

DigiSAFE A1000 ISDN BRI Line Encryptor

1. Introduction

DigiSAFE A1000 ISDN BRI Line Encryptor provides two B-channel content encryptions of ISDN Basic Rate Interfaces. This provides secure data transfer in networking applications such as video-conferencing and voice/fax services. Figure 1 illustrates an application of such a system.

Moreover, DigiSAFE uses standard cryptographic algorithm by employing a 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 A1000 provides a total number of four RJ45 type connectors for its S/T interfaces. One of the connectors allows it to connect to the public/external network and the rest of them are dedicated for internal connections to terminal equipments such as fax, telephone, router and ISDN-cards based system.

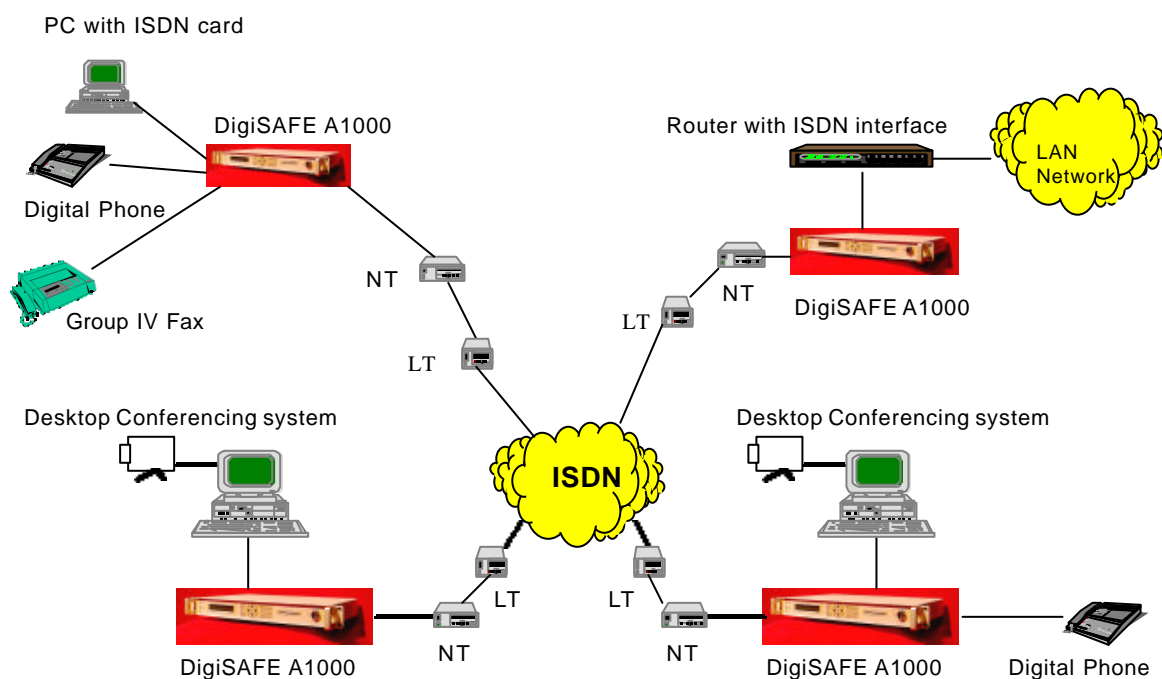


Figure 1. Typical DigiSAFE A1000 Application Diagram

2. Features

2.1 Independent B-channel Encryption

The handshaking and encryption of each B_channel are independent of each other. This allows two terminal equipments to be connected simultaneously to different locations in a physical link and yet deliver secure transfer of data. For each ISDN call, a new session key is generated for every B_channel connection.

2.2 Strong Encryption Algorithm

DigiSAFE A1000 is using a 168-bit Triple-DES algorithm with 64-bit Output Feedback mode. With a larger key size of DES algorithm, it provides higher security protection of data transfer over ISDN link.

Moreover with 64-bit Output Feedback mode, this guarantees no line error propagation to the subsequent 64-bit data block if an error bit occurs in the preceding data block.

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 A1000 uses two level of keys : KEK (Key Encrypting Key) and session keys. In DigiSAFE A1000, the two types of KEK are root key and base key. They are used for encrypting keys whereas session key is used for encrypting the actual data.

2.5.1 Key Generation of KEK

Key Generation of root and base keys is performed by selecting manual input functions on front panel of DigiSAFE A1000.

2.5.2 Storage of KEK

DigiSAFE products use 2 sets of smart cards to store the KEK. These are referred as the Supervisor and the Key cards. The Supervisor card stores the root key, which is used to encrypt/decrypt the base key whereas the Key card stores 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 when each new ISDN call is being established. 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 after each establishment of ISDN call. 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 A1000.

2.6 Downloading of Customized Encryption Algorithm

In the near future, DigiSAFE A1000 allows users to download their customized algorithm from the smart cards onto the encryptor through its manual input function on the front panel. The Algorithm Generation System software is used to facilitate the downloading of their customized cryptographic algorithm.

2.7 Full front panel Control

DigiSAFE A1000 provides full user-friendly features by offering easy-to-operate functions on its front panel.

2.8 Tamper-Resistance chassis design

Beside all the security features mentioned earlier on, DigiSAFE A1000 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.

2.9 Diagnostic Testing

Diagnostic test can be carried out by both power-up selftest 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.

2.10 Battery-backup of key variables

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

3. Conclusion

With the booming of ISDN link usage and lower charge rate, more organizations are using ISDN network for transfer of data, voice and multimedia application.

DigiSAFE A1000 is the solution for secure voice, data and multimedia application over the ISDN link

4. Typical Application

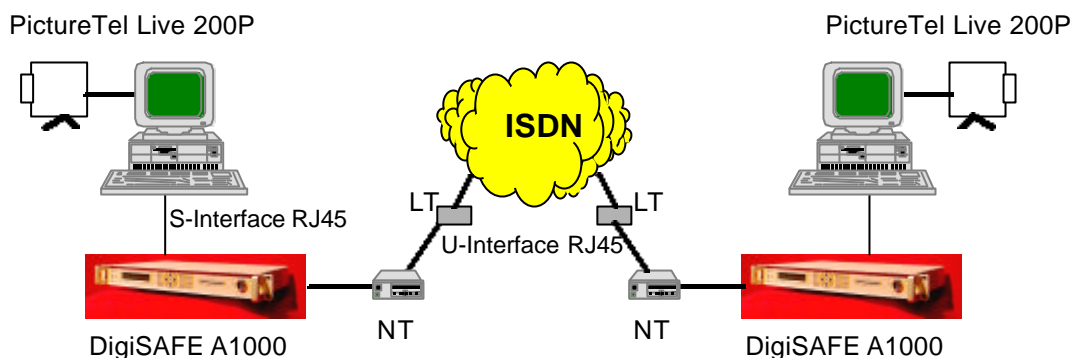


Figure 4.1 Video-Conferencing congifuration I : Securing 128Kbps (BRI) Video Conference link using desktop video conferencing system

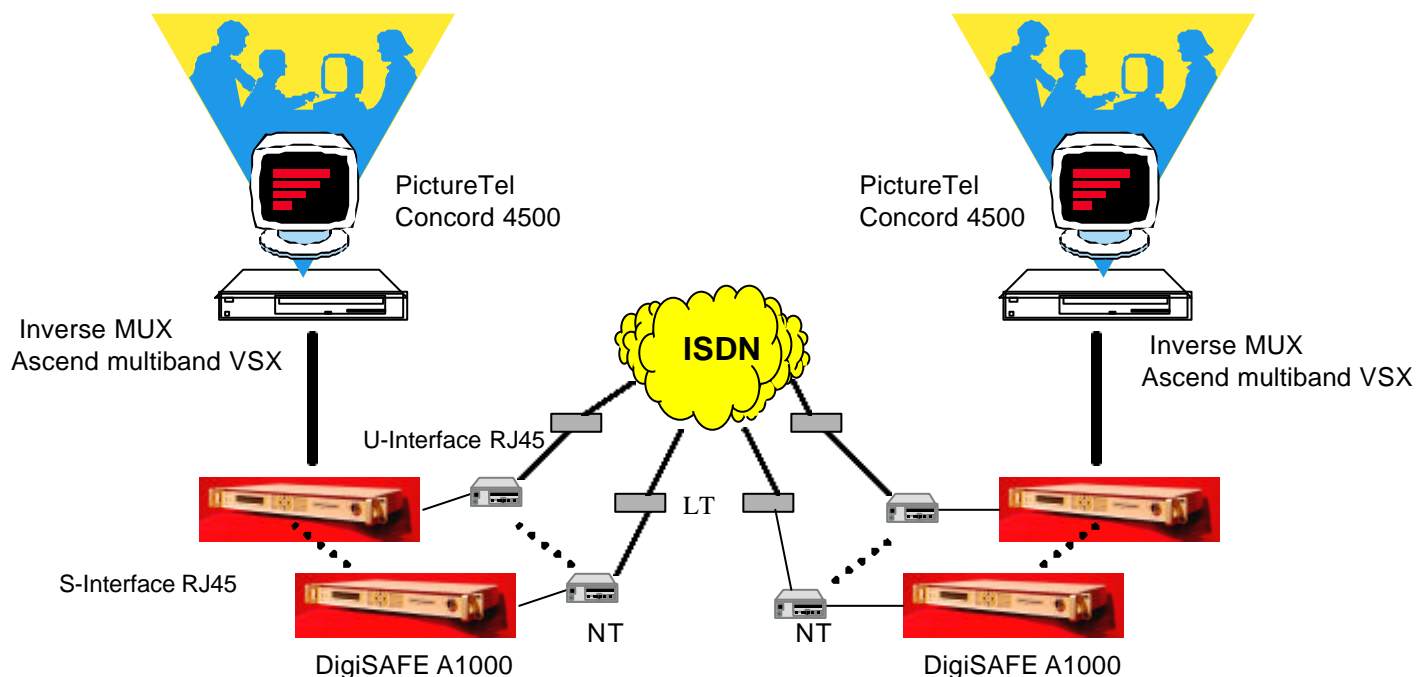


Figure 4.1 Video-Conferencing congifuration II : Securing Video Conference link using Video codec through Inverse-mux (Bonding of 2 or more ISDN BRI link)

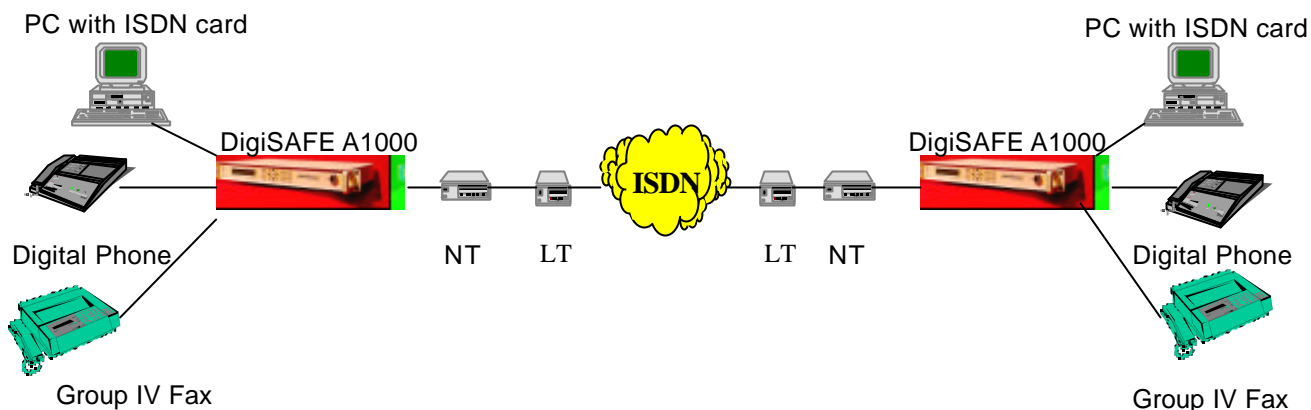


Figure 4.3 Secure Phone, Fax, Data services using DigiSAFE A1000

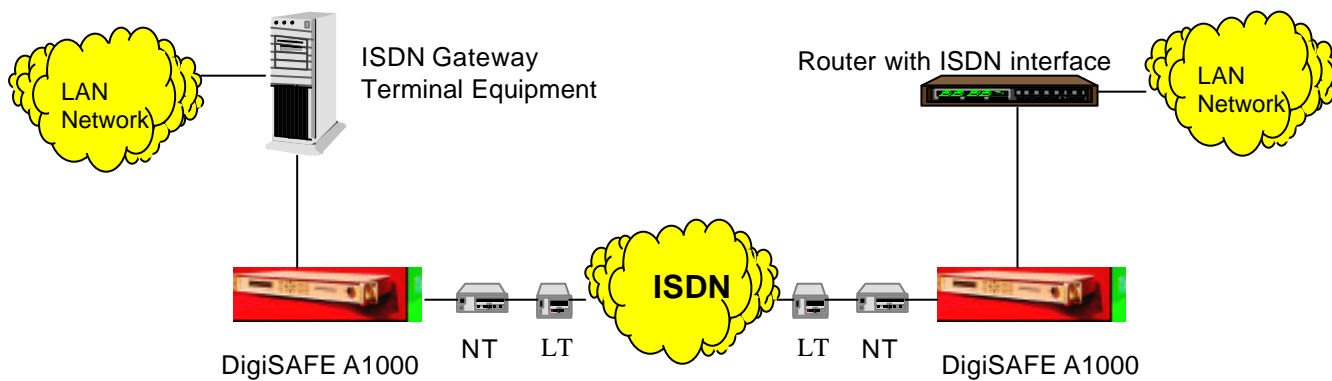


Figure 4.4 Standby link for lease line circuit LAN to LAN network