

DigiSAFE M3000 series Data link Encryptor

1. Introduction

DigiSAFE M3000 series Data-link Encryptor enables confidentiality of sensitive data to be transmitted from one party to another through modems by means of encryption. It is able to transmit sensitive data over point-to-point data links at speeds of $n \times 64$ kbps. It also supports synchronous full duplex communications with a unique cipher synchronization scheme. Figure 1 illustrates an application of such a system.

DigiSAFE M3000 series uses standard cryptographic algorithm by employing a 112-bit or 168-bit Triple-DES algorithm. Standard ciphers have the advantages over proprietary ciphers, as they have been scrutinized and well-tested by experts in the cryptographic field.

For physical connection, DigiSAFE M3000 series V.35 version provides a total number of two DB25 connector. One of the connectors allows it to connect to the data communication equipment such as modem. The other is used for connections to data terminal equipments such as router.

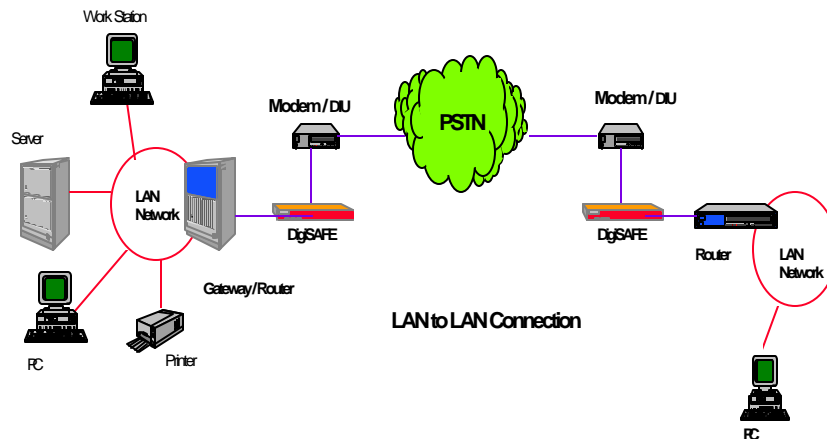


Figure 1. Typical DigiSAFE M3000 series Application Diagram

2. Features

2.1 Secure Data Communication for $n \times 64$ kbps lease line application

The DigiSAFE M3000 series is designed to operate at speed from 64 kbps up to 2048 kbps in synchronous applications. With DigiSAFE encryptor, no replacement of encryptor is required when network line speed is upgraded to higher speed. This is more economical and flexible than employing the fixed speed encryptor.

2.2 Strong Encryption Algorithm

DigiSAFE M3000 series is using a 112-bit/168-bit Triple-DES algorithm with Cipher Block Chaining Feedback mode or 64-bit Output Feedback mode. With a larger key size of DES algorithm, it provides higher security protection of data transfer over the lease line.

2.3 Self Synchronizing

In the event that encryption of two communicating parties gets out of synchronization, Bit Error Recovery Insertion Scheme helps them to achieve self-synchronization.

2.4 Protocol Transparency

The encryption and decryption processes take place at the physical layer. As a result, this provides complete higher-level protocol transparency. In other words, it frees user the restrictions of the use of higher-level protocols and applications.

2.5 Secure Key Management

The implementation of DigiSAFE M3000 series uses two level of keys: KEK (Key Encrypting Key) and session keys. In DigiSAFE M3000 series, the two types of KEK are root key and base key. They are used for encrypting keys whereas session keys are used for encrypting the actual data.

2.5.1 Key Generation of KEK

The Electronics Key Generation System software is used to facilitate the generation of root key and base key.

2.5.2 Storage of KEK

DigiSAFE products use 2 sets of smart cards to store the KEK. These are the Supervisor and the Key cards. The Supervisor card stores the root key which is

used to encrypt/decrypt the base key. The Key card however, is used to store the base key in an encrypted form. In turn, the base key is used to encrypt/decrypt the session key. Eventually, the session key is used to encrypt/decrypt the data.

2.5.3 Key Generation of Session Keys

Noise source on the circuit board is used to generate session key. It provides greater randomisation of key value as compare to pseudo-random source. The session key is generated at pre-selected time interval. This implies that the generation of session key is without user intervention and thereby, freeing users from inconvenience. Moreover, the session keys are only generated during session key exchange. In short, a session key is only generated when it is needed. This further increases the privacy of the session key by reducing its storage time in the DigiSAFE M3000 series.

2.6 Full front panel Control

DigiSAFE M3000 series provides full user-friendly features by offering easy-to-operate functions on its front panel.

2.7 Tamper-Resistance chassis design

Beside all the security features mentioned earlier on, DigiSAFE M3000 series provides physical security by implementing tamper resistant chassis design. For example, if the chassis cover is tampered with, this will activate an internal anti-tamper switch that will immediately erase all secret information.

2.8 Diagnostic Testing

Diagnostic test can be carried out by both the power-up self test and manual selective test on front panel. When a fault occurs, signal will light up the LEDs and at the same time, logging takes place.

2.9 Battery-backup of key variables

Back-up Battery will kick off in the event of power failure or when power drops below acceptable threshold values.

3. Conclusion

DigiSAFE M3000 series is bundled with self-sufficient security features and full key strength to ensure successful and secure communication to take place.

4. Application

4.1 LAN to LAN Connection

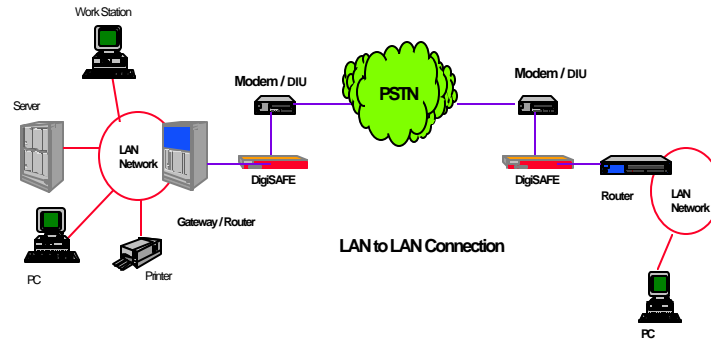
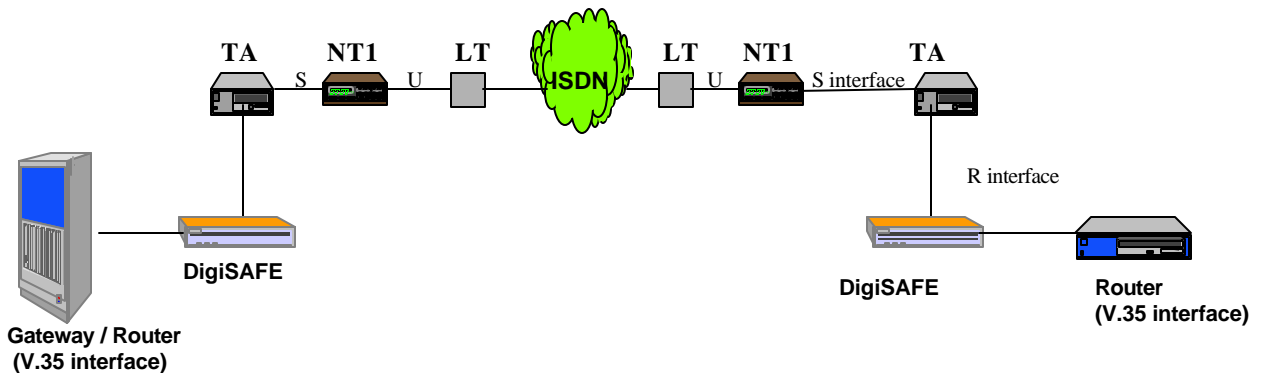


Figure 4.1 LAN to LAN application

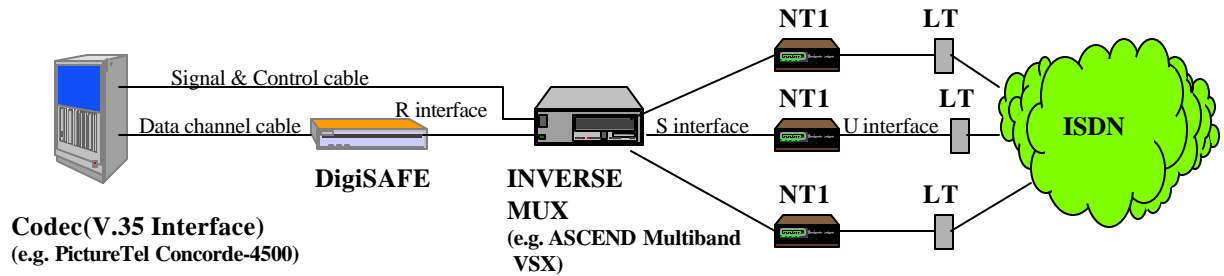
The encryptor is inserted between the modem and router, thus providing the secure link for organization's wide area network.

4.2 2B BRI ISDN Connection



For 2B-BRI ISDN application, the DigiSAFE encryptor is inserted between the Terminal Adapter (TA) and Terminal equipment (TE2). The DigiSAFE encryptor can only be connected to TE2 with a V.35 interface. The call establishment signal is bypassed when TE2 initiates the call setup through TA. Once the call setup is established, the DigiSAFE encryptor will encrypt all data information, thus providing a secure link through the ISDN network. This connection only permits point-to-point dial-up operation and is usually used as a standby link for lease line LAN-to-LAN network.

4.3 Dedicated ISDN Video-conferencing (thru Inverse-Mux) Application



For dedicated Video-conferencing through ISDN lines application, the DigiSAFE encryptor only encrypts the content of data channel. The signal and control port is connected directly to the inverse mux for call setup. The encryptor only starts operation after the call setup is established.