INTERNATIONAL STANDARDIZED PROFILE

ISO/IEC ISP 10609-16

First edition
1998-07-01

Information technology — International Standardized Profiles TB, TC, TD and TE — Connection-mode Transport Service over connection-mode Network Service —

Part 16:
Security employing the Network Layer Security Protocol — Connection-mode with No-header, for TB, TC, TD and TE profiles

Technologies de l'information — Profils normalisés internationaux TB, TC, TD et TE — Service de transport en mode connexion sur service de réseau en mode connexion —

Partie 16: Sécurité employant le protocole de sécurité de la couche réseau — Mode connexion avec en-tête NON, pour profils TB, TC, TD et TE

Reference number
ISO/IEC ISP 10609-16:1998(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. In addition to developing International Standards, ISO/IEC JTC 1 has created a Special Group on Functional Standardization for the elaboration of International Standardized Profiles.

An International Standardized Profile is an internationally agreed, harmonized document which identifies a standard or group of standards, together with options and parameters, necessary to accomplish a function or a set of functions.

Draft International Standardized Profiles are circulated to national bodies for voting. Publication as an International Standardized Profile requires approval by at least 75 % of the national bodies casting a vote.

International Standardized Profile ISO/IEC ISP 10609-16 was prepared with the collaboration of

— Asia-Oceania Workshop (AOW);

— European Workshop for Open Systems (EWOS);

— Open Systems Environment Implementors' Workshop (OIW).

ISO/IEC ISP 10609 consists of the following parts, under the general title *Information technology — International Standardized Profiles TB, TC, TD and TE — Connection-mode Transport Service over connection-mode Network Service*:

— *Part 1: Subnetwork-type independent requirements for Group TB*

— *Part 2: Subnetwork-type independent requirements for Group TC*

— *Part 3: Subnetwork-type independent requirements for Group TD*

— *Part 4: Subnetwork-type independent requirements for Group TE*

— *Part 5: Definition of profiles TB1111/TB1121*

— *Part 6: Definition of profiles TC1111/TC1121*

— *Part 7: Definition of profiles TD1111/TD1121*

— *Part 8: Definition of profiles TE1111/TE1121*

— *Part 9: Subnetwork-type dependent requirements for Network Layer, Data Link Layer and Physical Layer concerning permanent access to a packet switched data network using virtual calls*

— *Part 10: LAN subnetwork-dependent, media-independent requirements*

— *Part 11: CSMA/CD subnetwork-dependent, media-dependent requirements*

— *Part 12: Definition of profile TC51, provision of the OSI connection-mode Transport Service using the OSI connection-mode Network Service in an End System attached to a CSMA/CD/LAN*

— *Part 13: MAC sublayer and physical layer dependent requirements for a token ring local area network*

— *Part 14: Definition of profile TC53, provision of the OSI connection-mode Transport Service using the OSI connection-mode Network Service in an End System attached to a Token Ring LAN*

— *Part 15: Definition of profile TC54, provision of the OSI connection-mode Transport Service using the OSI connection-mode Network Service in an End System attached to an FDDI LAN*

— *Part 16: Security employing the Network Layer Security Protocol — Connection-mode with No-header, for TB, TC, TD and TE profiles*

— *Part 17: Security employing the Network Layer Security Protocol — Connection-mode with SDT-PDU based Protection, for TB/TC/TD/TEnnn profiles*

— *Part 20: Overview of the generalized multi-part ISP structure for TC and TD Group profiles for OSI-usage of ISDN*

— *Part 21: Subnetwork-type dependent requirements for Network Layer and Data Link Layer for ISDN B-channel X.25 DTE to DTE operation*

— *Part 22: Subnetwork-type dependent requirements for Network Layer and Data Link Layer for ISDN B-channel X.25 DTE to DCE operation*

— *Part 23: Subnetwork-type dependent requirements for Network Layer and Data Link Layer for Data Transfer concerning a packet switched mode Integrated Services Digital Network using virtual calls: B-channel access case*

— *Part 24: Subnetwork-type dependent requirements for Network Layer and Data Link Layer for Data Transfer concerning a packet switched mode Integrated Services Digital Network using virtual calls: D-channel access case*

— *Part 25: Subnetwork-type dependent requirements for Q.931 circuit-switched operation*

— *Part 26: Subnetwork-type dependent requirements for Network Layer for Call Control procedures concerning the outgoing call of a packet switched mode Integrated Services Digital Network in case B using virtual calls*

— *Part 27: Subnetwork-type dependent requirements for Network Layer for Call Control procedures concerning the incoming call of a packet switched mode Integrated Services Digital Network in case B using virtual calls*

— *Part 28: Subnetwork-type dependent requirements for Data Link Layer for end systems attached to an ISDN subnetwork*

— *Part 30: Definition of profile TC1131*

— *Part 31: Definition of profile TC1231*

— *Part 32: Definition of profile TC4111*

— *Part 33: Definition of profile TC4211*

— *Part 34: Definition of profile TC43111*
— *Part 35: Definition of profile TC43112*
— *Part 36: Definition of profile TC43211*
— *Part 37: Definition of profile TC43212*
— *Part 38: Definition of profile TC4331*
— *Part 40: Definition of profile TD1131*
— *Part 41: Definition of profile TD1231*
— *Part 42: Definition of profile TD4111*
— *Part 43: Definition of profile TD4211*
— *Part 44: Definition of profile TD43111*
— *Part 45: Definition of profile TD43112*
— *Part 46: Definition of profile TD43211*
— *Part 47: Definition of profile TD43212*
— *Part 48: Definition of profile TD4331*

Annex A forms an integral part of this part of ISO/IEC ISP 10609. Annex B is for information only.

Introduction

ISO/IEC ISP 10609 is defined in accordance with the principles specified by ISO/IEC Technical Report 10000.

The context of Functional Standardization is one area in the overall field of Information Technology (IT) standardization activities, covering base standards, profiles, and registration mechanisms. A profile defines a combination of base standards that collectively perform a specific well-defined IT function. Profiles standardize the use of options and other variations in the base standards, and provide a basis for the development of uniform, internationally recognized system tests.

ISPs are produced not simply to 'legitimize' a particular choice of base standards and options, but to promote real system interoperability. One of the most important roles for an ISP is to serve as the basis for the development (by organizations other than ISO and IEC) of internationally recognized tests. The development and widespread acceptance of tests based on this and other ISPs is crucial to the successful realization of this goal.

ISO/IEC ISP 10609 consists of several parts of which this is part 16. This part of ISO/IEC 10609 specifies the security subprofile employing the Network Layer Security Protocol (ITU-T X.273 | ISO/IEC 11577) connection-mode with no header.

This part extends existing TB, TC, TD and TE profiles adding security protection.

Information technology — International Standardized Profiles TB, TC, TD and TE — Connection-mode Transport Service over connection-mode Network Service —

Part 16:
Security employing the Network Layer Security Protocol — Connection-mode with No-header, for TB, TC, TD and TE profiles

1 Scope

1.1 General

ISO/IEC 10609 is applicable to End Systems concerned with operating in the Open Systems Interconnection (OSI) environment. It specifies a combination of OSI standards which collectively provide the connection-mode Transport Service using the connection-mode Network Service.

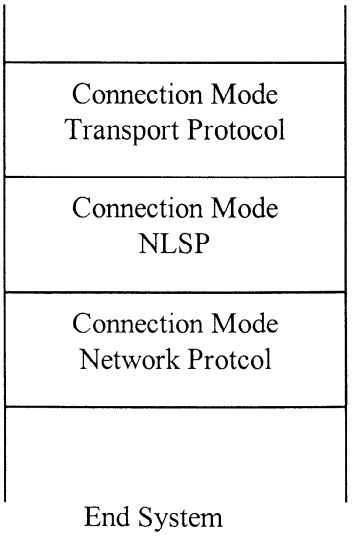
This part of ISO/IEC 10609 specifies a security sub-profile for the provision of security services using cryptographic techniques with Network Layer Security Protocol connection-mode and no-header mode.

1.2 Position within the Taxonomy

The taxonomy of profiles is specified in ISO/IEC TR 10000-2. This part of ISO/IEC ISP 10609 supports security services for any TB, TC, TD or TE profile specified in ISO/IEC ISP 10609 (Connection-mode transport over connection-mode Network Service).

Note: ISO/IEC TR 10000 currently does not identify security sub-profiles. Profiles based on this part of ISO/IEC ISP 10609 may be referred to as TB/C/D/EnnnS1, or TB/C/D/nnnS1C if confidentiality is selected.

1.3 Scenario



1.4 Security Services

The following security services are within the scope of this part of ISO/IEC ISP 10609:

a) Peer entity authentication

b) Connection confidentiality (optional)

Notes

1) It is strongly recommended that some form of access control is supported. However, this may be achieved using local access control lists which are outside the scope of this profile.

2) Limited connection integrity without recovery may be provided by the encipherment mechanism for confidentiality depending on the algorithm employed (e.g. stream ciphers and algorithms employing cipher block chaining may provide integrity protection whereas electronic code book ciphers are likely to provide little or no integrity protection).

1.5 Security Mechanisms

This part of ISO/IEC ISP 10609 provides no assurance as to the strength of the security mechanisms employed.

This part of ISO/IEC ISP 10609 does not specify the cryptographic algorithms to be employed.

2 Normative References

The following documents contain provisions which, through reference in this text, constitute provisions of this part of ISO/IEC 10609. At the time of publication, the editions indicated were valid. All documents are subject to revision, and parties to agreements based on this part of ISO/IEC ISP 10609 are warned against automatically applying any more recent editions of the documents listed below, since the nature of the references made by ISPs to such documents is that they may be specific to a particular edition. Members of IEC and ISO maintain registers of currently valid International Standards and ISPs, and the ITU maintains published editions of its current Recommendations.

- ITU-T Recommendation X.273 (1994) | ISO/IEC 11577: 1995 *Information technology - Open Systems Interconnection - Network layer security protocol.*

3 Definitions

The terms used in this part of ISO/IEC 10609 are specified in the base standards referenced (see clause 2).

4 Abbreviations

The abbreviations and acronyms used in this part of ISO/IEC 10609 are specified in the base standards referenced (see clause 2).

5 Requirements

5.1 General

The requirements stated in these clauses apply to all conforming systems, without regard to the type of subnetworks to which those end systems might be attached or the class of transport service used. Additional requirements are specified in other parts of ISO/IEC ISP 10609.

This part of ISO/IEC ISP 10609 specifies provision of security services using the Network Layer Security Protocol connection-mode with the no-header mode.

Additional requirements are given in annex A which specifies the IPRL for the Network Layer Security Protocol.

5.2. Static Conformance Requirements

A conforming system shall:

a) support the NLSP-CO mode conformance class capabilities as stated in 14.1.3 of ITU-T X.273 | ISO/IEC 11577.

b) support the CSC-PDU structure as specified in 13.5 of ITU-T X.273 | ISO/IEC 11577.

c) support peer entity authentication using the enciphered auth-data field as specified in 13.5.7 of ITU-T X.273 | ISO/IEC 11577.

d) if it claims support of connection confidentiality (sub-profile S1C), support this service though an encipherment mechanism.

e) if it claims support of the security association protocol, support the SA-PDU as specified in 13.4 and the SA-PDU SA Contents as specified in clause C.7 of ITU-T X.273 | ISO/IEC 11577.

Note: Use of the SA-P is recommended for this security sub-profile.

f) Map the NLSP PDUs directly onto ISO/IEC 8208 | CCITT X.25 as specified in Annex B of ITU-T X.273 | ISO/IEC 11577.

5.3. Dynamic Conformance Requirements

A conforming system shall:

a) exhibit external behaviour consistent with having implemented the common protocol functions specified in clause 6, the NLSP-CO protocol functions specified in clause 7 (for the modes described below) and the mechanism specific protocol functions specified in clauses 10 and 12 of ITU-T X.273 | ISO/IEC 11577.

b) support SA-ID parameter length of 4 octets.

Note: If required other SA-ID lengths may also be supported.

c) support NLSP-CONNECT in UN-CONNECT mode of connection establishment (optionally with SA-P) as specified in 8.5.2 and 8.5.3 of ITU-T X.273 | ISO/IEC 11577.

d) support NLSP-DISCONNECT in UN-DISCONNECT mode of connection release as specified in 8.10 of ITU-T X.273 | ISO/IEC 11577.

e) support the No-header mode of protection of userdata as specified in 8.6.

f) support protection of NLSP Userdata, optionally including protection of userdata in the NLSP CONNECT as specified in 5.5.1(b) of ITU-T X.273 | ISO/IEC 11577.

A conformant system may dynamically select the security services, and hence the security mechanisms employed on a particular security association.

5.4. Placement

The NLSP protocol shall operate above the connection-mode network protocol and below the transport protocol as described in clause E.4 of Annex E of ITU-T X.273 | ISO/IEC 11577.

Annex A

(normative)

International Standardized Profile Implementation Conformance Statement Requirements List (IPRL)

A.1 Introduction

The IPRL in this annex specifies the additional requirements for ITU-T X.273 | ISO/IEC 11577.

The requirements of ITU-T X.273 | ISO/IEC 11577 apply to each item for which there is no entry in this IPRL. This is excluding requirements specific to NLSP-CL which are outside the scope of this ISP.

The IPRL in the annex has been generated for this ISP based on ITU-T X.273 | ISO/IEC 11577.

A.2 Notation

The following tables specify the functions supported for which conformance is claimed, using the following keys.

a) Base standards status notation

M mandatory

O optional

O.<n> optional, but support of at least one of the group of options labelled by the same numeral <n> is required

X prohibited

<item>: conditional-item symbol, dependent upon the support marked for <item>

b) IPRL status notation

m mandatory (implementation is mandatory)

o optional (implementation is optional)

i out of scope (not relevant to this part of ISO/IEC ISP 10609)

A.3 Features Common to NLSP-CO and NLSP-CL

A.3.1 Major Capabilities (Common)

Base Standard Features				ISP Features	
Item	**Questions/Features**	**Ref.**	**Status**	**ISP Ref.**	**Status**
CO*	Is the connection-mode supported?	5.1	O.1	5.2 a	m
CL*	Is the connectionless-mode supported?	5.1	O.1	5.2 a	i
AC	Is Access Control supported?	5.2	O	1.3	o (see note)
TFC*	Is Traffic Flow Confidentiality supported?	5.2	O	1.3	i
ParamProt*	Is protection of all NLSP service parameters supported	5.5.1a	O.2	5.3 f	i
UserDatProt	Is protection of NLSP Userdata supported	5.5.1b	O.2	5.3 f	m
NoProt*	Is no protection supported	5.5.1c	O		o
SdtBasc*	Is any SDT PDU based encapsulation function supported?	5.5.3.	CO:O.3 CL:M ParamProt: M	5.3 a	i
NoHcad	Is any no header encapsulation function supported?	5.5.3	CO:O.3 CL:X ParamProt: X	5.3 a	m
SA-P*	Is any in-band SA-P supported?	5.4.1	O	5.2 e	o
LabMech*	Is the label mechanism supported	6.2g, 6.4.1.1e 6.4.2.1f	SdtBase:O		i
SDTMech*	Is the standardised SDT PDU based encapsulation functions supported	11	SdtBase:O	5.3 a	i
NoHeadMech	Is the standardised No Header encapsulation function supported	12	NoHead:O	5.3 a	m

Note: It is recommended that access control is supported through locally defined mechanisms (e.g. access control lists).

A.3.2 PDUs (Common)

Base standard features				ISP Features	
Item	**Questions/Features**	**Refs**	**Status**	**ISP Ref.**	**Status**
SDT*	Is the Secure Data Transfer PDU supported on transmission / receive?	6.4.1.1 13.3	SdtBase:M		i
SA*	Is the Security Association PDU supported on transmission / receive?	5.4.1, 13.4	SA-P:O	5.2 e	o

A.3.3 SDT PDU Fields Common to CO & CL & Generic to Mechanisms

Support for the SDT PDU is outside the scope of this part of ISO/IEC ISP 10609

A.3.4 SDT PDU Fields Common to CO & CL with Specific SDT Based Encapsulation Mech.

Support for the SDT PDU is outside the scope of this part of ISO/IEC ISP 10609

A.3.5 SA PDU Fields Generic to SA-P

Requirements as in clause D.5.5 of ITU-T X.273 | ISO/IEC 11577.

A.3.6 SA PDU Fields Specific to Key Token Exchange SA-P

Requirements as in clause D.5.6 of ITU-T X.273 | ISO/IEC 11577.

A.4 Features Specific to NLSP-CL

Support for NLSP-CL is outside the scope of this part of ISO/IEC ISP 10609

A.5 Features Specific to NLSP-CO

A.5.1 Major Capabilities (NLSP-CO)

Base standard features				ISP Features	
Item	**Questions/Features**	**Refs**	**Status**	**ISP Ref.**	**Status**
SNAcP	Is the protocol mapping directly onto CCITT Rec. X.25 | ISO 8208?	5.3, Annex B	CO:O.7	5.2 f	m
SNISP*	Is the protocol mapping onto CCITT Rec. X.213 | ISO 8348	5.3 Annex A	CO:O.7	5.2 f	i
COConf*	Is connection confidentiality supported?	5.2	CO:O.8	1.3	o
COInteg*	Is connection integrity without recovery supported?	5.2	CO:O.8	1.3	(see note below)
PEA	Is peer entity authentication supported?	5.2	CO:O.8	1.3	m
ExCSC*	Is Example CSC PDU procedures defined in NLSP supported?	10	CO:O	5.3 a	m

Note: Limited connection integrity without recovery may be provided by the encipherment mechanism for confidentiality depending on the algorithm employed.

A.5.2 PDUs (Connection Mode)

Base standard features				ISP Features	
Item	**Questions/Features**	**Refs**	**Status**	**ISP Ref.**	**Status**
CSC*	Connection Security Control PDU	8.5, 13.5	CO:M	5.2 b	m