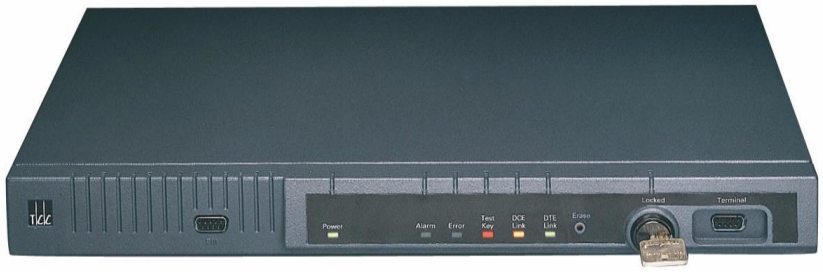
Cipher X ® 7100

AES-256

Frame Relay Data Encryptor

256-bit Session Key Advanced Encryption Standard (AES-256) per FIPS-197

Frame Relay Protocol Data Encryptor



***AES-256* Block Cipher Encryption**
- **256-bit Primary Key Variable**
- **256-bit Key Encrypting Keys**
- **256-bit Master KEKs**

AES offers 16-byte I/O Block Size
- **Cipher Feedback (CFB)**

Government and private organizations are exchanging ever-increasing amounts of data, while their network managers are generally faced with providing more bandwidth within ever-tightening budgets. Significant cost savings can be achieved by using publically available broadband data network backbones to augment and in some cases replace private data networks. The tradeoff to these potential cost savings comes with the increased risk of data compromise at exposure points within frame relay networks.

The *Cipher X 7100* Frame Relay data encryptor has been engineered to protect these mission critical communications backbones; thus enabling organizations to take advantage of the lower operational costs and trunk redundancies offered by using publically managed frame relay networks. The *Cipher X 7100* Frame Relay data encryptor provides strategic level protection from internal threats occurring on private, dedicated networks.

Defending ones sensitive information from cyber attacks and malicious threats, as well as the ever increasing sophistication of traffic intercepts, requires the latest advancements in communications security. The *Cipher X 7100* Frame Relay data encryptor has served TCC customers' for over a decade. During that time, new advances in encryption algorithms have led to the development of the FIPS 197 Advanced Encryption Standard (AES) algorithm, now offered by TCC.

TCC's frame relay data encryption system protects the privacy of data sent over public frame relay networks by securing selected permanent virtual circuits (PVCs).

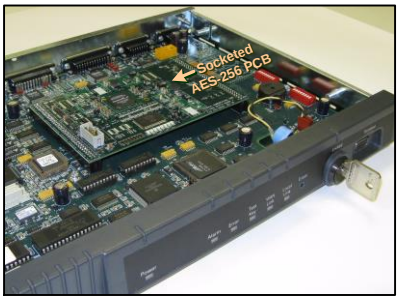
TCC's *Cipher X 7100* Frame Relay data encryptor offers full duplex 256-bit Advanced Encryption Standard (AES-256) encryption algorithms, incorporated within a hardware-based crypto processor module, ensuring low latency and maximum performance.

The *Cipher X 7100* requires little user training to install, configure and operate, minimizing operational cost to end-users. Security policies are intuitively easy to establish and enforce; each bi-directional data link connection identifier (DLCI) based link is configured as a transparently established secure connection. Once configured, insertion of *Cipher X 7100* data encryptors into the frame relay network is operationally transparent; no changes to the network are required.

Secure, AES-256 protected key and device management of each *Cipher X 7100* data encryptor can be performed remotely over a client-server connection using TCC's KEYNET Management System.

Incorporating a KEYNET centralized management function into the network makes the security policy configuration and periodic key management operations fully automatic.

Cipher X 7100 — specifications



Internal view of Cipher X 7100 Unit
showing **AES-256** Crypto Processor PCB

APPLICATION (Cipher X 7100)
Full Duplex Frame Relay Data Security
Synchronous Data Rates up to 2.048Mbps
Frame Size up to 4,096-Bytes

ENCRYPTION
Advanced Encryption Standard (AES)
256-bit Session Key Variable
16-Byte (I/O width) Block Cipher
FIPS 197 Compliant Implementation

KEY MANAGEMENT [1]
Local Management via Cipher Site Manager
Remote Centralized Management via KEYNET
Secured SNMP Key Service Messages
AES-256 Encrypted Key Service Msgs

DEVICE MANAGEMENT [1]
Local Monitoring / Setup - Cipher Site Manager
Custom Microsoft Windows® Application
Role-Based Functionality (User Passwords)
Remote Centralized Management via Keynet (SNMP)
AES-256 Protected Device Status & Control Msgs
Time & Date Stamped Audit Logs
Alarms, Errors, & Security Events

NETWORK PROTOCOL SUPPORT
ITU-T: Q.922; Q.933
ANSI: T1.606; T1.617; T1.618
FRF.1

SECURITY STANDARDS
FIPS-197; FIPS 140-1 [2];
ISO 8732

ELECTRICAL INTERFACES
V.35; X.21; RS-422 / RS-449;
RS-485; RS530; RS-232

PRIMARY POWER INPUT
85-264VAC, 45-65Hz; 20 Watts (typical)

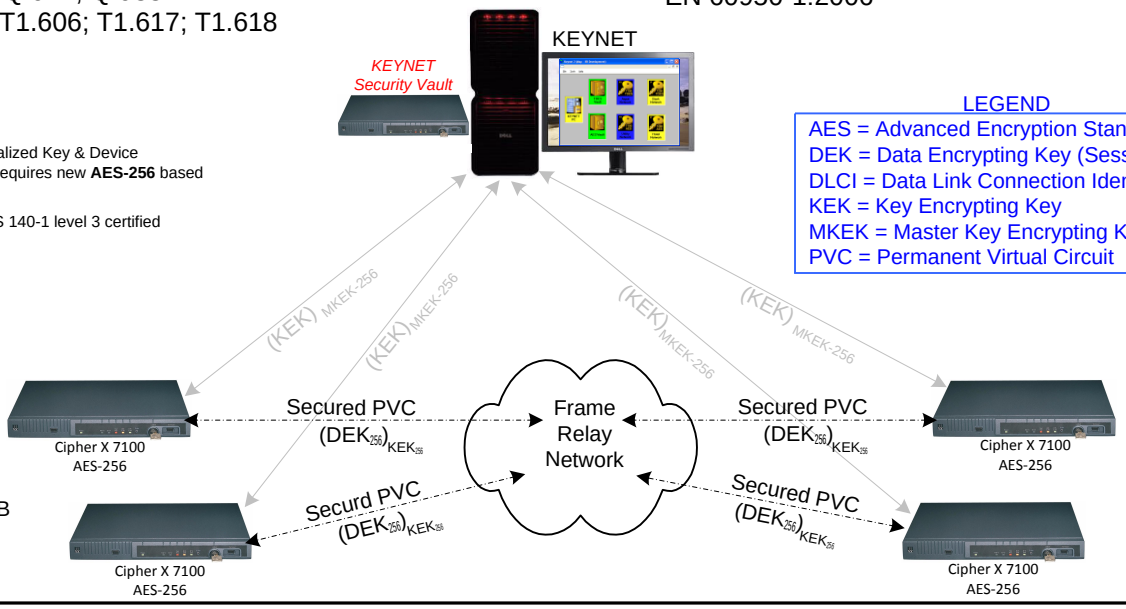
ENVIRONMENTAL
Operational Temp. 0°C to +50°C
Humidity 5% to 90% non-condensing

PHYSICAL PARAMETERS
Dims: 41.0cm(w) x 4.4cm(h) x 26.7cm(d)
19-Inch Rack Mountable: Flanges Included
Weight: 3.7kg (8.2lbs) less cables & flanges

AGENCY APPROVALS
FCC 47 CFR Part 15, Class A
ICES-003 Issue 4 Class A
EN55022:1998/A1:2000/A2:2003 Class A ITE
EN55024:1998/A1:2001/A2:2003 ITE
VCCI Class A ITE
IEC 60950-1:2005
EN 60950-1:2006

NOTES:
1 Remote Centralized Key & Device Management requires new **AES-256** based **Keynet**

2 Based on FIPS 140-1 level 3 certified platform



DCN 08-1005 Rev B

Communicate in Confidence®

Commitment to Quality

TCC designs, manufactures and supports high-grade secure communications systems that protect highly sensitive information transmitted over a wide range of data, voice and video networks. Government/military agencies, financial institutions, telecom carriers and other multinational corporations worldwide rely on TCC to protect their communications networks.

TECHNICAL COMMUNICATIONS CORPORATION 100 Domino Drive, Concord, MA 01742-2892, USA +1-978-287-6229 | www.tccsecure.com