

Technical
Communications
Corporation

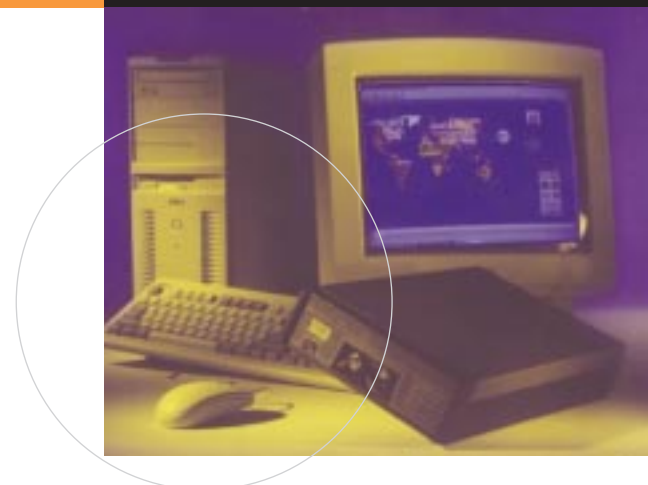
Keynet™ Release 2.0

security
management for
mission-critical
networks

The KEYNET Secure Management

Application enables key management, configuration, monitoring, and troubleshooting of a large, global network of Cipher X® encryption units from a single location. All key management messages are secured using the ANSI X9.17 banking security standard that defines 'prudent business practice' for the banking community. All other sensitive commands are encrypted using a secure SNMP protocol. These high security measures facilitate central management, while maintaining optimum security.

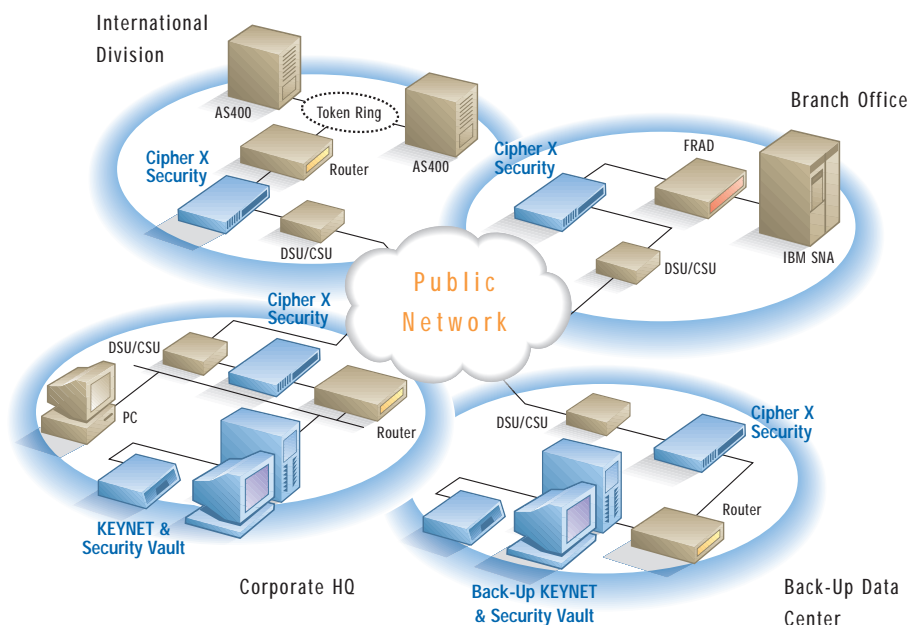
KEYNET fully meets the high availability requirements of mission-critical networks. Using the SNMP protocol, KEYNET can receive errors and alarms from the Cipher X or proactively poll the units to determine their status. This status information can also be sent to an enterprise management application, such as HP's OpenView or Tivoli's NetView, to integrate the Cipher X into the overall network management scheme. For disaster recovery or network outage conditions, a hot-standby KEYNET, complete with a replicated database, can be positioned to take over if the primary KEYNET is unavailable.



key benefits

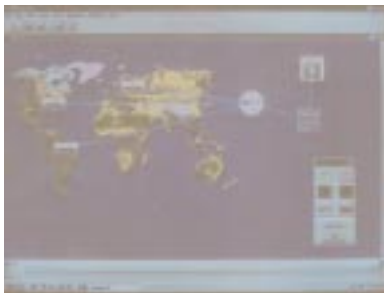
- > Drag and drop user interface simplifies adding and deleting units and forming key groups
- > Encrypted SNMP sets prevent spoofing attacks by hackers
- > Status at a glance is displayed via color-coded icons on the key management map
- > Low cost platform based on Windows NT application server
- > Anti-tamper, hardware-based Security Vault protects keys from physical compromise
- > Hot-standby mode provides restoration for mission-critical networks

Virtual Private Network



Keynet Release 2.0

specifications



KEYNET has an intuitive graphical user interface (GUI) making it very easy to use. Units are added or deleted to key groups by simply dragging and dropping Cipher X icons. Key distribution occurs automatically based on the key management map topology, enabling network managers to rekey a large network quickly. Color-coded indicators on each managed Cipher X quickly conveys network status at a

glance. Further troubleshooting is performed through audit logs and remote diagnostics.

The KEYNET architecture combines the benefits of low-cost and open systems with anti-tamper, hardware security.

The application server platform is based on Microsoft's Windows NT and uses Microsoft's SQL Server database. Report writing and management tools for these Microsoft products enable customization of the KEYNET system. For optimum security, however, the anti-tamper hardware is recommended to prevent a broad range of software attacks by hackers, viruses, etc. The KEYNET system stores all plain text keys and encrypts all data in the anti-tamper Security Vault. All security related information is automatically erased if the Security Vault is attacked.

Application

Management of Cipher X secure communication systems

Encryption

Triple DES

security
management for
mission-critical
networks

Key Management

ANSI X9.17

Security Standards Support

ANSI X9.17, ISO 8732,
FIPS 46, FIPS 140-1, FIPS 170

Network Protocol Support

SNMP MIB II

Customer Support

90 day software warranty
1 year Security Vault warranty
Extended support and maintenance
contracts available

Recommended System

KEYNET for Windows NT
> 300 MHz Pentium computer
> 256M RAM (minimum)
> 300M free hard disk space
> Windows NT Server 4.0 OS
> SQL Server 6.5 database



TCC secures mission-critical networks for governments, corporations, and financial institutions around the world. With over 35 years experience, TCC is the trusted supplier for organizations that place a high value on their data and its successful transmission.

Cipher X and KEYNET are trademarks of Technical Communications Corporation. Other brand and product names may be trademarks or registered trademarks of their respective owners.

Technical Communications Corporation
100 Domino Drive, Concord, MA 01742-2892, U.S.A.
Tel: 978-287-5100 Fax: 978-371-1280
E-Mail: info@tccsecure.com
Web Site: <http://www.tccsecure.com>