INTERNATIONAL STANDARD

ISO 8649

First edition
1988-12-15

AMENDMENT 1
1990-12-15

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

AMENDMENT 1: Authentication during association establishment

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

AMENDEMENT 1: Authentification pendant l'établissement d'association

Reference number
ISO 8649 : 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 8649/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 8649 : 1988 covering authentication during association establishment. In preparing this amendment, national bodies and liaison organizations agreed to minimize the changes to the ACSE services. This amendment does not add new services. It simply adds new parameters on existing services.

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 only references the functions of the original ACSE.

This amendment adds three optional parameters to the A-ASSOCIATE service. Two parameters may be used to carry authentication related information. The third parameter may be used to negotiate the ACSE functional units for the association. An optional parameter is also added to the A-ABORT service. This parameter may be used to express authentication-related diagnostics about why an association was abnormally terminated. This parameter may also be used to express diagnostics that do not relate to authentication.

To support the additions to the A-ASSOCIATE service, a new sub-clause has been added to clause 6 (Basic concepts). This sub-clause (6.2) introduces some new concepts for authentication within ACSE.

Additions have been made to clause 9 (Service definition) for the A-ASSOCIATE and A-ABORT services. In addition, minor editorial changes have been made to clauses 1 (Scope), 2 (References), 3 (Definitions) and 4 (Abbreviations). Clause 0 (Introduction) has been made a preliminary element.

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 8649 : 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 8649 : 1988) are indicated as deletions (~~this is deleted text~~), and insertions that are italicized and within « » («*This is inserted text*»). However, this notation is not used for replaced or inserted text.

Information processing systems — Open Systems Interconnection — Service definition 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 "iv" AND THE NUMBERS PRECEDING THE PARAGRAPHS OF THE ORIGINAL CLAUSE 0 WILL BE DELETED.}

~~0~~ Introduction

{MODIFY THE FOURTH PARAGRAPH (I.E. THE ORIGINAL 0.4) AS FOLLOWS.}

~~0.4~~ This International Standard defines services provided by the application service element for application-association control: the Association Control Service Element (ACSE). The ACSE provides basic facilities for the control of an application-association between two application-entities that communicate by means of a presentation-connection. *«The ACSE includes a functional unit for exchanging information in support of 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.}

Two functional units are defined in the ACSE. The mandatory Kernel functional unit is used to establish and release application-associations. The optional Authentication functional unit provides additional facilities for exchanging information in support of authentication during association establishment without adding services. The ACSE authentication facilities may be used to support a limited class of authentication methods.

{END OF INSERTED PARAGRAPH.}

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 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.*

{END OF ADDED REFERENCES.}

3 Definitions

3.1 Reference model definitions

3.1.1 Basic reference model definitions *{NEW HEADING}*

{MOVE TEXT FROM THE ORIGINAL SUBCLAUSE 3.1 TO THIS SUBCLAUSE AND ADD THE FOLLOWING TERMS MAINTAINING ALPHABETICAL ORDER.}

application-function

(N)-function

1) To be published.

{*INSERT NEW SUBCLAUSE 3.1.2.*}

3.1.2 Security architecture definitions {*NEW*}

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

a) credentials;

b) password; and

c) peer-entity authentication.

{*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 THE ORIGINAL 3.4 TO THIS SUBCLAUSE.*}

3.4 ACSE service definitions {*PREVIOUSLY 3.5*}

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

3.4._ authentication: The corroboration of the identity of objects relevant to the establishment of an association. For example, these can include the AEs, APs, and the human users of applications.

NOTE — This term has been defined to make it clear that a wider scope of authentication is being addressed than is covered by peer-entity authentication in ISO 7498-2.

3.4._ authentication-function: An application-function within an application-entity invocation that processes and exchanges authentication-values with a peer authentication-function.

3.4._ authentication-value: The output from an authentication-function to be transferred to a peer ACSE service-user for input to the peer's authentication-function.

3.4._ authentication-mechanism: The specification of a specific set of authentication-function rules for defining, processing, and transferring authentication-values.

{*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
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 Basic concepts

{*USING THE ORIGINAL CLAUSE 6 AS A BASE, REPLACE CLAUSE 6 WITH THE FOLLOWING TEXT.*}

{*INSERT NEW HEADING 6.1. MOVE ORIGINAL PARAGRAPHS 6.1 THROUGH 6.4 UNDER THIS NEW HEADING AS PARAGRAPHS 6.1.1 THROUGH 6.1.4. THEN, INSERT NEW PARAGRAPHS 6.1.5 THROUGH 6.1.7. ALSO, INSERT NEW SUBCLAUSE 6.2*}

6.1 General {*NEW HEADING*}

6.1.1 The reference model (ISO 7498) represents communication between a pair of application-processes (APs) in terms of communication between their application-entities (AEs) using the presentation-service. The functionality of an AE is factored into a number of application-service-elements (ASEs). The interaction between AEs is described in terms of the use of their ASEs' services.

6.1.2 This International Standard introduces the additional modeling concepts of application-association and application context.

6.1.3 An **application-association** is a cooperative relationship between two AEs. It provides the necessary frame of reference between the AEs in order that they may interwork effectively. This relationship is formed by the exchange of application-protocol-control-information between the application-entities through their use of presentation-services.

6.1.4 An **application context** is an explicitly identified set of application-service-elements, related options and any other necessary information for the interworking of application-entities on an application association.

6.1.5 {*NEW*} The ACSE service-user is that part of an application-entity that makes use of ACSE services. It may be the single association control function (SACF) or an ASE or some combination of the two.

6.1.6 {*NEW*} An ASE standard does not need to specify the use of ACSE service primitive parameters that are not relevant to the operation of the ASE. It may be assumed that the SACF passes such parameters between the ACSE service-provider and that part of the AEI to which the parameters are relevant.

6.1.7 {*NEW*} As an example, consider the authentication parameters of the Authentication functional unit discussed below in 6.2. The SACF may be used to model the passing of authentication-values between the authentication-func-

tion and the ACSE service-provider. An ASE that references ACSE need not be concerned with these parameters.

6.2 Authentication {*NEW*}

This International Standard includes the Authentication functional unit. The functional unit allows APIs, AEIs and their related objects to exchange authentication information during the establishment of an association.

6.2.1 Authentication concepts

This International Standard includes the modeling concepts of authentication-function, authentication-mechanism, authentication-mechanism name and authentication-value. Each is discussed below.

6.2.1.1 Authentication-function

6.2.1.1.1 For this International Standard, authentication is supported by a pair of authentication-functions. An **authentication-function** is modeled as an application-function (i.e., as an (N)-function as defined in ISO 7498) that is available to the ACSE service-user. Each is contained within the associated AEIs.

6.2.1.1.2 Modeling the authentication-function in this way allows ACSE to deal with authentication communication requirements without having to understand the semantics of the security information exchanged or how it is used.

6.2.1.2 Authentication-mechanism

6.2.1.2.1 An **authentication-mechanism** is a particular specification of the processing to be performed by a pair of application-functions for authentication. A specification contains the rules for creating, sending, receiving and processing information needed for authentication.

6.2.1.2.2 Annex B in ISO 8650 is an example of an authentication-mechanism. It defines the authentication of the sending AEI based on its AE title and its password. The password is contained in the Authentication-value parameter.

6.2.1.3 Authentication-mechanism name

6.2.1.3.1 An **authentication-mechanism name** is used to specify a particular authentication-mechanism. For example, the name of the authentication-mechanism specified in ISO 8650 annex B is assigned (i.e., registered) in the annex. The value has the data type of an OBJECT IDENTIFIER.

6.2.1.3.2 An authentication-mechanism name may also be used to specify a more general security mechanism that includes an authentication-mechanism. An example of a general security mechanism is an ASE that provides security facilities to its service-user).

6.2.1.3.3 Authentication-mechanism names and general security mechanism names are subject to registration within OSI (see clause 12 in ISO 8650).

6.2.1.4 Authentication-value

6.2.1.4.1 An **authentication-value** consists of information used by a pair of authentication-functions to perform authentication. It can consist of information such as, credentials, a time-stamp, a digital signature, etc. It can also identify the type and/or name of object to be authenticated, such as the AE, a human user, etc.

6.2.1.4.2 The semantic structure of an authentication-value is specified by the authentication-mechanism involved.

6.2.1.4.3 An authentication-function provides an authentication-value to its AEI to be sent to the peer AEI. The peer AEI's authentication-function receives and processes this authentication-value. For example, it may use the value to authenticate objects at the sending AEI.

6.2.1.4.4 An authentication-mechanism may be part of a ASE that provides security facilities to its service-user. In this situation, the authentication-mechanism name identifies the ASE; the authentication-value is an APDU of the ASE.

6.2.2 ACSE authentication facilities

6.2.2.1 The ACSE Kernel functional unit does not support authentication. However, AP Title, AE Qualifier, AP invocation-identifier and AE invocation-identifier values are optionally transferred during the establishment of an association. They may be used to identify the calling, called and responding AEIs.

6.2.2.2 The ACSE Authentication functional unit supports the transfer of authentication-values as part of the A-ASSOCIATE service. An authentication-value is treated as an atomic item by ACSE. Its semantics are transparent to the ACSE service-provider.

6.2.2.3 The facilities of the Authentication functional unit may be used to convey other security-related information. This may be done with the transfer of authentication information during association establishment.

{*END OF REPLACED CLAUSE 6.*}

7 Service overview

{*INSERT THE NEW HEADING 7.1.*}

7.1 ACSE services {*NEW HEADING*}

{*MOVE THE PARAGRAPHS UNDER ORIGINAL CLAUSE 7 TO THIS SUBCLAUSE AND RENUMBER THE PARAGRAPHS ACCORDINGLY. THEN INSERT NEW SUBCLAUSE 7.2.*}

7.2 Functional units {*NEW*}

7.2.1 Functional units are used by this International Standard to identify ACSE user requirements during association establishment. Two functional units are defined:

a) Kernel functional unit; and

b) Authentication functional unit.

7.2.2 The Kernel functional unit is always available, and includes the basic services identified in 7.1.

7.2.3 The Authentication functional unit supports authentication during association establishment. The availability of this functional unit is negotiated during association establishment. This functional unit does not include additional

services. It adds parameters to the A-ASSOCIATE and A-ABORT services.

7.2.4 Table a shows the services and parameters associated with the ACSE functional units. The services and their parameters are discussed in clause 9.

{INSERT NEW TABLE a. RENUMBER THE REMAINING TABLES AND ADJUST REFERENCES TO THESE TABLES IN THE TEXT.}

8 Relationship with other ASEs and lower layer services *{NO CHANGE}*

{NO CHANGE IS MADE TO THIS CLAUSE.}

9 Service definition

{NO CHANGE TO THE INTRODUCTORY TEXT}

9.1 A-ASSOCIATE service

{NO CHANGE TO THE INTRODUCTORY TEXT}

9.1.1 A-ASSOCIATE parameters

{TABLE 2 — ADD THE FOLLOWING PARAMETERS AFTER Responding AE Invocation-identifier.}

ACSE Requirements	U	C	C	C(=)
Authentication-mechanism Name	U	C(=)	U	C(=)
Authentication-value	U	C(=)	U	C(=)

{INSERT NEW SUBCLAUSES 9.1.1.14a, 9.1.1.14b AND 9.1.1.14c AFTER SUBCLAUSE 9.1.1.14 Responding AE Invocation-identifier.}

9.1.1.14a ACSE Requirements *{NEW}*

This parameter is used by the requestor to indicate the functional units requested for the association. If not present,

Table a — Functional unit services and their parameters *{NEW}*

Functional Unit	Service	Parameter
Kernel	A-ASSOCIATE	Mode 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 Responding AP Title Responding AE Qualifier Responding AP Invocation-identifier Responding AE Invocation-identifier User Information Result Result Source Diagnostic Calling Presentation Address Called Presentation Address Responding Presentation Address Presentation Context Definition List Presentation Context Definition Result List Default Presentation Context Name Default Presentation Context Result Quality of Service Session Requirements Initial Synchronization Point Serial Number Initial Assignment of Tokens Session-connection Identifier
	A-RELEASE	Reason User Information Result
	A-ABORT	Abort Source User Information
	A-P-ABORT	Provider Reason
Authentication	A-ASSOCIATE	Authentication-mechanism Name Authentication-value
	A-ABORT	Diagnostic

only the Kernel functional unit is available for the association. In supporting this negotiation mechanism, the ACSE service-provider removes values for unsupported functional units before issuing the indication primitive to the acceptor.

This parameter is used by the acceptor to indicate which of the requested functional units the acceptor selects. The acceptor shall not select a functional unit in the response primitive which was not requested in the indication primitive.

The value of the parameter in the response primitive is delivered unchanged in the confirm primitive.

This parameter takes on the following symbolic value:

—authentication.

9.1.1.14b Authentication-mechanism Name *{NEW}*

This parameter is only used if the ACSE Requirements parameter includes the Authentication functional unit. If present, the value of this parameter identifies the authentication-mechanism in use. If not present, the communicating AEIs must implicitly know the mechanism in use, e.g., by prior understanding.

NOTES

1 Some authentication-mechanisms may require this parameter, and if so, will state this in their specification.

2 This parameter may specify a more general authentication mechanism. For example, it may specify an ASE that provides security facilities to its service-user.

9.1.1.14c Authentication-value *{NEW}*

This parameter shall only be used if the ACSE Requirements parameter includes the Authentication functional unit.

The Authentication-value parameter is used as defined below.

a) If present on the request or the response primitive, it contains an authentication-value generated by the authentication-function in the AEI that issued the service primitive. It is intended for the peer's authentication-function.

b) If present on the indication or the confirm primitive, it contains an authentication-value generated by the authentication-function in the AEI that issued the corresponding request or response primitive. It is intended for the peer's authentication-function.

{END OF INSERTED SUBCLAUSES 9.1.1.a, 9.1.1.b AND 9.1.1.c.}

9.1.1.18 Diagnostic

{REPLACE THE FIRST PARAGRAPH USING THE FOLLOWING TEXT.}

This parameter may be used by the acceptor to provide diagnostic information about the establishment of the association.

{TO THE LIST OF SYMBOLIC VALUES FOR THE ACSE SERVICE-USER ADD THE FOLLOWING.}

Authentication-mechanism Name not recognized;

Authentication-mechanism Name required;

Authentication failure; or

Authentication required.

{END OF ADDED SYMBOLIC VALUES.}

9.1.2 A-ASSOCIATE procedure *{NO CHANGE}*

{NO CHANGE IS MADE TO THIS SUBCLAUSE.}

9.2 A-RELEASE service *{NO CHANGE}*

{NO CHANGE IS MADE TO THIS SUBCLAUSE.}

9.3 A-ABORT service

{NO CHANGE TO THE INTRODUCTORY TEXT}

9.3.1 A-ABORT parameters

{TABLE 4 — ADD THE FOLLOWING PARAMETER AFTER Abort Source.}

Diagnostic	U	C(=)

{RENUMBER THE ORIGINAL 9.3.1.2 AS 9.3.1.3. INSERT NEW SUBCLAUSE 9.3.1.2 USING THE FOLLOWING TEXT.}

9.3.1.2 Diagnostic

The requestor may optionally include diagnostic information on the request primitive. It takes one of the following symbolic values:

No reason given;

Protocol error;

Authentication-mechanism Name not recognized;

Authentication-mechanism Name required;

Authentication failure; or

Authentication required.

9.3.2 A-ABORT service procedure *{NO CHANGE}*

{NO CHANGE IS MADE TO THIS SUBCLAUSE.}

9.4 A-P-ABORT service *{NO CHANGE}*

{NO CHANGE IS MADE TO THIS SUBCLAUSE.}

10 Sequencing information *{NO CHANGE}*

{NO CHANGE IS MADE TO THIS CLAUSE.}