

Procedures for

**Achievement of
interoperability and
security by use of
encipherment at the
physical layer of OSI in
telecommunication
systems conveying
automatic data
processing information**

Committees responsible for this British Standard

The preparation of this British Standard was entrusted by the Information Systems Technology Standards Policy Committee (IST/-) to Technical Committee IST/33, upon which the following bodies were represented:

- Association of Cryptographic and Security Equipment Manufacturers
- British Telecommunications plc
- Communications-electronics Security Group (Cesg Ccta)
- Computing Services Association
- Department of Trade and Industry (National Physical Laboratory)
- EEA (the Association of Electronics, Telecommunications and Business Equipment Industries)
- Health and Safety Executive
- Mercury Communications Limited
- Ministry of Defence
- User Standards Forum for Information Technology (Institute of Data Processing Management)

This British Standard, having been prepared under the direction of the Information Systems Technology Standards Policy Committee, was published under the authority of the Standards Board and comes into effect on 31 May 1991

© BSI 10-1999

The following BSI references relate to the work on this standard:
Committee reference IST/33
Draft for comment 87/98227 DC

ISBN 0 580 17787 4

Amendments issued since publication

Amd. No.	Date	Comments

Contents

	Page
Committees responsible	Inside front cover
National foreword	ii
0 Introduction	1
1 Scope and field of application	1
2 References	1
3 Definitions	1
4 Applicable interfaces	2
5 General requirements	4
6 Synchronous encipherment operation	4
7 Asynchronous encipherment operation	4
8 Bypass control facility (Optional)	5
Annex A Background Information on Encipherment in the Physical Layer	11
Annex B Requirements for IV Structure and Transmission for DEA	12
Figure 1 — Operation of the V.24 Interchange circuits showing data encipherment in one direction only	6
Figure 2 — V.24 Half Duplex Transmission Signalling Sequence for Synchronous Encipherment, Alternative A	7
Figure 3 — V.24 Half Duplex Transmission Signalling Sequence for Synchronous Encipherment, Alternative B	8
Figure 4 — Start of asynchronous encipherment and a Class A BREAK operation	9
Figure 5 — Class B BREAK operation	9
Figure 6 — Bypass of encipherment for Test Loop Operation	10
Figure 7 — SV Derivation from 49-bit IV, 7-bit Characters, Preferred Alternative	13
Figure 8 — SV Derivation from 63-bit IV, 7-bit Characters, Acceptable Alternative 1	14
Figure 9 — SV Derivation from 70-bit IV, 7-bit Characters, Acceptable Alternative 2	14
Table 1 — IV Derivation	12
Table 2 — IV Option 1	12
Table 3 — IV Option 2	12
Publication(s) referred to	Inside back cover

National foreword

This British Standard has been prepared under the direction of the Information Systems Technology Standards Policy Committee (IST/-). It is the UK implementation of, and is identical to, ISO 9160:1988 “*Information processing — Data encipherment — Physical layer interoperability requirements*”, published by the International Organization for Standardization (ISO), except that the title of the British Standard differs in order to more accurately reflect the actual content of the text.

This standard implements the international text without change for the reasons given below (see “Reasons for implementation”), even though particular attention is drawn (see “Special attention”), to some features that may need special consideration when this standard is being used.

The UK actively participated in the development of the International Standard through BSI Technical Committee IST/33 and fully approved publication of the International Standard.

The information provided is considered sufficient to act in the UK as a basis for achieving interoperability and security for use of encipherment as the physical layer of Open Systems Interconnection (OSI) in telecommunication systems conveying information for automatic data processing.

There are no plans at present to supplement this British Standard with any additional guidance, and any comments or enquiries on the International Standard or its application should be addressed to the Secretary to IST/33 at the BSI headquarters address.

Reasons for implementation

- a) Because information technology equipment, services and systems tend to be, and generally need to be, designed, purchased and used in a world-wide context IST/- policy is to agree, wherever possible, standards at international level and not to prepare unique national standards. At the time of its approval, the text of the International Standard was considered to be the best that could be achieved, taking into account both the needs of the “market place” and the “state of the the art” in this subject area, and the International Standardization process.
- b) Further development of the international text at international level has been accorded relatively low priority in relation to other projects in the same international committee.
- c) Publication of British Standards corresponding to the International Standards in which IST/- resources were invested will ensure that the BSI Catalogue becomes, and then remains, a comprehensive first source of information for UK users of information technology equipment and services about the availability of International Standards on information technology subjects. In turn, this will facilitate UK use of, and access to, those standards.

Special attention Special attention is drawn to the following features of the International Standard, but it is emphasized that these features do not prevent use of this standard as a set of basic guidelines and, with appropriate care, products and systems can be effectively standardized. Users of this British Standard, however, might need supplementary information on these features from the BSI Technical Committee or from experts in the field.

(Note that, whilst agreements between individual trading or communicating partners can be made, and might suffice, additional care might be needed to avoid creating agreements that differ only slightly between different parties.)

- a) *Cipher algorithm*. Excluded from the International Standard is any particular cipher algorithm, but the algorithm used needs particular characteristics (see clause 5, paragraph 2).

b) *DEA algorithm*. The use of DEA (see Annex B and BS 6718) may involve the application of items subject to patents in the UK and elsewhere. It is expected that the first edition of ISO 8372:1987 will be amended soon to include information on possible patent issues.

c) *ANSI and CCITT publications*. Reference is given (see clause 2) to publications of the American National Standards Institute (ANSI) and the International Telegraph and Telephone Consultative Committee (CCITT). Such publications can be obtained in the UK from the BSI Sales Department, Linford Wood, Milton Keynes MK14 6LE.

Cross-references

International Standard	Corresponding British Standard
ISO 2382-9:1984	BS ISO 2382-9:1984 <i>Data processing — Vocabulary — Part 09: Data communication</i> (Identical)
ISO 7498:1984	BS 6568 <i>Reference model of Open Systems Interconnection</i> Part 1:1988 <i>Basic reference model (incorporating connectionless-mode transmission)</i> (Identical)
ISO 7498-2:1989	BS ISO 7498-2:1989 <i>Information processing systems — Open Systems Interconnection — Basic Reference Model — Part 2: Security Architecture</i> (Identical)
ISO 8372:1987	BS 7111:1991 <i>Guide to modes of operation for a 64-bit block cipher algorithm</i> (Identical)

The technical committee has reviewed the provisions of the following publications, to which reference is made in the text, and considers them acceptable for use in conjunction with this British Standard.

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

Information on the availability of interim ISO documents, as well as up-to-date information on existing and projected British Standards publications in the general area of Information Technology, is included in the “BASIC LIST” and regular Newsletter published as part of the BSI Information Technology Services (BITS) initiative.

For details, contact the Sales Department, BSI, Linford Wood, Milton Keynes MK14 6LE.

A British Standard does not purport to include all the necessary provisions of a contract. Users of British Standards are responsible for their correct application.

Compliance with a British Standard does not of itself confer immunity from legal obligations.

Summary of pages

This document comprises a front cover, an inside front cover, pages i to iv, pages 1 to 14, an inside back cover and a back cover.

This standard has been updated (see copyright date) and may have had amendments incorporated. This will be indicated in the amendment table on the inside front cover.

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 Annex A and Annex 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*

3 Definitions

3.1

this International Standard makes use of the following data communication terms defined in ISO 2382-9:

Physical layer	Serial transmission
Data communication	Asynchronous transmission
DTE	Start Stop transmission
DCE	Start signal
DCE/DTE Interface	Stop signal
Call establishment	Synchronous transmission
Data transfer	Duplex transmission
Test loops	Half duplex transmission

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