

DLE-7050

Synchronous / Asynchronous Data Encryptor

DACE Mark XII
TCC-Proprietary
Encryption Algorithm
180-bit Data Encryption



Multi-Mode Digital Data Encryptor supporting Multiple Data Protocols and Electrical Interfaces

Available Interface Variants Include:

- **RS-232C / V.24**
- **CEPT E1 / G.703 (2,048kbps)**
- **US (ANSI) T1 (1,544kbps)**

APPLICATIONS

Available versions of the DLE-7050 support a wide variety of interfaces, data rates, and communications protocols.

CEPT E1 (G.703) and ANSI T1 (T1.403) units operate as 'frame sensitive' data encryptors, encrypting only the payload data leaving frame signaling information unencrypted. This supports installations where network devices or other higher order multiplexer devices need to see unencrypted framing information.

When configured for operation with RS-232 equipment, the DLE-7050 performs as a synchronous, 'bulk' data encryptor. Operation on asynchronous RS-232 data connections is also supported where the start and stop bits are left plaintext, but the payload data is encrypted in bulk data encryption fashion. Half duplex versions of the asynchronous RS-232 DLE-7050 are also available.

The DLE-7050's rugged design allows it to be inserted into many environments where commercial grade devices would not survive. Unit set-up may be performed using an attached data terminal, or via the unit's front panel controls and liquid crystal display.

DATA ENCRYPTION

The DLE-7050 uses dual, independent, bi-directional encryption engines incorporating TCC's proprietary, hardware (ASIC) based *DACE Mark XII* encryption algorithm. This ASIC chip delivers highly non-linear, non error propagating key generation fully supporting all of the interface options and data rates noted above.

Two menu-selectable methods of key management are supported: (a) manually distributed traffic keys (called 'Master Keys'), or (b) manually distributed key encrypting keys ('KEKs') used to encrypt locally-generated traffic keys ('Session Keys') over the established data link between two data encryptor devices. The second method is also referred to as 'Key-Auto-Key'.

The *DACE Mark XII* crypto engines use three different keys when encrypting or decrypting data traffic. Two are 'long term' key variables (the Family Key and the Custom Key) while the other is a 'short term' key variable. Depending on key management mode, the short term data encrypting key (DEK) is either a 'Master Key', or a unit self-generated 'Session Key'. Together they provide a total of 308-bits of key diversity.

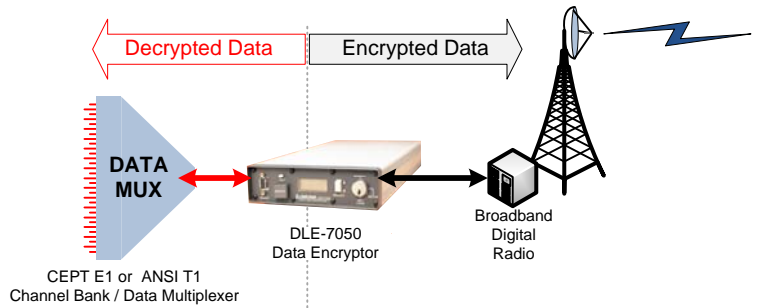
- Master Key (or Session Key) = 180-bits
- Family Key = 64-bits
- Custom Key = 64-bits

In addition to the three keys above, a random initialization vector (IV) is generated. After it is encrypted for transport, is referred to as a Message Key. A new Message Key is generated each time an encryptor and its associated decryptor state machines synchronize.

- Message Key = 33-bits

DLE-7050

specifications



ENCRYPTION / CRYPTOGRAPHY

DACE Mk XII Proprietary Key Stream Generator

- ▶ Pre-Loaded *Primary Keys* (180-bits each)
 - 'Master Keys' = Data Encrypting Keys (32 Master Keys Maintained in the DLE)
 - or -
 - Locally-Generated Primary Keys (180-bits)
 - 'Session Key' = Data Encrypting Key
 - Session Key Encrypted by selected Master Key
- ▶ Two *Secondary* (Longer-Term) Keys
 - 'Family Key', User-Programmable (64-bits)
 - 'Custom Key', TCC Factory Programmed (64-bits)
- ▶ Key Management Keys (2 each/ 180-bits each)
- ▶ 'Message Key' (33-bits)
 - Randomly Generated Initialization Vector (IV)
 - Sending Unit Encrypts IV yielding Message Key
 - Receiving Unit Decrypts Message Key yielding IV

SYNCHRONIZATION METHODS

- (1) Exchange of Master Key's Index
Key Index = 01 to 32
- (2) Exchange of Encrypted Session Key
("Key-Auto-Key" Mode)
DLE-7050 Generates its own Session Keys

SECURITY FEATURES

- ▶ Front Panel Key Erase
- ▶ Internal Anti-Tamper Protection
- ▶ Menu Access Protection (physical key)
- ▶ Menu-selectable Anti-Spoof feature

ELECTRICAL INTERFACES

(Device Dependent)

- ▶ CEPT E1 (G.703/G.704) @ 2,048kbps
- ▶ US (ANSI) T1 (T1.403) @ 1,544kbps
- ▶ ITU-T V.24 / RS-232 Synchronous
- ▶ ITU-T V.24 / RS-232 Asynchronous
- ▶ ITU-T V.24 / RS-232 Async Half Duplex

PRIMARY POWER INPUT

- ▶ 9VDC – 13VDC -or-
- ▶ 115/230VAC 50/60Hz
- ▶ 15 Watts (maximum)

PHYSICAL PARAMETERS

- ▶ 172mm X 57mm X 355mm
(6.75" X 2.25" X 14")
- ▶ 2.04kg (5.0lbs)

ENVIRONMENTAL

- ▶ Operating Temperature: 0°C to +50°C
- ▶ Storage Temperature: -40°C to +85°C
- ▶ Humidity: ≤ 95% non-condensing
- ▶ EMI/EMC: MIL-STD-461 Class A3 Part 4

KEY MANAGEMENT

- ▶ Local Key Management
- ▶ Remote Key Management
 - Personal Computer-Based System
 - Key Fill Device

All Specifications Are
Subject To Change
Without Notice
Copywrite: TCC 2009

Sheet 2

DCN 00-1015

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.

