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.