contained handset is a member of the DSP 9000 family and offers a cryptographically strong, portable solution achieving tactical-level voice encryption over narrowband audio channels. Interface settings, configuration, and key management feature sets, may be programmed into a SmartModule™ key fill device allowing simply and intuitively movement between different HF, VHF, and UHF radios and landline audio channels. The DSP 9000HS provides excellent recovered voice quality over poor quality audio channels using a robust, in-band synchronization method designed for use on long range HF single sideband (HF-SSB) voice 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 9000HS allows a variety of different fielded radio equipment to be seamlessly integrated using one common cryptographic system. It can be rapidly reconfigured for situations where switching between radios requiring different audio level settings is required, simply by loading a preprogrammed 'configuration' **SmartModule**™.

EASE OF USE – The DSP 9000HS design offers user-friendly controls and audio feedback prompts. Day-to-day key management tasks are simplified through the use of Crypto Management System (CMS-9000), where the Crypto Officer role provides the ability to make all key management related decisions and selection. In addition to generating Local Keys, the Crypto Officer can program and download the selected key period. Keys are then automatically changed with no handset operator involvement.

CRYPTOGRAPHY – The DSP 9000HS is cryptographically identical to the DSP 9000 parent product, and 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.

A 10-bit pointer within the 74-bit synchronization signal (Sync Burst) remotely identifies the chosen Local Key in a process called 'Down-line Key Indexing'. The Sync Burst also provides the 16-bit Initialization Vector (IV). To provide anti-spoof protection, the IV is crypto-graphically message authenticated (MACed). A MACed clear voice override (CVO) Sync Burst is sent upon the release of the handset's PTT. The CVO directs receiving DSP 9000HS devices (or other DSP 9000 products) to return to Plain mode to await the next incoming transmission.

★ ★ ★ Features ★ ★ ★

High Grade Voice Security

Replaces any Tactical Radio Handset
- ◊ H-250 or H189 = Direct Replacement
- ◊ DC Power (6-pin circ. Connector Pin F)

Exceptional Recovered Voice Quality

SmartModule Programmable Settings
- ◊ Key Management functions
- ◊ Configuration functions / settings
- ◊ Interface I/O levels

Unit-to-Unit Synchronization
- ◊ Push-to-Talk (PTT) Sync mode
  - ◊ Used for broadcasts
  - ◊ Used for point-to-point calls
  - ◊ Select Call private call feature

Automated Key Management
- ◊ Local Key select configuration options
  - ◊ Automatically (time-of-use setting)
  - ◊ Manually (keypad command)
- ◊ Key selection at synchronization
  - ◊ TX unit sends 'Key Index'
  - ◊ RX unit(s) receive Key Index (index points to 1 of 200 Local Keys)

Highly Flexible Interface Range Settings

Highly Reliable Design
- ◊ Quality MIL-SPEC components
- ◊ Rugged Physical Design

AUTOMATED KEY MANAGEMENT – TCC's Crypto Management System (**CMS-9000**) key management support system allows a user, logged in as a 'Crypto Officer', to generate and autonomously manage all keying materials. The CMS personal computer is attached to a TCC **Security Vault™**, which generates and stores keying materials in its anti-tamper protected enclosure. The CMS is also able to program interface levels and configuration settings into SmartModules (with or without including keying materials). 'Configuration' SmartModules allow rapid reconfiguration of the DSP 9000 to move from one radio to another radio with different audio level interface settings.

DSP 9000HS

Voice Encryption System

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

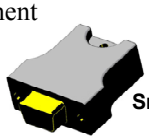
specifications

DSP 9000 Key Generator Design
Highly Non-Linear
Produces 16-bit 'SSB' variables to the EDT processing ...
production rate ~ 200ms (cryptographically varying)

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 100 keys (200 total)
Stored in EEPROM
Network Key (also in EEPROM)
System Keys – maintained in an EPROM device
IVs – Generated in Software at each PTT Sync actuation
All keying materials are under end-customer's control and management


SmartModule

Key Fill Device Support
SmartModule-2K, each stores one or both Keybanks

Enhanced Domain Transform (EDT)™ Processing
Cryptographically-Controlled
Three distinct DSP-based audio manipulations
Retains 3kHz bandwidth containment

Environmental & EMI/EMC
Operational Temp: -20°C to +60°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. III)
Immersion: MIL-STD-810D, Method 512.1 (Proc. I)
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)

Frequency Offset Synchronization Recovery Range: ±120Hz

Frequency Reference / Control: TCXO Crystal Oscillator

Synchronization Method
Frequency Shift Keying: In-Band Sync Burst: 74-bits
◊ Single Path Autonomous (Simplex) 'PTT Sync' mode
◊ Sync Burst transmitted at each PTT
◊ Cryptographically-Authenticated Sync Bursts (16-bit MAC)

Audio Channel Bandwidth Requirement (Minimum / Optimum)
400Hz to 2,500Hz (3dB) / 200Hz to 2,800Hz (3dB)

Black (Encrypted Audio) Interface
Handset Connector (6-pin circular MIL-C-55116 circular)
SmartModule-Programmable, Audio Amplitude Range Selection:
◊ Transmit -42.5dBm to +7.5dBm (selectable in 2.5dB steps)
◊ Receive -38.0dBm to +8.0dBm (selectable in 2dB steps)

Controls & Audible Indicators
PLAIN / CIPHER mode toggle switch
◊ Large 90° throw lever with excellent positional tactile feel

Keypad – 21 push-button switches (3 x 7 array)
◊ Volume settings
◊ Key Erase
◊ Key / Keybank (manually executed changes)
◊ Manual Keypad Local (or Network) Key Entry
◊ Key Fill and Configuration SmartModule load execution
◊ Test Key selection / de-selection
◊ Built-In Test execution

Audio Prompts:
◊ Plain Mode warning tone
◊ Test Key On warning tone
◊ Key / Keybank change tones
◊ Various Alarm / Error / Warning tones

Key Management
Symmetric / Black (Encrypted) Manually Distributed Local Keys
Crypto Management System (CMS-9000) – available from TCC

Functional Design
Rugged, High Impact Plastic and Aluminum Enclosure
Lightweight: 0.48kg / 1.05 pounds (less attached cord)

DC Prime Power
9V to 36VDC @ 0.75Watt (nominal)

NOTE
All specifications are subject to change without notification.

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.

TCC Proprietary Information

Technical Communications Corporation 100 Domino Drive Concord, Massachusetts, USA 01742-2892 +1-978-287-6229