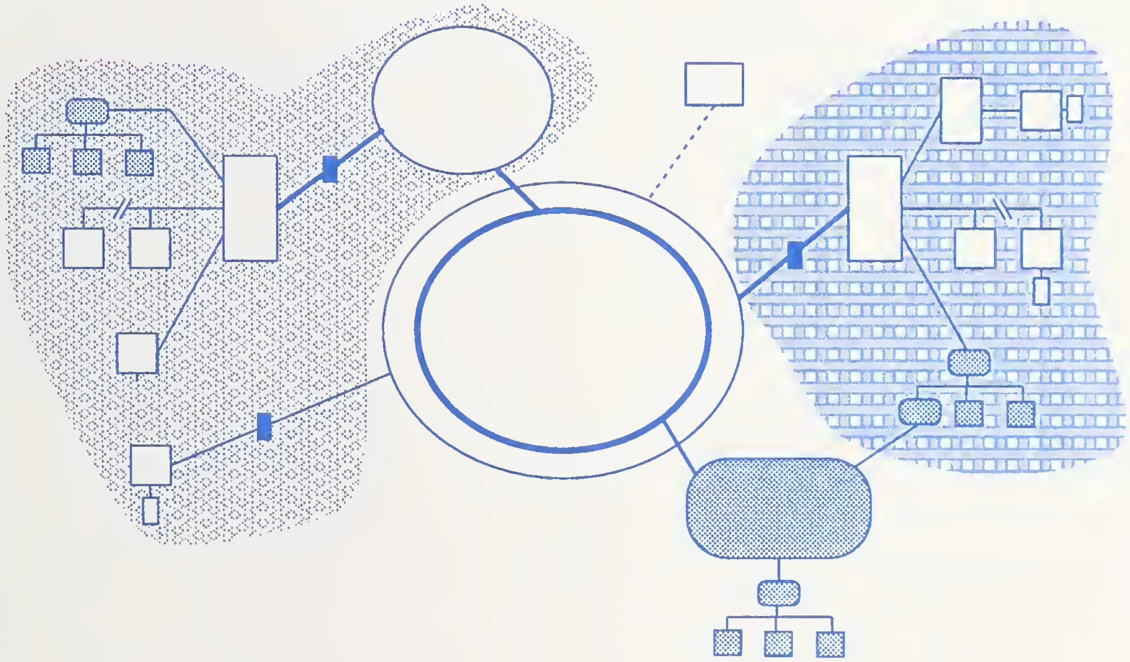
NIST Special Publication 500-189

Computer
Systems
Technology

U.S. DEPARTMENT OF
COMMERCE
National Institute of
Standards and
Technology

Security in ISDN

William E. Burr



NIST Special Publication 500-189

Security in ISDN

William E. Burr

Computer Systems Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899

September 1991

U.S. DEPARTMENT OF COMMERCE
Robert A. Mosbacher, Secretary

NATIONAL INSTITUTE OF STANDARDS
AND TECHNOLOGY
John W. Lyons, Director

Reports on Computer Systems Technology

The National Institute of Standards and Technology (NIST) has a unique responsibility for computer systems technology within the Federal government. NIST's Computer Systems Laboratory (CSL) develops standards and guidelines, provides technical assistance, and conducts research for computers and related telecommunications systems to achieve more effective utilization of Federal information technology resources. CSL's responsibilities include development of technical, management, physical, and administrative standards and guidelines for the cost-effective security and privacy of sensitive unclassified information processed in Federal computers. CSL assists agencies in developing security plans and in improving computer security awareness training. This Special Publication 500 series reports CSL research and guidelines to Federal agencies as well as to organizations in industry, government, and academia.

National Institute of Standards and Technology Special Publication 500-189
Natl. Inst. Stand. Technol. Spec. Publ. 500-189, 76 pages (Sept. 1991)
CODEN: NSPUE2

U.S. GOVERNMENT PRINTING OFFICE
WASHINGTON: 1991

For sale by the Superintendent of Documents, U.S. Government Printing Office, Washington, DC 20402

Table of Contents

ABSTRACT: The Integrated Services Digital Network (ISDN) standards will provide worldwide digital communications service and will play a key role in the transition to electronic documents and business transactions. ISDN has been developed with little thought to security. ISDN security will become a pressing concern for both government and business. ISDN's digital nature facilitates adding security, but the deployment of ISDN in the public network is well under way and the present investment in ISDN equipment, as well as the commercial necesity to deploy ISDN in a timely manner, constrains how security features may be added. ISDN security standards should take advantage of, and be compatible with, emerging standards for Open System Interconnection (OSI) security. International Standard 7498-2 defines five security services for OSI: Confidentiality, Access Control, Authentication, Data Integrity and Non-repudiation. The challenge of ISDN security is to extend these concepts to all ISDN applications, including voice use of the public network. Terminal-to-terminal link encryption provides a powerful ISDN security mechanism, because of ISDN's ability to provide circuit switched connections throughout the world. A standard for the reliable authentication of human users is badly needed for ISDN security.

KEYWORDS: authentication, encryption, ISDN security, link encryption, network security, OSI security, public network security.

The technical efforts documented within this Special Publication were conducted under the auspices of the Integrated OSI, ISDN, and Security Program of the Computer Systems Laboratory at the National Institute of Standards and Technology.

1. Introduction

The *Integrated Services Digital Network (ISDN)* standard will largely govern the operation of the world's public networks in the coming decades. The ISDN provides digital-circuit switched voice and data services, as well as packet-switched data services to users. In addition to end-to-end digital services, ISDN supports interworking with existing analog voice circuits and equipment. Although the provisioning of digital switching capability in the public network, which can ultimately support the ISDN, is well along, ISDN services are just beginning to become available to users in 1991. Because of the ISDN's importance in future communications, security of the ISDN applications is a significant concern. This report provides a discussion of the standards needed to implement ISDN user security.

The technical efforts leading to this Special Publication were conducted under the auspices of the Integrated OSI, ISDN and Security Program of the Computer Systems Laboratory at the National Institute of Standards and Technology.

1.1 Scope

This paper focuses primarily on security for users of the public ISDN. It considers voice and data security in the general context of communications and open systems security and provides a broad discussion of user security needs and possible solutions. It does not attempt to prescribe specific detailed solutions.

These user needs include:

- protecting information confidentiality,
- identifying the parties in communications (authentication),
- assuring the integrity of communicated information,
- controlling access to network services and customer equipment and data,
- being able to prove to a third party the fact that a communication occurred, the contents of the communication, and the identities of the parties to the communication (non-repudiation).

This report assumes that the public ISDN is largely defined and, although some additions may be possible in the interest of security, the public ISDN switching equipment already designed and installed will not be substantially changed to provide user security. Most needed user security can be provided either in user terminal equipment or by adding supplementary services accessible to users through the network.

One user security need, not treated in detail here, is availability of service. Using the technologies and methods discussed in this report users can protect themselves from most security threats except for denial of service attacks. The protection of the public network from deliberate or accidental disruption and fraud is a serious problem to users, but it is largely separable and must be addressed by the network service providers. If intruders penetrate the *Operational Support Systems (OSSs)* of the public ISDN, which manage and maintain the network, they can potentially intercept, divert or prevent user communications. With appropriate security procedures, users can prevent compromises of the confidentiality of their data, and detect impersonations, if the public ISDN OSSs are penetrated, but they cannot prevent denial of service. Attacks on the OSSs could also reveal customer service records and traffic flow information. There are now no standards for OSSs, however efforts have begun to standardize a user network management interface. The security of OSSs is an important concern of ISDN users. However, it is not clear that the needed security provisions should be the subject of public standards and the responsibility for this rests primarily with the network service providers. It is not a subject of this report.

Some view ISDN as strictly a lower-layer communication service, without concern for the applications it carries. This is not entirely satisfying from a security perspective. On the other hand, the set of applications which may be supported by ISDN is nearly unbounded; it will be difficult to provide for the specific security needs of all applications carried over ISDN, as an integral feature of the network. For example, ISDN cannot in itself satisfy the security requirements of an application such as electronic mail (which will operate over other networks as well as ISDN), but it must provide the necessary security support which this application requires of any network.

The mechanisms needed in ISDN to support user security requirements will be defined. The appropriate location of those mechanisms within the structure of ISDN will be discussed. The relationship of ISDN security with the general concepts of security in *Open Systems* and *Open Systems Interconnection (OSI)* will be considered and this report outlines an approach to ISDN security which is consistent with developing OSI security standards. In many cases the needed services and protocols may be defined in a general manner for all networks; that is, they are not specifically ISDN problems, but more general problems, and may be addressed in a more general context than ISDN standards. It is highly desirable that the ISDN adopt security protocols and services developed for OSI wherever possible, so that information systems security as a whole can be as consistent and simple as possible. Areas where ISDN has unique requirements and where specific ISDN security standards are needed will be identified.

1.2 Need for Security in ISDN

The need for routine security in wide area telecommunications remains largely unsatisfied. Both the present pre-ISDN voice oriented network and the ISDN, which will replace it, make little provision for security. There is no systematic provision for protecting the confidentiality of user communications and, in many cases, it is comparatively easy for intruders to intercept, understand, and alter communications or originate forgeries. The network itself is vulnerable to various types of frauds. Since there is no standard, effective method for the authentication of network users, the network provides an excellent vehicle for allowing the criminal to remain anonymous while committing frauds.

In the past, the public analog telephone network used *in-band signaling* for network control. The tones used by switches to signal other switches could be introduced by users through their telephone instruments. This was widely exploited to defraud network service providers. The public network has now been substantially converted to *out-of-band* signaling between switches, eliminating this opportunity for fraud. The ISDN extends the out-of-band signaling to the local loop and user terminal, through a separate 16 kbps digital *D channel* used for signaling between the terminal and the network.

This itself does not make ISDN public networks secure from fraud. It remains to be seen how vulnerable the ISDN terminal-to-network signaling protocols will prove to be to fraud, when ISDN is widely available to the public. There are no access control, authentication or confidentiality provisions in the ISDN terminal to network signaling protocol. Moreover, users will also be able to obtain X.25 packet services through the D channel. The operational, maintenance and administrative systems of the public network typically use X.25 packet services. If it is possible to penetrate these systems from any D channel via X.25, then the security exposure may be grave.

The need for strong security in telecommunications is becoming urgent as electronic documents replace paper in commercial transactions. Many of the traditional safeguards and practices which applied to paper have not been adequately extended to cover electronic documents. Forgery or alteration of unprotected electronic documents is simple compared to forging or altering paper documents. It is often easier to tap a communications line and intercept all the traffic on that line, than to intercept and read paper mail.

As the public network is converted to the ISDN standards, ISDN will become pervasive and will broadly affect citizens, businesses and government. Ordinary analog voice telephones are now routinely used to check account status, place orders, transfer funds and pay bills. Protection for these transactions is provided only by rudimentary authentication checks such as Personal Identification Numbers or credit card expiration dates. The ISDN will facilitate a great expansion of personal and business transactions over the public network. The potential for electronic fraud and gross intrusions on privacy and confidentiality through the public network will expand correspondingly, unless suitable standards are adopted and pervasively used.

1.3 The Opportunity

The combination of digital communication via ISDN and evolving security technology provide an opportunity for significant improvements in public network security. When ISDN makes ubiquitous digital communication of voice and data a reality, the digital signals can readily be encrypted to maintain confidentiality and integrity of voice, data and image traffic. The inclusion of a packet data facility for signaling will allow fairly basic ISDN voice terminals to implement digital security protocols. Public key cryptography makes key management practical on a large scale, allows electronic signatures that cannot be forged, and provides a means for reliable authentication without shared secret keys.

A foundation of common security standards for ISDN, particularly for authentication, confidentiality and integrity can provide the needed platform upon which the specific security needed by various ISDN applications can be built. Because of its digital nature, ISDN can accommodate this foundation. The needed security technology exists; it remains only to adopt it to ISDN and incorporate it in standards.

Security is not free, but if implemented on a wide scale with suitable standards, the benefits are significant and the cost need not be excessive. If the market is sufficient, then the cost of developing integrated circuit security devices is justified. It remains only to develop and implement the needed standards and to incorporate them in ordinary practice. The availability of pervasive security in the ISDN network would provide a strong incentive for users to convert from analog service to digital service.

1.4 Security Policies and Domains

For effective communications security an explicit and well-defined *security policy* must be enforced. A security policy is, "The set of laws, rules and practices that regulate how an organization manages, protects and distributes sensitive information."[DOD 5200]. A security program includes the set of measures used to implement the policy. Measures to protect data include physical security (*e. g.*, locks, guards and perimeter alarms), procedural security (*e. g.*, separation of duties and authority, review and release procedures, etc.) and cryptography. A *security domain* is a set of users who share the same security policy.

Although it is not normally formalized, each individual or family may be considered a separate security domain having its own security policy. How an individual locks his doors, how he lists his telephone number (is it unlisted? does the listing reveal his sex?), how he answers his door and telephone, how he responds to requests for information and what he considers private are just a few aspects of the informal security policy that each of us individually has.

A security policy covers more than communications security. Data is stored, processed and accessed as well as transported. Communications, however, often involves crossing boundaries between security domains. Each independent company or organization, or each subunit of the same organization may have its own security policy, suited to its needs and capabilities. Any confidential communication between these organizations crosses security domain boundaries. Business and commerce are international. Laws regulating security and privacy vary from state to state and country to country. In some countries the law may forbid sending encrypted data across borders. Security policies must comply with different national laws, subdividing security domains within international business organizations. To meet commercial needs, ISDN security must cross not only security domains but also international borders.

Although the basic cryptographic technology to support secure communications is well known, interworking between separate security domains remains a difficult problem. ISDN security must support a range of policies suitable for different communities and applications, as well as interworking among them.

Many significant social policy concerns can be viewed as security domain interworking problems. Consider, for example, credit records. They are compiled by one party but are properly confidential to the subject of those records. In most circumstances they should be released only to parties specifically authorized by the subject. Those parties must also maintain the confidentiality of the records. The addition of data from unreliable sources to credit records and particularly the deliberate addition of false credit reports must be prevented.

Similar issues attend many financial, medical and criminal justice records. The confidentiality and use of records are now the subject of legislation and will receive more legislative attention.

Today individuals are increasingly mobile, often moving to pursue their careers. The use of cash for large transactions, or simply to rent a car or buy an airline ticket, is considered unusual at best and possibly a sign of criminal activity. On the basis of the possession of plastic credit cards merchants broadly extend credit to complete strangers with no authentication of personal identity. A large catalog industry now takes orders primarily over the telephone, shipping merchandise, often within 24 hours, on the basis of a credit card number given over the telephone. A good credit rating and possession of credit cards are necessities of modern everyday life.

The public network is the main carrier by which these sensitive records are gathered and accessed. It must support users with a great variety of security policies. The problem is compounded by the successive chain of domains which is involved. By itself, ISDN cannot solve the crossdomain interworking, a problem which is general to all communications systems, but it must support some of the basic mechanisms required to provide secure interworking between domains. The problem is central to the fabric of modern society, and is as much a social policy issue as a security issue.

1.5 Federal Role in ISDN Security

In the United States, the *National Security Agency (NSA)* is charged by law with protecting classified data. The security resources and expertise of NSA are unrivaled. The *National Institute of Standards and Technology (NIST*) has responsibilities for the security of unclassified information. Under PL 100-235, The Computer Security Act of 1987, NIST is assigned the, "responsibility for developing standards and guidelines needed to assure the cost-effective security and privacy of sensitive information in federal computer systems drawing on the technical advice and assistance of the National Security Agency,"...

NIST participates in voluntary security standards efforts. The Federal Information Processing Standards (FIPS) and Guidelines developed by NIST are used by federal agencies, by state and local governments and by private industry to protect sensitive information. The best known of the security FIPS is FIPS PUB 46-1 *Data Encryption Standard (DES).* The DES defines a symmetric-key encryption algorithm that is widely implemented in commercially available products. In addition to its use by Federal agencies, the DES is widely used by business, particularly in banking and other financial applications.

NIST works with industry to develop security standards that are broadly acceptable and meet the needs of both industry and government. In doing this, NIST draws upon the expertise of NSA and attempts to bridge the gap between the world of classified security, where many of the algorithms and security devices are classified and must be themselves protected, and the world of commercial security and standards, where the algorithms are typically known and often published in standards.

If security is to be broadly implemented across independent domains throughout the world, with widely available, inexpensive equipment, then it must use algorithms and protocols known to all. The only secrets will be the sensitive data and a limited number of security parameters (e. g., keys, passwords, etc). The security hardware itself must be sensitive only to the extent that it stores secret security parameters.

Both classified and sensitive but unclassified communications can use the same basic protocols with appropriate specific algorithms for encryption, authentication, access control and the like. This will facilitate the use of commercial networks and communications equipment for national security purposes, providing additional alternatives for classified communications, saving users money and providing additional revenues for commercial carriers and equipment vendors. NSA and NIST are working cooperatively toward this goal. The protocols for ISDN security must therefore support both the open algorithms for commercial security and the more restricted algorithms needed for classified information.

In addition to NSA and NIST, many Federal agencies have a strong interest and role in the general subject of communications security policy. Many agencies maintain large electronic databases of sensitive information that are accessed, collected or distributed electronically. Obvious examples include the Internal Revenue Service and the Social Security Administration. The confidentiality of various official economic estimates must be maintained until they are released. The data upon which they are based may be reported electronically. The integrity of the electronic communications of the Treasury and the Federal Banks are vital. An intrusion into the Air Traffic Control communications system could cause disaster.

Among the most directly affected agencies are law enforcement agencies. They maintain databases of sensitive information, disseminate that information where needed and yet must protect that information from misuse. A great part of law enforcement consists of compiling databases of information and correlating that information to reveal a pattern which indicates an illegal activity. Computers and electronic communications greatly facilitate this, but at the same time raise the specter of infringement of the privacy of the public. Widespread dissemination of security technology may also frustrate law enforcement data gathering. Law enforcement agencies, the Congress and the courts will all deal with the implications of communications security standards and policy.

At least one security relevant feature of ISDN, *Calling Line ID*, (often referred to as *Automatic Number Identification* or *ANI*) is under attack as an invasion of privacy. This issue is discussed in Section 1.6 below. It is likely that Federal action may be required if this feature is to be generally available or differing state restrictions may make it impossible to provide a consistent nationwide network service.

1.6 Privacy and Confidentiality versus Accountability

While the terms *confidentiality* and *privacy* share a common context of secrecy, privacy is used to describe the desire or right to be left alone and not be disturbed. Confidence implies trust and belief, that is, the sharing of secrets. A secret, not shared with another, is private, but not a confidence. In the context of ISDN security, the term confidentiality is used to describe the transmission of information between two or more parties without divulging that information to any unintended parties or intruders. Privacy in ISDN refers to the capture, accumulation and release of information about subscribers, particularly where that information may enable intrusion upon the seclusion of the subscribers, or the use of the network for unwanted intrusion on network subscribers.

Balanced against the legitimate desire of subscribers for confidentiality and privacy is the need to hold them accountable for their use of the ISDN. When subscribers misuse the network, they should be held accountable. If commercial transactions are conducted over the network, rather than with paper, then the parties must be able to hold each other accountable. Achieving accountability, however, is to some extent in conflict with broad constructions of confidentiality and privacy.

Confidentiality involves both the contents of communications and *traffic flow confidentiality* (*i. e.,* protecting the identities of the parties, amount of traffic, length of transmission, *etc*). Confidentiality can be compromised in a number of ways. An intruder may be deliberately intercepting information. Deliberate intrusion may be easy in the case of cellular radio telephony or wireless telephones and local area networks (LANs), but signals can be intercepted by intruders on copper wires, fiber optic cables, and along either terrestrial or satellite microwave links. Confidentiality can also be compromised by crosstalk in the network, although all-digital transmission significantly reduces the likelihood of this.

Intrusions may or may not be illegal, depending upon the circumstances. Federal laws forbid wiretaps on domestic private electronic communications by private parties and by law enforcement or other government agencies, except under limited circumstances as specifically defined by law. Nevertheless, illegal or not, it is usually easy to tap local communications loops.

While confidentiality may be achieved by physically protecting the communications links and, to some degree, by legislation forbidding the interception of communications, the most general and convenient means of ensuring confidentiality are cryptographic techniques. As more and more business transactions take place electronically over ISDN, the use of cryptography to protect the communications of private businesses and individuals will grow.

There are several ISDN privacy concerns. The first involves the Calling Line ID supplementary service. Unlisted subscribers pay to keep their numbers secret to deny others the ability to intrude on their privacy by calling the unlisted number. If every time someone is called from an unlisted number, this number is revealed to the called party, the caller's privacy is allegedly infringed.

Absent legislation forbidding this, Calling Line ID can be used to build the network equivalent of mailing lists, which undoubtedly intrudes upon the privacy of subscribers. The use of police tip lines, whistle blower lines, suicide counseling lines and similar valuable services may be curtailed as the public fears that their anonymity is compromised by Calling Line ID. It is argued that there is an established right to anonymity over the telephone. The reporting of Calling Line ID has been limited in some states by public utility commissions and in other states has been held by courts to be illegal. Some operating companies now offer blocking services which block the Calling Line ID service on selected outgoing calls, while at least one state requires that Calling Line ID be blocked on all calls from unlisted numbers.

While Calling Line ID has legitimate uses, it is objectionable in that it may be automatic. It is dangerous in that it is at best a weak form of authentication. A standard form of strong personal authentication via ISDN terminals might be possible via D-channel user-to-user signaling. A caller could be requested to authenticate by the called party. Such a standard form of voluntary strong authentication, which is discussed further in section 6.4, would solve many security problems and the privacy concerns of Calling Line ID.

By tradition there is also an expectation that telephone conversations are private conversations between two parties, as if those parties were conversing face to face in some isolated location. This makes these conversations private and deniable, in that what was said is the word of one party against another. Recording telephone conversations without advising the other party may violate laws and generally violates normal conventions of privacy.

Another major privacy concern is the observation and accumulation of data about subscribers. Privacy implies freedom from systematic observation, and the systematic recording of personal data. Although each event recorded might be innocuous in itself, and not essentially private, the systematic accumulation and analysis of these events may be regarded in the aggregate as infringing individual privacy. Thus the call detail records legitimately kept by service providers may be held to be confidential between the subscriber and the service provider. Unauthorized release of these records to a third party, even (or perhaps particularly) a law enforcement or security agency, may be considered an intrusion upon privacy.

Detection and recovery from security violations requires the maintenance of security audit information. Without appropriate safeguards such records may be misused, and there is the potential that systematic records of electronic communications kept to detect fraud, intrusion or for other security purposes will be considered to violate the legitimate privacy of innocent users.

As electronic transactions continue to replace paper transactions and, as the power of networks and computers to recognize, store and analyze data increases, these privacy concerns will grow. Any attempt to monitor the public ISDN and collect data to detect fraud, illegal activity or security violations must be conducted with due concern for privacy. When such databases are created, access to them must be strictly controlled, and their use limited to a narrowly defined legitimate purpose.

Both privacy and confidentiality rights must be balanced against the need for accountability and legitimate social, law enforcement and security needs. If Calling Line ID discourages reporting of crimes, it may also discourage harassing calls and false alarms. If it can allow the building of intrusive phone lists, it can also facilitate better customer service. It may even enhance privacy by facilitating the screening of incoming calls. If every state has a different law and policy on this feature, it may become impractical for ISDN service providers to provide it in the cases where it is legal and would be useful.

As it becomes pervasive, cryptographic technology will not only be used to protect legitimate communications, but those of criminals as well. By its very nature large scale organized crime involves extensive communication. The interception of communications by law enforcement agencies is a powerful tool against such criminal organizations. Widely available cryptographic products may render useless approved interception of communications for law enforcement.

When does the systematic monitoring of calls and the recording of the Calling Line ID to detect the penetration attempts of hackers, or other frauds, become an infringement of the privacy rights of all users? What safeguards are required to ensure that it does not? What are private communications and what, if any, private communications should not be lawfully encrypted? Can an individual be compelled to reveal a cryptographic key protecting an encrypted communication that may be incriminating? Do the special privacy privileges of telephone conversations extend to text or facsimile messages delivered over the public ISDN network or to voice mail?

These issues are much broader than just ISDN security; they involve all electronic communications and records and encompass fundamental notions of the privacy and confidentiality rights of citizens. However, the problem is particularly acute with ISDN, because of its roots in the public telephone network and the consequent pervasive involvement in everyday life. These and many other such questions must be answered in the coming years to provide ISDN security which properly balances privacy, confidentiality and accountability concerns.

2. Security Architecture(s) for Open Systems

Two related efforts have set the stage for the development of security standards in Open Systems. The first of these, ISO 7498-2, provides an architecture for security in Open Systems Interconnection, that is communications between open systems. The second, developed by the *European Computer Manufacturers Association (ECMA)*, addresses the somewhat broader scope of overall open systems. Both efforts are essentially architectural and neither have yet resulted in specific final protocol standards.

NSA and NIST, in cooperation with industry, have sponsored the development of the *Secure Data Network System (SDNS)*, a set of protocols which operate in the general framework of Open Systems Interconnection protocol standards. They augment the OSI protocols to provide needed security services, and are expected to provide the basis for specific OSI security protocol standards.

2.1 Open Systems Interconnection (OSI)

A security architecture for OSI and a set of protocols that implements a part of that architecture have been defined. They should serve as the basis for specific International Standard security protocols.

2.1.1 ISO 7498-2, Security Architecture

The one generally accepted standard in security for open systems is ISO 7498-2-1988 *Security Architecture*, Part 2 of ISO 7498, *Open Systems Interconnection - Basic Reference Model.* ISO 7498 provides a reference model for communications between open systems (the well known *OSI Reference Model*) and ISO 7498-2 covers communications security for OSI protocols, but not the more general problem of security in open systems (including processing and storage, etc. as well as communications).

The OSI Reference Model seven layer communications protocol stack is illustrated in figure 1 [OSI 7498]. In the model the protocols are defined on a peer protocol to peer protocol basis. The vertical interfaces between layers are logical service primitives, that are never observed directly; the only external observation possible is of peer entity to peer entity communications.

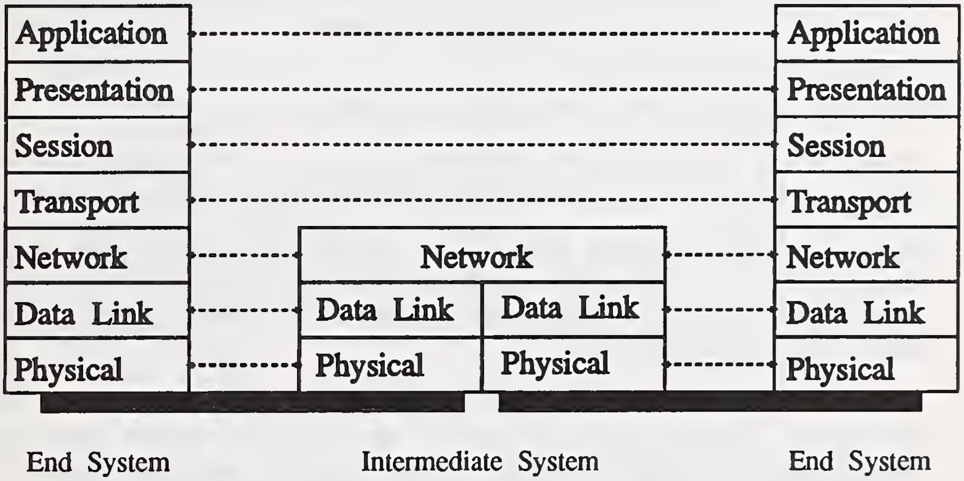


Figure 1 - Open Systems Interconnection Reference Model.

The *Protocol Data Unit (PDU)* of each layer or sub layer is encapsulated in the PDU of the lower layer. That is, when transmitting user data, each layer protocol entity applies a header and trailer to the data delivered by the layer above and may also subdivide the higher PDU into several of its own PDUs. When receiving, each layer strips its headers and trailers and reassembles any subdivided PDUs before passing them up. Layers may be divided into sublayers (this is most common at the lower three layers, which are conventionally divided into a total of as many as seven sublayers), and the sublayers act with peer sublayers similarly to layer protocols. According to 7498-2, the security services which may be provided at each layer are either peer entity to other peer entity at that layer, or refer to the protocol entity immediately above.

ISO 7498-2 defines five basic security services for secure open systems communication. They are:

- *Authentication.* This service basically provides a reliable answer to the question, with whom am I communicating? Authentication services are provided by an (N)-layer entity to the (N+1)-layer entity above it. *Peer entity* authentication, when provided by an (N)-layer entity, corroborates that the remote (N+1)-layer is the claimed entity. *Data origin* authentication is provided by a (N)-layer entity to the (N+1)-layer entity above and corroborates that the source of the data is the claimed peer to the (N+1)-layer entity.
- *Access Control.* This service controls access to the resources which may be accessed via OSI communications as well as to the communications themselves. It relies upon the authentication service to reliably identify the entity seeking access.
- *Data Confidentiality.* This service protects data from unauthorized disclosure. All user data may be protected or fields may be selectively protected. *Traffic flow confidentiality* may also be provided, protecting the information which may be derived from a traffic analysis.
- *Data Integrity.* This service guarantees the integrity of data. It protects against the modification, insertion, deletion or replay of data. The integrity service may provide for recovery from integrity faults, or it may simply detect them. It may protect all data or only selected fields.
- *Non-repudiation.* This service prevents the parties to a communication from denying that they sent or received it, or disputing its contents. It may provide either *proof of origin* or *proof of delivery.*

To implement the services, ISO 7498-2 defines eight mechanisms. They are:

- *Encipherment.* This refers to cryptographic technology. Two classes of encipherment are defined, *symmetric* (*i. e.,* secret key), and *Asymmetric* (*i. e.,* public key).
- *Digital Signature.* A digital signature can only be produced using the private information of the signer. Therefore it can be proven that only the holder of that private information could have originated the signature. Asymmetric key encipherment is used to produce the signature.
- *Access Control.* Access control mechanisms control access of authenticated entities to resources. They may be based upon access control information bases, authentication information, capabilities, security labels, the time of attempted access, the rout of attempted access, and the duration of access.
- *Data Integrity* Data Integrity is broken into the integrity of a single PDU (*connectionless integrity*) and of the sequence of PDUs (*connection integrity*). The usual

Service	Level						
	Physical	Data Link	Network	Transport	Session	Presentation	Application
Authentication							
Peer Entity			★	★		★	★
Data Origin			★	★		★	★
Access Control			★	★			★
Confidentiality							
Connection	★	★	★	★		○	★
Conectionless		★	★	★		○	★
Selective Field						○	★
Traffic Flow	★		★			★	★
Data Integrity							
Connection with Recovery				★		★	★
Connection without Recovery			★	★		★	★
Selective Field Connection						★	★
Connectionless			★	★		★	★
Selective Field Connectionless						★	★
Non-repudiation							
Proof of Origin						★	★
Proof of Delivery						★	★

★ Service *may* be provided

○ Service *will* be provided

(a) Security Services by OSI Level

Service	Mechanism							
	Encipherment	Digital Signature	Access Control	Data Integrity	Authentication Exchange	Traffic Padding	Routing Control	Notarization
Authentication								
Peer Entity	★	★			★			
Data Origin	★	★						
Access Control			★					
Confidentiality								
Connection	★						★	
Conectionless	★						★	
Selective Field	★							
Traffic Flow	★					★	★	
Data Integrity								
Connection with Recovery	★			★				
Connection without Recovery	★			★				
Selective Field Connection	★			★				
Connectionless	★	★		★				
Selective Field Connectionless	★	★		★				
Non-repudiation								
Proof of Origin		★		★				★
Proof of Delivery		★		★				★

(b) OSI Security Services & Mechanisms

Figure 2 - Security Services, OSI Levels and Mechanisms.

means of ensuring the integrity of a single PDU is a checkvalue which is a function of all the data in the PDU. The checkvalue may then be enciphered to prevent its alteration. The sequence of PDUs may be ensured by sequence numbering, time stamping or cryptographic chaining.

- *Authentication Exchange.* This is used to authenticate protocol entities. Passwords and cryptographic techniques, with suitable handshakes provide either unilateral or mutual authentication.
- *Traffic Padding.* Observation of traffic patterns, even when enciphered, may yield information to an intruder. This mechanism may be used to confound the analysis of traffic patterns.
- *Routing Control.* Routes can be chosen so as to use only secure links.
- *Notarization.* This mechanism is used to assure that communications cannot be repudiated.

ISO 7498-2 defines the appropriate protocol layers for each security service and the mechanisms which may be used to implement them. Figure 2(a) illustrates the assignment of services to layers while figure 2(3) shows the mechanisms used by each service.

2.1.2 Secure Data Network System (SDNS)

SDNS provides an architecture and several protocols which are overlayed on the OSI communications protocol stack. The SDNS protocols all work in a somewhat similar fashion by encapsulating *Protocol Data Units (PDUs)* in a "security envelope" as illustrated in figure 3. A protected header for the protocol is appended in front of the PDU. The protected header optionally contains security labels, sequence numbers, NSAP addresses, or CLNP headers, depending upon the specific protocol. An Integrity Check Value (ICV) is computed from the protected header and the PDU and added behind the PDU. The PDU, the protected header and the ICV are optionally encrypted. A clear header is then appended in front of the protected header. The primary function of the clear header is to identify the key used.

SDNS defines two somewhat similar protocols, one, *Security Protocol 4 (SP4)* [SDN.401], at the bottom of the Transport Layer and the other, *Security Protocol 3 (SP3)* [SDN.301], at the top of the Network Layer. Two variants of SP4 and four variants of SP3 are defined as summarized in table 1.

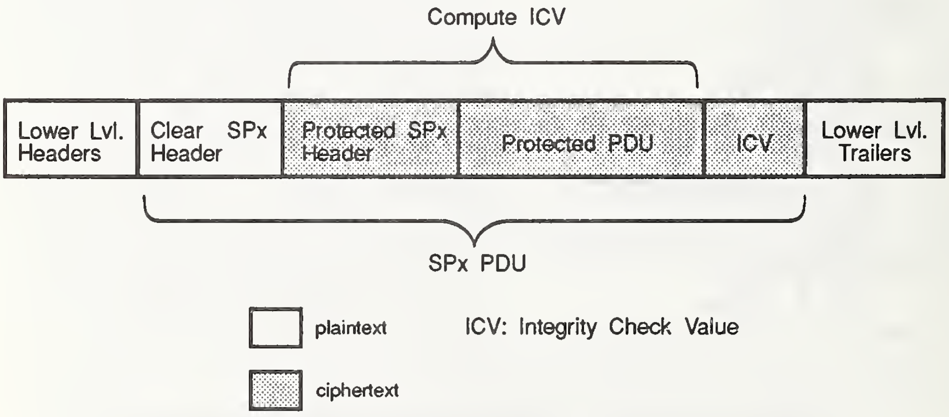


Figure 3 - SP3 and SP4 Security Encapsulation.

SP4 implements two modes, while SP3 implements four. Each mode logically fits into the OSI protocol stack in a somewhat different position. Figure 4 attempts to distinguish each of the modes by their location in the OSI protocol stack. By definition a layer 4 protocol operates from end system to end system. SP4C is a sublayer near the bottom of the transport layer. A separate security association with a separate key is formed for each transport connection, even when the transport connections are between the same transport entities., facilitating multilevel security.

SP4E and SP3N are between the transport and network layers. They are simple protocols and could be applied between almost any network and transport layer protocols, however they depend for connection integrity upon the services of the transport layer above them. When TP4 is used above SP3E, then the integrity of the TP4 protocol fields are protected, and, since TP4 provides connection error detection and recovery, the combination prevents most replay, deletion and insertion attacks. All connections between the same pair of end systems are protected by the same keys.

SP3A, SP3I and SP3D may operate from end system to end system, end system to intermediate system or intermediate system to intermediate system. SP3A is at the very top of the network layer. It includes source and destination NSAP addresses in the protected header. SP3I lies

Table 1 - SP3 and SP4 Protocols

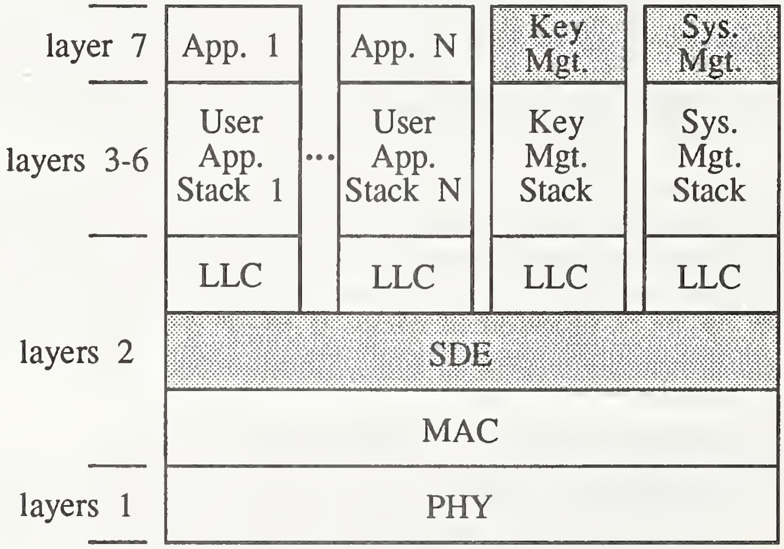
Protocol	Description
SP4C	Provides connection oriented security services with a key per transport connection. Is closely integrated with the ISO 8073 connection oriented Transport protocol. Includes full connection integrity and prevents modification, replay, insertion and deletions. Confidentiality and security labels are optional.
SP4E	Provides connectionless security services with a key per transport entity pair. Supports connectionless integrity and prevents modification of Transport Protocol Data Units. Security labels and confidentiality are optional. Provides a simple encapsulation of Transport PDUs; any protection against replay, insertion and deletion depends upon services of the Transport layer above.
SP3N	Used only in end systems and is identical to SP4E.
SP3A	Provides connectionless integrity, optional user data confidentiality, and optional security labels. Protects end system OSI *Network Service Access Point (NSAP)* addresses in the secure header. Encapsulates complete *Network Service Data Units (NSDUs)*. Used in end systems or intermediate systems.
SP3I	Services similar to SP3A but Protects *Connectionless Network Protocol (CLNP)* headers in the secure header. Encapsulates entire NSDUs or fragments.
SP3D	Similar to SP3I except that DoD IP formats and rules are used.

below the CLNP network sublayer, and includes the CLNP header in the protected header. SP3D is similar to SP3I except that it lies below the DoD IP protocol.

An Access Control Specification and a Key Management protocol are also under development for SDNS as application processes. The Key Management protocol can provide key management for cryptography in SP3 and SP4.

Either SP3 or SP4 may be applied to communications which use ISDN, however even SP3 is above the highest layer that is ordinarily considered an integral part of the ISDN, the *X.25* [ISO 8208, CCITT recommendation X.25] *Subnetwork Access Protocol (SNAcP).* Every variant of SP3 is either intended for end systems, or explicitly associated with a specific *SubNetwork Independent Convergence Protocol (SNICP)* computer packet protocol (OSI NSAPs, CLNP or DoD TCP/IP). None provides a general X.25 solution which could be included in any X.25 ISDN intermediate system or packet handler and be used whatever the higher layer protocol.

In addition, application layer work is under way to add needed security features to the X.400/ISO 8505-1 Message Handling System (MHS) and the X.500/ISO DIS 9594 Directory Services standards. The SDNS extensions to MHS will provide for message confidentiality, integrity, data origin authentication access control and non-repudiation with proof of origin and signed receipt requests. In general the SDNS Directory extensions do not require new protocols (Directory Access Control may be the exception), rather they provide new Directory attributes to support security.



LLC: Logical Link Control
SDE: Secure Data Exchange Protocol
MAC: Medium Access Control (CSMA/CD, token ring, etc.)
PHY: PHYsical level

Figure 4 - SILS Protocols for LANs.

In the *Local Area Network (LAN)* arena, IEEE 802.10 is developing a *Standard for Interoperable Local Area Network (LAN) Security (SILS)*, [P802.10]. LANs are broadcast networks, with particular security concerns, including secure broadcast messages. SILS, which is illustrated in figure 4, will include three standards:

- *Secure Data Exchange (SDE)*, a Data Link layer protocol providing Confidentiality, Integrity, Data Origin Authentication and Access Control services. Note that ISO 7498-2 specifies only Confidentiality and Traffic Flow Confidentiality at layer 2.
- *Key Management Protocol*, a layer 7 function which supports SDE.
- *System/Security Management*, which is a layer 7 set of services used to manage the security protocols.

Figure 5 illustrates the combination of the various SDNS, application security and SILS protocols, and their relationship to ISDN. The SDNS protocols are expected to serve as the basis for international standards development to provide standards for security in OSI. Although working prototypes of SP3 and SP4 protocols exist, the international standards work is still at an early stage, and the protocols can be expected to evolve considerably before they are adopted as International Standards. It appears likely that SP4 or its ISO standard successor protocol will be widely used to ensure secure communications between open computer systems. When ISDN is

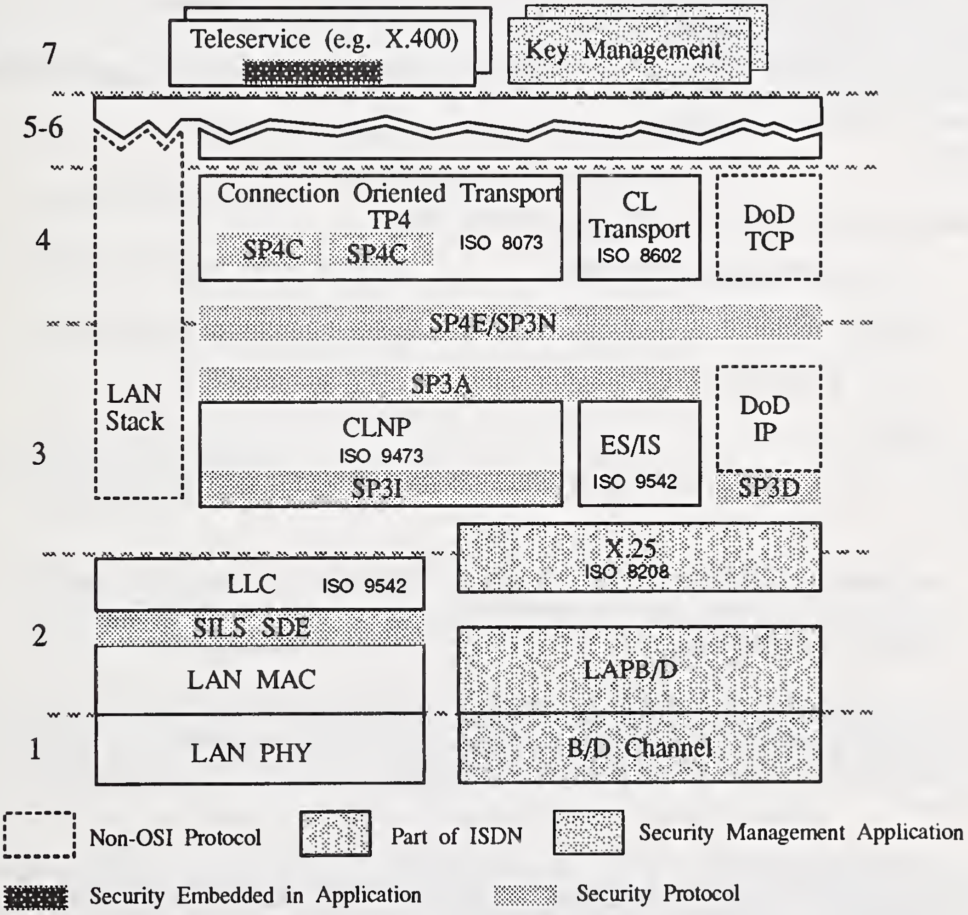


Figure 5 - SDNS and SILS Security Protocols.

used to provide a Data Link or Network Layer services for OSI communications, then SP4 or the equivalent standard protocol can ensure end to end confidentiality and integrity.

2.2 ECMA Security Architecture

Two documents produced by ECMA, ECMA TR/46, *Security in Open Systems a Security Framework,* and ECMA 138 *Security in Open Systems Data Elements and Service Definitions,* describe an approach to security in the context of complete open systems, rather than just communications. However, the ECMA model deals primarily with only two of the five security services defined in ISO 7498-2: Authentication and Access Control.

ECMA adapts an object orientated client-server model of security interactions. Figure 6 illustrates the ECMA object model and its relation to security services. In this model a human user interacts with an initiator (client) object which operates on a target (server) object. In the object orientated model, data is contained within the object and both applications and data are objects. The security services mediate between the human user and the objects in the system and they mediate between the objects themselves in accordance with the security policy of the system.

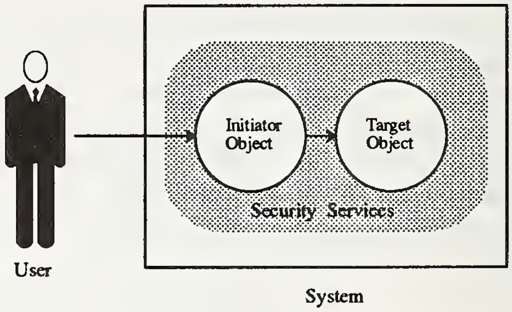


Figure 6 - Object Oriented Security Model.

Four classes of security services are defined by ECMA:

- Security Information Providing
- Security Control
- Security Monitor
- Other

Three Security Information Providing services are defined which provide trusted security information:

a. **Authentication Service.** Both human users and objects require authentication before they are allowed access to other objects, and objects may be authenticated before they are accessed.

b. **Security Attribute Service.** An attribute is an item of information associated with a user or an object. An attribute associated with a user or an initiator is a *Privilege Attribute*, while an attribute associated with a target object is a *Control Object.*

c. **Interdomain Service.** This service provides for mapping Security Attributes between domains, and for the sealing of identities and attributes by a Security Authority recognized in the target domain.

Three Security Control services are defined, which use attributes to control access to objects:

a. **Authorization Service.** The authorization service controls access to objects based upon the initiator and target Security Attributes.

b. **Secure Association Service.** In a distributed system this service has a component in each end-system, which associates a target and an initiator.

c. **Subject Sponsor Service.** The Subject Sponsor is the trusted facility that acts for any remote subject, particularly a human user, and arranges for the subjects authentication and access privileges to the objects it requires.

Two Security Monitor services are defined to maintain the integrity of the security system:

a. **Security Recovery Service.** The Security Recovery Service is an integral component of the other services. When the security of the system is threatened or violate, then recovery is required.

b. **Security Audit Information Collection Service.** This service collects audit information, the nature and analysis of which are dependent on the security policy.

Other Security Services may be required to support specific mechanisms and security policy requirements. They may include a Notary Service, a Key Management Service, a Data Flow Control Service and a Labelling Service, none of which are described in the ECMA standard.

The Security Services, in turn are supported by eight Security Facilities:

a. **Authentication Facility.**

b. **Attribute Management Facility.**

c. **Association Management Facility.**

d. **Inter Domain Facility.**

e. **Authorization Facility.**

f. **Audit Facility.**

g. **Recovery Facility.**

h. **Cryptographic Support**

In each case except for Recovery, the facility is implemented in the corresponding service. The Recovery Facility is contained in each of the services, and each service contains an authorization facility, which provides the access control for the management of the service. The Audit and Cryptographic Support facilities are optionally contained in all of the services.

The ECMA standards define the concept of a security domain, as a set of entities subject to a single security policy and a single security administration. They further recognize that security domains may be separate peers, or there may be a domain to sub-domain relationship. Each sub-domain is treated as a separate autonomous domain unless it is useful or necessary to consider it as a sub-domain. The Interdomain Service provides for secure interworking between objects in different domains.

Distributed systems require that initiator privileges be transferred via communications protocols. The ECMA Data Elements and Service Definitions also defines a *Privilege Attribute Certificate (PAC).* PACs state the privileges of an object and are bound together under the seal of the Authority which issues them. They must be protected against undetected modification, use by the wrong initiator, use against the wrong target, use outside stated constraints, or use by the right initiator for the wrong purpose.

ECMA 138 addresses security in distributed systems, in contrast to ISO 9478-2, which addresses only communications security. Unfortunately, the terminology of the two are not consistent. ISO defines five security services, and discusses them in terms of the mechanisms which may be used to implement the services and the layer of the ISO model where they may appropriately be implemented. ECMA defines eight rather different security services and eight security facilities they contain. However the focus of ECMA corresponds to the ISO Authentication and Access Control Services. In this document references to security services will follow the ISO model, unless otherwise stated. We will, however, adopt the concepts of security domains, the interdomain facility, and PACs from ECMA.

3. Discussion of ISDN and Security

This section provides an introduction to the ISDN and ISDN security.

3.1 Overview of ISDN

At its conception a decade and a half ago, the ISDN was projected to be the universal network which would go everywhere and handle all voice and data applications. Developing one integrated network to serve nearly all voice and data applications was probably never realistic. As ISDN becomes a reality, it is proving to be somewhat less than universal. Nevertheless, it is an important development in the worldwide public network and will considerably extend its utility for data. The digital nature of ISDN also offers an opportunity to provide security services which were previously impractical.

3.1.1 ISDN User Service Interfaces

The ISDN provides digital voice and data services to public network subscribers. Two somewhat different service interfaces are offered by public network service providers:

- *Basic Rate Interface (BRI)*, which provides a single physical line with two independent, circuit switched 64 kbps "*B channels*" and one 16 kbps packet "*D channel.*" The B channels may be used for digital voice or to provide a direct digital 64 kbps isochronous channel between computers or other digital devices. Service providers and independent networks will also offer B channel packet services. The D channel is used for signaling, that is to exchange control information between an ISDN terminal and a network switch (for example to set up B channel calls). The B channel also provides packet switched services to users. The ISDN network provides for conversion between the new digital voice services and existing analog terminals, so it is possible to complete a voice call between a digital ISDN terminal and an analog telephone. Up to eight terminals can share one ISDN line in an arrangement called a passive bus. The BRI service is often called "2B + D."

- *Primary Rate Interface (PRI)*, which, in North America, bundles together 23 64 kbps B channels and one 64 kbps D channel (or "23B + D"). It is equivalent to the established T1 1.536 Mbps telephone carrier. The 23 B channels can be independently circuit switched through the network, and each can carry voice or data. The D channel again carries signaling packets (for example to set-up each of the B channels). It may also carry packet switched user data packets. The PRI is primarily used to connect a user Private *Branch Exchange (PBX)* or multiplexor to the public network. In the world outside North America, the PRI is usually 30 B channels plus 1 D channel (30 B +D).

At the present time the ISDN services are just becoming available from network services providers. They are expected to be widely available by the mid 1990's. There will be a transition period of more than a decade while the ISDN gradually supplants the present analog service. There are a number of texts which provide a detailed introduction to ISDN [STAL 89], [VERM 90], [BOCK 88].

3.1.2 Historical Perspective

The conversion of the analog telephone network to a digital network has been under way for about 30 years. Digital computers proved to be first a flexible way to control and add new features to otherwise conventional analog switches. Digital trunks provided a means of carrying signals without adding noise as lengths were extended. By 1980 advances in digital semiconductor components made all digital switches advantageous.

By the mid 1970s it was apparent that new standards would be required for the interworking of the emerging digital networks and the CCITT began the process of developing the Integrated Serviced Digital Network. The CCITT operates on a 4 year cycle in issuing its recommendations. By 1980 the general architecture of ISDN we know today had been defined by CCITT, specifically the basic circuit switched 64 kbps B channel and the bundling of two B channels with a 16 kbps packet for out-of-band signaling, into the fundamental 2B + D service. The concept of primary rate service at higher rates (1.536 Mbit/s in North America and 2.048 Mbit/s in Europe) and various user interfaces (S and T interfaces) and Network terminations (NT1, and NT2) were well established.

The 1984 CCITT recommendations provided the basis for the first commercial ISDN products. In general, however, they were not sufficient for interworking of products from different vendors. The refinement and completion of the recommendations continued in 1988, improving interworking, but products based on the 1988 recommendations still fall short of the goal of full interworking of terminals with switches from different vendors.

In the mid 1970s when the ISDN was conceived, international telephony was largely characterized by national *Postal, Telephone and Telegraph (PTT)* government monopolies. That is, one government agency typically controlled all national communications services. Competition for network switching equipment was generally limited to one or two national suppliers (except in third world countries without an electronics industry). In the United States there was not a PTT, however one large regulated private company, AT&T,* dominated long distance and local telephone service, as well as the manufacturing of switching gear and terminals. Although about half the local lines in the country belonged to smaller independent companies, AT&T effectively provided the technical standards for the entire nation.

ISDN, as originally conceived, dealt largely with the interfaces between terminals and the network, and with the international services to be transferred across network boundaries, but not with the interconnection of switches within the network. ISDN defined interfaces with customer premisses equipment, not network trunk interfaces. The market for terminals was seen as broadly competitive, requiring standards, but not the market for switches or network trunks. Standardization of services was required to permit their transportation across (usually international) network boundaries. The internal organization of national networks was seen as not subject to standardization, and the interfaces between national networks could even be accomplished in a case by case manner, if the services were standardized.

Security, except as it is improved by the out-of-band D channel signaling, was not considered in the development of the ISDN standards.

The situation has changed. In the United States AT&T has been broken up into seven regional operating companies and one long distance and manufacturing company. Two other significant companies contend for long distance business, and the long distance carriers compete with the regional companies to interconnect large accounts within the territories of the regional companies. An apparatus of standards committees has partially replaced the technical standards setting function of AT&T. Only local residential and small business service remains a monopoly, reflecting the high cost of the copper twisted pair local distribution plant. Even this monopoly

* Certain commercial organizations are identified in this publication. Such identification does not imply recommendation or endorsement by the National Institute of Standards and Technology.

may be subject to challenge in the next decade by cable TV operators and cellular telephone networks.

Other parts of the world are moving in the same direction, introducing competition and privatizing national telephone systems. Moreover, a number of companies have built large private networks to serve their needs. The largest of these has 8 million km of cable and connects 300 mainframe computers, 2,000 minicomputers, 300,000 computer terminals and 250,000 telephones [ECON 90].

Traditional telephone carriers are also being forced to compete with mobile telephone systems. The cellular mobile telephones market over the past decade has been the big new growth area in telephony. Emerging standards for digital mobile cellular telephony will further enhance the capacity of these networks. It is not unthinkable that residences might be served by cellular radio telephone service, perhaps greatly reducing the cost of the local plant. Unprotected broadcast telephone service is, of course, easily intercepted.

There has been an increase in competition between central office switch vendors and a consolidation of that business. At the same time, within networks, the diversity of switching equipment is increasing as traditional exclusive ties to vendors are cut. To compete, network service providers need alternative switch suppliers.

There is now a stronger need for standards affecting the internal aspects of ISDN networks, including internal network security (that is to protect the integrity of the network itself and to protect service providers against fraud, rather than to protect the security of user communications). With more diversity in the networks, there may also be more exposure to security vulnerabilities. Moreover, as the number of networks proliferates, the need for security standards between networks increases. When one monopoly service provider served a nation, internal network security could be treated as an internal concern of that supplier and not properly the subject of standards. When that monopoly is replaced by many competing but interoperating networks, many aspects of network security can only be dealt with via broadly accepted standards. A detailed consideration of this important subject is beyond the scope of this document.

Another consequence of the breakup of national monopolies is that it reduces any possibility of the user simply relying on the public network to provide secure communications, even within one nation. Whatever network security standards there may eventually be, there will be too many independent service providers for users to rely on the "public network" to provide him with strong, consistent security. While it may be possible for network service providers to offer some security features and services, it will not be practical to simply secure the link to the network switch and then rely on the network thereafter. Users who wish secure end-to-end communications will have to rely on user to user protocols and standards. This report focuses on the user-to-user protocols and the services which will be needed to support them.

3.1.3 ISDN Principles & Goals

The original principles of the CCITT ISDN standards are outlined in CCITT Recommendation I.100. They are:

a) *the standardization of services offered to subscribers, so as to enable services to be internationally compatible;*

b) *the standardization of user-network interfaces so as to enable terminal equipment to be portable (and to assist in a);*

c) *the standardization of network capabilities to the degree necessary to allow user-to-network and network-to-network interworking and to achieve a) and b) above.*

Terminal portability and the ability to transport services internationally were the major goals. To those ends user-network interfaces, services and capabilities are standardized. While network capabilities are standardized, internal network interfaces are not included in this list, and portability of network switching or transmission equipment between networks was not a goal.

The present goals of network service providers have undoubtedly evolved and are much broader. One principle, not stated by I.100, but undoubtedly implicit in ISDN from the very beginning, is that ISDN is compatible with the preexisting analog/digital telephone system and interoperates with it over a long transition period. A corollary to this principle is that ISDN must preserve the large investment in copper twisted pair distribution loops, that is it must operate over them. They are one of the principle assets of network service providers.

Another goal is to provide end-to-end digital connectivity. Although computer data traffic is a small part of the overall network load, it is a fast growing part. Facsimile, traffic, also digital, is growing very rapidly. The digital B channel service provides about a 4:1 improvement over the data rates which can ordinarily be achieved over analog voice circuits.

Integration of access and service is implicit in the name. One unified access method is defined for a variety of services and features. Customers can request the services they require on a call by call basis.

While terminal interfaces (the S and T interface points - see sec. 5.1.4 and fig. 11 below) were standardized by CCITT, the network interface was explicitly not defined. In the spirit of keeping the network itself relatively unconstrained by ISDN standards, a network provided termination (NT1) converted the network interface to the terminal standard at the user premises. Each network might theoretically have its own interface. In the United States, this has been overturned by the FCC, and a standard for the U interface has been defined. Neglecting differences in connectors, however, the S and T interfaces remain consistent.

Interchangability of network switching equipment and communications links has become a goal of the service providers. Network service providers need the advantage of multiple equipment suppliers to be able to offer competitive prices and services to their customers. This change in emphasis may not yet be fully reflected in the present CCITT ISDN standards, but it is the focus of much service provider activity. Indeed the present emphasis is more on installing the ISDN infrastructure in the network switching plant and internal operation of the public network than in broadly offering ISDN services to users.

3.1.4 Reference Models for ISDN and the Relationship to OSI

The Reference Model for Open Systems Interconnection was briefly described in section 4.1 above. Figure 1 above illustrates the seven layer OSI protocol stack. As noted above, the OSI protocols are peer-to-peer protocols, and the vertical interfaces are defined only as logical service primitives. An observer on the interconnection medium will see a series of nested encapsulated PDUs, with the PDU of each layer encapsulated in those of its lower neighbor.

An Application layer PDU can be both fragmented into multiple lower layer packets and encapsulated as many as eight or more times (including sublayers). Opening and closing sessions or connections also generate exchanges of packets on the physical medium. While the resulting packet exchanges can be complex, OSI is a very simple and powerful paradigm. Its major goal is broad interconnection of open systems, not high efficiency. OSI expects to be able to reliably get packets across many successive concatenated dissimilar networks. While quality of service parameters may be specified, OSI makes few performance guarantees, is in no sense "real time" and there is no concept of synchronism in OSI.

ISDN has a different original paradigm. Although a packet D channel service is provided for signaling, which can also be used for user to user packet services, and various packet networks may be accessed through the circuit switched B channel, ISDN is first a circuit switched network. The fundamental service is a 64 kbps, isochronous, full duplex, circuit switched, 8-bit byte aligned, point to point B channel. It offers a modest and unvarying delay and a constant data rate. Provided that the rate is adequate, then it is suitable for real time applications and telemetry. Furthermore, because of the pervasive nature of the telephone network, if ISDN becomes universal in the telephone system, then these B channel circuits become available on demand from nearly anywhere direct to nearly anywhere else. We can go end to end, from terminal equipment to terminal equipment, anywhere, on what amounts to a single link.

A rather complex reference model has been defined for ISDN [I.324]. It was derived from the OSI model and is illustrated in figure 7. This model is primarily useful for circuit switched B channel connections. With seven layers and three planes, it is somewhat difficult to follow. The front, or user, plane, represents the circuit switched B channel. Except in the end terminals, this plane never rises above the Physical layer. The second, or control plane, deals with signaling and control of switching. This is defined between *customer premises equipment (CPE)* and the network by the Q.931 [T1.607] [Q.931] signaling protocol, which is a layer three protocol. Between the public network switches this function is performed by the *Signaling System Seven*

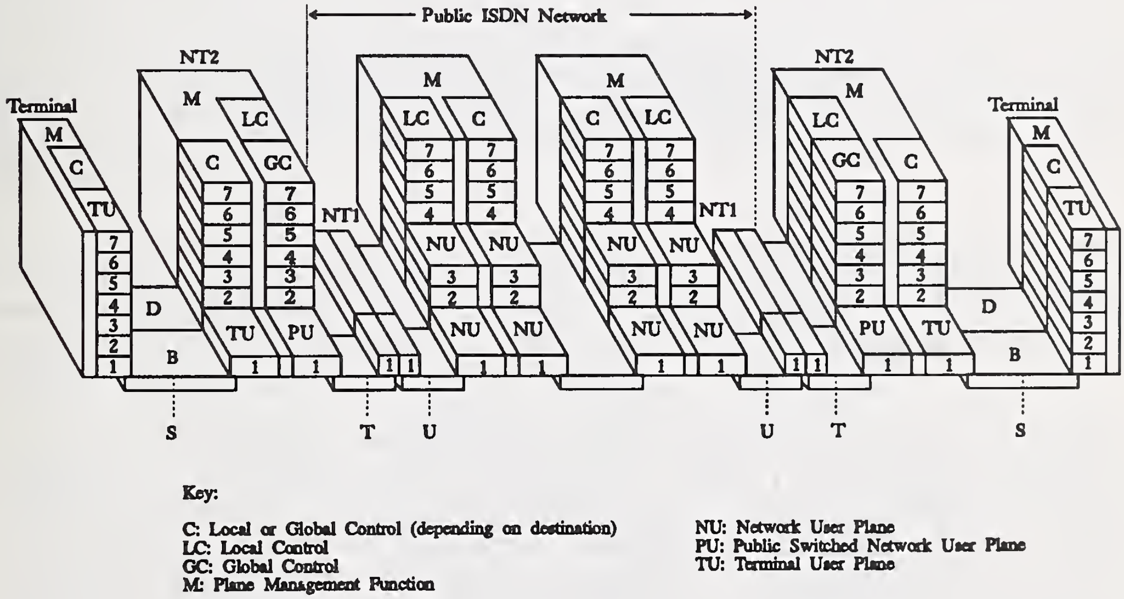


Figure 7 - ISDN Protocol Reference Model.

(SS7) protocol. The rear, or management plane, is concerned with the management of the network.

In OSI systems the management function is usually conceived as an application layer function with special access to the internals of each of the layers. There is no concept of a separate out of band signaling path for network control, all control is an in band function of either the *System Management Application Process (SMAP)* or peer layer management protocols.

Some general texts on ISDN attempt to decompose the model of figure 7 into a single plane, or separate single planes for the B and D channels, and make the model appear more OSI-like (*e. g.*, [STAL 89], [BOCK 88]). By isolating separate functions, these models may be somewhat easier to understand. Figure 8 is typical of such models, illustrating two separate stacks for the packet D channel and the circuit switched B Channel.

This model is more easily understood, but ISDN does not map into the OSI model in an entirely satisfying way. OSI is defined in terms of peer-to-peer protocols, while ISDN is defined primarily in terms of interface points and highly asymmetric protocols between a terminal and the network defined at those points. In ISDN peers do not talk directly to peers, at least in most cases.

There are two fundamentally different modes of operation in ISDN, corresponding to the circuit switched B channels and the packet D channel. The circuit switched B channel roughly corresponds to the front, or "user" plane of the model shown in figure 7, and the packet D channel corresponds roughly to the middle or "control" plane.

In normal operation a TE uses the D channel for signaling. Using an asymmetric protocol usually called *Q.931*, the TE sends packets to the network switch to which it is attached to set up

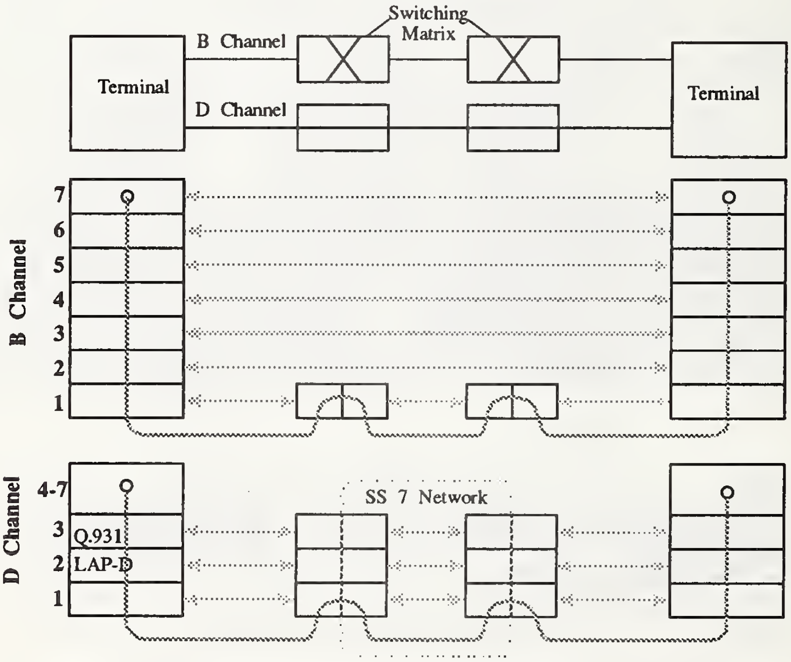


Figure 8 - ISDN Circuit Switching Protocol Model.

a circuit connection on the B channel. The network uses another somewhat similar protocol, SS7, to communicate between network switches, or separate networks, and the destination switch sends Q.931 packets to the destination TE. Q.931 packets which effectively go from TE to TE are translated into SS7 packets while they cross the network. Other Q.931 packets are generated by the network switches and sent to the TEs.

If the destination TE accepts the call, then a B channel connection is established between the two TEs. Actual data transfer, be it data or voice, normally takes place on the B-channel.

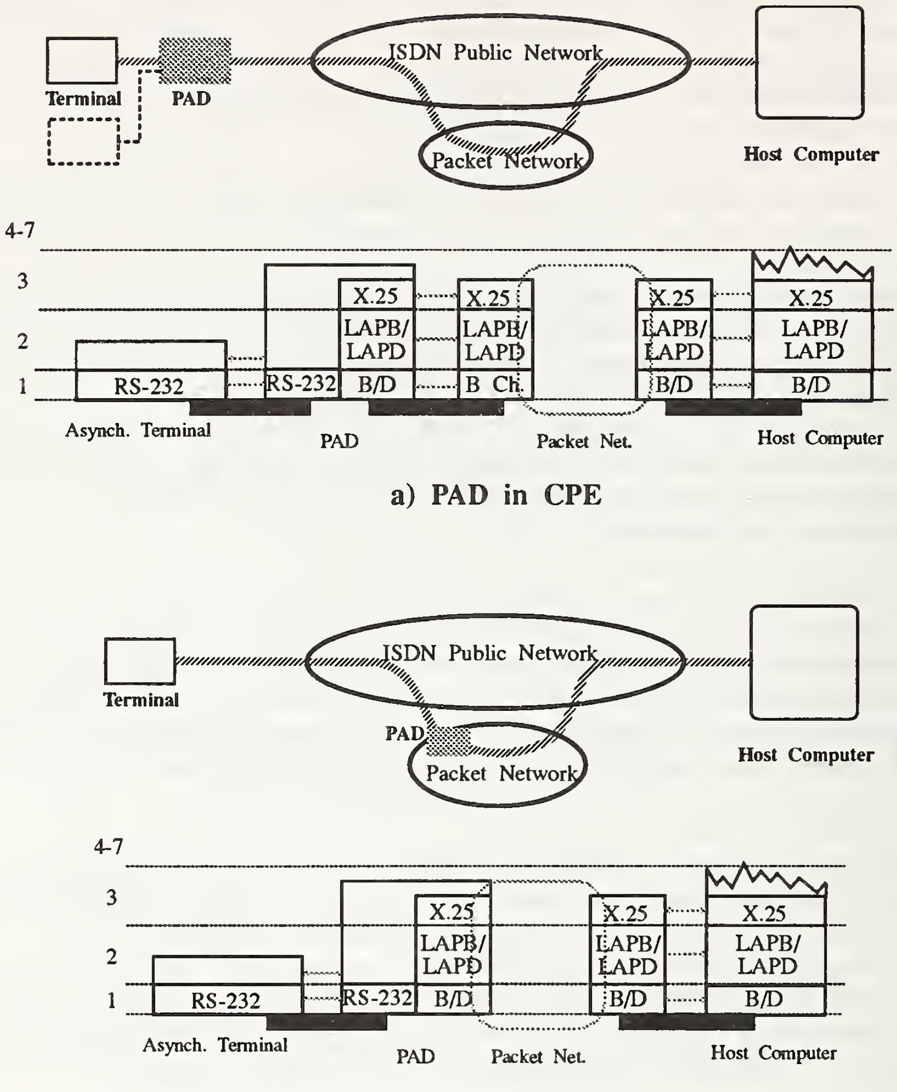
In recent years, there has been a trend to increase the integral user-to-user packet data functionality of the ISDN. The use of the ISDN as a user-to-user packet network is hardly represented in figure 7, and not at all in figure 8. Two methods of sending data in packets over the D channel are defined. One incorporates a user-to-user field in SS7 packets packets and sends those packets through SS7 along with call setup and other signaling. Although user-to-user signaling is defined in ISDN, service providers have been reluctant to offer the service. The other mechanism routes D channel packets to a separate packet handler and packet network rather than using the SS7 network.

When the B channel is to be used for packet data, the B channel is circuit switched to a packet handler. Although the service providers will purport to provide B channel packet services as a built-in feature of their ISDN, there is logically no difference from a circuit switched connection to a packet handler provided by an independent service provider. For this reason, in this report no distinction will be made in most cases between B channel packet services provided by the ISDN service provider and packet services provided by an independent service provider. Packet networks will generally be represented as separate parallel networks.

When user data is transferred over the B Channel, or through the D channel over a separate packet handler, the usual mechanism today is the X.25 *Packet Layer Protocol (PLP).* X.25 is considered to be a layer 3 protocol, specifically a SNAcP at the bottom of layer 3, which operates over a family of related layer 2 bit oriented protocols. These protocols operate over any duplex bit synchronous binary channel, relying on a technique known as *bit stuffing* to frame packets and obtain byte alignment. The specific Data Link Layer protocol used with X.25 on the B Channel is LAPB, and on the D channel is LAPD (which is also used with Q.931 signaling packets).

X.25 is a mature protocol which considerably predates both ISDN and the ISO reference model. It is widely used with modems as well as with ISDN. X.25 is primarily an asymmetric protocol between a terminal (*Data Terminal Equipment* or *DTE*) and a packet switching network *(Data Communications Equipment* or *DCE*), not a peer-to-peer protocol, however a direct DTE to DTE mode is also defined.

Figure 9 illustrates common configurations for X.25 and ISDN, with an asynchronous terminal connected to an X.25 *Packet Assembler Disassembler (PAD).* The PAD may be either in the user premises (fig. 9-a) or in the packet network (fig. 9-b). On the D channel only the arrangement in figure 9-a is practical, since data must be packetized to enter the D channel. The PAD is an ISDN Terminal Adapter and connects the terminal to the ISDN network and the X.25 packet network to a host computer. Although the figure shows OSI layers, note the asymmetry between the terminal and the computer, this is not conceptually a peer-to-peer, end-to-end connection, even though the terminal today is likely to in fact be a personal computer, fully capable of peer-to-peer relations, but emulating a "dumb" asynchronous terminal.



a) PAD in CPE

b) PAD in Network

Figure 9 - X.25 Terminal to Host Communications.

In combination with the Data Link layer protocol, X.25 provides for the establishment of logical connections between terminals through a packet switching network, link by link checking for transmission errors, packet sequence checking and *go back N ARQ* retransmission of lost or damaged packets. This facilitates the use of X.25 with terminals, which have no error detection and recovery capability. There are no end to end checks, however, only link by link checks, unless, in the DTE to DTE mode, one X.25 link extends from end to end.

Computer systems may not be willing to trust link by link checks without an end to end check at the Transport layer. There is a significant processing cost to each X.25 link and it is considered difficult to take advantage of channels faster than the 64 kbps B Channel with X.25. When X.25 is used in OSI networks, the processing overhead of the Transport layer is added to that of X.25.

Another service called *frame relay*, is being developed as an alternative to X.25 for use with ISDN and computer networks. Sequence checks and error recovery will not be performed, they will be deferred to higher layers. If packet errors are detected in intermediate systems the packets are discarded. This will speed packet processing in intermediate systems. There are two implicit assumptions here:

1. Errors rarely occur, therefore there is no performance advantage to recovering from them on a link by link basis.

2. There will be an end-to-end check at the Transport layer which will detect and recover from those infrequent errors which do occur.

Frame relay, which provides services on an ISDN communications link roughly analogous to the Logical Link Control (LLC) services of Local Area Networks, fits better with the North American OSI protocol stack than does X.25, since X.25 provides a quasi end-to-end service which duplicates many of the error detection and recovery functions of the Transport Layer, and frame relay does not. In many large organizations LANs will be the major vehicle for communications between computers and workstations. ISDN frame relay LAN gateways will be used to connect the LANs.

Figure 10 illustrates the use of either X.25 or frame relay to connect OSI stations on different LANs through the public network. Frame relay is sometimes considered to be at the top of layer 2, while X.25 is at the bottom of layer 3. The view taken here is that their position in the OSI stack is nearly indistinguishable, and both are considered to sit atop the layer 2/3 border.

Frame relay standards and products are just emerging. For the moment, X.25 is the primary packet service available over ISDN B and D channels. In time frame relay may take the place

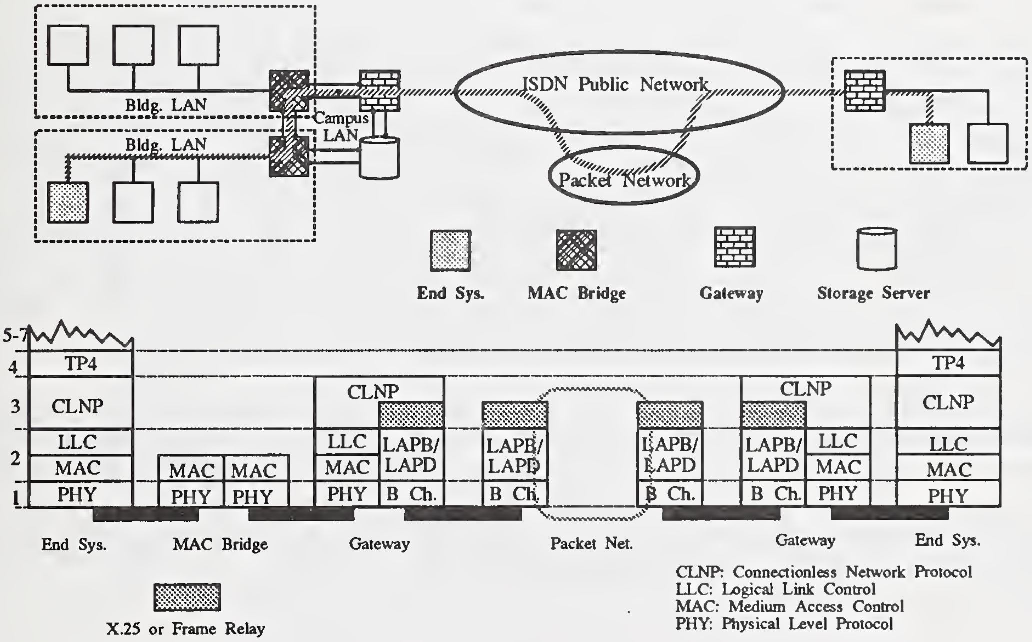
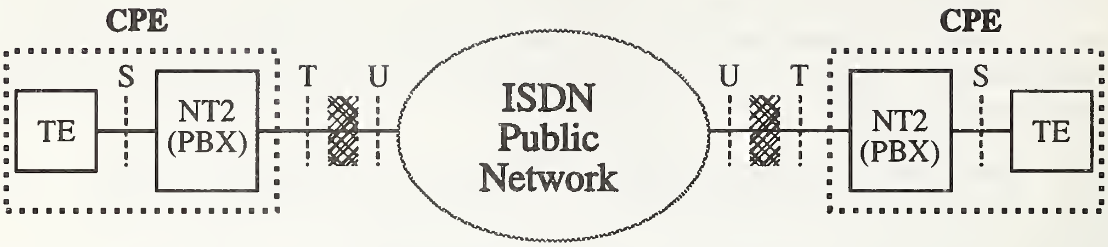


Figure 10 - Concatenated Subnetworks.



▨ NT1: Network Termination 1

CPE: Customer Premises Equipment

TE: Terminal Equipment

NT2: Network Termination 2; typ. a PBX or multiplexor

S/U/T: ISDN Interface Points

Figure 11 - ISDN Interface Reference Points.

of X.25 in many OSI applications. Frame relay is best suited to communications between end systems, since it is not a reliable service, while X.25 attempt to guarantee reliable service and can be used with simple terminals.

A model which is often used to describe ISDN is interface oriented rather than protocol oriented. ISDN defines four interface points as illustrated in figure 11.* The *U* interface is used to connect the network transmission and switching equipment to the user premises. A *Network Termination 1 (NT1)* converts the U interface to the *T* interface. The T interface, in turn connects the NT1 to a *Network Termination 2 (NT2).* An NT2 is a piece of customer premises switching equipment such as a Private Branch Exchange (PBX) or a multiplexor. The *S* interface, in turn connects an NT2 to a *Terminal Equipment (TE)* or to a *Terminal Adaptor (TA).* A TE is an ISDN telephone, a computer terminal, a FAX machine and the like. A TA adapts some pre-ISDN terminal for use with ISDN, at the *R* interface point. In many cases the R interface would be the familiar RS 232 serial interface. In some cases, there is no NT2, and the S and T interfaces, which are electrically identical, collapse into an S/T interface. The S interface includes a provision for a *passive bus* to which up to eight TEs may be attached.

When the passive bus is used, all TEs share the D channel on a contention per packet basis and a D channel packet protocol with the network switch or NT2 is used to connect TEs to a specific B channel. Only one TE may use a B channel for the duration of a call. Although eight TEs may share the bus, the B channel is not a party line, and only two TEs may be active at one time. If two TEs on the same bus communicate over the B channel, they do so through the NT2 or the local office switch, and both B channels on the bus are used.

* A standardized U interface was not a part of the original conception of ISDN. In the United States, however, there will be a single standard U interface between the network and customer premises.

For users the major purpose of OSI is a number of Application layer services. Among them are the *File Transfer, Access and Management (FTAM)* protocol, *Directory Services* protocol and the *Message Handling System (MHS)* electronic mail protocol. Some of these applications, particularly the last two, are intended as much specialized teleservices which run directly on ISDN with X.25 as they are OSI applications. Therefore the application itself can provide whatever end to end services may be needed in the application, including security services, and does not depend entirely upon OSI end to end services. Moreover these applications involve functions beyond the scope of data transmission, in particular data storage, with its own distinct security requirements.

In addition to the Directory Services and MHS, which are intended to run directly on ISDN as well as the OSI stack, there are several other specialized services or teleservices defined for operation over ISDN, and more may be expected. The existing services are primarily derived from services defined for the analog telephone network. They include, Facsimile, Teletex, Videotex and Telex. We may soon expect standards for motion video over the B channel and video conferencing. Some of these services use the ISDN B channel as an end to end pipe, and the functionality is embodied in the TEs. Some however, for example mail or directory services, may rely on a service provider attached to the network. Many other specialized information services, although not necessarily fully defined by standards, may be attached to the network.

The OSI Reference model and the various International Standards which specify the layers of the model are insufficient to guarantee interoperation of conforming equipment. There are too many options. To enhance interoperability, the *Government Open Systems Implementation Profile (GOSIP)* [FIPS 146] governs the specific selection of OSI protocols suites used in the Federal Government. Both ISDN and the SP4 Transport layer security protocol are expected to be included in future versions of GOSIP. Their relationship to the other protocols included in GOSIP is shown in figure 12.

3.2 ISDN Standards Status

The *International Telecommunications Union (ITU)* is an international organization which promotes cooperation and development in telecommunications, particularly in the provision of worldwide service capabilities. Only national governments may be members of the ITU. One of the organizations in the ITU is the *International Telegraph and Telephone Consultative Committee (CCITT)*, which is the organization which develops the international ISDN standards. These international ISDN standards are called *Recommendations*, and the ISDN Recommendations are produced on a four year cycle and adopted at a four year plenary meeting. The most recent ISDN Recommendations were adopted at the Ninth Plenary Assembly in 1988 and are informally called the *Blue Book.* The previous recommendations, adopted at the Eight Plenary Assembly were called the *Red Book.* The individual subcommittees of the CCITT are called *Study Groups*, and Study Group XVIII is the primary ISDN committee. A faster process for adopting Recommendations was accepted at the 1988 Assembly, and it is possible that the process will be faster in the future.

Since the ITU is an organization of governments, the State Department of the United States is the official member of the CCITT. However, the national positions are primarily developed by the U. S. industry, largely through the vehicle of the *Exchange Carriers Standards Association (ECSA).* Within the ECSA, *Standards Committee T1 - Communications* serves as the U. S. technical equivalent of the CCITT. T1 is accredited by the *American National Standards Institute (ANSI)* and standards developed by T1 become ANSI standards. T1 develops the U. S. technical positions for the CCITT and produces ANSI standards which generally follow the outline of the CCITT recommendations, but interpret them in the context of the United States.

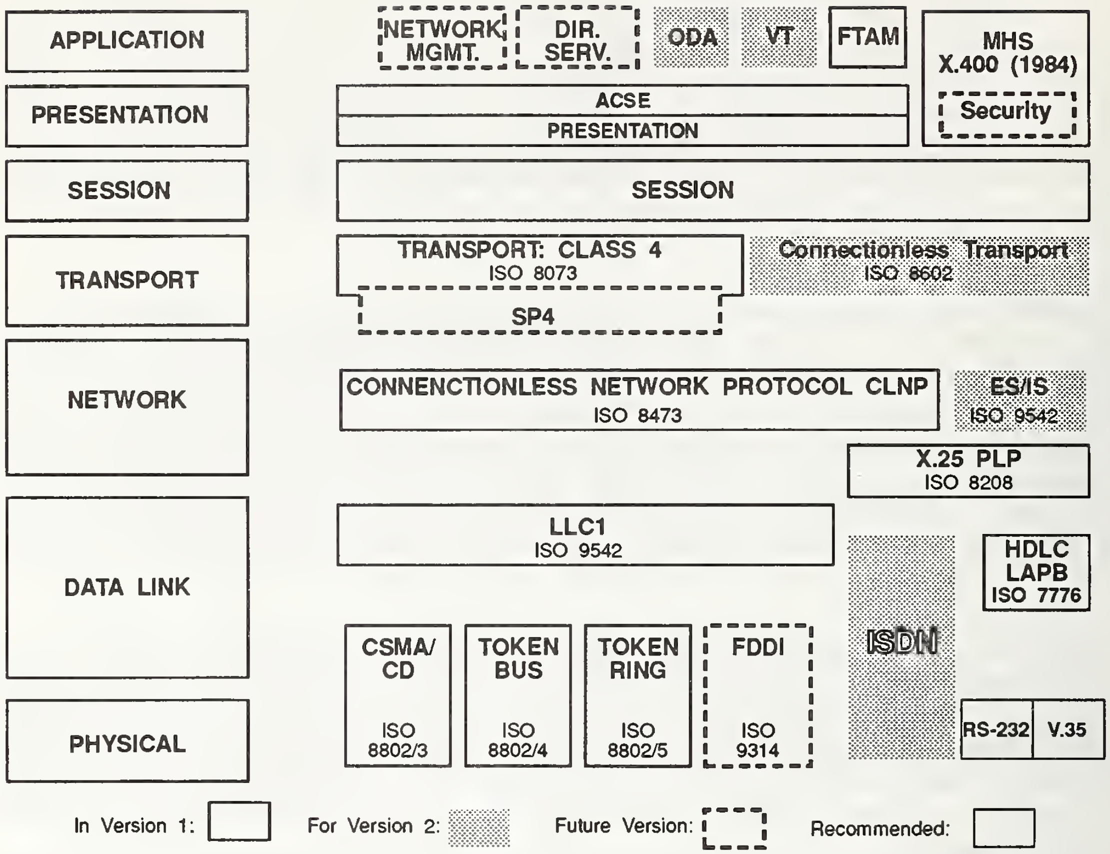


Figure 12 - U. S. GOSIP Profile.

The ANSI standards may select from the options or alternatives in the CCITT recommendations and add features or options not included in the recommendations. Within T1, ISDN is dealt with by *Technical Subcommittee T1S1: Integrated Services Digital Networks*. T1S1 is effectively the U. S. counterpart to CCITT Study Group XVIII.

Before the divestiture of AT&T into the present AT&T, which manufactures switching equipment, computers and terminals, and is the nations largest interexchange (long distance) carrier, and seven independent *Regional Bell Operating Companies (RBOCs)*, the Bell System Technical Standards provided the detailed specifications which allowed the national telephone network to operate together. This function has been largely assumed by *Bell Communications Research (Bellcore)*, which produces *Technical Requirements (TR)* documents which are used by the RBOCS as equipment procurement documents, and further define the ISDN standards and services as implemented by the RBOCs.

The RBOCs serve about 100 million subscriber lines, about half of those in the United States. Other carriers may choose to follow the TRs in many cases. Bellcore does not coordinate the business decisions of the RBOCs, which individually choose which services to offer and their deployment schedule. Moreover, granting the Bellcore TRs the status of recognized national standards is inherently objectionable to independent operating companies and long distance carriers who are not owners of Bellcore and have no say in its decisions. On the one hand the

Bellcore TRs will surely exert a powerful force for practical standardization, because of the market they represent, but on the other hand they probably cannot be considered standards, nor be referenced as standards in federal procurements, because of Bellcore's restricted ownership.

To further promote ISDN compatibility and define specific services, a *North American ISDN User's (NIU) Forum* has been created with the sponsorship of the National Institute of Standards and Technology. The forum has three principal objectives:

- Provide a forum for users to influence the developing ISDN to reflect their needs.
- Identify ISDN applications and develop implementation requirements for those applications to facilitate timely and interoperable multi-vendor implementations.
- Solicit user and product provider participation in this process.

The NIU forum consists of two workshops, the *ISDN User's Workshop (IUW)* and the *ISDN Implementor's Workshop (IIW)*. In the NIU process, the IUW produces Applications requirements, which describe potential applications of ISDN and their requirements. The IIW then develops Applications Profiles, Implementation Agreements and Conformance Criteria which allow interoperable implementations of solutions to the Applications Requirements. The IIW includes Applications Profile Teams and expert groups. There is an Expert Group on ISDN Security. In general, the Application Profiles are to be based upon approved standards. Since there are now few approved ANSI, ISO or CCITT standards for security, the ISDN Security Expert Group in the IIW has a challenging task. The NIU Security Expert Group has developed a list of security services for ISDN which includes the five OSI services (Confidentiality, Access Control, Authentication, Non-repudiation and Data Integrity) and adds to them Availability and a Notary Service.

One of the major goals of ISDN is terminal portability. Current ISDN standards and products do not meet this goal. In general, present TE equipment must be designed and tested to work with specific switch products. Indeed, some switch vendors maintain two models of terminals to work with different generations of their switches. TE vendors find that TE firmware must be updated whenever switch software is updated, and a TE which used to operate properly with a switch may fail to do so when the software of the switch moves to a new release.

A part of the reason for terminal nonportability is the many options and features allowed by the ISDN standards. Different switch vendors select different sets of features. Switch vendors also implement many proprietary features which are not defined in ISDN. Many of these proprietary features are motivated by a desire to allow public telephone service providers to offer Centrex services comparable to the advanced features of private branch exchanges.

At the present time ISDN implementations are confined to small islands, typically only a single switch or a few similar switches. This is a far cry from the vision of a vast global ISDN. Bellcore is attempting to address these problems with a series of TR's called Phase 1. They include ISDN Foundation TRs and End User Feature TRs. If all goes well, some degree of practical terminal portability should be a reality by the end of 1991, with more complete service portability in Phase 2 by 1993. This applies to the areas serviced by the RBOCs, and it is to be hoped that Bellcore's work will be adopted more broadly. The operation across international boundaries of any services beyond basic voice and 64 kbps circuit switched data services is very uncertain.

The ISDN was also broadly conceived as a universal service for all network users. It was once thought that, at some point in time, all subscribers in the network would be converted over to

ISDN lines. For all practical purposes this goal has been abandoned; it is recognized by network service providers that there is no advantage to ISDN for many subscribers and a forced conversion would be an untenable political and business proposition.

Indeed there are several disadvantages to ISDN for residential and small business subscribers, who may have little use for the 64 kbps digital service. They have a large investment in their present terminal equipment and wiring. For example, although ISDN supports up to 8 terminals on the same passive bus, two or three parties cannot simply pick up extensions on the same line and participate in the conversation as they do now. Another disadvantage to ISDN service for some purposes is that the TE is not powered by the network as are analog telephones. With ISDN a backup power supply is needed for TEs, or a power failure causes a telephone failure.

Instead of pressing for universal ISDN service, service providers are installing the ISDN infrastructure in their networks, but unbundling the ISDN features and making them available to analog subscribers. Call waiting, call forwarding and calling line ID features are now widely available to analog subscribers. They are supported by ISDN capable switches and SS7. Although estimates vary somewhat, it is more or less generally agreed that, while only a small fraction of subscriber lines in the United States will be ISDN lines in 1995, the majority of subscriber lines will be serviced by switches which support SS7.

Eventually, the ISDN standards will provide the infrastructure for worldwide telephony. ISDN services will be available anywhere in the developed world. Full portability of ISDN terminals and switches may never be a reality, but the basic services will be transportable across national boundaries between TEs. An all-ISDN world wide telephone network, however, seems improbable. Many users will continue to use analog terminals for the foreseeable future.

Finally, another development not originally anticipated by ISDN is mobile cellular telephony. The 1980s was a period of explosive growth for cellular telephone systems. The present system uses digital control but analog voice channels. Work has recently begun on standards for an advanced digital cellular mobile telephone system. The data rate for this service will probably be 8 kbps, and it will require the development of inexpensive voice coders at this rate. With a number of 8 kbps channels assigned to one higher rate carrier on a time division multiplexing basis, broadcast spectrum utilization will be enhanced. There also has been some speculation about using cellular radio to deliver voice services to residences, perhaps as a competitive alternative to traditional wire line carriers, or as a less expensive alternative to copper where densities are low.

There are many implications for ISDN security. The first is, that for the near term, ISDN security services should require little more from the ISDN than the ability to set-up and terminate 64 kbps B channels. Broad, consistent near term availability of any other services is uncertain. Longer term security may be able to use D channel packet services; certainly this would be highly desirable. A second is that any supposition of an all ISDN network is unrealistic for the foreseeable future. Security functions developed for ISDN may have to interoperate with pre-ISDN terminal equipment. It should also be designed to interoperate with new digital cellular telephone services, not originally anticipated by ISDN.

3.3 Threats

The ISDN security threats include:

- Denial of service
- Intrusion into network customer data

- Use of ISDN network to penetrate a customer system
- Use of the network for fraud
- Intrusion on the confidentiality of ISDN communications.
- Modification of communications

Denial of service attacks include physical damage to CPE, network links and switches. Even if no actual attack is involved, accidents and disasters can cause loss of service. Switches can also be attacked by penetrating the switch software to either disable the entire switch or to affect a particular subscriber in some way, perhaps by diverting his calls or disabling his line.

ISDN networks will maintain subscriber data, particularly the records of calls made. This information is properly confidential to the subscriber and may be quite sensitive. If the network systems are penetrated, then an intruder may obtain this information. Both the operational network, which collects the data and the administrative system are possible points of attack.

Since the telephone network is the principal means of providing remote access to computer systems and networks of all sorts, it is an obvious and widely used vehicle for intrusion into these systems. Almost every outside penetration of a computer system begins with a telephone call. The purpose of the intrusion may be fraud or theft, sabotage, to obtain confidential information, or simply for the fun of doing it. The ISDN network cannot prevent such attacks, but it can make available confidentiality and authentication means which the end systems can use to detect and thwart the attacks.

The telephone network is one of the principal instruments of fraud in modem society. Much of the fraud is petty, some is major, and the total cost is undoubtedly substantial. Electronic fraud sometimes involves substantial funds transfers, and may not always be detected or reported. Some telephone fraud involves obtaining confidential information, including credit records, law enforcement records, telephone numbers, and the like. The network itself is often defrauded. Since the telephone network is a pervasive communications medium, this will continue; it is impossible to entirely eliminate fraud via telephone. The inherent anonymity of callers in the present network is the great advantage of the telephone as an instrument of fraud.

It is illegal to tap ISDN phone lines without a court wiretap order. It is, however, not difficult to do so. The law is not likely to significantly deter wiretapping in espionage cases, and may not do so in other cases. Cellular and wireless telephones are particularly vulnerable. It is also possible to modify data sent over the network for fraudulent or malicious purposes. Although this requires more sophistication than a simple wiretap, it would not be extremely difficult.

ISDN security is however, more than simply responses to specific deliberate threats. Much damage may be done by error, noise, accident, confusion, misunderstanding and inadvertence as well as by intent. The same signature, integrity, notarization and authentication services may also apply in these cases as in cases of deliberate fraud. A digitally signed and notarized electronic document may settle a dispute caused simply by an error. The value of good security practices is not limited to preventing deliberate attacks, and much security would still be good business practice in a world free from deliberate fraud, theft and intrusion.

3.4 The ISDN Security Environment

Figure 13 illustrates the broad environment into which ISDN security must fit. ISDN security must begin with the user. For the purposes of ISDN security a user may be a person, some organizational entity (e. g., the dispatcher), or a computer process acting for either the person or

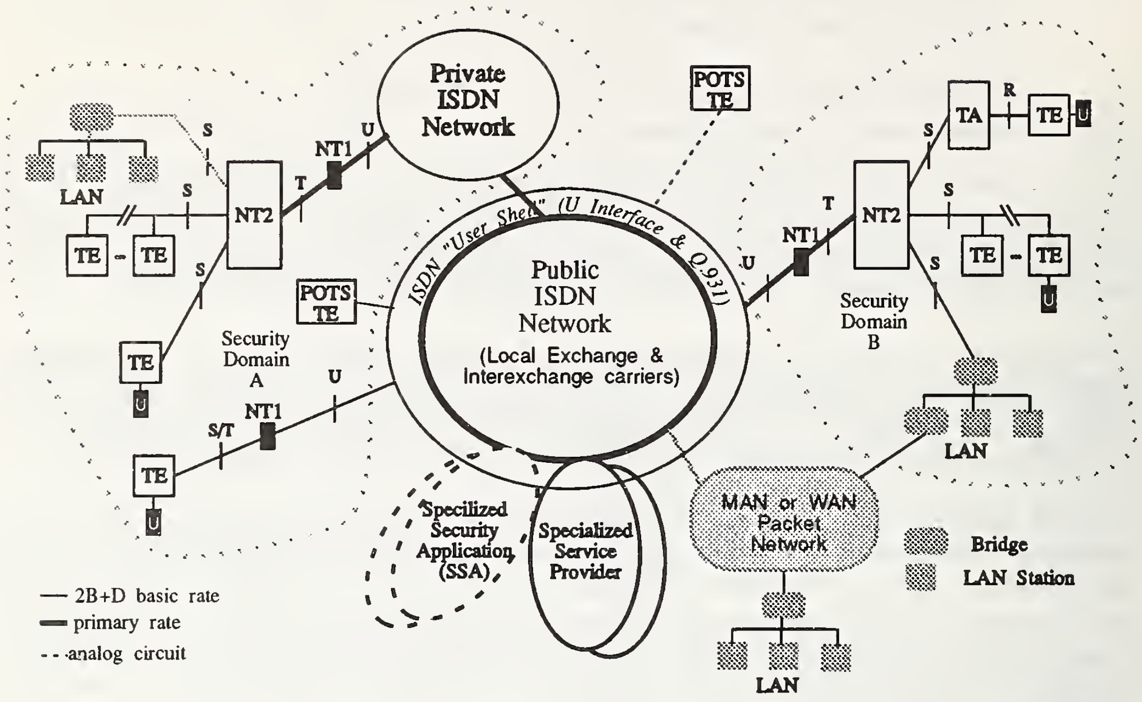


Figure 13 - ISDN Security Environment.

the entity. The user may or may not be bound to a specific line or terminal, indeed the user may be highly mobile and may carry his security attributes with him wherever he goes. Since humans use any available simple telephone instrument for a wide range of transactions, the reliable authentications of human users of ordinary ISDN telephones is a serious concern.

The user interacts with ISDN *Terminal Equipment (TE)*. TEs include voice phones, answering machines, integrated voice/data terminals facsimile machines, specialized terminals such as automated teller machines and the like. In many cases, the TE will be a computer connected to the ISDN network thorough some sort of ISDN interface device or card. When the TE is a computer, the user is a computer process acting as the agent for either a person or an organizational entity.

The TE may either be directly connected to the ISDN network, or it may be connected to a *Private Branch Exchange (PBX)*, which is in turn connected to the ISDN public network. In the ISDN jargon, a PBX is a *Network Termination 2* or *NT2*. Collectively, the TEs and the NT2 equipment are called *Customer Premises Equipment (CPE)*.

The public ISDN is an amalgam of numerous interconnected service providers. In the United States they are either considered local exchange carriers (local telephone companies) or interexchange carriers (long distance telephone companies). In general, the local exchange carriers have a monopoly over residences and small businesses in their operating areas. Local exchange carriers are regulated by both the Federal Communications Commission (FCC) and state Public Utility Commissions (PUCs). There is constant tension over the respective authority of the FCC and the PUCs. There are three main interexchange carriers. The local exchange carriers include seven large former AT&T Regional Operating Companies (RBOCs), which serve about half the telephone lines in the country, one large "independent" local exchange carrier (of size comparable to the RBOCs), and numerous smaller local exchange carriers.

The public network must be able to protect itself from fraud and threats to service availability. This is a business necessity for the service providers. Service providers must also preserve the confidentiality of customer service records. The public network is too diverse to be expected to provide strong assurances of user to user security, particularly confidentiality and authentication. There is no one authority capable of imposing and managing a security program which could ensure this.

Application layer services, called *specialized services* or *teleservices* may be provided to users through the ISDN. Specialized services include (X.500), packet Message Handling Service (X.400) and a variety of other value added application services. The *network service providers* themselves may be *specialized service providers* or the services may be provided by other service providers with access to the network switches.* Some general teleservices, such as X.400, will incorporate security into the more general application. The specialized service providers may also offer security applications, such as key management. In this report, such a security oriented application will be called a *Specialized Security Application (SSA).*

In addition to the specialized services which may be attached to the network, packet handlers may be incorporated in network switches to provide packet services as a part of the public network. Independent packet networks may also be connected to the local exchange switches. A variety of packet network services, including "secure" networks may ultimately become accessible through the local switches.

Users in many different security domains will communicate with each other over the ISDN network. In addition to the public ISDN network, there will be private ISDN networks, and a variety of data networks, including Local Area Networks (LANs), Metropolitan Area Networks (MANs), and Wide area Networks (WANs), which may be connected to the public ISDN network through gateways. Analog *Plain Old Telephone Service (POTS)* will continue to be supported by the public network and may consist of a majority of local lines for the next few decades.

The burden of user-to-user security over ISDN will fall of necessity on the CPE. The security solutions chosen in the CPE, should allow not just for ISDN, but for the alternative communications available.

3.5 The Human Component of ISDN Security

ISDN is both a telephone network and a data network. People interact with people, relatively "stupid" machines, and computer systems over the ISDN network. Computers will also interact with computers. The previous communications standards work of OSI and ECMA have dealt largely with the interactions of computer systems. In ISDN security we must also consider security in the context of human interaction, often largely unaided by a computer, or consider if there are means whereby computer based security functionality can be extended to all telephone users.

* The rights of local exchange carriers, particularly the RBOCs, to provide value added services, the conditions under which they may do so, and the nature of the access which they must provide to independent supplementary service providers is currently a matter of regulatory, political and legal dispute.

The fundamentals of human to human interaction over ISDN remain nearly the same as they have been in the analog telephone era, except that the called party may have a fairly reliable indication of the caller's number, until some general human authentication system is adopted for ISDN. The essential question is, "to whom am I speaking?"

Where parties are known to each other, they may recognize each other's voice. Traditional challenge and reply password authentication can be applied over the telephone. However only rudimentary protocols are practical with untrained humans. For the general public, memorizing and using a 4 digit personal identity number (PIN) is probably about the practical limit. An individual can only be expected to memorize at most two or three such PINs. If more are needed, the individual can be expected to write them down and carry them, compromising security. Thorough training and discipline are required to maintain security on normal telephone calls.

Humans are capable of exercising judgement. They may detect an attempted telephone fraud or penetration by exercising judgement. In some emergencies good judgement may dictate abandoning normal procedures, but this is also a weakness for the impostor to exploit. Telephone impostors practice "social engineering," making posing as someone else a fine art.

A reliable and socially acceptable means of strong personal authentication through normal ISDN telephones is badly needed. If available, it would make a great contribution to security. Telephone access to confidential information should be based upon reliable authentication, business transactions should be authenticated or signed, and access to information resources should require authentication.

When humans deal with intelligent machines through a telephone a basic mismatch in capabilities exists. The telephone keypad provides a very limited interface to computer systems. Only rather simple protocols are practical. In many cases the human will be untrained, further limiting the interface. Applications to date include dial-up account inquiry services and automated teller banking machines. Remote voice mail capabilities are now being offered by local operating companies.

Much more elaborate services are potentially possible using personal computers. The computer provides a much more elaborate interface to support the application and can implement security protocols. Banking services, shopping services, reservation services and the like are now offered.

It is likely that inexpensive home and office computer systems will soon include a powerful computer, page display, scanner, page image printer, ISDN port or modem, voice telephone, and voice answering machine with storage equivalent to a filing cabinet or more, all integrated into a compact desktop package, with appropriate integrated software. Such an integrated voice, data and image system will provide a single integrated personal solution to document preparation, storage and communications.

By extrapolation from the past decade, such systems should be widely available by 1995 and ubiquitous by the end of the century. Already hardware to support all the functions described above can be added to standard personal computers for comparatively modest prices. All that remains is to integrate the hardware, and, what will be more difficult, the software. It is reasonable to expect that nearly all offices will use such systems by the end of the century and most professionals will have home systems.

These will be very powerful general computers, perhaps supported by graphics or digital signal processors. They will have at least the computational power of present mainframe computers (just as today's PCs easily match the power of 1980 vintage mainframes). They will be capable of encrypting digital voice in real time, using fairly strong algorithms, without dedicated cryptographic circuits.

Increasingly, computers are portable. The portable computer may simply be a module which detaches from the standard desktop integrated computer. The portable unit may include most of the functions described above, except perhaps the printer and scanner. A portable computer system may become a basic tool for every business traveler. Every person who now carries a briefcase home may soon put a portable computer in it. If this occurs, however, it will reflect a communications failure, because the ISDN network should provide the needed communications between home and office.

A security mismatch may occur when computer systems are connected to "dumb" equipment, such as existing FAX machines, particularly when they are not attended by an operator. Compatibility with existing equipment will be necessary, but this equipment cannot accommodate complex protocols as the computer can. The security problem is likely to be most acute with equipment such as facsimile machines intended for unattended operation. This should only be a transitional problem, however, as older equipment passes on to oblivion. The dumb FAX machine may shortly become as irrelevant as the black and white television.

Computer mail and directory services will become available. Mail services will include security to limit access and protect confidentiality. Directory services will provide key management and might provide Privlege Attribute Certificate services.

While powerful security functions can be built into these computers, a formidable educational process is required on the part of the humans who operate them. Even assuming "user friendly" security software, there will be much to learn. Teaching users good security practices and getting them to use it will not be easy.

Indeed, access to such computers and the skills to operate them may be a divisive force in society. As user friendly as software may become, mastering it will be a barrier for those long out of school and the educationally disadvantaged. Computer access and literacy may become key to full participation in society and as fundamental as reading, writing and arithmetic. The introduction of widespread communications security and the integration of it into ordinary life and business will be as much a social and educational problem as a technical problem.

Voice only telephones will remain. We may hope, however, that they will increasingly provide a port to attach a computer, or perhaps a simple authentication device. It will be desirable to provide at least some sort of authentication for voice telephone users. While existing terminals such as FAX machines will complicate the transition, in the end security need support only voice terminals and end computer systems. The greatest security problem will be education.

4. Security Services

In this section the OSI security services are reviewed as they apply to ISDN. The possibility of extending the services to include additional services from ECMA 138 is also discussed.

4.1 Integrity Service

Integrity services are generally provided for digital data by means of an *Integrity Check Value (ICV)*. The ICV is a field whose value is a known function of all the protected bits in a packet. The ICV is then encrypted with a private or secret key. An intruder can modify a packet and can compute the correct ICV of the modified packet, but cannot then encrypt the ICV. Alteration of the packet can be detected. This provides connectionless integrity. If the ICV covers an appropriate timestamp field, then connection replay attacks can be prevented. The integrity can be extended to full connection integrity by including appropriate sequence number fields within the range of the ICV.

To provide connectionless integrity it is only necessary to encrypt the ICV of a packet. Many packet protocols include a *Frame Check Sequence (FCS)* which is a value computed from all the bits of a packet, used to detect transmission errors. Similarly, many protocols include sequence numbers in each packet, and may use them to detect lost or duplicate packets. Although common FCS's are not ideal ICV's, when packets from such a protocol are encrypted, at a lower layer, then at least a degree of connection integrity is the result. The LAPB and LAPD Data Link layer protocols used with ISDN provide both sequence numbers and an FCS. X.25 provides 3 or 8 bit sequence numbers, which might allow some replay attacks. Security protocols may provide extended sequence number or timestamp protection.

4.2 Non-Repudiation Service

A message may be signed by encrypting the ICV of a packet or message with a private key known only to the originator of a message. If the message contains a date and time, and the recipient checks the time of arrival and keeps a signed copy of the message, then the recipient has non-repudiation with proof of origin.

The purpose of non-repudiation with proof of delivery is to prevent a recipient from falsely denying that he received a message. A form of non-repudiation with proof of delivery can be obtained if the recipient signs the message he receives plus a timestamp and returns that to the originator. While such a mechanism will cover many needs, it is not a complete solution, because the recipient, having seen the message, can decline to confirm its receipt. If electronic communications are to substitute for registered mail, or a process server, then some mechanism which does not require the cooperation of the recipient is required.

Notary mechanisms have been proposed, involving a trusted third party, which delivers the message to the recipient and keeps a copy of the message or a digest of the message. The recipient, having read the message, may, however, falsely claim that the communication line was broken. It may be useful, then, to perform a test of the communication line, requesting a signed acknowledgment prior to sending the data itself. This would be proof that the communications were operational at least immediately prior to sending the message. If, however, a recipient is expecting the equivalent of an unwelcome subpena, the recipient may not respond to the initial communication. Legislation may be needed before non-repudiation services can supplement or replace traditional mechanisms for provable communications.

Non-repudiation is ordinarily considered a layer 7 function, and outside the normal scope of ISDN. However, voice, or facsimile non-repudiation services, may appropriately be considered

ISDN services. Modern digital signal and image processing probably makes it practical, perhaps easy, to make undetectable alterations to any electronic image or voice recording, unless the image is protected by a digital signature. A trusted voice notary service, for example, might be used to produce a signed digital recording of a voice call. Such a recording could not be altered by either of the parties to the call.

4.3 Confidentiality Service

Confidentiality can be assured by end-to-end encryption, physical protection of the entire network, or by secure routing, which ensures that each subnetwork or link through which the data passes is protected by either encryption or by physical means.

Since the cost of physical protection increases with distance, physical protection of the entire ISDN public network is infeasible. Nor is it practical to physically protect long individual communications links. It is feasible to have protected installations, which are closely guarded. This generally requires that all personnel entering the installation be cleared or escorted. While this is expensive and cumbersome, it may be required by the nature of the work done in the installation. In such an environment additional protection is sometimes provided by enclosing communications links in a pressurized shield and detecting the loss of pressure which may accompany any attempt to penetrate the shield.

It is sometimes claimed that fiber optic links are difficult or impossible to tap. While noncryptographic means of protecting fiber communications exist, these means are logically equivalent to link encryption. It is only marginally more difficult to tap fiber links than electrical networks. Security is somewhat improved when particularly vulnerable links, such as terrestrial or satellite microwave links are replaced by optical fiber, but fiber optics by itself does not provide strong confidentiality.

Encryption will be the principal mechanism for ensuring confidentiality in wide area networks such as ISDN, because its cost does not scale with distance. Encryption can be located at any layer of the OSI model and provide both confidentiality and (often in combination with an integrity check value and/or appropriate message sequence numbers) integrity services. Perhaps most important, it can provide end-to-end confidentiality and integrity through otherwise insecure channels, without any change to the network.

Encryption algorithms are conventionally broken down into two general classes:

- *symmetric* or *secret key* algorithms, in which both parties share the same secret key. Examples include the DES [FIPS 46] and the *Fast Data Encipherment Algorithm FEAL-8* [MIYA 88]. These algorithms can be computationally efficient, and the DES has been studied for more than a decade without publication of successful attacks, leading to some confidence in their basic security. The greatest difficulty symmetric key algorithms is the difficulty of managing the secret keys.
- *Public key* algorithms, which use both a public and a private key. In the most general case plaintext enciphered with the public key can be recovered only by use of the private key and vice versa. In some cases the algorithms simply allow two parties to securely negotiate a secret key over a nonsecure link. The *Diffie-Hellman* algorithm [DIFF 76] and the *Rivest, Shamir, Adleman (RSA)* algorithm [RIVE 78] are probably the best known algorithms published to date. These two algorithms, as do several other algorithms, require the exponentiation of large numbers, a computationally intensive process, which limits their speed. Breaking these two algorithms is believed

(but not proved) to be respectively equivalent to two intensively studied difficult problems in mathematics, the discrete logarithm problem and factoring large numbers.

Both symmetric key and public key cryptography can be combined on one system, using each to best advantage. For example, one experimental X.25 cryptographic system uses the Diffie Hellman algorithm to derive a common secret DES session key, and uses the RSA algorithm for authentication and signatures.

4.4 Authentication Service

The framework for Directory authentication is ISO/IEC 9594-8, while a draft OSI Authentication Framework [JTC1 1] provides a draft authentication framework for OSI. The Directory application (X.500) provides a repository for attributes (information) about named objects in a *Directory Information Base (DIB).* The Directory will provide a digital signature mechanism, which will allow users to verify information placed in the DIB by a *Certification Authority* , including the public keys of users. The main security feature of the Directory is to provide a secure mapping between users and their public keys.

The draft OSI Authentication Framework provides a broad overview of authentication and outlines a number of schemes for authentication. It defines two classes of authentication, Class 1, which provides protection against disclosure of authentication information, but is vulnerable to replay attacks, and Class 2, which provides assurances against replay and masquerade attacks. Class 1 mechanisms require encryption or one-way hash functions. Class 2 functions require unique numbers and challenges as well as encryption or one-way hash functions.

A one-way hash function transforms data in a way that is not reversible. A one-way hash function is easy to compute but difficult to invert. Given the output of the hash function it is not practical to compute an input value which results in that output.

ISO/IEC 9594-8 defines two classes of authentication, *simple authentication* and *strong authentication.* Simple authentication procedures rely upon a secret password known to the user. The name and password of user A are transferred to B, possibly with a timestamp and random number. The passwords may be protected by a one-way hash function. In a simple protected authentication, for example, A sends B an authenticator consisting of a timestamp, a random number, A's distinguished name, all in the clear, and a protection parameter generated with a one-way function from the first three parameters plus A's secret password. B then accesses a local copy of A's password to generate the protection parameter, which it compares to the protection parameter received from A.

Simple authentication is most useful for access to local systems and equipment. Where access is restricted to ISDN TE or services, a simple user authentication process is appropriate. Simple authentication is less useful in the more general case, where A wishes to be able to authenticate to any B through the ISDN network. B must either have A's protected key, requiring that B be trusted by A, or some third party trusted by both A and B, with knowledge of the secret key, must be invoked to check the authentication.

Strong authentication requires the use of public key cryptography. Public key algorithms used for strong authentication have the property that $X_p \bullet X_s = X_s \bullet X_p$, where X_p and X_s are the encipherment functions using the public and secret keys, respectively. A certification authority produces *certificates* for users which include the distinguished name of the user, the validity dates of the certificate and the public key of the user. The certificate is protected by the *digital signature* of the certification authority. That signature contains a summary of the certificate produced by a one-way hash function and enciphered with the secret key of the certification authority. The encipherment ensures that the certificate cannot be forged.

The certificate is not secret and can be contained in the Directory without protection and be freely distributed. Because it is signed it cannot be forged or altered without knowledge of the certification authority's secret key. Any user knowing the public key of the certification authority can check the validity of the certificate. Two users, A and B, may not share the same certification authority. However, the certification authority for each may contain certificates for other certification authorities through which it is possible to construct a *certification path* between A and B. A certification path forms a logically unbroken chain of trusted points between two users who wish to authenticate. When A authenticates to B, B obtains A's public key from A's certificate. A produces an authentication token message containing the certification path from B to A, and a signed portion consisting of a timestamp, a non-repeating number and B's name. B can obtain the public key of A from the certification path and decrypt the signature which can only be produced using A's secret key. A two-way strong authention requires B to return an authentication token including the random number from A in the signature. An alternative three-way authentication allows the timestamp to be dispensed with.

ISO/IEC 9594-8 provides a directory foundation upon which ISDN authentication may be built. ISDN users may be bound to a specific TE, in which case the necessary authentication processes, keys and passwords may be stored in the TE. Access to the TE may be physically controlled, the user may authenticate to the TE (typically with a password and simple authentication), or possession of a physical token may be required for authentication of the user to the TE, which then authenticates to remote TEs. In this mode ISDN places no additional constraints on normal OSI authentication.

ISDN users, however, are frequently not bound to a specific terminal. They wish to be able to use any ISDN telephone terminal and authenticate from it. In the absence of a better authentication service for terminals, the Calling Line ID supplementary service will be used for authentication. This service, while useful to businesses (for example, to automate the retrieval of customer records when a call is received), is not a reliable means of authentication of individuals and is objectionable to some in that as implemented it is often automatic and involuntary. Moreover, individuals wish access to services from any terminal, not simply their home telephone.

Today, when ordinary telephones are used for remote access to services requiring some form of authentication, an account number and a password or *personal identification number (PIN)* of some kind is usually entered through the keyboard. An intruder tapping the communications link immediately learns the password. A different password is required by each user. Since passwords should be memorized, so that they cannot be stolen, they are usually only a few digits and an individual can only memorize a few frequently used passwords.

Many specialized transaction terminals now use standardized plastic magnetic stripe cards. These may be calling cards, bank cards or travel credit cards. These cards can be read with readers built in terminals, and may be augmented by requesting a password or PIN. These cards at present are widely used as authentication tokens for a variety of commercial transactions. When used through the telephone network without a special reader, the number of the card is either stated verbally, or entered through the telephone keyboard. When used without a reader the number is stated verbally, or entered through the keypad.

Cards can be stolen and numbers obtained by employees of businesses when the cards are used. The cards are vulnerable in that they can easily be copied. While card transactions are routinely checked via the public network against lists of valid and stolen card numbers, fraud is widespread. Many individuals find it expedient or necessary to carry several different bank, credit, travel and calling cards. Each may have its own unique PIN. Individuals, unable to memorize several different PINs, write them down and carry them, allowing both the PIN and card to be stolen.

"Smart cards," which contain integrated circuits on a small card somewhat similar to a credit card in size offer the prospect of strong personal authentication. Haykin [HAYK 88] provides an introduction to smart card technology, which is evolving rapidly. The authentication card would be issued by a certification authority to a person and might include a certificate signed by the authority, giving the privileges of the person, and perhaps containing personal identification information, or even an image of the person. The person's private key would be stored on the card and the card would be designed to prevent it from being read directly. Logic to perform a one way hash function to check a personal password might also be contained on the card.

If a standard for such cards were adopted, interfaces to the cards could be built into ISDN terminals and other equipment, such as personal computers, requiring user authentication. The card could be used as an unforgable authentication token. If personal identification information were included in the certificate, then sales personnel could compare the user with the information. As further a check against stolen cards, the user might be required to furnish a password to activate the authentication.

While universal, standardized strong personal authentication would make a dramatic contribution to ISDN security, the topic transcends ISDN and the communications industry. It involves the financial, banking, retail and service industries, and has profound social implications. An authority (or multiple authorities) must be recognized to issue certificates. A widespread standard for strong personal authentication could be a major social issue and could easily be viewed as a sort of national identity card.

4.5 Access Control Service

Access control in the context of a communication network such as ISDN is not quite as complex as it is in the context of distributed computer systems, since a network does not store data beyond that required for its operation. There are three principal access control concerns for ISDN security:

- Network access
- Terminal or CPE access
- Access to network data bases

The ISDN access control issue is, is the user authorized to use the network or a particular network service? For example, is the user authorized to place a long distance call, an international call, or, perhaps, a secure call? In the case of an installation with ISDN PBX, the PBX can enforce user access control checks. While standards are not necessary for such services in PBX's, without them terminal interchangability might be poor. The simplest solution is to bind the access privileges to the terminal. This changes the access control problem to one of controlling access to terminals.

In the context of the public network, the problem is more complex. There is no good personal authentication standard. It is reasonable to expect that service providers might eventually offer some sort of password protection for specific services. This would probably not provide strong protection, but might, for example, suffice to prevent children from making long distance calls or from calling 900 numbers. Indeed it is possible that carriers may be forced by PUCs or legislation to provide some sort of access control, particularly in the context of controlling access to sexually oriented 900 services.

Terminals can have both inward and outward access controls. With outward access controls the issue is, may the user place a particular type of call (based upon its service class or destination) from the terminal? With inward access controls the issue is, is the caller authorized to call this terminal?

Outward access controls can be readily built into terminals, with or without standards. Some sort of token or password may be required to use a terminal. If this is done, and there is some sort of authentication of the terminal to the switch, or if it is physically difficult for an intruder to exchange his terminal for a controlled terminal on a particular line, then network access controls based on binding privileges to specific lines may be extended to the user layer. Even if there are no network access limitations on a line, a terminal with built in access controls may prevent use of that terminal by unauthorized individuals.

Inward access controls require standards. The only present useful standardized ISDN service is the Calling Line ID supplementary service. Terminals (or PBX's) could refuse to accept calls from any number other than those specifically authorized. This should be thought of more as a screening mechanism than a strong access control, since it is not built upon strong authentication.

Control of access to the network databases (including databases maintained by PBXs) is vital. The subject is complex and largely beyond the scope of this report. Databases containing records of calls are confidential and unauthorized users must be prevented from accessing them. Databases maintained for routing and the management or maintenance of the network must be protected from unauthorized modification. An intruder might either modify them to perpetrate a fraud (for example by deflecting calls from their proper destination) or to disrupt the operation of the network.

Effective access control requires effective authentication. The primary need, then, to enable access control, is standards for effective authentication. If a standard system for strong personal authentication were adopted, for example using smart card technology, identification and authentication could be separated from privileges, or provision could be made to bind all privileges in one card. Including privileges (*e. g.*, a credit limit of a certain amount) with authentication in one card would simplify exercising those privileges, since no check with any remote authority would be required. However, since privileges may change rapidly, it would be more secure to separate privileges from authentication, and maintain them in a secure database. ECMA 138 proposes such a mechanism for Privilege Attribute Certificates.

4.6 Security Services From ECMA-138 for ISDN

In addition to the five security services of ISO 7598-2, it is useful to consider extending the services for ISDN to adopt concepts introduced in ECMA 138. As stated in section 4.2 above, ECMA 138 deals with Authentication and Access Control in the broad context of distributed computer systems. ECMA 138 articulates the concept of a Privilege Attribute Certificate (PAC) as well as a Security Attribute service and an Interdomain service, which provide an approach to addressing Access Control and Authentication.

ECMA expands the Directory Certificates, used only for public keys, to PACs which contain additional security attributes. ECMA 138 does not consider the X.400 Directory to be sufficiently secure for PACs. ECMA 138 also considers interworking between different security domains and postulates a Security Attribute Service, which maps or translates attributes for labelled objects and an Interdomain Service, which is trusted to translate PACs between domains and reseal them.

In general, ECMA go well beyond what is ordinarily thought of as communications security. However it has application to two specific problems in ISDN:

- ISDN network database access control, which in a public network is a serious and difficult problem.
- Interdomain security interworking, which is also a serious concern for a public network. It is also essentially a research subject at this point, in any general context.

ECMA 138 also explicitly recognizes that, to maintain security, security information must be collected and defines a Security Audit Information Service. This service automatically records security-related events. For example any access or attempt to access the databases maintained by the network itself is a security-related event. In principle, any use of the network is potentially security-related, however privacy concerns will require that suitable criteria be developed for screening the events to be recorded in a public network, and only the time, parties and network services utilized will probably be recorded (which are needed for billing as well).

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.

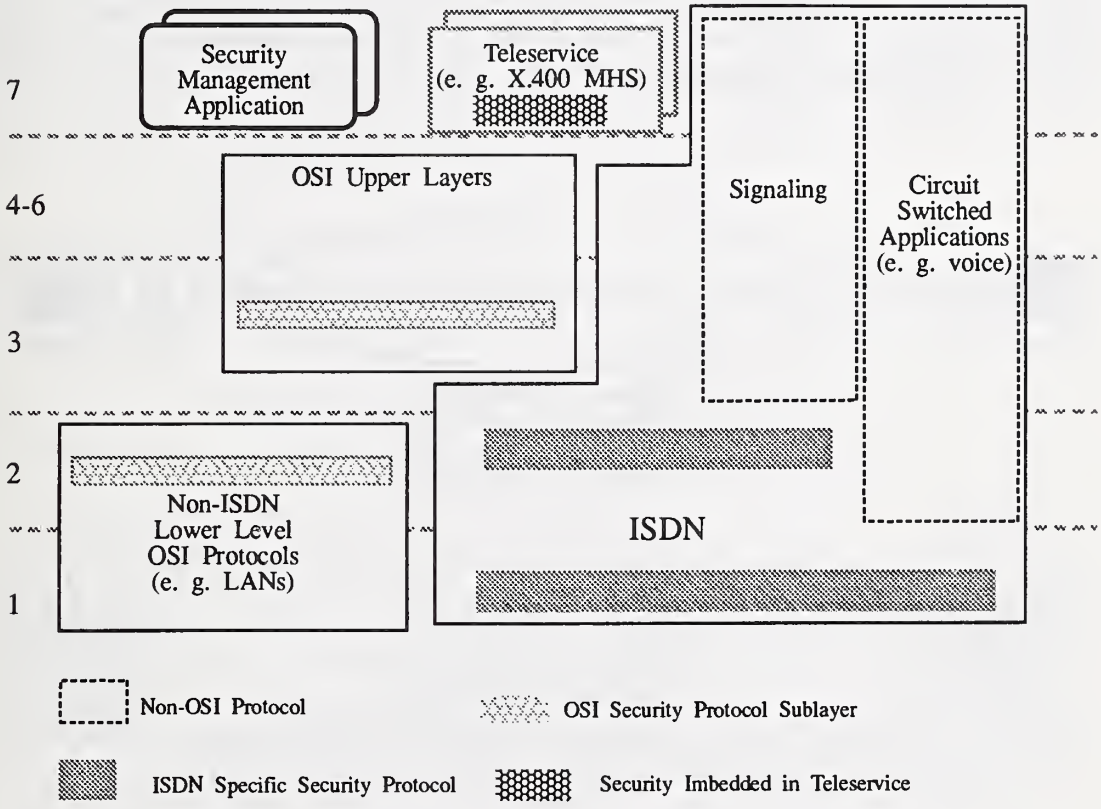

7
4-6
3
2
1
Security Management Application
Teleservice (e. g. X.400 MHS)
OSI Upper Layers
Signaling
Circuit Switched Applications (e. g. voice)
Non-ISDN Lower Level OSI Protocols (e. g. LANs)
ISDN
Non-OSI Protocol
OSI Security Protocol Sublayer
ISDN Specific Security Protocol
Security Imbedded in Teleservice

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.

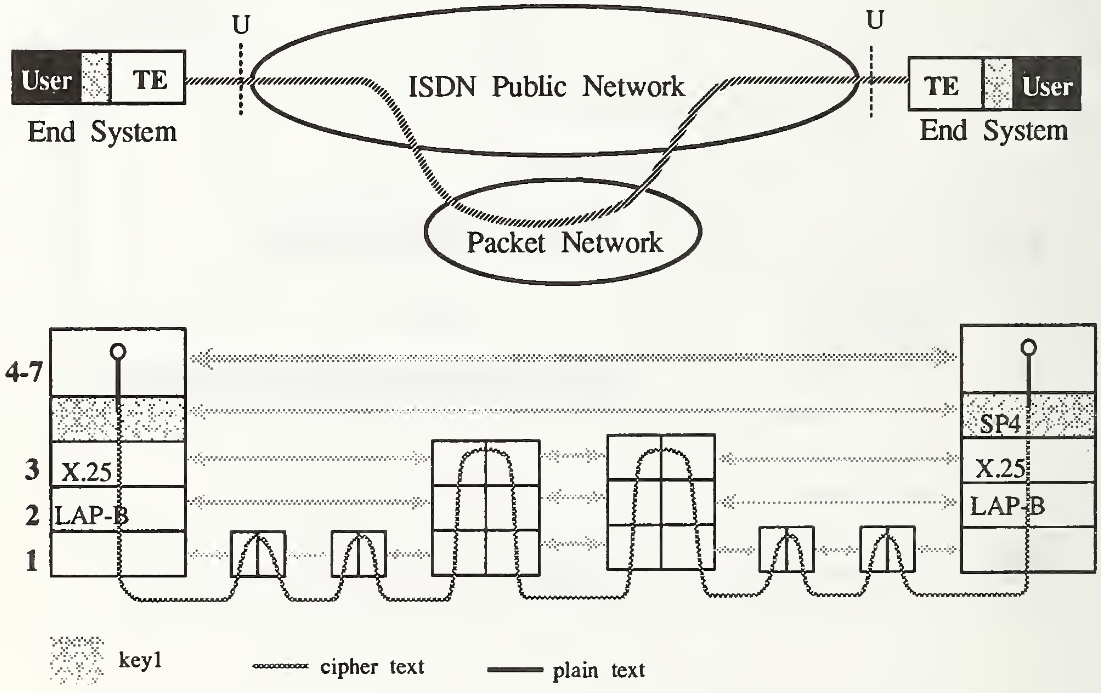


Figure 15 - Transport Layer End-to-End Encryption.

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

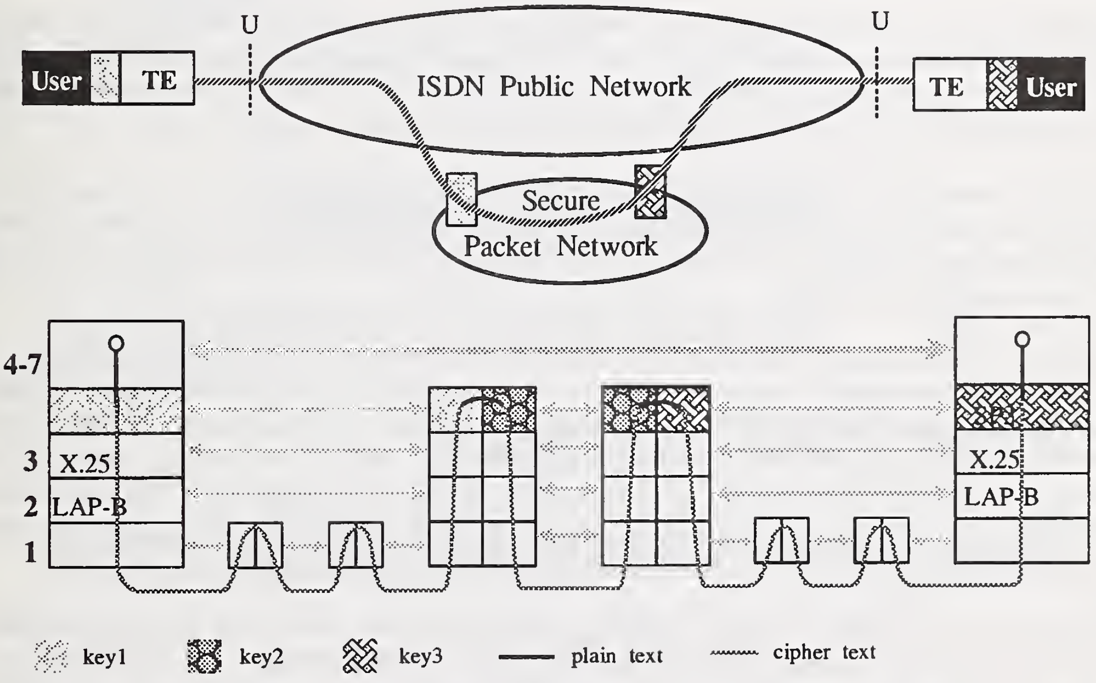


Figure 16 - Network Layer Packet Encryption.

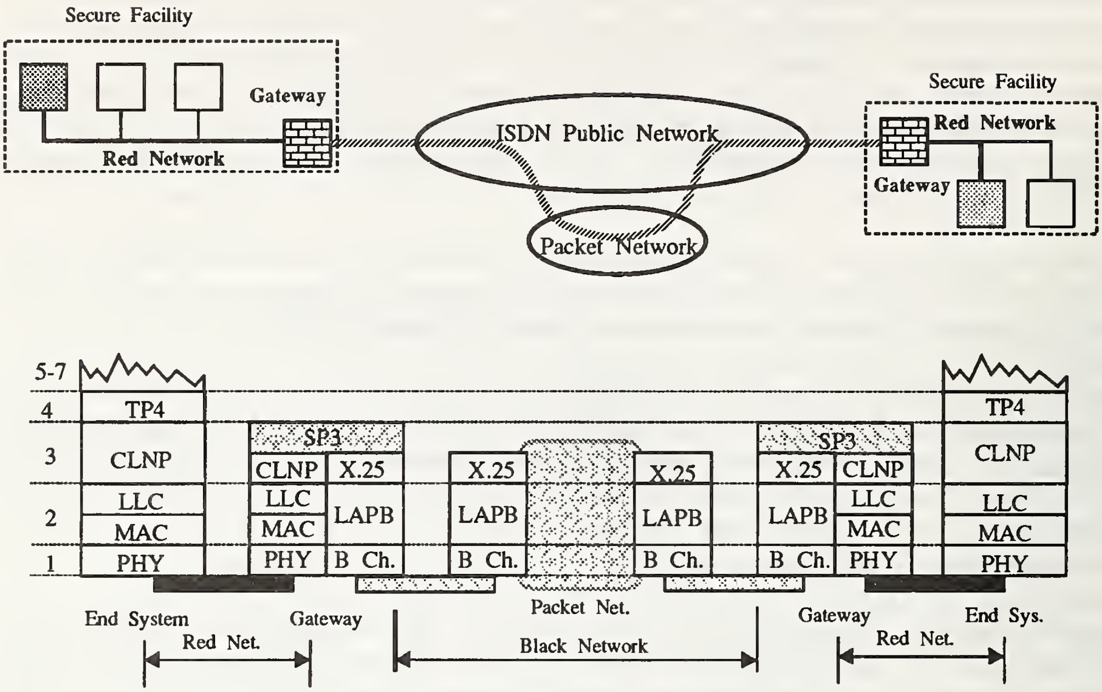


Figure 17 - Network Layer Packet Encryption.

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.

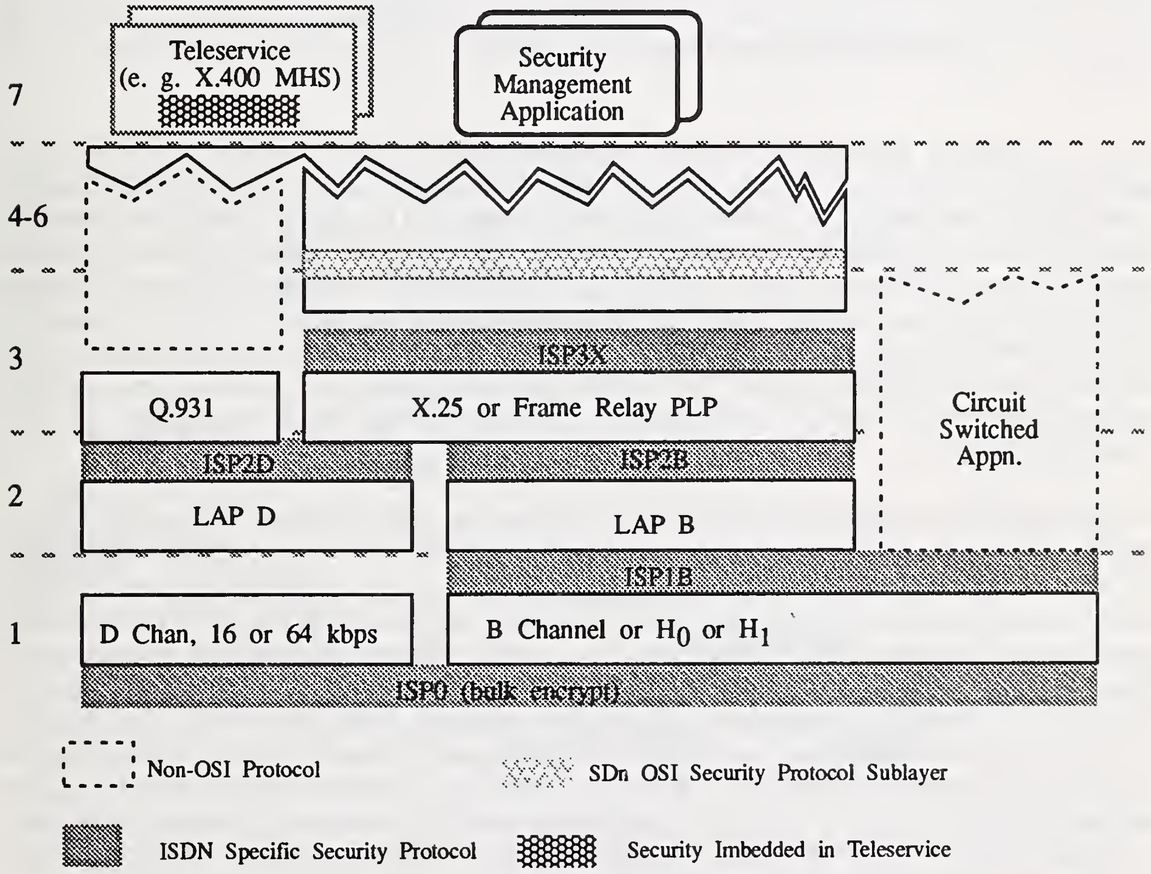


Figure 18 - Potential ISDN-Specific Security Protocols.

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.

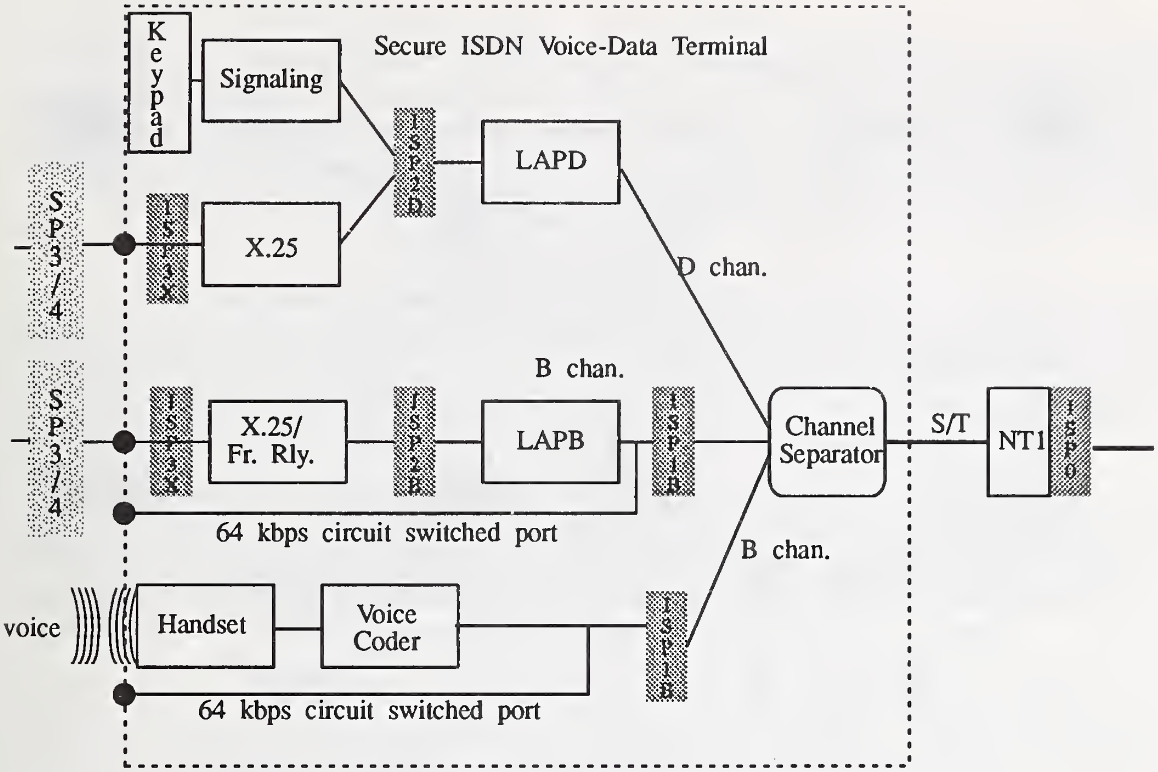


Figure 19 - Secure ISDN Terminal Block Diagram.

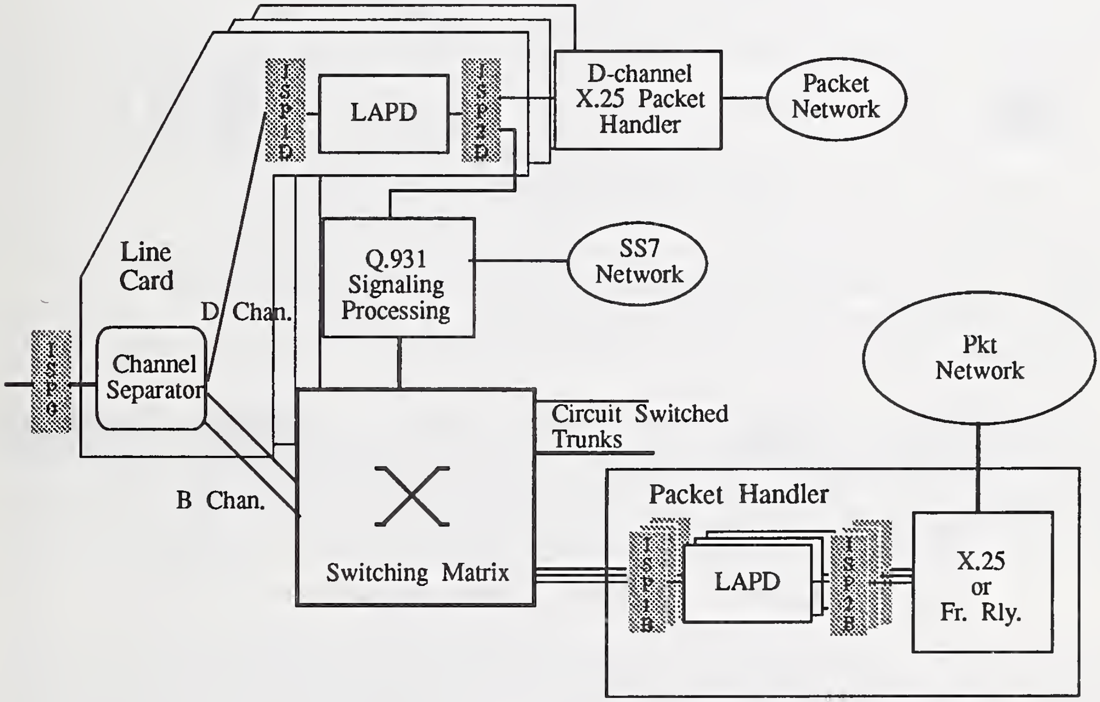


Figure 20 - Secure ISDN Switch Block Diagram.

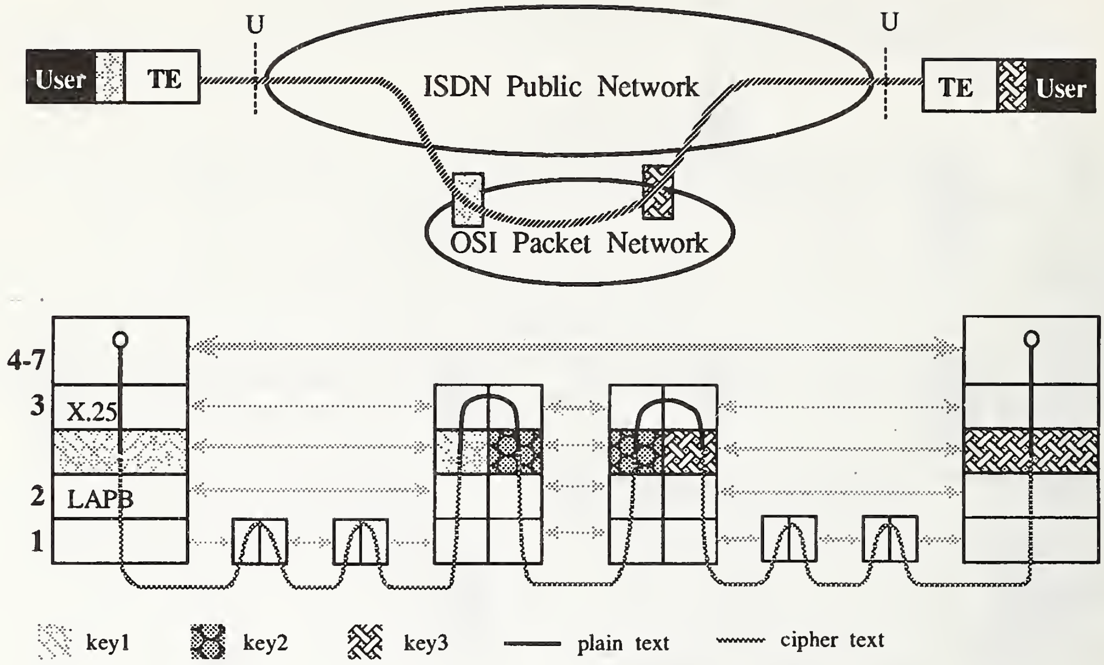


Figure 21 - Data Link Layer Packet Encryption.

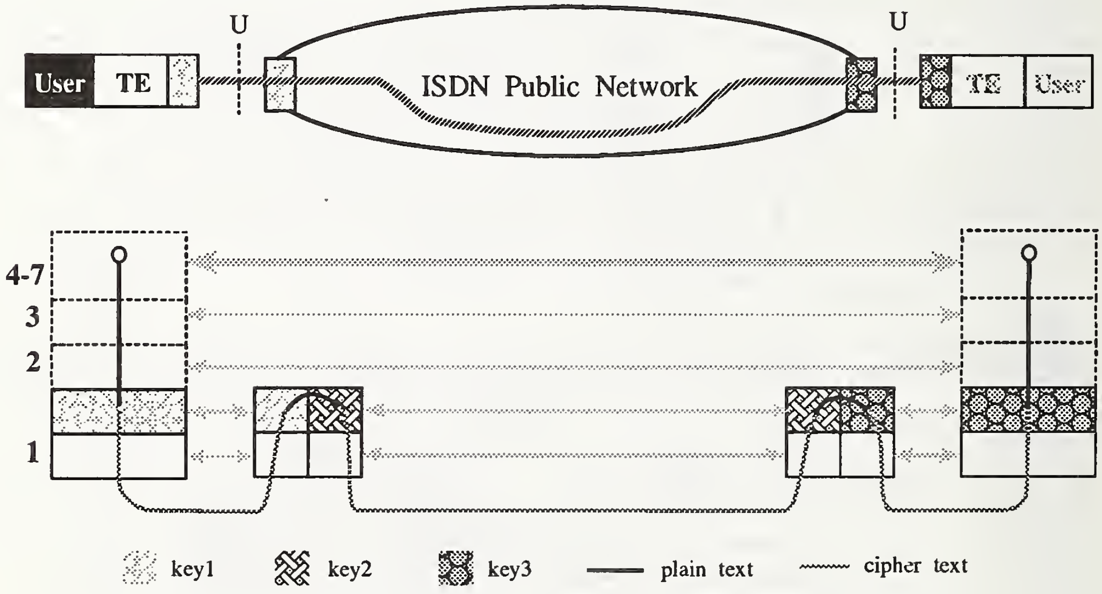


Figure 22 - TE to Network Physical Layer Encryption.

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

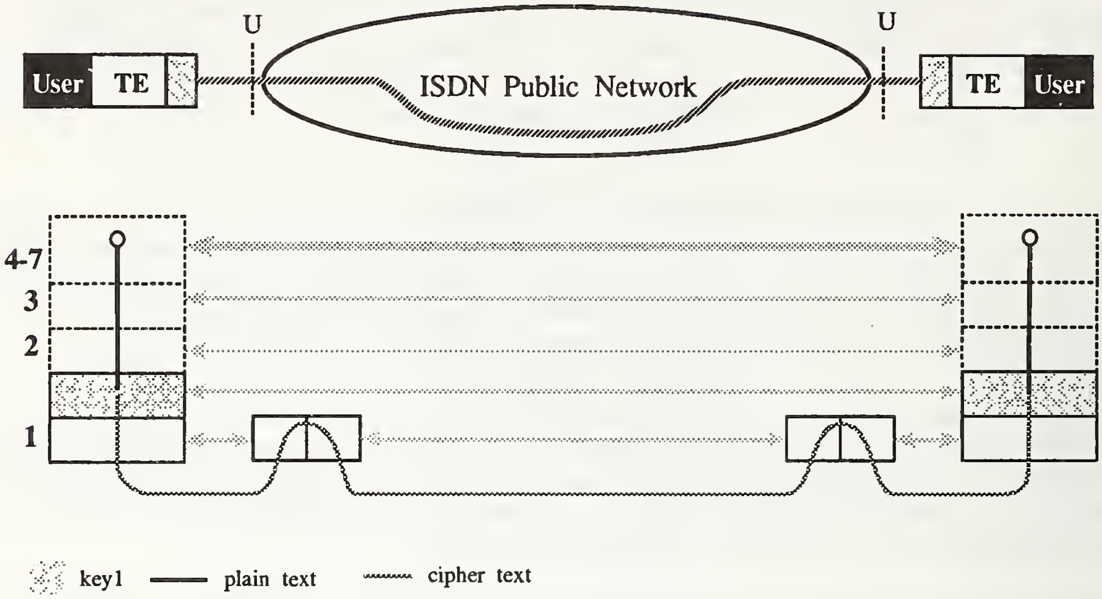


Figure 23 - TE to TE Physical Layer Encryption.

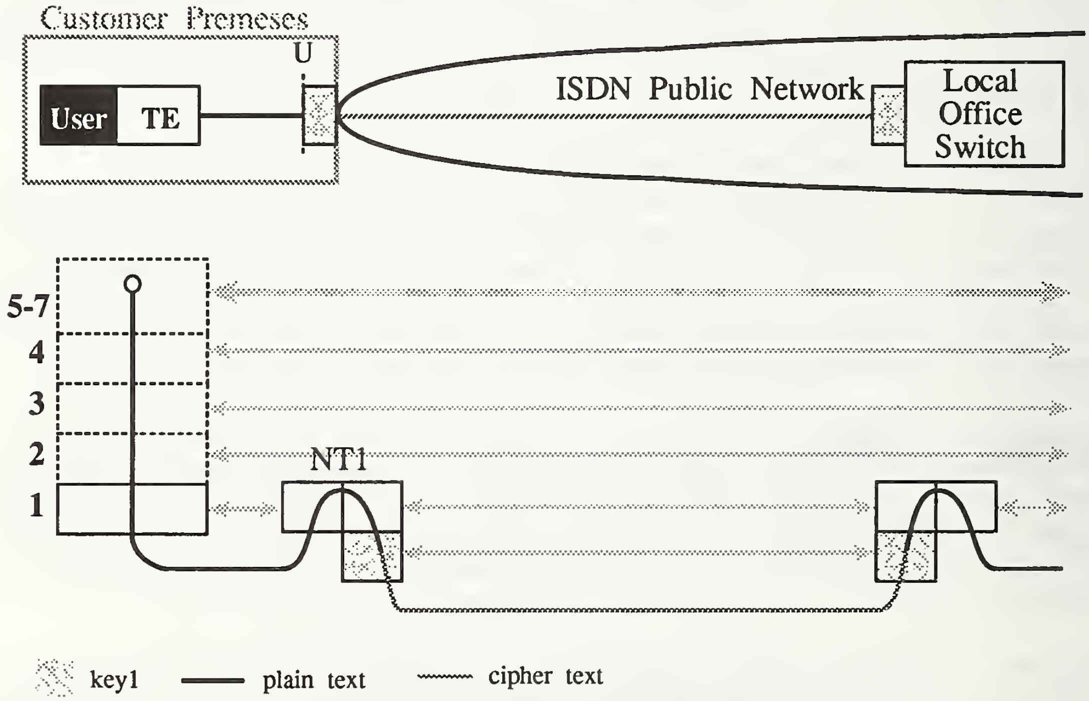


Figure 24 - NT1 to Local Office Link Encryption.

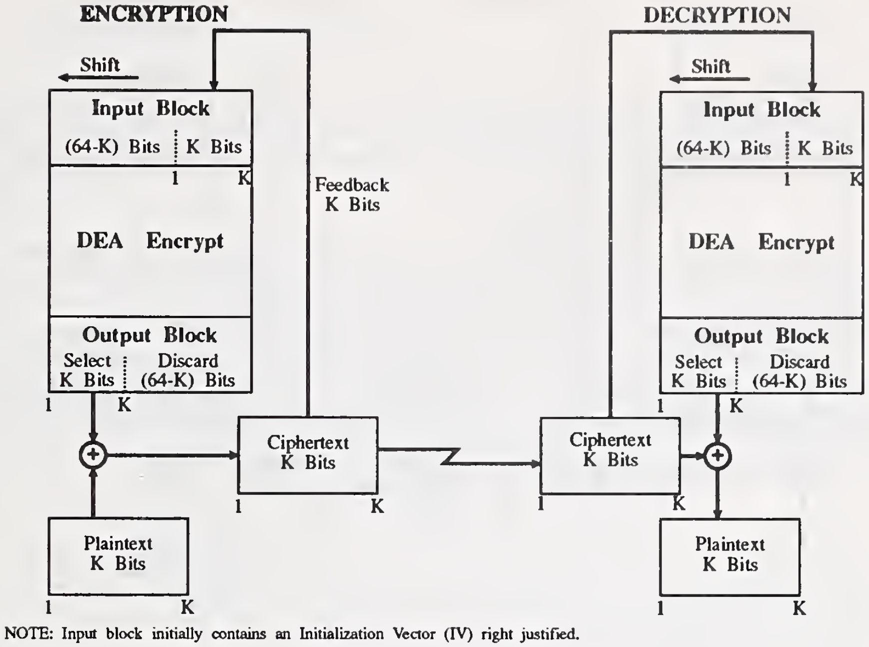


Figure 25 - DES K-bit Cipher Feedback (CFB) Mode .

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.

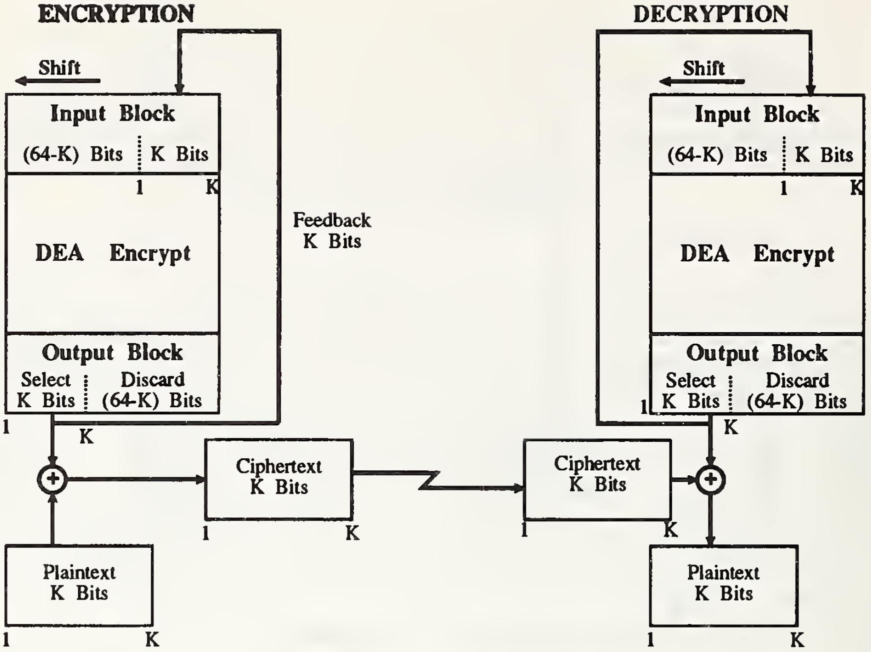


Figure 26 - DES K-bit Output Feedback (OFB) Mode.

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.

6. Placement of ISDN Security Services

Figure 27 illustrates the possible ISDN security interactions. In this illustration a user may be either an Application layer computer process or an actual human user. The TE or terminal is the initial point of connection to the ISDN network. Users may be associated with a particular TE, or they may be mobile. The TE may be connected directly to the public ISDN network, or through an NT2 (typically a PBX). The TE and NT2 are collectively *Customer Premises Equipment (CPE). Specialized Security Applications (SSA)* are connected to the users through the public network.

6.1 User-to-CPE

The primary user-to-CPE security interaction is authentication and access control. If privileges are to be bound to specific lines and terminals, then access to the terminals must be controlled. In some cases this may be by physical control of access to the terminal, but in most cases it will require that authentication and access control be built into the terminal or the PBX, or both.

A significant advantage of authentication and access control at this layer is that broad standards are not necessarily required. Access control could be built into a terminal by requiring a personal token and perhaps a password to activate the terminal. This could be done as a proprietary feature of the terminal.

A weakness in access control which is confined to a terminal is that an intruder might physically remove the protected terminal and substitute his own terminal. Therefore for strong access control it should extend to the next layer of the network hierarchy, either to the PBX or to the public network. The terminal should be required to authenticate to the PBX or public network. Where terminal or user authentication is implemented in a PBX, standards are not strictly necessary, however without standards secure terminals will not be portable with different PBXs. At the

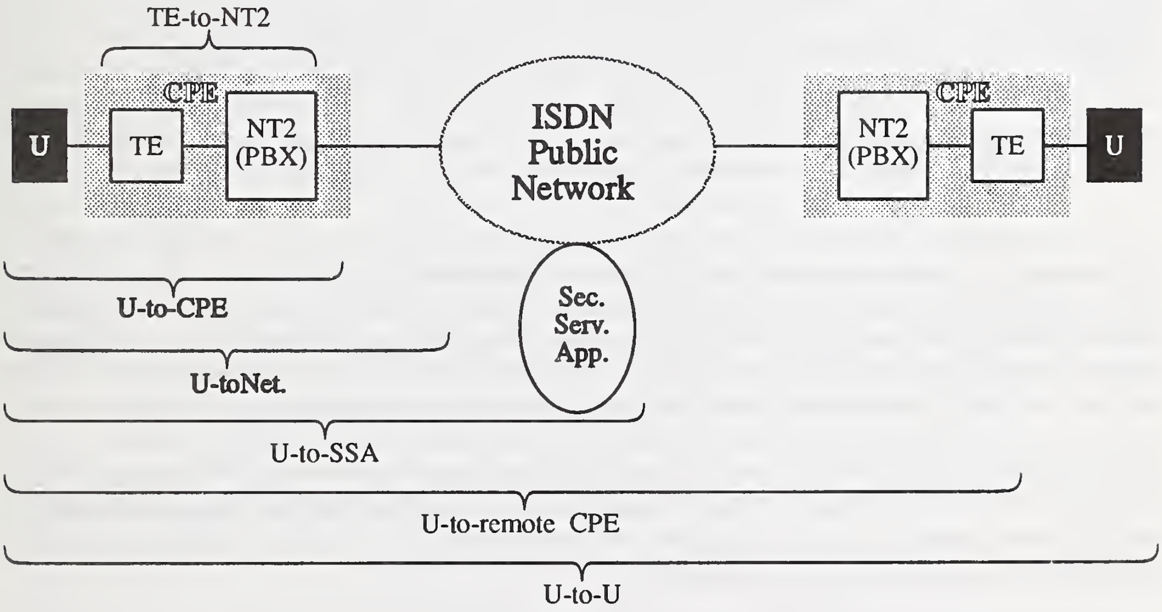


Figure 27 - Diagram of ISDN Security Interactions.

present time, ISDN PBXs typically implement many proprietary features, and terminal portability is more a pious sentiment, than a reality, in the PBX environment.

Security audit information could also be collected in CPE. If users authenticate before using a terminal, then a record of the user who placed each call would be appropriate security audit information in a highly secure environment.

6.2 User-to-Network

For the purpose of this discussion, and subsequent sections it is not necessary to distinguish between the user and the CPE. To the extent required, the user is assumed to authenticate himself to the CPE, to have passed whatever access controls are required by the CPE. For security purposes the user and CPE are bound together.

The primary user-to-network security functions, if implemented, would be authentication and access control. In this case standards would clearly be required. Significant enhancements would be needed in public network switches to implement user authentication. In the context of the public network, the primary access control consideration would be user access to network services, such as 900 or long distance. Such access control services might be offered to subscribers to prevent unauthorized use of business phones or to prevent children from making inappropriate use of home telephones.

Unless forced to do so by regulatory agencies or legislation (for example to prevent children from calling sexually oriented telephone services), the implementation of access control features is a business issue for service providers. Would a business oriented centrex authentication and access control feature generate significant additional revenues for public network service providers? It might eventually be necessary for public networks to offer such centrex services to compete with similar services offered by PBX vendors, even if the direct extra revenues for these services did not pay for their provisioning.

Public network service providers may also be motivated to provide improved authentication for the use of telephone calling cards to reduce fraud. This, again, is a business issue, and may be resolved only in the broader context of personal identification for all credit and financial transactions. Also, to the extent that public networks allow dial up access to sensitive resources and databases, and to operational and maintenance facilities, improved authentication standards could make a significant reduction to network vulnerability to fraud and denial of service attacks.

It is reasonable to expect that carriers will eventually encrypt most trunks, and may reasonably be expected to offer secure routing to major users who require it. User to network local office (ISP1 or ISP0 layer) services are more problematic, and will depend upon the development of suitable switch line cards and software to manage them. Encryption at this layer provides a degree of traffic flow confidentiality which is difficult to achieve otherwise, but it is not likely that there will be a large market for this service, and it may not be commercially viable.

The principal presently defined user-to-network service, which will be used for security, is the Calling Line ID. In the absence of better authentication, it will be used for this purpose and for inward access control. There is a danger that this relatively weak feature will be too heavily relied upon, because it is what is available.

In general, ISDN standards will be required to support user-to-network security, or any other user-to-network service.

6.3 User-to-SSA

A large variety of User-to-Security Service Application (SSA) interactions may eventually result. The major ones will probably be for key distribution, authentication, and access control, where the SSA will be a trusted third party which supplies PACS or verifies security attributes. Others may offer notarization services, secure conversion services (*i. e.*, conversion of secure analog to secure ISDN digital voice), or secure mail services.

Standards will be necessary to make most user to SSA functions practical. Since the SSA usually provides a trusted functionality, authentication standards will be necessary for most SSA applications.

6.4 User-to-User

A great many ISDN security services will be implemented primarily on a user-to-user basis, perhaps with the assistance of an SSA for authentication or access control. There are three principal reasons for this:

- The public ISDN network is ponderous and evolves slowly. The provisioning of security functions in the network may not offer service providers a strong return on the investment required. Although ISDN services are only just beginning to become available from the nation's public networks, there is already a huge investment in ISDN compatible switching equipment which does not incorporate security. While some security features might be incorporated as software changes to the switches, such changes require years to design, code, test and deploy. Hardware changes are even more difficult. At this point user investment in ISDN is minor, but current service provider investment is significant.
- User-to-user security is transparent to the network, and can be implemented by users where and as needed, much more quickly than features or services can be added to the network.
- Many security concerns are essentially end-to-end concerns and it is desirable that only the end entities need participate in the security and be trusted. Several networks and service providers may be involved in a secure communication and it would be difficult to be assured of consistent security and trust except on a user-to-user basis.

Authentication, access control and confidentiality are all likely to be addressed primarily on a user-to-user basis, with assistance in some cases from an SSA or the network. For example, if traffic flow confidentiality is required, then user-to-network services are required.

In a strict sense, standards are not absolutely required for user-to-user services. For some applications, there could be proprietary secure terminals. This would be quite undesirable, and standards will be needed to develop a large commodity market for secure terminals, and allow users to communicate securely with all users with secure terminals, rather than with just those with the same brand or model. However, except for certain specific ISDN related functions, such as circuit switched services, the standards do not necessarily have to be specifically ISDN standards. Broader, OSI oriented security standards will suffice for many data applications which use ISDN for some or all of the low layer data transport.

7. Standards Needed for ISDN Security

ISDN has been under development for many years and has been the subject of many standards activities. However, there presently are no standards specifically for ISDN security and few are in development. In contrast, the OSI community is actively pursuing standards for OSI security. When the ISDN is used as a transport mechanism for OSI traffic, then these standards are applicable and should be reviewed for their adequacy in the ISDN environment. However, many ISDN applications and the ISDN itself may require specific security provisions that are not available in the OSI family of standards. This section outlines where security standards are needed for ISDN and discusses possible inputs and alternatives for the needed standards as well as applicable standards under development.

7.1 ISDN-Specific Standards

ISDN has been depicted as both a data communication system and a broader set of applications which utilize that system. In addition, OSI has been presented as an architecture for communicating among peer end computer systems that may utilize the ISDN data communication system. The section deals with security standards that are specific to either of the two areas of ISDN outside OSI.

7.1.1 ISDN Security Architecture

The first standard that is needed in ISDN security is a security architecture. This report discusses the issues which need to be addressed and where standards are needed. The architecture standard should select which alternatives to be developed as standards. The architecture should support many security policies and would not dictate what policy would be followed. The architecture should be more specific than this report but still would not specify which security services and facilities are to be implemented in products. Security service and protocol specification standards would be needed to provide these specifications.

7.1.2 ISDN Communication System Security Services

A standard is needed that specifies how security services would be provided in the ISDN communication system. The architecture would specify what services are required and where they would be offered and would dictate the scope of this standard.

7.1.3 ISDN Communication System Security Protocols

In section 7.1.2, several possible ISDN-specific security protocols are specified and discussed. There is an urgent need for at least one of these. A simple physical layer confidentiality protocol operating on any circuit switched ISDN channel octet stream using intra-channel security set-up signaling (called ISP1B in sec. 7.1.2) is clearly required. The protocol should support any circuit rate defined in ISDN (*i. e.*, B channel, Primary rate, H_0 and H_1) and provide confidentiality protection, including partial traffic flow confidentiality, for any use of the channel, including voice, data, video and facsimile. The protocol must allow for the separate specification cryptographic algorithms.

7.1.4 ISDN Application Security Services

There are a number of ISDN applications for which specific security standards are needed. Some of these overlap with OSI applications such as electronic mail, electronic data interchange and file transfer. The OSI security standards can be utilized for equivalent ISDN applications.

ISDN specific applications, such as voice conferencing, require special security services and special security protocols. A secure, or trusted, conference bridge would be needed to allow a number of parties, each with a secure voice terminal (i.e., implementing the ISP1B protocol), to hold a secure conference call. Voice and video conferences share some characteristics but will probably require different specific security services and definitely require different protocols.

Transition plans will be required when converting from secure analog telephone services to secure digital ISDN services. The basic security service of confidentiality of the voice transmission will be the same but many supplemental voice services in ISDN will require special security services and mechanisms. Call forwarding will require new and innovative security standards for authentication and supporting key management. There are now a large number of secure telephones (STU III) that use digital encryption of a compressed speech signal that will require some standard interface to ISDN uncompressed digital speech.

Needed application security services include authentication and non-repudiation as well as large granularity access control. Security support services would include key management, auditing and security fault recovery. While these may be the same as Application layer OSI security services, standards for implementing and supporting the services in an ISDN environment may be necessary. Authentication is a particularly difficult and important problem in the public ISDN network. A universal means of strong personal authentication is badly needed in the public network.

7.1.5 ISDN Application Security Protocols

The application specific security service standards outlined above will require security protocol standards between communicating entities which support and provide the security services. For example, the access control service will require specific protocols to obtain or transmit the Personal Access Certificate containing identification, authentication and/or authorization information. Access control in public networks will require authentication protocols for performing identity based access control. Access control in closed or classified networks will require these plus clearance (need-to-know) information for making rule-based access control decisions. Access control may be on outbound connections (to prevent children from accessing undesired advertising or pornographic services) or on inbound connections (to prevent unauthorized connections to classified computer systems or voice terminals).

In addition to application specific security protocols, security support service protocols are needed. Key management is a prime example. Protocols are required to make initial connections to Key Management Centers to obtain initial or seed key after proper authentication is performed. Signature Certificates are required in addition to seed key in commercial applications. Security officer (crypto custodian) protocols are required to manage the distributed security features in an ISDN environment.

7.2 Standard Security Mechanisms Required for ISDN

A number of security mechanisms standards are needed for ISDN but need not be specific to ISDN. The OSI standards developed to provide the security mechanisms defined in IS 7498/2 should be utilized to the maximum extent possible. Specific security mechanisms are the subject of standards development efforts of the new JTC1/SC27. The following sections provide a brief overview of these security mechanisms.

7.2.1 Cryptographic Algorithms

While not the subject of international standardization, cryptographic algorithms of several types are required for ISDN. First, data encipherment algorithms are required to provide confidentiality protection to user and management data. Second, cryptographic based key establishment or distribution algorithms are needed to establish a data encipherment key wherever necessary.

Third, cryptographic based digital signature algorithms are needed for user and data authentication. Some of these algorithms may be the same to save implementation costs.

The Data Encryption Standard [FIPS 46] is presently the only recognized, publicly available standard for enciphering data and distributing keys. While able to perform data authentication and limited personal authentication, it is not satisfactory for signatures in open system environments. There is a need for digital public key signature algorithms and simpler key distribution is also possible with public key cryptographic techniques. In addition, new symmetric key algorithms may be necessary to support international commercial applications if DES devices are not exportable. These new algorithms may be faster when implemented in software or satisfy other special requirements.

7.2.2 Cryptographic Modes of Operation

Standard modes of operation must be available for each of the standard cryptographic algorithms. Interoperability and security require using the same mode that has been approved for an application with the same algorithm.

7.2.3 Mobile User Key Token Standards

Personal authentication and data protection standards will rely on cryptographic methods which require a personal key for signatures and data protection. Standard key carriers, token, "smart cards," etc. are required to support a mobile user seeking access to a secure distributed systems from ultiple locations. Several ANSI and ISO standards activities are addressing standard tokens that may be used to access control and data protection keys. The STU III telephone uses a standard token (DATAKEY) to hold a cryptographic key but can only be used with a limited number of telephone terminals.

References

[BOCK 88] Peter Bocker, *ISDN The Integrated Services Digital Network Concepts, Methods, Systems*, Berlin, Springer-Verlag, 1988.

[DIFF 76] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory*, vol. IT-22, pp. 644-654, Nov. 1976.

[DOD 5200] Department of Defense Standard DOD 5200.28-STD, *Department of Defense Trusted Computer System Evaluation Criteria*, December 1985.

[ECMA 138] ECMA-138, *Security in Open Systems Data Elements and Service Definitions*, European Computer Manufacturers Association, Geneva, Dec. 1989.

[ECMA TR/46] ECMA TR/46, *Security In Open Systems, A Security Framework*, European Computer Manufacturers Association, Geneva, 1988.

[ECON 90] "Telecommunications Survey", *The Economist*, vol. 314, no. 7645, March 10, 1990., pp. SURVEY 33.

[FIPS 46] FIPS PUB 46-1, *Data Encryption Standard (DES)*, NBS, 1977.

[FIPS 81] FIPS PUB 81, *DES Modes of Operation*, NBS, 1980.

[FIPS 74] FIPS PUB 74 *Guidelines for Implementing and Using the NBS Data Encryption Algorithm*, NIST, 1980.

[FIPS 140-1] DRAFT FIPS PUB 140-1, *Security Requirements of Cryptographic Modules (DRAFT)*, NIST, July 13, 1990

[FIPS 146] FIPS PUB 146-1, *Government Open Systems Interconnection Profile (GOSIP)*, Version 2.0, NIST, October 1990.

[HAYK 88] Martha E. Haykin and Robert B. Warner, *Smart Card Technology: New Methods for Computer Access Control*, NIST Special Publication 500-157, 1988

[I.100] CCITT Recommendation I.100, *Preamble and General Structure of I-Series Recommendations*, 1988.

[I.320] Recommendation I.320, *ISDN Protocol Reference Model*, CCITT, 1988.

[I.324] Recommendation I.324, *ISDN Protocol Reference Model*, CCITT, 1988.

[ISO 7498] ISO 7498, *Information Processing Systems - Open System Interconnection - Basic Reference Model*, International Standards Organization, Geneva, 1984.

[ISO 7498-2] ISO 7498-2-1988(E), *International Standard Security Architecture*, International Standards Organization, Geneva, 1988.

[ISO 7776] ISO 7776:1986, *Information Processing Systems - Data Communications - High-Level Data Link Control Procedures - Description of the X.25 LAPB Compatible DTE Data Link Control Procedures*, International Standards Organization, Geneva, 1986.

[ISO 8073] ISO 8073:1984, *Information Technology - Open Systems Interconnection - Transport Protocol Specification,* International Standards Organization, Geneva.

[[ISO 8208] ISO 8208:1987, *Information Processing Systems - Data Communications - X.25 Packet Level Protocol for Data Terminal Equipment*, International Standards Organization, Geneva, 1987.

[ISO 9594-8] ISO/IEC 9594-8, *Information Technology - Open Systems Interconnection - The directory - Part 8: Authentication Framework,* International Standards Organization, Geneva.

[JTC1 1] ISO/IEC JT1/SC 21 N 4207, DPxxxx-2, *Information Processing Systems - Security Frameworks for Open Systems - Part 2: Authentication Framework*, draft standard dated Dec 12, 1989.

[MIYA 88] Shoji Miyaguchi, Akira Shiraishi and Akihiro Shimizu, "Fast Data Encipherment Algorithm FEAL-8," *Review of the Electrical Communications Laboratories*, Nippon Telegraph and Telephone Corporation, vol.36, no. 4, 1988, pp.433-437.

[P802.10] IEEE P802.10, *Standard for Interoperable Local Area Network (LAN) Security, Part A - The Model*, Unapproved Draft, December 9, 1989.

[Q.931] CCITT Recommendation Q.931, "ISDN user-network interface layer 3 specification, " *Blue Book*, 1988.

[RIVE 90] R. Rivest, A. Shamir and L. Adleman, "A method for obtaining digital signatures and public key cryptosystems," *Communications of the ACM*, vol. 21, no. 2, pp. 120-126, Feb. 1978.

[SDN.301] Specification SDN.301, *SDNS Secure Data Network System Security Protocol 3 (SP3)*, Revision 1.5, 1989-05-15, reprinted in NISTIR 90-4250, *Secure Data Network System (SDNS) Network, Transport, and Message Security Protocols*, National Institute of Standards and Technology, February 1990.

[SDN.401] Specification SDN.401, *SDNS Secure Network Systems Security Protocol 4 (SP4)*, Revision 1.3, 1989-05-02, reprinted in NISTIR 90-4250, *Secure Data Network System (SDNS) Network, Transport, and Message Security Protocols*, National Institute of Standards and Technology, February 1990.

[STAL 89] William Stallings, *ISDN: An Introduction*, New York, Macmillan, 1989.

[T1.607] T1.607-1990, *American National Standard for Telecommunications - Digital Subscriber Signalling System NO.1 - Layer 3 Signalling Specification for Circuit Switched Bearer Service*, ANSI, 1990. (USA national standard corresponding to [Q.931].)

[VERM 90] Pramode K. Verma, ed., *ISDN Systems, Architecture, Technology and Applications*, Englewood Cliffs, NJ, Prentice Hall, 1990.

[X.25] Recommendation X.25, "Interface between Data Terminal Equipment (DTE) and Data Circuit-Terminating Equipment (DCE) for Terminals Operating in the Packet Mode and Connected to Public Data Networks by Dedicated Circuit," *Blue Book*, ITU, 1988.

Abbreviations and Acronyms

This appendix contains a list of the abbreviations and acronyms. At the end of most of the entries is a note enclosed in [], pointing to the origin or identifying the general context where the acronym is used. "[TEL]" indicates jargon in general use in the United States telephone industry. In many cases the note refers to another acronym in the list.

ANI	Automatic Number Identification [TEL]
ANSI	American National Standards Institute [Standards Body]
BRI	Basic Rate Interface [ISDN]
BER	Bit Error Rate
CCITT	International Telegraph and Telephone Consultative Committee [Standards Body / ITU]
CFB	Cipher Feedback [DES Mode of Operation]
CLNP	Connectionless Network Protocol [CLNP]
CPE	Customer Premises Equipment [Telephone]
DCA	Defense Communications Agency [U. S. Department of Defense]
DCE	Data Communications Equipment [X.25]
DES	Data Encryption Standard [FIPS 46]
DIB	Directory Information Base [X.500]
DIS	Draft International Standard [ISO]
DTE	Data Terminal Equipment [X.25]
ECMA	European Computer Manufacturers Association [Standards Body]
ECSA	Exchange Carriers Standards Association [Standards Body / Trade Association]
FCS	Frame Check Sequence [X.25 / LAN]
FEAL-8	Fast Data Encipherment Algorithm FEAL-8 [Encryption Algorithm / MIYA 88]
FIPS	Federal Information Processing Standard [NIST]
FTAM	File Transfer, Access and Management [ISO/CCITT, X.400]
GOSIP	Government Open Systems Implementation Profile [FIPS 146]
ICV	Integrity Check Value [SDNS]
IEEE P802	Institute for Electrical and Electronics Engineers Project 802 [LAN Standards Body]
IIW	ISDN Implementor's Workshop [NIUF]
ISDN	Integrated Services Digital Network [CCITT]
ISO	International Standards Organization [Standards Body]
ITU	International Telecommunications Union [Standards Body / Treaty Organization]
IUW	ISDN User's Workshop [NIUF]
LAN	Local Area Network [OSI/IEEE 802]
LAPB	Link Access Protocol B [ISDN]
LAPD	Link Access Protocol D [ISDN]
LLC	Logical Link Control [IEEE 802]

MAC	Medium Access Control [LAN]
MAN	Metropolitan Area Network [IEEE P802]
MHS	Message Handling System [ISO/CCITT X.500]
NIST	National Institute of Standards and Technology [U. S. Dept. of Commerce]
NIUF	North American ISDN User's Forum [Standards Workshop]
NSA	National Security Agency [U. S. Department of Defense]
NSAP	Network Service Access Point [OSI]
NSDU	Network Service Data Unit [OSI]
NT1	Network Termination 1 [ISDN]
NT2	Network Termination 2 [ISDN]
OFB	Output Feedback [DES Mode of Operation]
OSI	Open Systems Interconnection [ISO 7498]
OSS	Operation Support System [TEL]
PAC	Privilege Attribute Certificate [ECMA]
PAD	Packet Assembler Disassembler [X.25]
PABX	Private Access Branch Exchange [Telephone]
PBX	Private Branch Exchange [Telephone]
PDU	Protocol Data Unit [OSI]
PIN	Personal Identification Number
PLP	Packet Layer Protocol [X.25]
POTS	Plain Old Telephone Service [TEL]
PRI	Primary Rate Interface [ISDN]
PSDU	Protocol Service Data Units [OSI]
PTT	Postal, Telephone and Telegraph
RBOC	Regional Bell Operating Company [TEL]
RSA	Rivest, Shamir, Aldeman [Encryption Algorithm / RIVE 78]
SDE	Secure Data Exchange [SILS]
SDNS	Secure Data Network System [SDNS]
SILS	Standard for Local Area Network (LAN) Security [LAN]
SMAP	System Management Application Process [OSI]
SNAcP	Subnetwork Access Protocol [OSI]
SNICP	SubNetwork Independent Convergence Protocol [OSI]
SP3	Security Protocol 3 [SDNS]
SP4	Security Protocol 4 [SDNS]
SS7	Signaling System Seven [ISDN]
SSA	Specialized Security Application [This document]
TA	Terminal Adaptor [ISDN]
	Technical Advisory [Bellcore]

TCP/IP	Transport Control Protocol/Internet Protocol [widely used *de facto* standard layer 3 & 4 protocol suite]
TE	Terminal Equipment [ISDN]
TR	Technical Requirements [BELLCORE]
X.25	Packet Switched Protocol [ISO 8208, CCITT X.25]
WAN	Wide Area Network

* U.S. G.P.O.:1991-281-557:40046

NIST-114A
(REV. 3-90)

U.S. DEPARTMENT OF COMMERCE
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

BIBLIOGRAPHIC DATA SHEET

1. PUBLICATION OR REPORT NUMBER
NIST/SP-500/189

2. PERFORMING ORGANIZATION REPORT NUMBER

3. PUBLICATION DATE
September, 1991

4. TITLE AND SUBTITLE

Security in ISDN

5. AUTHOR(S)

William E. Burr

6. PERFORMING ORGANIZATION (IF JOINT OR OTHER THAN NIST, SEE INSTRUCTIONS)

U.S. DEPARTMENT OF COMMERCE
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
GAITHERSBURG, MD 20899

7. CONTRACT/GRANT NUMBER

8. TYPE OF REPORT AND PERIOD COVERED
Final

9. SPONSORING ORGANIZATION NAME AND COMPLETE ADDRESS (STREET, CITY, STATE, ZIP)

National Institute of Standards and Technology
Computer Systems Laboratory
Bldg. 225/Rm. A216
Gaithersburg, MD 20899

10. SUPPLEMENTARY NOTES

11. ABSTRACT (A 200-WORD OR LESS FACTUAL SUMMARY OF MOST SIGNIFICANT INFORMATION. IF DOCUMENT INCLUDES A SIGNIFICANT BIBLIOGRAPHY OR LITERATURE SURVEY, MENTION IT HERE.)

The Integrated Services Digital Network (ISDN) standards will provide worldwide digital communications service and will play a key role in the transition to electronic documents and business transactions. ISDN has been developed with little thought to security. ISDN security will become a pressing concern for both government and business. ISDN's digital nature facilitates adding security, but the deployment of ISDN in the public network is well under way and the present investment in ISDN equipment, as well as the commercial necessity to deploy ISDN in a timely manner, constrains how security features may be added. ISDN security standards should take advantage of, and be compatible with, emerging standards for Open Systems Interconnection (OSI) security. International Standard 7498-2 defines five security services for OSI: Confidentiality, Access Control, Authentication, Data Integrity and Non-repudiation. The challenge of ISDN security is to extend these concepts to all ISDN applications, including voice use of the public network. Terminal-to-terminal link encryption provides a powerful ISDN security mechanism, because of ISDN's ability to provide circuit switched connections throughout the world. A standard for the reliable authentication of human users is badly needed for ISDN security.

12. KEY WORDS (6 TO 12 ENTRIES; ALPHABETICAL ORDER; CAPITALIZE ONLY PROPER NAMES; AND SEPARATE KEY WORDS BY SEMICOLONS)

authentication; encryption; ISDN security; link encryption; network security; OSI security; public network security

13. AVAILABILITY

☒ UNLIMITED

□ FOR OFFICIAL DISTRIBUTION. DO NOT RELEASE TO NATIONAL TECHNICAL INFORMATION SERVICE (NTIS).

☒ ORDER FROM SUPERINTENDENT OF DOCUMENTS, U.S. GOVERNMENT PRINTING OFFICE, WASHINGTON, DC 20402.

☒ ORDER FROM NATIONAL TECHNICAL INFORMATION SERVICE (NTIS), SPRINGFIELD, VA 22161.

14. NUMBER OF PRINTED PAGES
76

15. PRICE

ELECTRONIC FORM

ANNOUNCEMENT OF NEW PUBLICATIONS ON COMPUTER SYSTEMS TECHNOLOGY

Superintendent of Documents
Government Printing Office
Washington, DC 20402

Dear Sir:

Please add my name to the announcement list of new publications to be issued in the series: National Institute of Standards and Technology Special Publication 500-.

Name ____

Company ____

Address ____

City ____________________ State ________________ Zip Code ____________

(Notification key N-503)

NIST Technical Publications

Periodical

Journal of Research of the National Institute of Standards and Technology—Reports NIST research and development in those disciplines of the physical and engineering sciences in which the Institute is active. These include physics, chemistry, engineering, mathematics, and computer sciences.

Papers cover a broad range of subjects, with major emphasis on measurement methodology and the basic technology underlying standardization. Also included from time to time are survey articles on topics closely related to the Institute's technical and scientific programs. Issued six times a year.

Nonperiodicals

Monographs—Major contributions to the technical literature on various subjects related to the Institute's scientific and technical activities.

Handbooks—Recommended codes of engineering and industrial practice (including safety codes) developed in cooperation with interested industries, professional organizations, and regulatory bodies.

Special Publications—Include proceedings of conferences sponsored by NIST, NIST annual reports, and other special publications appropriate to this grouping such as wall charts, pocket cards, and bibliographies.

Applied Mathematics Series—Mathematical tables, manuals, and studies of special interest to physicists, engineers, chemists, biologists, mathematicians, computer programmers, and others engaged in scientific and technical work.

National Standard Reference Data Series—Provides quantitative data on the physical and chemical properties of materials, compiled from the world's literature and critically evaluated. Developed under a worldwide program coordinated by NIST under the authority of the National Standard Data Act (Public Law 90-396). NOTE: The Journal of Physical and Chemical Reference Data (JPCRD) is published bi-monthly for NIST by the American Chemical Society (ACS) and the American Institute of Physics (AIP). Subscriptions, reprints, and supplements are available from ACS, 1155 Sixteenth St., NW., Washington, DC 20056.

Building Science Series—Disseminates technical information developed at the Institute on building materials, components, systems, and whole structures. The series presents research results, test methods, and performance criteria related to the structural and environmental functions and the durability and safety characteristics of building elements and systems.

Technical Notes—Studies or reports which are complete in themselves but restrictive in their treatment of a subject. Analogous to monographs but not so comprehensive in scope or definitive in treatment of the subject area. Often serve as a vehicle for final reports of work performed at NIST under the sponsorship of other government agencies.

Voluntary Product Standards—Developed under procedures published by the Department of Commerce in Part 10, Title 15, of the Code of Federal Regulations. The standards establish nationally recognized requirements for products, and provide all concerned interests with a basis for common understanding of the characteristics of the products. NIST administers this program as a supplement to the activities of the private sector standardizing organizations.

Consumer Information Series—Practical information, based on NIST research and experience, covering areas of interest to the consumer. Easily understandable language and illustrations provide useful background knowledge for shopping in today's technological marketplace.

Order the **above** *NIST publications from: Superintendent of Documents, Government Printing Office, Washington, DC 20402.*

Order the **following** *NIST publications—FIPS and NISTIRs—from the National Technical Information Service, Springfield, VA 22161.*

Federal Information Processing Standards Publications (FIPS PUB)—Publications in this series collectively constitute the Federal Information Processing Standards Register. The Register serves as the official source of information in the Federal Government regarding standards issued by NIST pursuant to the Federal Property and Administrative Services Act of 1949 as amended, Public Law 89-306 (79 Stat. 1127), and as implemented by Executive Order 11717 (38 FR 12315, dated May 11, 1973) and Part 6 of Title 15 CFR (Code of Federal Regulations).

NIST Interagency Reports (NISTIR)—A special series of interim or final reports on work performed by NIST for outside sponsors (both government and non-government). In general, initial distribution is handled by the sponsor; public distribution is by the National Technical Information Service, Springfield, VA 22161, in paper copy or microfiche form.

U.S. Department of Commerce
National Institute of Standards and Technology
Gaithersburg, MD 20899