ABSTRACT: The Integrated Services Digital Network (ISDN) standards will provide world-wide 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.