

# Keynet 2

Version 4

**AES-256** based  
data protection  
for mission critical  
data networks

- Advanced Encryption Standard protection
- User-friendly Graphics User Interface (GUI)
- Services any number of Cipher X 7100 & Cipher X 7200 units



In support of the release of its new 256-bit Advanced Encryption Standard (AES-256)-based *Cipher X 7100* (Frame Relay) and *Cipher X 7200* (Internet Protocol) data encryption products, Technical Communications Corporation (TCC) also offers a new, custom developed *Keynet 2*<sup>TM</sup> management system.

The automated *Keynet 2* system seamlessly connects to a customer's network, where it transparently performs all centralized key management functions required of a secret distributed key based encrypted data network. In addition, *Keynet 2* performs device status monitoring (auditing), as well as securely collecting traffic statistics. The prior version of *Keynet* was based (solely) on Triple DES (TDES). This newest release delivers 256-bit AES message encryption as well as (optionally) supporting a TDES capability for networks in transition between older TDES and newer AES-based Cipher X units. Dual vault *Keynet* systems incorporate two separate *Security Vaults*, one supporting the AES-256-based units and the other supporting the TDES-based units.

The *Keynet 2* support system is comprised of a custom Windows XP-based application that runs on a host personal computer (PC), and is attached to one or more Security Vaults. Each Security Vault securely generates and retains all of the keying materials in an anti-tamper protected enclosure. It also encrypts and decrypts all of the SNMP messages that are either sent to or received from each Cipher X data encryption device on the data network.



Security Vault

All key management messages are secured using FIPS 171 (ANSI X9.17) banking security standard. All other sensitive messages are likewise encrypted between the *Keynet 2* server and the fielded Cipher X 7x00 devices using secure SNMP messaging.

# Keynet 2 Version 4

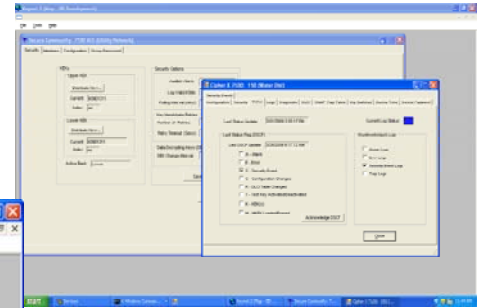
## specifications

AES-encrypted  
key management and  
device management  
protecting mission critical  
data networks

### ENCRYPTION

- Advanced Encryption Standard
  - Block Cipher / 256-bit keys
  - Triple DES (TDES)
- Block Cipher / 112-bit keys
- AES and TDES dual configuration supports networks consisting of both Cipher X 7100 and Cipher X 7200 devices while transitioning from TDES to AES

Keynet™ provides an intuitive graphical user interface that is very easy to learn and to use. Cipher X encryption devices are added to secure user groups by simply dragging and dropping the Cipher X 7100 and the Cipher X 7200 icons.



### SECURITY STANDARDS

- FIPS 197 (AES-256)
- FIPS 46-3 / ANSI X9.52 (TDES)
- NIST SP 800-38A (AES & TDES)
- FIPS 140-1 Level 3
- FIPS 171 (Key Management)
- ISO 8732



color coded icons

coded device type **LEGEND**

- AES = Advanced Encryption Standard
- DEK = Data Encrypting Key (Session Key)
- FIPS = Federal Information Processing Std.
- IP = Internet Protocol
- KEK = Key Encrypting Key
- MKEK = Master Key Encrypting Key
- SA = Secure Association
- TDES = Triple Data Encryption Standard

### COMPONENTS

- Security Vault (one or both used)
  - AES Security Vault
  - TDES Security Vault
- Desk-Top Personal Computer
- Keynet Application
- Windows XP (opt. Vista or Windows 7)
- SmartModule-2K Key Fill Devices
- 256-bit SKEKs (Security Vault KEKs)
- 256-bit MKEKs Loaded into Cipher X 7x00

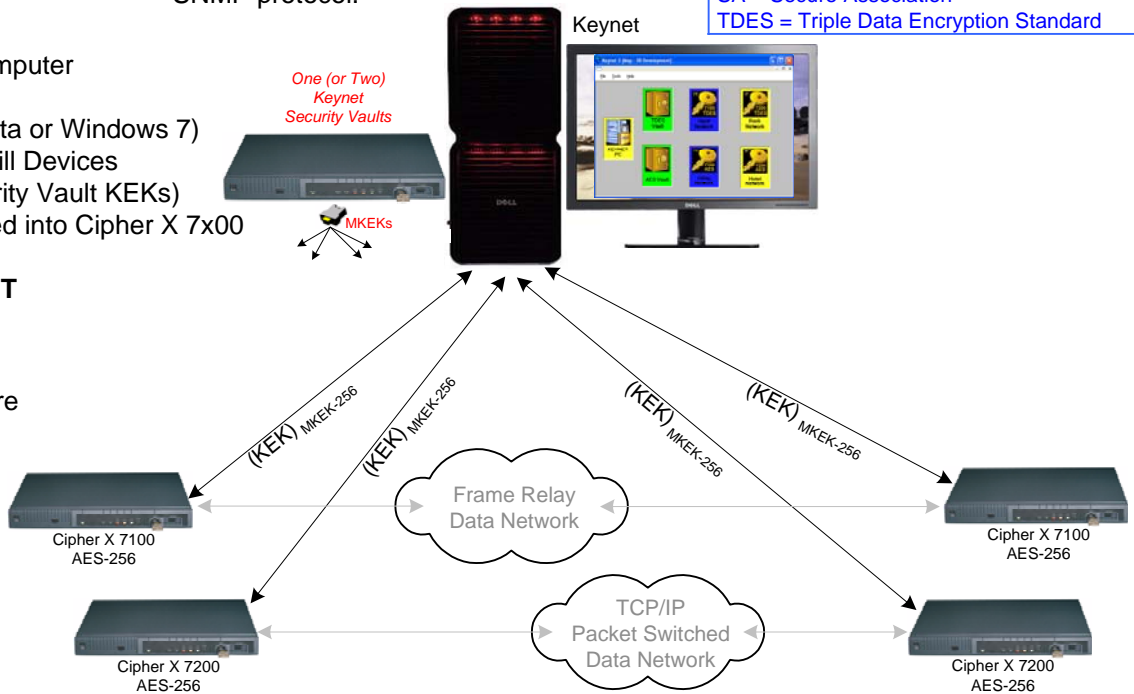
Keynet interconnects to the network, communicating with the Cipher X 7x00 devices via a secure SNMP protocol.

### PRIMARY POWER INPUT

85-264VAC, 45-65Hz

### ENVIRONMENTAL

- Operational Temperature
  - 10°C to 35°C
- Humidity
  - 5% to 90% (Non-condensing)



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



DCN 09-1024

### 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.

