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

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

ISO/IEC 9834-6[1], *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.*}

6 Overview of the protocol

6.1 Service provision {*NO CHANGE*}

{*NO CHANGE IS MADE TO THIS SUBCLAUSE.*}

{*INSERT THE FOLLOWING TEXT AS NEW SUBCLAUSE 6.1a BETWEEN SUBCLAUSES 6.1 AND 6.2.*}

6.1a Functional units {*NEW*}

6.1a.1 Functional units are used by this International Standard to negotiate ACSE user requirements during association establishment. Two functional units are defined:

a) Kernel functional unit; and

b) Authentication functional unit.

6.1a.2 The ACSE Requirements fields on the AARQ and AARE APDUs are used to select the Authentication functional units for the association.

6.1a.3 The Kernel functional unit is always available. It is the default functional unit. To be included, the Authentication functional unit shall be explicitly requested on the AARQ APDU and accepted on the AARE APDU.

6.1a.4 The selection of the Authentication functional unit supports additional fields on the AARQ, AARE, and RLRQ APDUs. It does not affect the elements of procedure. Table 1a shows the services, APDUs and APDU fields associated with the ACSE functional units.

{*END OF INSERTED SUBCLAUSE 6.1a. INSERT NEW TABLE 1a. RENUMBER THE TABLES AND ADJUST REFERENCES TO THESE TABLES IN THE TEXT.*}

6.2 Use of presentation-service {*NO CHANGE*}

{*NO CHANGE IS MADE TO THIS SUBCLAUSE.*}

6.3 Relationship to session-service {*NO CHANGE*}

{*NO CHANGE IS MADE TO THIS SUBCLAUSE.*}

6.4 Model

{*INSERT THE FOLLOWING NEW NOTE AFTER PARAGRAPH 6.4.1.*}

NOTE — An ASE standard that references ACSE need not specify the use of ACSE service primitive parameters that are irrelevant to its operation. The SACF can be modeled to pass such parameters between the ACPM and that part of the AEI to which the parameters are relevant.

{*END OF INSERTED NOTE.*}

Table 1a — Functional unit APDUs and their fields {*NEW*}

Functional Unit	Service	APDU	Field Name
Kernel	A-ASSOCIATE	AARQ	Protocol Version Application Context Name Calling AP Title Calling AE Qualifier Calling AP Invocation-identifier Calling AE Invocation-identifier Called AP Title Called AE Qualifier Called AP Invocation-identifier Called AE Invocation-identifier Implementation Information User Information
		AARE	Protocol Version Application Context Name Responding AP Title Responding AE Qualifier Responding AP Invocation-identifier Responding AE Invocation-identifier Result Result Source - Diagnostic Implementation Information User Information
	A-RELEASE	RLRQ	Reason User Information
		RLRE	Reason User Information
	A-ABORT	ABRT	Abort Source User Information
Authentication	A-ASSOCIATE	AARQ	ACSE Requirements Authentication-mechanism Name Authentication-value

7 Elements of procedure

{NO CHANGE IS MADE TO THE INTRODUCTORY TEXT.}

7.1 Association establishment

{TABLE 2 (AARQ APDU FIELDS) — ADD THE FOLLOWING ROWS AFTER Called AE Invocation-identifier AND BEFORE Implementation Information.}

ACSE-requirements	U	req ind
Authentication-mechanism Name	U	req ind
Authentication-value	U	req ind

{ADD THE FOLLOWING NOTE TO TABLE 2.}

NOTE — The Authentication-mechanism Name and Authentication-value fields are only present if the ACSE-requirements field includes the Authentication functional unit.

{TABLE 3 (AARE APDU FIELDS) — ADD THE FOLLOWING ROWS AFTER Result Source - Diagnostic AND BEFORE Implementation Information.}

ACSE-requirements	U	rsp	cnf
Authentication-mechanism Name	U	rsp	cnf
Authentication-value	U	rsp	cnf

{ADD THE FOLLOWING NOTE TO TABLE 3.}

NOTE — The Authentication-mechanism Name and Authentication-value fields are only present if the ACSE-requirements field includes the Authentication functional unit.

7.1.1 Purpose *{NO CHANGE}*

{NO CHANGE IS MADE TO THIS SUBCLAUSE.}

7.1.2 APDUs used *{NO CHANGE}*

{NO CHANGE IS MADE TO THIS SUBCLAUSE.}

7.1.3 Association establishment procedure

{MODIFY PARAGRAPH 7.1.3.2.4 AS FOLLOWS.}

7.1.3.2.4 If the P-CONNECT indication primitive and its AARQ APDU are acceptable, the ACPM *«inspects the ACSE-requirements field if it is present. It removes functional units that it does not support. The ACPM then issues»* an A-ASSOCIATE indication primitive to the acceptor. The A-ASSOCIATE indication primitive parameters are derived from the AARQ APDU and the P-CONNECT indication primitive. The ACPM waits for a primitive from the acceptor.

7.1.4 Use of AARQ APDU fields

{INSERT NEW SUBCLAUSES 7.1.4.10a, 7.1.4.10b AND 7.1.2.10c AFTER SUBCLAUSE 7.1.1.10 Called AE Invocation-identifier.}

7.1.4.10a ACSE-requirements

For the requesting ACPM: The value assigned to this field is determined by the value of the ACSE Requirements parameter of the A-ASSOCIATE request primitive.

For the accepting ACPM: This value is used to determine the value of the ACSE Requirements parameter of the A-ASSOCIATE indication primitive, if issued. The ACPM inspects the ACSE-requirements field and removes any functional units not supported by the ACPM before issuing it to the service-user.

7.1.4.10b Authentication-mechanism Name

For the requesting ACPM: The value assigned to this field is determined by the value of the Authentication-mechanism Name parameter of the A-ASSOCIATE request primitive.

For the accepting ACPM: This value is used to determine the value of the Authentication-mechanism Name parameter of the A-ASSOCIATE indication primitive, if issued.

7.1.4.10c Authentication-value

For the requesting ACPM: The value assigned to this field is determined by the value of the Authentication-value parameter of the A-ASSOCIATE request primitive.

For the accepting ACPM: This value is used to determine the value of the Authentication-value parameter of the A-ASSOCIATE indication primitive, if issued.

{END OF INSERTED SUBCLAUSES 7.1.4.10a, 7.1.4.10b AND 7.1.4.10c.}

7.1.5 Use of AARE APDU fields

{INSERT NEW SUBCLAUSES 7.1.5.8a, 7.1.5.8b AND 7.1.5.8c AFTER SUBCLAUSE 7.1.5.8.2 Diagnostic Value.}

7.1.5.8a ACSE-requirements

For the accepting ACPM: The value assigned to this field is determined by the value of the ACSE Requirements parameter of the A-ASSOCIATE response primitive. This value shall only include functional units that were on the indication primitive.

For the requesting ACPM: This value is used to determine the value of the ACSE Requirements parameter of the A-ASSOCIATE confirm primitive.

7.1.5.8b Authentication-mechanism Name

For the accepting ACPM: The value assigned to this field is determined by the value of the Authentication-mechanism Name parameter of the A-ASSOCIATE response primitive.

For the requesting ACPM: This value is used to determine the value of the Authentication-mechanism Name parameter of the A-ASSOCIATE confirm primitive.

7.1.5.8c Authentication-value

For the accepting ACPM: The value assigned to this field is determined by the value of the Authentication-value parameter of the A-ASSOCIATE response primitive.

For the accepting ACPM: This value is used to determine the value of the Authentication-value parameter of the A-ASSOCIATE confirm primitive.

{END OF INSERTED SUBCLAUSES 7.1.5.8a, 7.1.5.8b AND 7.1.5.8c.}

7.1.6 Collisions and interactions *{NO CHANGE}*

{NO CHANGE IS MADE TO THIS SUBCLAUSE.}

7.2 Normal release of an association {*NO CHANGE*}

{*NO CHANGE IS MADE TO THIS SUBCLAUSE.*}

7.3 Abnormal release of an association {*NO CHANGE*}

7.3.1 Purpose {*NO CHANGE*}

{*NO CHANGE IS MADE TO THIS SUBCLAUSE.*}

7.3.2 APDUs used

{*NO CHANGE IS MADE TO THE TEXT IMMEDIATELY UNDER 7.3.2*}

{*TABLE 6 — ADD THE FOLLOWING ROW AFTER Abort Source AND BEFORE User Information.*}

Diagnostic	U	req	ind

7.3.3 Abnormal release procedure {*NO CHANGE*}

{*NO CHANGE IS MADE TO THIS SUBCLAUSE.*}

7.3.4 Use of ABRT APDU fields

{*RENUMBER THE ORIGINAL 7.3.4.2 AS 7.3.4.3. INSERT NEW SUBCLAUSE 7.3.4.2.*}

7.3.4.2 Diagnostic

For the requesting ACPM: This value is determined by the value of the Diagnostic parameter of the A-ABORT request primitive.

For the accepting ACPM: This value is used to determine the value of the Diagnostic parameter of the A-ABORT indication primitive.

{*END OF INSERTED SUBCLAUSE 7.3.4.2.*}

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

{*NO CHANGE IS MADE TO THIS CLAUSE.*}