
British Standard for

Open Systems Interconnection: protocol specification for the Association Control Service Element

[ISO title: Information processing systems—Open Systems Interconnection—Protocol specification for the Association Control Service Element]

Interconnexion de systèmes ouverts: Spécification de protocole pour les éléments de service du noyau de case

Kommunikation Offener Systeme: Festlegung von Protokollen für die Assoziationssteuerung

National foreword

This British Standard has been prepared under the direction of the Information Systems Technology Standards Policy Committee. It is identical with ISO 8650 : 1988 'Information processing systems—Open Systems Interconnection—Protocol specification for the Association Control Service Element'. The international standard was prepared and published by the International Organization for Standardization (ISO) with the active participation and approval of the UK. It is a revision of DD 132 : 1986 which is withdrawn.

Addenda to the international standard are planned to cover the following areas:

- (a) peer authentication;
- (b) application context management;
- (c) Protocol Implementation Conformance Statement (PICS) proforma.

These addenda are expected to be incorporated in BS 7092 when they have been published by ISO.

This standard is closely related to the companion service standard BS 7091 'Open Systems Interconnection: service definition for the Association Control Service Element'. A Standard to cover the A-UNIT-DATA protocol is under consideration.

Up-to-date information on existing and projected British Standards publications for Open Systems Interconnection is included in the 'Basic List', published as part of the BSI Information Technology Services (BITS) initiative. For details contact: Marketing Department, BSI, Linford Wood, Milton Keynes, MK14 6LE.

Terminology and conventions. The text of the international standard has been approved as suitable for publication as a British Standard without deviation. Some terminology and certain conventions are not identical with those used in British Standards; attention is drawn especially to the following.

Wherever the words 'International Standard' or 'ISO 8650' appear, referring to this standard, they should be read as 'British Standard' or 'BS 7092' respectively.

Cross-references

International standard	Corresponding British Standard
ISO 7498 : 1984	BS 6568 Reference model of open systems interconnection Part 1 : 1988 Basic reference model (incorporating connectionless-mode transmission) (Identical)
ISO 8326 : 1987	BS 6960 : 1988 Open Systems Interconnection: basic connection-oriented session service definition (Identical)
ISO 8327 : 1987	BS 6961 : 1988 Open Systems Interconnection: basic connection-oriented session protocol specification (Identical)
ISO/TR 8509 : 1987	DD 108 : 1988 Open Systems Interconnection: service conventions (Identical)
ISO 8649 : 1988	BS 7091 : 1989 Open Systems Interconnection: service definition for the Association Control Service Element (Identical)
ISO 8822 : 1988	BS 7093 : 1989 Open Systems Interconnection: connection-oriented presentation service definition (Identical)
ISO 8824 : 1987	BS 6962 : 1988 Open Systems Interconnection: specification for Abstract Syntax Notation One (ASN.1) (Identical)
ISO 8825 : 1987	BS 6963 : 1988 Open Systems Interconnection: specification for basic encoding rules for Abstract Syntax Notation One (ASN.1) (Identical)

The Technical Committee has reviewed the provisions of ISO 7849-3 and CCITT Recommendation X.410*, to which reference is made in the text, and has decided that they are acceptable for use in conjunction with this standard.

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

* Available from Sales Department, BSI, Linford Wood, Milton Keynes, MK14 6LE.

Implementation of Technical Corrigendum 1

**published and effective from 31 July 1991
to BS 7092 : 1989 (ISO 8650 : 1988)**

**Open Systems Interconnection : protocol specification
for the Association Control Service Element**

AMD 6735

ISO 8650 : 1988/

Cor. 1 : 1990

AMD 6735
July 1991

National foreword (as amended by Amendment 1)

In line 3, after 'Amendment 1', insert 'and Technical Corrigendum 1'.

AMD 6735
July 1991

ISO text

Insert the attached as appropriate.



**INTERNATIONAL STANDARD ISO 8650 : 1988
TECHNICAL CORRIGENDUM 1**

Published 1990-06-01

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION • МЕЖДУНАРОДНАЯ ОРГАНИЗАЦИЯ ПО СТАНДАРТИЗАЦИИ • ORGANISATION INTERNATIONALE DE NORMALISATION
INTERNATIONAL ELECTROTECHNICAL COMMISSION • МЕЖДУНАРОДНАЯ ЭЛЕКТРОТЕХНИЧЕСКАЯ КОМИССИЯ • COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

Information processing systems — Open Systems Interconnection — Protocol specification for the Association Control Service Element TECHNICAL CORRIGENDUM 1

Technical corrigendum 1 to ISO 8650:1988 was developed by ISO/IEC JTC 1, *Information technology*.

Introduction

This is technical corrigendum 1 to ISO 8650. It covers defect 8650/001 which aligns ISO 8650 with the wording in CCITT Recommendation X.227, clause 10 (Conformance) in reference to the X.410-1984 mode. It also covers defect 8650/004 which specifies the ASN.1 definition of AE title.

This technical corrigendum is applied to ISO 8650. Insertions are contained between « and » and are in italics: « *This is an example of inserted text.* » Deleted text is marked by strike-thru. ~~This is an example of deleted text.~~ Editing instructions are within { and }, are capitalized, and are in italics.

UDC 681.3.01

Ref. No. ISO 8650 : 1988/Cor.1 : 1990 (E)

Descriptors : data processing, information interchange, network interconnection, open systems interconnection, communication procedure, control procedures, protocols.

© International Organization for Standardization, 1990 •

Printed in Switzerland

Price based on 3 pages

AVA Documents
Document Sharing Hub

9 Structure and encoding of ACSE APDUs

{IN PARAGRAPH 9.1 INSERT THE FOLLOWING ASN.1 PRODUCTION FOLLOWING THE BEGIN OPERATOR:}

```
IMPORTS  Name, RelativeDistinguishedName
        FROM InformationFramework
        { joint-iso-ccitt ds(5) modules(1)
          informationFramework(1)
        }
```

—The data types Name and RelativeDistinguishedName are imported from ISO 9594-2.

{ALSO, IN PARAGRAPH 9.1, REPLACE THE EXISTING ASN.1 FOR AP-TITLE, AE-QUALIFIER, AND AE-TITLE WITH THE FOLLOWING ASN.1 PRODUCTIONS AND COMMENTS:}

```
AP-title      ::= CHOICE { AP-title-form1, AP-title-form2 }
```

```
AE-qualifier ::= CHOICE { AE-qualifier-form1, AE-qualifier-form2 }
```

—When both AP-title and AE-qualifier data values are present in an
—AARQ or AARE APDU, both must have the same form to allow the
—construction of an AE-title as discussed in ISO 9834-6.

```
AP-title-form1      ::= Name
```

—The value assigned to AP-title-form1 is The Directory Name of an
—application-process title.

```
AE-qualifier-form1 ::= RelativeDistinguishedName
```

—The value assigned to AE-qualifier-form1 is the relative
—distinguished name of a particular application-entity of the
—application-process identified by AP-title-form1.

```
AP-title-form2      ::= OBJECT IDENTIFIER
```

```
AE-qualifier-form2 ::= INTEGER
```

—As defined in ISO 7498-3, an application-entity title is composed
—of an application-process title and an application-entity
—qualifier. The ACSE protocol provides for the transfer of an
—application-entity title value by the transfer of its component
—values. However, the following data type is provided for
—International Standards that reference a single syntactic structure
—for AE titles.

```
AE-title ::= CHOICE { AE-title-form1, AE-title-form2 }
```

AE-title-form1 ::= Name

-For access to The Directory (ISO 9594), an AE title has
-AE-title-form1. This value can be constructed from
-AP-title-form1 and AE-qualifier-form1 values contained in an
-AARQ or AARE APDU. A discussion of forming an AE-title-form1
-from AP-title-form1 and AE-qualifier-form1 may be found in
-ISO 9834-6.

AE-title-form2 ::= OBJECT IDENTIFIER

-A discussion of forming an AE-title-form2 from AP-title-form2
-and AE-qualifier-form2 may be found in ISO 9834-6.

10 Conformance

{CHANGE 10.0.3 TO READ:}

10.0.3 The X.410-1984 mode exists to allow compatibility with message handling systems implementing the protocol specified in CCITT Recommendation X.410-1984.

{CHANGE SUB-ITEM 2) OF ITEM c) OF 10.1 TO READ:}

2) the X.410-1984 mode of ACSE protocol to support a message handling system; or

10.1 Statement requirements

{NO CHANGE}

10.2 Static requirements

{NO CHANGE}

10.3 Dynamic requirements

10.3.1 Normal mode

{NUMBER THE EXISTING PARAGRAPH AS 10.3.1.1. ADD THE FOLLOWING TEXT AS PARAGRAPH 10.3.1.2:}

10.3.1.2 The requesting AE may choose to send either form 1 or form 2 for AP title and AE qualifier. The accepting AE may respond with either form. Thus, both the requesting and responding AE must be capable of receiving both forms.

10.3.2 X.410-1984 mode

{NO CHANGE}



**Implementation of Amendment 1
Authentication during association establishment**

**published and effective from 31 July 1991
to BS 7092 : 1989 (ISO 8650 : 1988)**

**Open Systems Interconnection : protocol specification
for the Association Control Service Element**

AMD 6734
ISO 8650 : 1988/
Amd 1 : 1990

AMD 6734
July 1991

National foreword

In line 3, after 'Element', insert ',including Amendment 1'.

AMD 6734
July 1991

ISO text

Insert the attached as appropriate.

INTERNATIONAL STANDARD

**ISO
8650**

First edition
1988-12-15

AMENDMENT 1
1990-12-15

Information processing systems — Open Systems Interconnection — Protocol specification for the Association Control Service Element

AMENDMENT 1: Authentication during association establishment

*Systèmes de traitement de l'information — Interconnexion de systèmes ouverts —
Spécification du protocole pour l'élément de service de contrôle d'association*

AMENDEMENT 1: Authentification pendant l'établissement d'association



Reference number
ISO 8650 : 1988/Amd.1 : 1990 (E)

Contents

Foreword iv

Introduction to this amendment v

~~0~~ Introduction 1

1 Scope and field of application 1

2 «Normative» references 1

3 Definitions 2

 3.1 Reference model definitions 2

 3.2 Service conventions definitions {PREVIOUSLY 3.3} 2

 3.3 Presentation service definitions {PREVIOUSLY 3.4} 2

 3.4 ACSE service definitions {PREVIOUSLY 3.5} 2

 3.5 Application Layer Structure definitions {NEW} 2

4 Abbreviations 2

5 Conventions {NO CHANGE} 2

6 Overview of the protocol.....3

 6.1 Service provision {NO CHANGE} 3

 6.1a Functional units {NEW} 3

 6.2 Use of presentation-service {NO CHANGE} 3

 6.3 Relationship to session-service {NO CHANGE} 3

 6.4 Model 3

7 Elements of procedure 4

 7.1 Association establishment 4

 7.2 Normal release of an association {NO CHANGE} 5

 7.3 Abnormal release of an association {NO CHANGE} 5

© ISO/IEC 1990
All rights reserved. No part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from the publisher.
ISO/IEC Copyright Office • Case postale 56 • CH-1211 Genève 20 • Switzerland
Printed in Switzerland

8 Mapping to the presentation-service {NO CHANGE} 5

9 Structure and encoding of ACSE APDUs 6

10 Conformance 8

 10.1 Statement requirements 8

 10.2 Static requirements {NO CHANGE} 8

 10.3 Dynamic requirements {NO CHANGE} 8

11 Precedence {NO CHANGE} 8

12 Registration requirements {NEW} 8

 12.1 Application titles 8

 12.2 Application context 8

 12.3 Authentication-mechanism 8

Annexes

A ACPM state table 9

B Authentication-mechanism using password {NEW} 10

B.0 Introduction 10

B.1 Assigned name 10

B.2 Authentication-value ASN.1 datatype.....10

B.3 Processing specification..... 10

B.3.1 Requesting authentication 10

B.3.2 Performing authentication 10

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1. Draft International Standards adopted by the joint technical committee are circulated to the national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

International Standard ISO 8650/Amd.1 was prepared by the Joint Technical Committee ISO/IEC JTC 1, *Information technology*.

Introduction to this amendment

This is amendment 1 to ISO 8650 : 1988 covering authentication during association establishment. In preparing this amendment, national bodies and liaison organizations agreed to minimize the changes to the ACSE service definition and protocol specification. This amendment does not add APDUs. It simply adds new fields in the existing APDUs.

The essential requirement addressed was to enable some simple forms of authentication at an early date. It was recognized that a generalized two-way handshake can support a very useful class of authentication methods. These methods include simple password mechanisms that are widely used.

This amendment defines the Authentication functional unit for ACSE, which is the first for ACSE. The functions of the original ACSE become the Kernel functional unit. The new functions are the Authentication functional unit. The approach of adding a functional unit rather than creating version 2 of ACSE was done in response to the liaison from the ULA ad-hoc group meeting in Hull, Quebec, 5-9 June 1989. By using this approach, ACSE remains version 1 as advised by the ULA ad-hoc group.

The Kernel is the default functional unit. An implementation that either explicitly or implicitly (i.e., by default) requests only the Kernel functional unit then references only the facilities and abstract syntax definitions of the original ACSE.

This amendment adds three optional fields to the AARQ and AARE APDUs. Two fields may carry authentication related information. The third field is the optional ACSE Requirements field to express the ACSE functional units requested. An optional field is also added to the ABRT APDU. This field may carry authentication related diagnostic about why an association was abnormally terminated. This field may also be used to carry diagnostics that do not relate to authentication.

Clause 0 (Introduction) is now a preliminary element. Clause 1 (Scope) mentions the Kernel and Authentication functional units. Clause 7 (Elements of procedure) and clause 9 (Structure and encoding of ACSE APDUs) reflect the additions of the new fields. Minor changes have been made to other clauses. Annex A (ACPM state table) is not changed.

Annex B is new. It is a specification for an authentication-mechanism that uses a password with an AE title. This authentication-mechanism is intended for general use. It also serves as an example of the specification of an authentication-mechanism. This authentication-mechanism is registered in ISO 8650 and has an OBJECT IDENTIFIER assigned to it. Other authentication-mechanisms may be specified and registered in ISO 8650 as future amendments or they may be registered within OSI as defined in ISO/IEC 9834-1.

It was recognized that extensive work is going on throughout JTC1 covering all aspects of security. This work may result in more comprehensive forms of authentication, linked to other security services and based on a comprehensive model. The current functional unit may therefore provide only a limited solution in the long term, but it does provide useful facilities at an early date.

Format and notation

This amendment is written as a "delta document." That is, it will be merged with the base document, ISO 8650 : 1988. Editing instructions are in *italic caps* and are contained within { }:

{THIS IS AN EXAMPLE OF AN EDITING INSTRUCTION.}

Modifications to original text (i.e., ISO 8650 : 1988) are indicated as deletions (~~this is deleted text~~), and inserted text that its italicized and within « » («*This is inserted text*»). However, this notation is not used for replaced or inserted text.

Information processing systems — Open Systems Interconnection — Protocol specification for the Association Control Service Element

AMENDMENT 1: Authentication during association establishment

{MOVE THE INTRODUCTION (THE ORIGINAL CLAUSE 0) TO THE FRONT OF THE INTERNATIONAL STANDARD AS A PRELIMINARY ELEMENT. WHEN THIS IS DONE, THE INTRODUCTION WILL BE ON PAGE "v" AND THE NUMBERS PRECEDING THE PARAGRAPHS OF THE ORIGINAL CLAUSE 0 WILL BE REMOVED.}

0 Introduction

{ADD THE FOLLOWING SENTENCE TO THE END OF THE THIRD PARAGRAPH (I.E., THE ORIGINAL 0.3).}

The ACSE protocol also includes an optional functional unit for exchanging information to support authentication during association establishment. The ACSE services apply to a wide range of application-process communication requirements.

1 Scope and field of application

{INSERT THE FOLLOWING TEXT AS THE NEW SECOND PARAGRAPH OF CLAUSE 1.}

The Kernel functional unit is used to establish and release application-associations. The Authentication functional unit provides additional facilities for exchanging information in support of authentication during association establishment without adding new services. The ACSE authentication facilities can be used to support a limited class of authentication methods.

{MODIFY THE NEW THIRD PARAGRAPH (I.E., THE ORIGINAL SECOND PARAGRAPH) AS FOLLOWS.}

This International Standard specifies:

- a) procedures for the transfer of information ~~«for» relating to application-association control «and the authentication of» between~~ application-entities; and
- b) the abstract syntax for the representation of the ACSE APDUs.

2 «Normative» references

{INSERT THE FOLLOWING TEXT AS THE NEW PARAGRAPH UNDER CLAUSE 2 BEFORE THE LIST OF REFERENCES.}

The following standards contain provisions which, through reference in this text, constitute provisions of this International Standard. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based on this International Standard are encouraged to investigate the possibility of applying the most recent editions of the standards listed below. Members of IEC and ISO maintain registers of currently valid International Standards.

{ADD THE FOLLOWING REFERENCES.}

ISO 6523, *Data interchange — Structure for identification of organizations*.

ISO 7498-2:1989, *Information processing systems — Open Systems Interconnection — Basic Reference Model — Part 2: Security architecture*.

ISO/IEC 9545:1989, *Information technology — Open Systems Interconnection — Application Layer Structure*.

ISO/IEC 9834-1¹, *Information technology — Open Systems Interconnection — Procedures for the operation of OSI registration authorities — Part 1: General procedures*.

ISO/IEC 9834-6¹, *Information technology — Open Systems Interconnection — Procedures for the operation of OSI registration authorities — Part 6: AP titles and AE titles*.

1) To be published.

3 Definitions

3.1 Reference model definitions

3.1.1 Basic reference model definitions {NEW HEADING}

{MOVE TEXT FROM ORIGINAL 3.1 TO THIS SUBCLAUSE.}

{INSERT NEW SUBCLAUSE 3.1.2.}

3.1.2 Security architecture definitions {NEW}

This International Standard makes use of the following term defined in ISO 7498-2:

password.

{END OF INSERTED SUBCLAUSE 3.1.2.}

3.1.3 Naming and addressing definitions {PREVIOUSLY 3.2}

{MOVE TEXT FROM ORIGINAL 3.2 TO THIS SUBCLAUSE.}

3.2 Service conventions definitions {PREVIOUSLY 3.3}

{MOVE TEXT FROM ORIGINAL 3.3 TO THIS SUBCLAUSE.}

3.3 Presentation service definitions {PREVIOUSLY 3.4}

{MOVE TEXT FROM ORIGINAL 3.4 TO THIS SUBCLAUSE.}

3.4 ACSE service definitions {PREVIOUSLY 3.5}

{MOVE TEXT FROM ORIGINAL 3.5 TO THIS SUBCLAUSE AND ADD THE FOLLOWING DEFINITIONS MAINTAINING ALPHABETICAL ORDER.}

authentication

authentication-function

authentication-value

authentication-mechanism

{INSERT NEW SUBCLAUSE 3.5.}

3.5 Application Layer Structure definitions {NEW}

This International Standard makes use of the following terms defined in ISO/IEC 9545:

a) application-entity invocation;

b) single association control function; and

c) single association object.

{END OF INSERTED SUBCLAUSE 3.5.}

4 Abbreviations

{ADD THE FOLLOWING ABBREVIATIONS MAINTAINING ALPHABETICAL ORDER.}

AEI application-entity invocation

RPOA recognized private operating agency

SACF single association control function

SAO single association object

{END OF ADDED ABBREVIATIONS.}

5 Conventions {NO CHANGE}

{NO CHANGE IS MADE TO THIS CLAUSE.}