5. ISDN Security Protocols and Applications

This section describes a general structure, similar to SDNS or SILS, for ISDN security. It is illustrated in figure 14 and is composed of *security protocols* and *security applications*. This structure allows implementation of the security services listed in section 7 above. It includes some protocols and applications specific to ISDN, but as far as possible uses the emerging services now in the early stages of standardization for OSI. For the purposes of this discussion a security protocol is a peer to peer process running at the transport layer or below. Security protocols typically provide confidentiality, integrity and security labeling during data exchange. Security applications are processes at the application layer which support security protocols. The functions of security applications include security attributes, authentication and access control. Security applications may require a trusted specialized service application or third party. Security applications are ordinarily invoked as a part of establishing or terminating a secure association or connection.

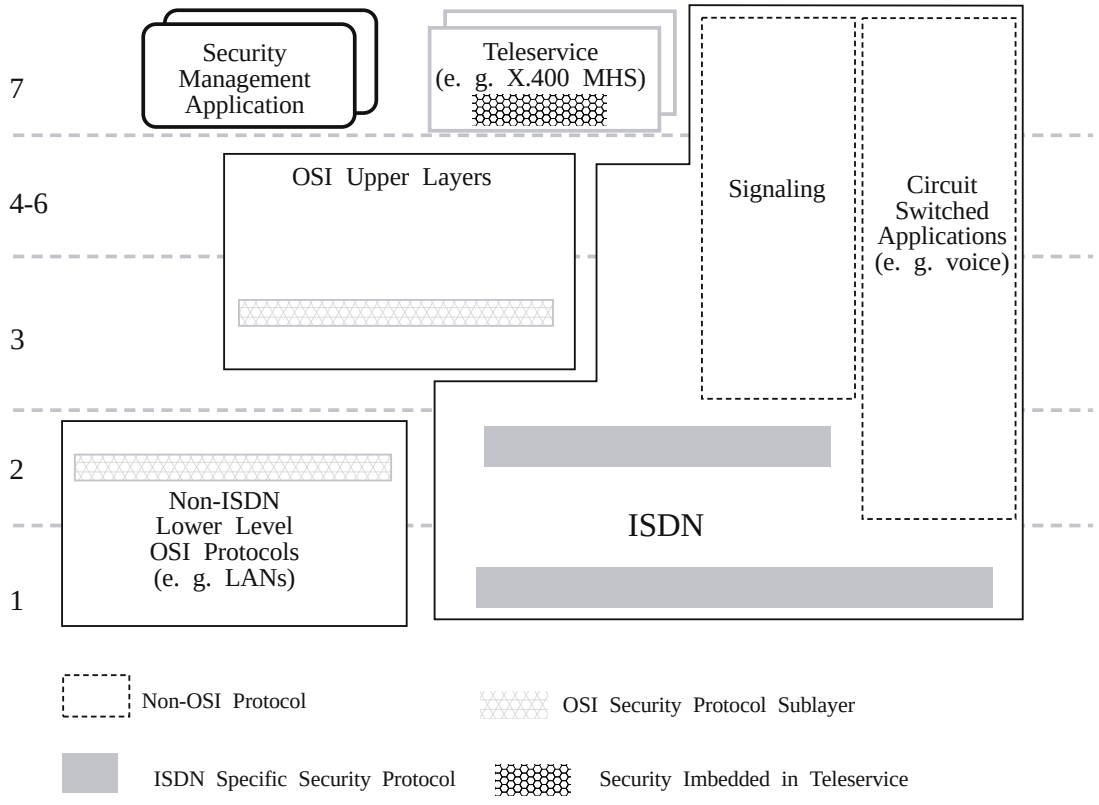

Figure 14 - ISDN/OSI Security Structure.

5.1 Security Protocols

The overall function of security protocols is the secure exchange of data. The first function of security protocols is integrity, and that may be the only service required. The second major function is confidentiality. Both integrity and confidentiality ordinarily are implemented with cryptographic techniques, although confidentiality may be provided by secure routing. Security labels may also be provided by security protocols, and the use of the correct key provides a means of authentication on a per packet basis. In general, however, such functions as authentication, access control, key management and notarization are primarily implemented as security management applications.

5.1.1 Security Protocols above ISDN

As described in section 5.1.2 above, SDNS defines several security protocols which are suitable for use with the OSI and DoD protocol stacks above ISDN at layers 3 and 4. These protocols are above ISDN proper, but are associated with ISDN, when ISDN is used as a part of the OSI (or DoD) protocol stacks. They are expected to provide a starting point for the development of OSI standard security protocols, or similar protocols will be developed for OSI security at layers 3 and 4.

Figure 5, above, illustrates the locations of the specific SDNS protocols, which are located above ISDN at layers 3 and 4. The specific variants of the SDNS SP4 and SP3 protocols are discussed in table 1 above. In this section we will simply use “SP3" to mean an OSI network layer security protocol standard and “SP4” to mean an OSI Transport layer security protocol standard, without necessarily meaning a specific SDNS protocol as presently defined.

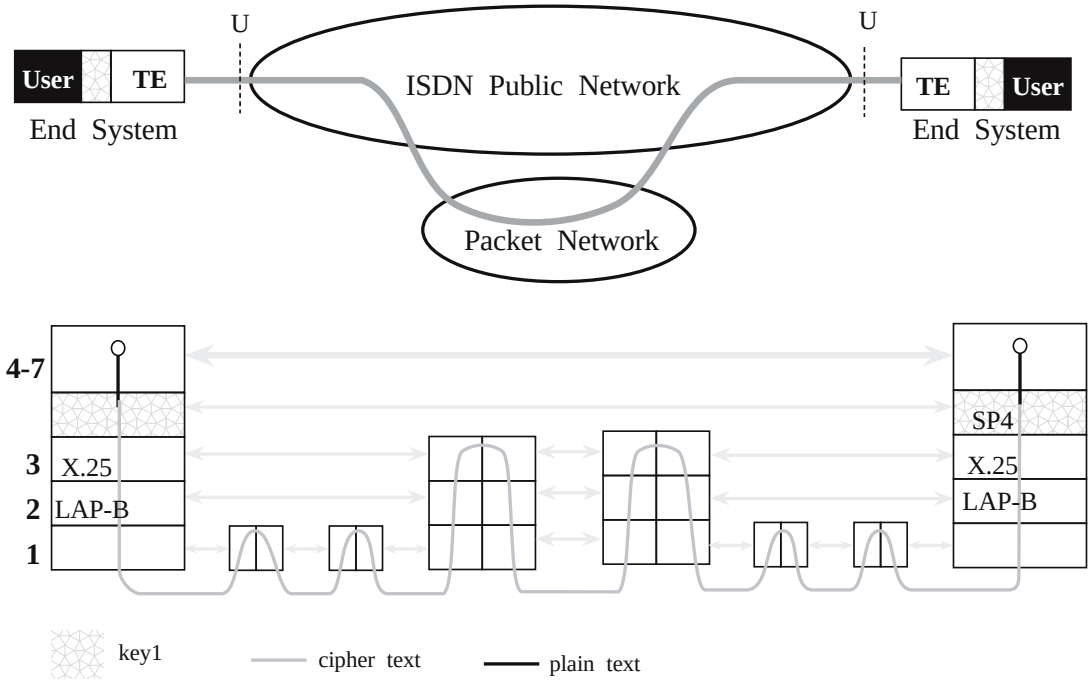

Figure 15 - Transport Layer End-to-End Encryption.

Where an OSI packet data stack utilizes ISDN to provide at least some (but not necessarily all) of the network layer connections, a Transport layer security protocol, such as SP4, can provide a powerful end-to-end confidentiality solution. This solution is illustrated in figure 15 for a B channel connection to a packet network, however it is equally applicable to D channel packet user data services. In figure 15 the packet network may be implemented by packet handlers in the local office switch, or it may be an independent network reached through the circuit switch. The packet network may in fact be a LAN, or some other network which is entirely independent of ISDN.

An intruder monitoring the U interface point sees the Network layer headers as plaintext and the Transport PDU as ciphertext. Since the Network headers and addresses are plaintext, and the size and frequency of packets are apparent, traffic analysis may be fruitful.

The SP3 protocols can also be used above ISDN in a variety of ways. Figure 16 illustrates the use of network layer encryption to encrypt B channel data on a subnetwork by subnetwork basis. This approach has the advantage of simplifying key management for the terminals, since only the one key is used to protect communications with the secure packet network, whatever the destination. It has the disadvantage that the secure packet network must be trusted, since red data exists at least in the packet switches.

Figure 17 illustrates what is probably a more typical use of an SP3 protocol. In figure 17 two X.25 gateways, incorporating the SP3 protocol, connect two red LANs through a black public network (alternatively the terminals can be asynchronous terminals and the gateway a PAD). This arrangement requires the gateways to manage keys for all destination gateways. Cryptographic protection is provided between the gateways over the public network. The red LAN

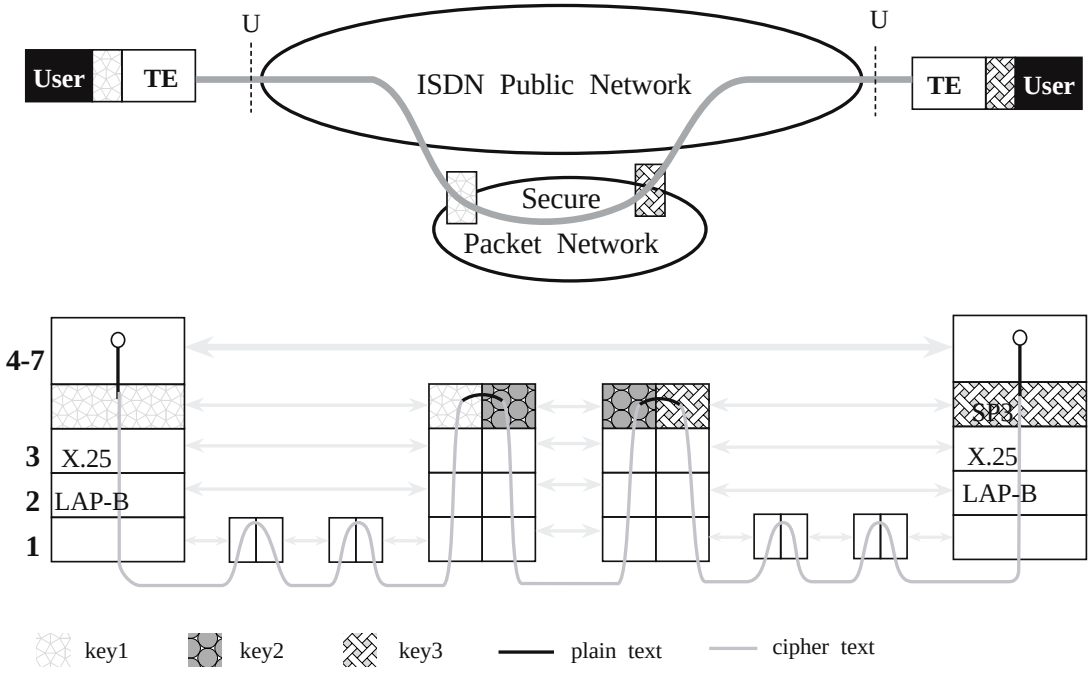

Figure 16 - Network Layer Packet Encryption.

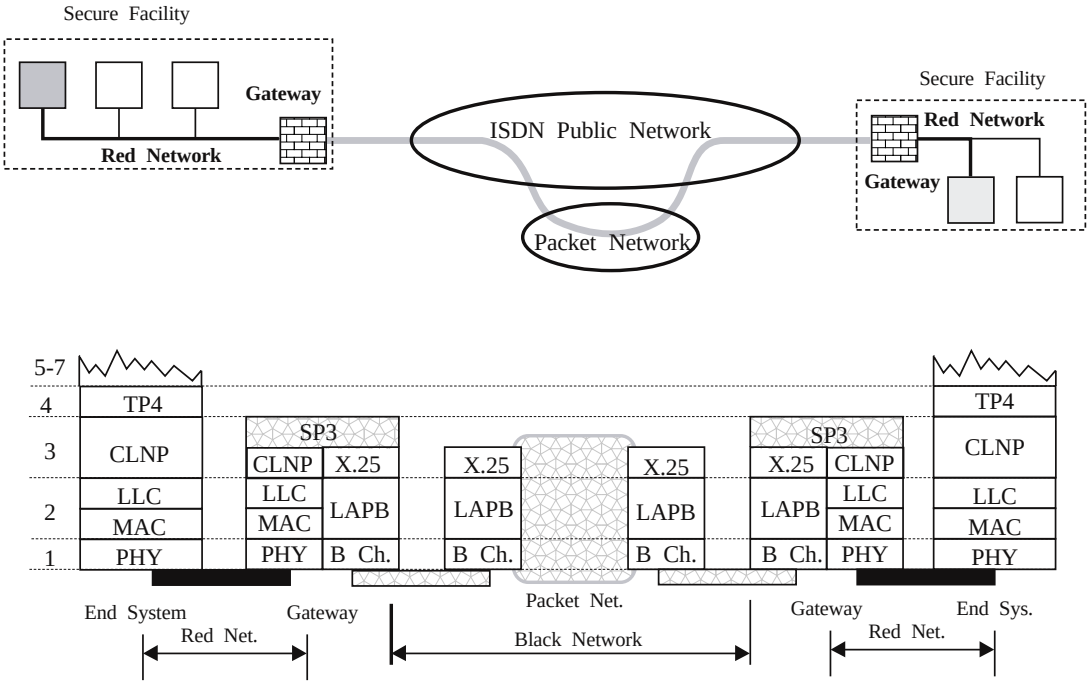

Figure 17 - Network Layer Packet Encryption.

networks must be physically protected. With this type of gateway it is easy to ensure that all traffic leaving the secure facility is encrypted. The cost of cryptographic hardware is minimized. This scheme is most useful when the general nature of the facility requires strict general security, or when the red network can be confined to a small area which is easy to protect.

SP3 layer protocols can provide more address confidentiality than does SP4. The specifics of what is revealed depends upon the specific SP3 mode. Often an intruder intercepting the communications at a U interface can discover the addresses of the destination gateway, but not the end system or NSAP address.

A practical disadvantage of Network layer encryption for ISDN is that the secure gateway can also become a bottleneck, if traffic loads are heavy. Protocol processing for X.25 places limitations on performance and the SP3 protocol will increase the processing load. If frame relay secure gateways were used, then it is likely that the security protocol processing would have an even greater relative effect on the gateway's performance (since frame relay otherwise minimizes processing in intermediate systems) and would physically split the security protocol from the transport layer in end systems, the place where error recovery is intended.

Where the TE is in fact a "dumb" terminal, with no Transport layer, then the confidentiality service is logically a Network layer protocol in a Packet Assembler/Disassembler (PAD) or a gateway. It is probably meaningless to discuss SP4 or end to end encryption for devices which are not end systems. Such terminals are very common in existing systems, and secure X.25 gateways, using SP3 equivalent protocols are available for both commercial and classified use. In the near term, such devices Network layer security may be the only commercially available solution.

5.1.2 ISDN-Specific Security Protocols

Security protocols are possible at every layer of the OSI reference model. Some applications, such as X.400 MHS will incorporate security, including encryption, in the application itself. This will provide consistent security for a service which may be accessed through many networks, including ISDN. Selective field confidentiality may eventually be provided in Presentation layer protocols. At the Transport layer and the upper part of the Network layer the SP3 and SP4 protocols, discussed in section 5.1.1 above, should provide a foundation for building OSI security protocols.

When appropriate higher layer OSI security protocols are used, there may be no need for ISDN specific security protocols, except to provide traffic flow confidentiality, if needed. However many ISDN applications, such as voice or video are not served by OSI protocols. Much non-OSI data traffic will also be carried by the ISDN public network. In these cases appropriate ISDN security protocols can provide needed security.

In this section the various locations at which ISDN specific security protocols may be located and the consequences for encryption, confidentiality and integrity are considered. Figure 18 illustrates potential locations for ISDN-specific security protocols. In figure 18 each of the potential ISDN protocols is identified by a name, ISPnx, where n is number of the OSI layer to which the protocol belongs, x is either “X”, “B” or “D” signifying an X.25 specific protocol or a B channel D channel protocol.

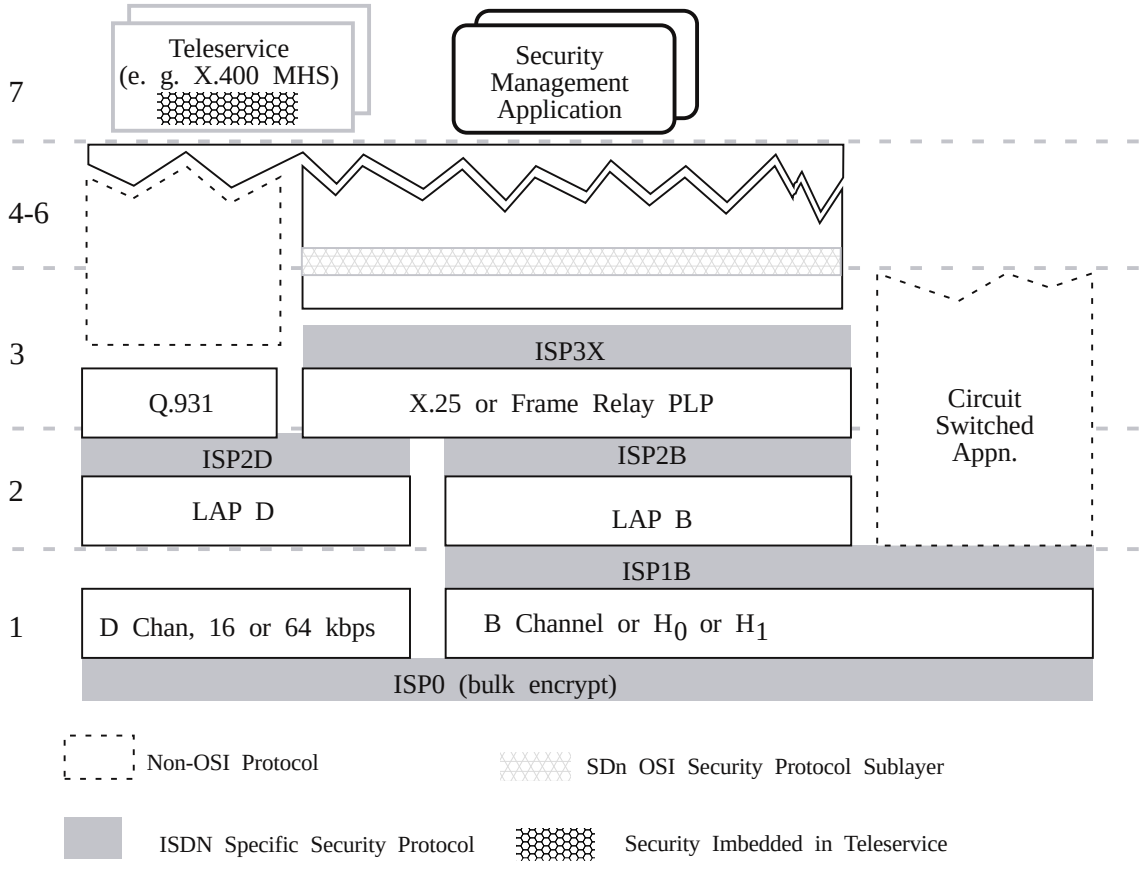

Figure 18 - Potential ISDN-Specific Security Protocols.

Figure 19 shows a block diagram of a secure ISDN voice-data terminal, showing where each of the protocols would be implemented in a terminal. Figure 20 provides a block diagram illustrating where each of the protocols which are appropriate to an ISDN switch or packet handler, would be implemented.

The ISP3X protocol would be a gateway-to-gateway protocol, specific to X.25 (or, potentially, Frame Relay). Although it would provide confidentiality and authentication services, its main purpose would be to provide connection integrity from X.25 gateway or terminal to X.25 gateway or terminal, independently of any higher layer. The protocol would be used to provide security over a black X.25 network as shown in figure 17 above. Existing secure X.25 devices now implement such protocols. While there would be little reason for the ISP3X protocol if all traffic used appropriate SP3 or SP4 protocols, the ISP3X protocol does implement consistent security in a heterogeneous protocol environment, with no constraint on the higher layer protocols.

The ISP2B and ISP2D protocols would be immediately above either the LAPB or LAPD link layer protocols. They are link layer protocols and therefore must be implemented on line cards in switches (ISP2B) or packet handlers (ISP2D). When the D channel is used for B channel call setup, the ISP2B protocol would provide destination address traffic flow confidentiality. An intruder monitoring the U interface would know that a call had been made, but not its destination. While the substitution of a line card with a security function seems straightforward, key management might prove to be quite difficult with existing switches. It might, however, be possible to devise an autonomous key management scheme, which confined the problem to the line card and TE, and did not involve the normal switch management functions. This would permit the substitution of secure line cards in switches not intended to provide this level of security.

The ISP2B protocol would be implemented in packet handlers. Its use is illustrated in figure 21 and its major advantage would be to provide traffic flow confidentiality; the X.25 Call Request, Incoming Call and other X.25 control packets which reveal DTE addresses would be protected. Connectionless integrity and confidentiality would be provided between the DTE and the packet handler. When X.25 is used directly from DTE to DTE, through a switched B channel, then the ISP2B protocol would provide DTE to DTE confidentiality, but ISP2D would be needed to provide destination address confidentiality. The overhead of security headers and trailers with the relatively small packets allowed by the LAPB protocol would be a practical problem, and some modifications to LAPB, to allow larger packets, might be required to maintain the payload expected by X.25.

The ISP1B protocol would sit atop the B channel and encrypt the entire 64 kbps bit stream. Similar protocols could apply to the H_0 or H_1 rate services when they are available. The protocol would begin with an authentication (possibly using the D channel User-to-User signaling special service during call setup) and then provide link confidentiality for all bits transmitted. Integrity could not be provided transparently (*i. e.*, without reducing the data rate), however most higher layer protocols provide integrity checks, which when combined with confidentiality, would make it difficult or impossible to alter or replay packets. Partial traffic flow confidentiality would be provided, because an intruder monitoring the B channel would not be able to determine how many packets were being sent, nor their size. Addresses contained in B channel packets (such as those in X.25 Call Request packets) would be concealed. However, unless the D channel were protected, the destination and duration of B channel calls could be determined by an intruder monitoring the D channel.

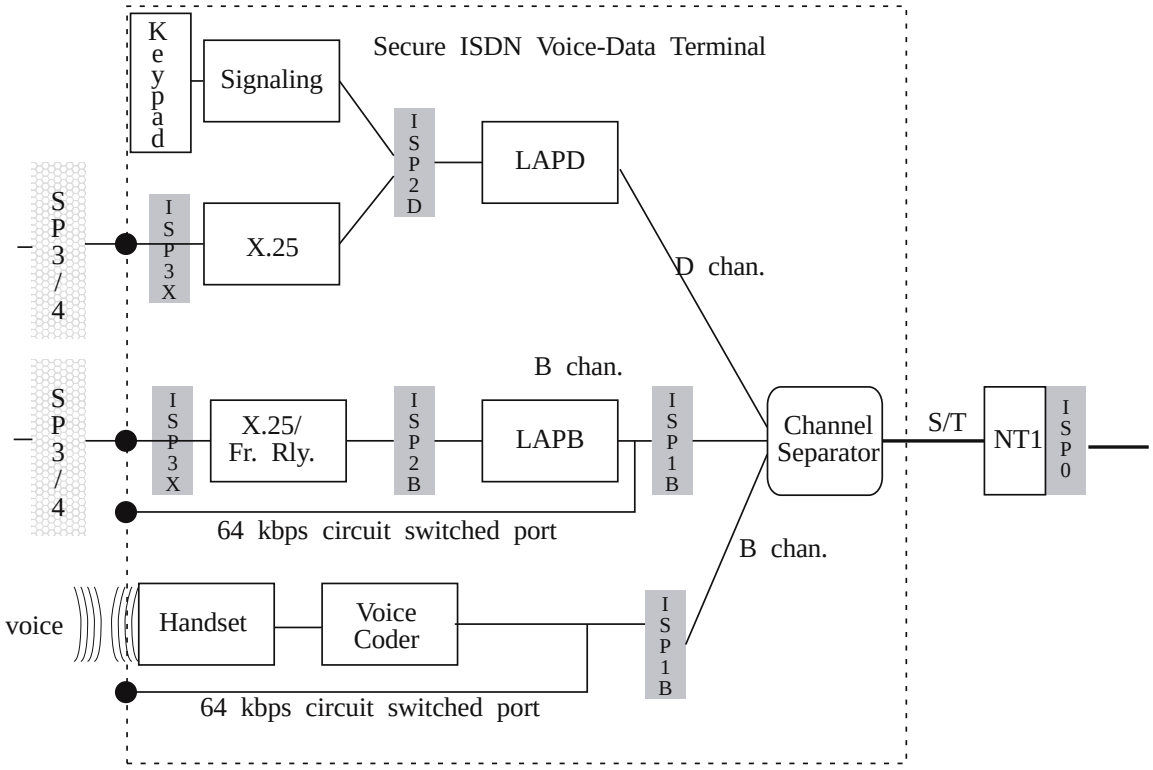

Figure 19 - Secure ISDN Terminal Block Diagram.

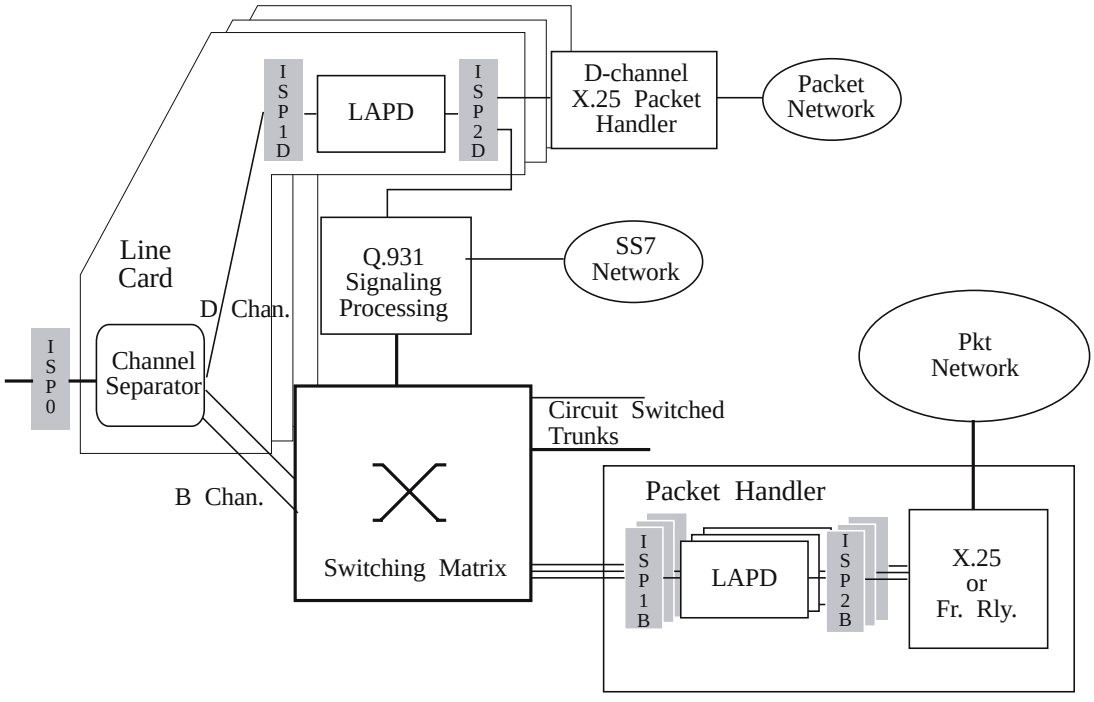

Figure 20 - Secure ISDN Switch Block Diagram.

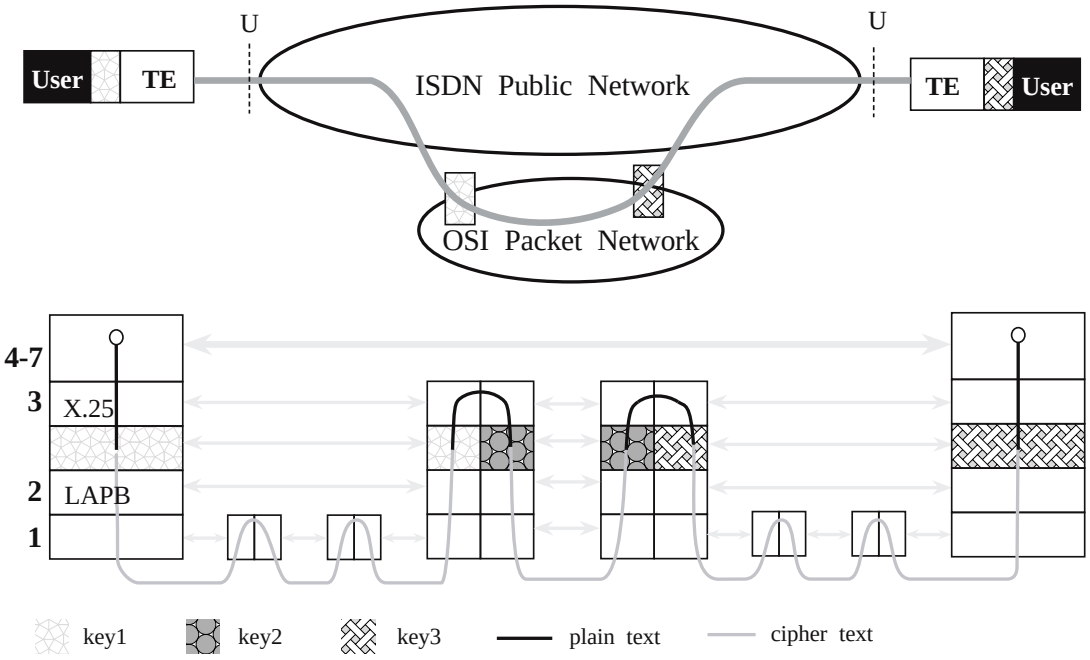

Figure 21 - Data Link Layer Packet Encryption.

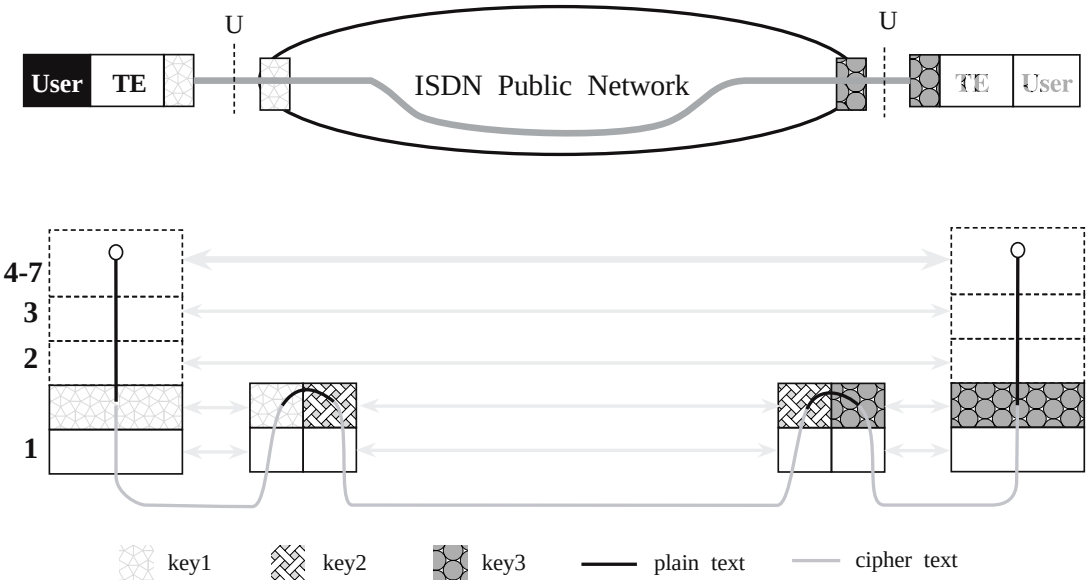

Figure 22 - TE to Network Physical Layer Encryption.

Unlike higher layer protocols, which apply only to packet traffic, the ISP1B protocol would protect any use of the B channel, including voice, video and packet services. Figure 22 illustrates the use of the protocol to protect the B channel between the TE and switch. This would simplify key management in the terminal, but would require a red switch and network. Special, secure ISDN networks, with secure switches, and secure trunks between switches, may be practical for special applications, but would not be practical in the context of the public ISDN network.

However, the encryption need not stop at the network switch. TE-to-TE encryption, as illustrated in figure 23 is transparent to the network, and could be used between any two suitably equipped terminals, provided a 64 kbps unrestricted digital channel is available between them. A companion packet application protocol, possibly using the D channel during call set-up, is necessary for key management and authentication, to initialize the secure link.

Symmetry would indicate that if there might be an ISP1B protocol, atop the B channel, then there might also be a similar ISP1D protocol. Such a protocol does not appear to be practical, however, because it would confound the contention mechanism used to share the D channel on a passive bus. If complete B channel traffic flow confidentiality is required, this can be provided by the combination of the ISP2D and the ISP1B protocols.

Finally, ISP0 encryption at the bottom of the Physical layer is also possible, as illustrated in figure 24. In this case both B channels, the D channels and the associated framing, balance and control bits would all be encrypted in one 192 kbps stream. Encryption at this layer could not be end-to-end since the encrypted signal could not cross the NT1. In effect, the cryptographic device would be inserted in the NT1 device and in front of the line card (see figs. 19 and 20) in the local office switch. This would have the advantage of denying an intruder between the NT1 and the switch any traffic flow information. It would be practical on a limited scale and would completely protect a user's confidentiality where it is most vulnerable, on his line between his premises and the telephone local office. With optical-fiber links there are non-cryptographic means of protecting confidentiality at this layer as well.

5.2 Physical Layer Encryption Considerations

Physical layer or link encryption provides the most general encryption facility available to ISDN. It works with any B channel application, including voice. An intruder learns nothing by observing a B channel with Physical layer link encryption. It can operate between a TE and a gateway to a secure ISDN network, between a TE and a secure specialized service provider, or between any two TEs. There is an immediate need for a direct TE-to-TE B channel physical encryption standard, and the remainder of this section will outline the requirements for such a standard.

The first requirement for such a standard is that it supports a variety of encryption algorithms. This requirement is common to encryption at all layers. A second requirement is that the encryption should not constrain or limit the use of the B-channel. That is, the B channel should remain an isochronous byte aligned 64 kbps pipe, with no (or at least very little) further limitations, except during the period required to initialize encryption on the link and except for the effects of noise.

Noise and synchronization provide special problems for encrypted links. They will be discussed here in terms of the Data Encryption Standard (DES); similar considerations apply to other algorithms. The DES algorithm is a symmetric key algorithm which uses a 56-bit key which is expanded with 8 parity bits to 64 bits. It operates on a 64 bit input block, producing an

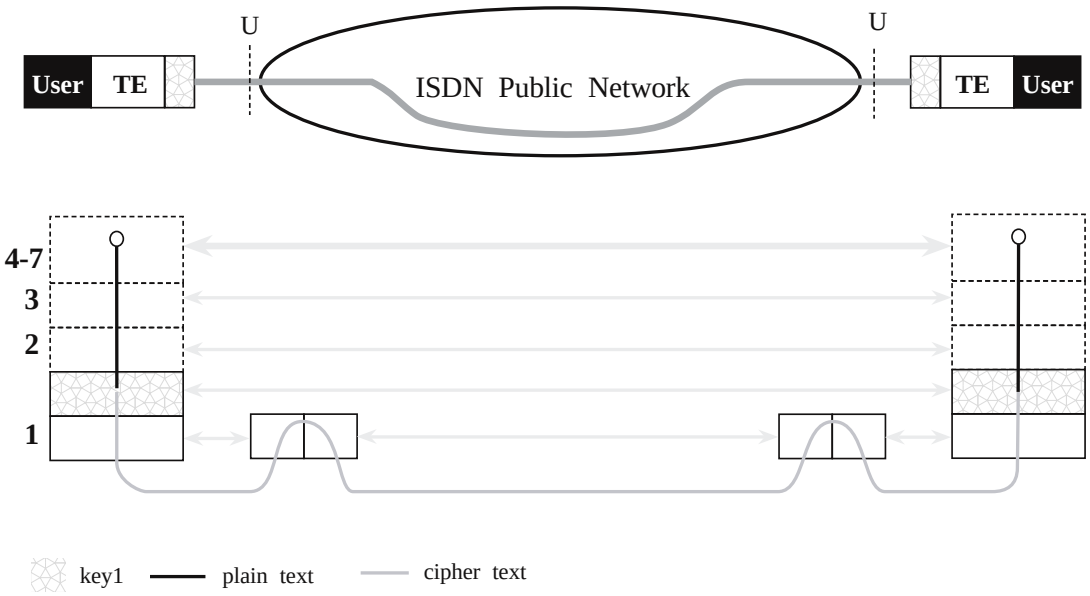

Figure 23 - TE to TE Physical Layer Encryption.

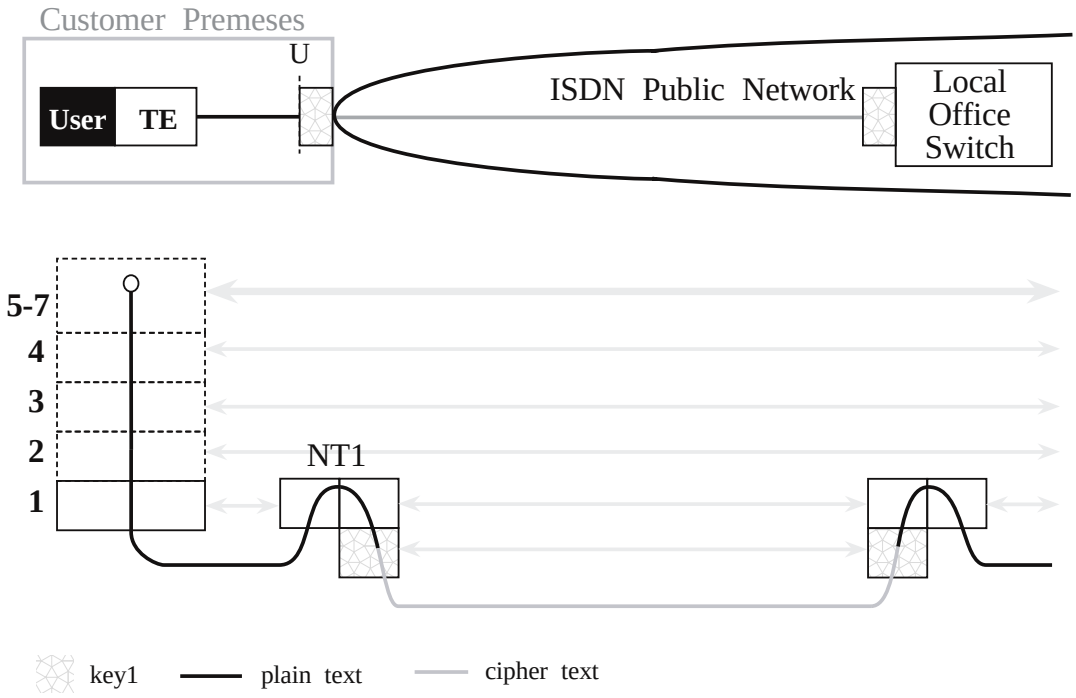

Figure 24 - NT1 to Local Office Link Encryption.

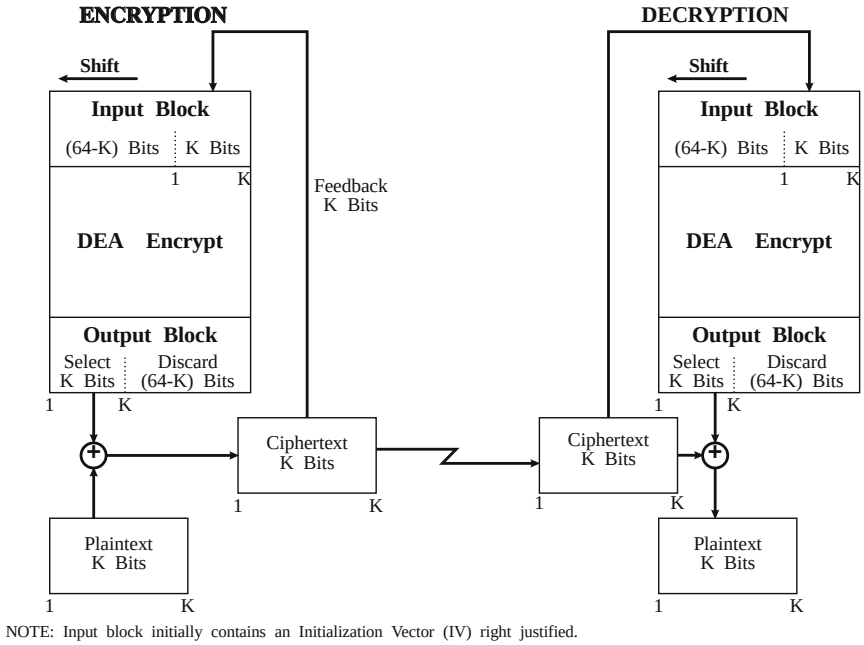

Figure 25 - DES K-bit Cipher Feedback (CFB) Mode .

encrypted 64 bit cipher text output. When the cipher text is used as input with the same key, the output is plaintext.

Four different modes of operation have been defined [FIPS 81]. Two are block oriented, and two operate on arbitrary bit streams. Because they would impose a block structure on the B channel, the block structured modes will not be considered here.

The *Cipher Feedback (CFB)* mode is illustrated in figure 25. In this case the DES algorithm is used as a random number generator. At both the transmitter and receiver the generator is seeded with a 64-bit Initialization Vector (IV) and a secret 56-bit key. If identical IVs are not used, only the first 64-bits transmitted are affected. The key and IV are used to generate a pseudo-random number, from which K-bits are selected and exclusive-ored with K-bits of the plaintext. At the destination K-bits of cipher text are shifted into the DES input, and the received cipher text is exclusive ored with the DES output to recover the plaintext.

The advantage of CFB mode is that it is self synchronizing. Within 64 bits of the loss of synchronism it is recovered automatically. The disadvantage is that a single bit error expands to a block of 64 bits. Long block errors are potentially serious. The 16-bit Frame Check Sequence (FCS) used with LAPB will detect any single or double bit error in a frame, however it is not guaranteed to detect error bursts longer than 16 bits.* There will be approximately one chance

---

* CCITT also defines a 32-bit FCS, which would reduce the probability of falsely accepting a packet with a long error burst to one in 2^{32}, for most purposes a negligibly small number. The CRC-32 widely used in LANs, which allow longer packets, increasing the probability of two random errors in the same packet. LAPB is limited to an information field of only 260 bytes, and the CRC-16 is used with both LAPB and LAPD.

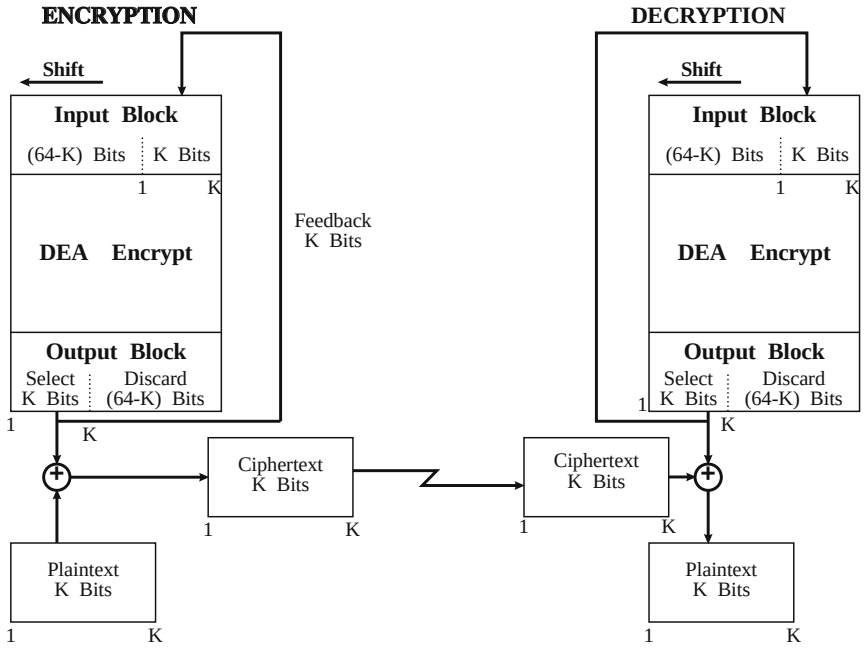

Figure 26 - DES K-bit Output Feedback (OFB) Mode.

in 2^{16} of a 64 bit error burst not being detected by the FCS. The nominal ISDN B channel bit error rate is 10^{-7}. At this rate, with 2,000 bit packets, about 3 packets in 10^{9} transmitted packets will falsely pass the FCS check.

Forward error correction could be applied to the ciphertext to single bit errors at the expense of some channel bandwidth. Error correction applied to the plaintext would have to be capable of correcting 64-bit bursts, a formidable requirement.

The *Output Feedback (OFB)*, illustrated in figure 26, is similar, except that it is the output of the DES that is fed back rather than the cipher text. Now there effectively are two free running (in the sense of the transmitted cipher text) pseudorandom number generators, whose outputs are exclusive-ored with the plaintext to create the cipher text and exclusive-ored with the cipher text to recover the plaintext. Transmission bit errors are not expanded, but synchronism becomes the problem. Both DES algorithms must be seeded with the same IV and key, must start in synchronism, must maintain synchronism and must recognize the loss of synchronism and recover from it. Since ISDN provides a byte synchronized service, bit errors do not affect synchronism.

With ISDN B channels, OFB synchronism, once achieved, is normally easily maintained, however "byte slips," which may normally occur on an ISDN circuit within the continental United States on the order is once a day, will cause the loss of synchronism. It is therefore necessary to recognize loss of synchronism and resynchronize the encryption. Recognizing the loss of synch is a higher layer problem; at the physical layer there is no way for the receiver to know that an encrypted data stream is corrupted. Cryptographic Synchronism must be achieved in band in the B channel, since the D channel is not itself synchronized with the B channel across the network.

A TE, having detected the loss of cryptographic synchronism must also notify the other terminal, to begin resynchronizing. This can be done with a normal ISDN disconnect, or, perhaps less traumatically, with a special escape sequence. Any escape sequence violates transparency, but a

particular cipher text string of, for example, 1000 consecutive zeroes, is so unlikely to occur as to be a vary small compromise of transparency.

In general, other symmetric key algorithms will have similar cipher feedback or output feedback modes. Cipher feedback provides automatic cryptographic resynchronization but magnifies the effects of bit errors. Output feedback does not resynchronize automatically, but also does not magnify bit errors.

At the nominal worst case ISDN bit error rate of 10^{-7}, a bit error will occur on average every 156 seconds, or 552.96 times a day.* With a voice service the effect of the magnified bit error is a more audible noise burst, probably perceived as a click or a pop. With a packet data service, approximately the same number of packets are damaged with CFB or OFB, since a 1-bit error damages the packets also, and no forward error correcting code is used with LAPB or LAPD. In a few cases, the expanded 64-bit burst may span two packets, slightly increasing the CFB mode packet error rate. The primary adverse effect on packet data will be an increase in damaged packets falsely accepted by LAPB as good.

5.3 Security Applications for ISDN

While security protocols implement security services at layers 1 through 6, they require a number of layer 7 applications for their operation. An example is key management. Other ISDN security applications may provide services directly to users rather than to lower layer protocols. An example would be a notarization application, which provides non-repudiation services to users.

Security applications may require a trusted third party, for example a certification authority or a notary. Where a trusted third party is required, that service may be provided either by the public network, or an independent *Specialized Service Provider* connected to the public network. Specialized Service Providers connect to the public network and provide a variety of information services, such as Message Handling Services. In this report a trusted third party provider of security services is called a *Specialized Security Application (SSA)*, as shown in figure 13 above. The SSA may be provided by the public network service provider, or it may be provided by some independent Specialized Service Provider. In some cases, applications such as the Directory may provide security services (*i. e.*, access to certificates containing public keys), with other non-security services.

Not all security applications require an SSA. Some may be implemented entirely as distributed peer-peer application protocols. Many security applications would not be ISDN-specific, and standards for them might be adopted from OSI security. Possible security applications include:

- *Key Management.* It is likely that key management will be implemented in whole or in part in the Directory. The Directory may contain certificates stating a users public key. Such keys would be used for authentication and validate signatures. It is possible that session keys for confidentiality might be agreed to by the source and destina-

---

* Bit error rate is meaningful only for random, uncorrelated errors, for example where shot and thermal noise in the receiver are the source of errors. Although too simple a metric to fully describe the noise characteristics of many real transmission systems, bit error rate is the usual metric for comparing the quality of transmission links, and is the only measure of digital link quality for which figures are generally given. Most of the nominal 10^{-7} ISDN bit error rate is attributed to the local loop. Where local loops are short, error rates should be significantly better.

tion using a public key algorithm and then discarded; it is not clear that any centralized key management SSA would be necessary for this.

– *Certification.* A trusted certification SSA might provide Privilege Attribute Certificates (PACs), containing the security attributes of users, or might verify the security attributes of users. The attributes then would be used in accordance with local security policy to make access control decisions.

– *Notarization.* A notarization application would provide non-repudiation services. In some cases the application might be fully distributed; this would generally require the explicit cooperation of both parties to the notarized communication. A trusted notarization SSA might be required to prevent repudiation of voice or video communication, or to assume the role of a process server, in the case of an uncooperative recipient of a message. A notarization SSA might also assume the role of a registered letter in proving that a good faith attempt was made to send a particular communication, even if its receipt is not acknowledged.

– *Secure Conferencing.* A secure conferencing application for voice or video would probably require a secure conference bridge.

– *Secure Mail.* Security provisions are being incorporated into the X.400 MHS. An analogous secure voice mail application would provide secure voice terminal users with similar voice messaging capabilities.

– *Secure Conversion.* A large number of secure analog telephone devices now exist. A secure conversion SSA would be a trusted party to perform conversion between secure analog and secure digital voice.