INTERNATIONAL STANDARD

ISO
9160

First edition
1988-02-01

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION
ORGANISATION INTERNATIONALE DE NORMALISATION
МЕЖДУНАРОДНАЯ ОРГАНИЗАЦИЯ ПО СТАНДАРТИЗАЦИИ

Information processing — Data encipherment — Physical layer interoperability requirements

Traitement de l'information — Chiffrement de données — Caractéristique interfonctionnement dans la couche physique

Reference number
ISO 9160 : 1988 (E)

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work.

Draft International Standards adopted by the technical committees are circulated to the member bodies for approval before their acceptance as International Standards by the ISO Council. They are approved in accordance with ISO procedures requiring at least 75 % approval by the member bodies voting.

International Standard ISO 9160 was prepared by Technical Committee ISO/TC 97, *Information processing systems*.

Users should note that all International Standards undergo revision from time to time and that any reference made herein to any other International Standard implies its latest edition, unless otherwise stated.

Information processing — Data encipherment — Physical layer interoperability requirements

0 Introduction

This International Standard specifies interoperability and security related requirements for using encipherment at the physical layer of the ISO Open Systems Interconnection (OSI) Reference Model in telecommunication systems conveying Automatic Data Processing (ADP) information.

This International Standard will facilitate the interoperation of data encipherment equipment used in data communication facilities and systems that require cryptographic protection.

The objectives of physical layer encipherment are to protect against all forms of passive attack including traffic analysis. Full protection against traffic analysis can only be provided in synchronous operation where all bits can be enciphered, whereas in asynchronous operation the start and stop bits can never be enciphered. This International Standard does not provide for protection of physical connection establishment.

This International Standard contains two annexes, A and B. Annex A is not an integral part of this International Standard. Annex B is an integral part of this International Standard.

1 Scope and field of application

This International Standard applies to systems for encipherment of ADP information in the physical layer of data communications.

This International Standard is equally applicable whether the Data Encipherment Equipment (DEE) is implemented as a physically separate piece of equipment or implemented as part of the Data Terminal Equipment (DTE) or as part of the Data Circuit terminating Equipment (DCE). When the encipherment is integrated into the DTE or DCE, this International Standard applies to those portions of the DTE or DCE design which implement the requirements of this International Standard. Interoperability requirements are defined for the following physical interface definitions: V.24, X.20 bis, X.21 bis, X.20, and X.21.

The physical layer is described in the Open Systems Interconnection Reference Model, ISO 7498. In physical layer encipherment, all of the SDU is normally enciphered. The interoperability requirements described in this International Standard apply to both synchronous and asynchronous operation in both full duplex and half duplex modes.

The main body of this International Standard specifies requirements which are applicable to the use of various encipherment algorithms. Annex B specifies additional requirements for the use of DEA (ANSI X3.92 – 1981).

This International Standard also specifies two alternative modes of synchronous operation – the delayed option and the immediate option – which are mutually incompatible.

This International Standard also specifies two alternative actions for BREAK signalling for asynchronous operation – Class A and Class B – which are mutually incompatible.

2 References

The following documents are referenced in this International Standard:

ISO 2382 – 9, *Data Processing – Vocabulary – Part 9: Data Communication.*
ISO 7498, *Information processing systems – Open Systems Interconnection – Basic Reference Model.*
ISO 7498 – 2, *Information processing systems – Open Systems Interconnection – Basic Reference Model. Part 2: Security Architecture*[1)]
ISO 8372, *Information processing – Modes of operation for a 64 – bit block cipher algorithm*
ANSI X3.92 – 1981, *Data Encryption Algorithm.*
CCITT, *Recommendations X.20, X.20bis, X.21, X.21bis – Red Book VIII.3 – 1984.*
CCITT, *Recommendations V.24, V.54 – Red Book VIII.1 – 1984*

1) At present at the stage of draft; publication anticipated in due course.