INTERNATIONAL STANDARDIZED PROFILE

ISO/IEC ISP 10608-7

First edition
1998-08-01

Information technology — International Standardized Profile TAnnnn — Connection-mode Transport Service over Connectionless-mode Network Service —

Part 7:

Security employing the Network Layer Security Protocol — Connectionless-mode for TAnnnn profiles

Technologies de l'information — Profil normalisé international TAnnnn — Service de transport en mode connexion sur service de réseau en mode sans connexion —

Partie 7: Sécurité employant le protocole de sécurité de la couche réseau — Mode sans connexion, pour profils TAnnnn

Reference number
ISO/IEC ISP 10608-7:1998(E)

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS

Not for Resale

Contents

1. SCOPE 1

1.1. General 1

1.2. Position within the Taxonomy 1

1.3. Scenario 1

1.4. Security Services 2

1.5. Security Mechanisms 2

2. NORMATIVE REFERENCES 2

3. DEFINITIONS 2

4. ABBREVIATIONS 2

5. REQUIREMENTS 3

5.1. General 3

5.2. Static Conformance Requirements 3

5.3. Dynamic Conformance Requirements 3

5.4. Placement 4

ANNEX A - INTERNATIONAL STANDARDIZED PROFILE IMPLEMENTATION CONFORMANCE STATEMENT REQUIREMENTS LIST (IPRL) 5

A.1 Introduction 5

A.2 Notation 5

A.3 Features Common to NLSP-CO and NLSP-CL 6

A.3.1 Major Capabilities (Common) 6

A.3.2 PDUs (Common) 7

A.3.3 SDT PDU Fields Common to CO & CL & Generic to Mechanisms 7

A.3.4 SDT PDU Fields Common to CO & CL with Specific SDT Based Encapsulation Mech. 8

© ISO/IEC 1998

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and micro-film, without permission in writing from the publisher.

ISO/IEC Copyright Office • Case postale 56 • CH-1211 Genève 20 • Switzerland

Printed in Switzerland

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

A.4 Features Specific to NLSP-CL 9

A.4.1 Major Capabilities (NLSP-CL) 9

A.4.2 Initiator/Responder (Connectionless Mode) 9

A.4.3 Environment (Connectionless Mode) 9

A.4.4 SDT PDU Fields (Connectionless Mode) 10

A.5 Placement 10

ANNEX B- ADDITIONAL AGREEMENTS REQUIRED 11

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

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 10608-7 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 10608 consists of the following parts, under the general title *Information technology — International Standardized Profile TAnnnn — Connection-mode Transport Service over Connectionless-mode Network Service*:

— *Part 1: General overview and subnetwork-independent requirements*

— *Part 2: TA51 profile including subnetwork-dependent requirements for CSMA/CD Local Area Networks (LANs)*

— *Part 4: Definition of profile TA53, operation over a Token Ring LAN subnetwork*

— *Part 5: TA1111/TA1121 profiles including subnetwork-dependent requirements for X.25 packet-switched data networks using virtual calls*

— *Part 6: Definition of profile TA54, operation over an FDDI LAN subnetwork*

— *Part 7: Security employing the Network Layer Security Protocol — Connectionless-mode for TAnnnn profiles*

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

— *Part 8: Security employing the Network Layer Security Protocol — Connection-mode with SDT-PDU based protection over X.25 packet switched data networks using virtual calls, for TA1111/TA1121 profiles*

— *Part 12: MAC sublayer and physical layer dependent requirements for a CSMA/CD LAN subnetwork*

— *Part 13: MAC sublayer and physical layer dependent requirements for a Token Ring LAN subnetwork*

— *Part 14: MAC, PHY and PMD sublayer dependent and Station Management requirements over an FDDI LAN subnetwork*

Annex A forms an integral part of this part of ISO/IEC ISP 10608. Annex B is for information only.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Introduction

ISO/IEC ISP 10608 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 10608 consists of several parts of which this is part 7. This part of ISO/IEC 10608 specifies the security profile requirements employing the Network Layer Security Protocol (ITU-T X.273 | ISO/IEC 11577) connectionless-mode.

This part extends existing TA profiles adding security protection.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

Information technology — International Standardized Profile TAnnnn — Connection-mode Transport Service over Connectionless-mode Network Service —

Part 7:

Security employing the Network Layer Security Protocol -- Connectionless-mode for TAnnnn profiles

1 Scope

1.1 General

ISO/IEC 10608 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 connectionless-mode Network Service.

This part of ISO/IEC 10608 specifies the profile requirements for the provision of security services using cryptographic techniques with the Network Layer Security Protocol connectionless-mode.

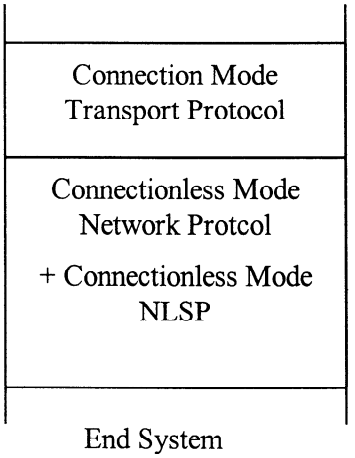
This part of ISO/IEC 10608 specifies profile requirements that are applicable to any type of subnetwork.

1.2 Position within the Taxonomy

The taxonomy of profiles is specified in ISO/IEC TR 10000-2. This part of ISO/IEC ISP 10608 supports security services for any TA profile specified in ISO/IEC ISP 10608 (Connection-mode transport over Connectionless-mode Network Service).

Note: ISO/IEC TR 10000 currently does not identify security sub-profiles. Profiles based on this part of ISO/IEC ISP 10608 may be referred to as TAnnnS1, or TAnnnS1C if confidentiality is selected.

1.3 Scenario



Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Note: The relationship between the Connectionless Mode Network Protocol and Connectionless Mode NLSP is specified in 5.4

1.4 Security Services

The following security services are within the scope of this part of ISO/IEC ISP 10608:

a) Data origin authentication

b) Connectionless integrity

Note: 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 ISO/IEC ISP 10608.

c) Access control using security labels (optional)

d) Connectionless confidentiality (optional)

e) Traffic flow confidentiality (optional)

1.5 Security Mechanisms

This part of ISP 10608 provides no assurance as to the strength of the security mechanisms employed.

This part of ISO/IEC ISP 10608 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 10608. 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 10608 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 10608 are specified in the base standards referenced (see clause 2).

4 Abbreviations

The abbreviations and acronyms used in this part of ISO/IEC 10608 are specified in the base standards referenced (see clause 2).

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

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. Additional requirements are specified in other parts of ISO/IEC ISP 10608.

This part of ISO/IEC ISP 10608 specifies provision of security services using the Network Layer Security Protocol connectionless-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-CL mode conformance class capabilities as stated in 14.1.2 of ITU-T X.273 | ISO/IEC 11577.

b) support the SDT-PDU structure as specified in 13.3 of ITU-T X.273 | ISO/IEC 11577.

c) support the static requirements for mechanisms to support connectionless integrity and data origin authentication using the ICV field as specified in 13.3.3.2, and optionally the ISN field as specified in clause 13.3.5.1, of ITU-T X.273 | ISO/IEC 11577.

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

e) support protection of NLSP Userdata as specified in 5.5.1 b of ITU-T X.273 | ISO/IEC 11577. Protection of all NLSP Service Parameters is outside the scope of the scope of this part of part of ISO/IEC ISP 10608.

f) if a system claims to support the security association protocol, this is carried in the SDT PDU content fields with the data type field SA Protocol as specified in 13.3.4.2 of ITU-T X.273 | ISO/IEC 11577.

Notes:

1) The details of the SA Protocol is currently outside the scope of this part of ISO/IEC ISP 10608.

2) Use of the SA-P is not recommended except in specific environments where it is known that the subnetworks utilised provide a reliable communications service.

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-CL protocol functions specified in clause 7 and the mechanism specific protocol functions specified in clause 11 of ITU-T X.273 | ISO/IEC 11577.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

b) discard any padding fields in the received STD-PDU (single octet, traffic pad, integrity pad and encipherment pad; see 13.3.5 of ITU-T X.273 | ISO/IEC 11577) and STD PDUs without any Userdata .

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

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

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

5.4 Placement

The system shall support placement of the NLSP protocol in relation to the connectionless network protocol - CLNP (ITU-T X.233 | ISO/IEC 8473) either:

a) With a (protected) CLNP protocol layer operating above NLSP which operates above a second (unprotected) CLNP protocol layer, as described in clauses E.5 of Annex E of ITU-T X.273 | ISO/IEC 11577, or

b) Using a dynamic relationship between CLNP and NLSP as specified in clause E.7 of Annex E of ITU-T X.273 | ISO/IEC 11577.

Note: A system may also support the following alternative placements as described in clauses E.5 of Annex E of ITU-T X.273 | ISO/IEC 11577 however, these placements are outside the scope of this part of ISO/IEC ISP 10608.

c) With NLSP operating above CLNP. (This can only be used between end systems)

d) With a (protected) CLNP protocol layer operating above NLSP which operates directly over a sub-network. (This can only be used across a single subnetwork)

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

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-CO 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)

o.<n> optional, but implementation of at least one of the group of options labelled by the same numeral <n> is mandatory

i out of scope (not relevant to this part of ISO.IEC 10608)

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

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	i
CL*	Is the connectionless-mode supported?	5.1	O.1	5.2 a	m
AC	Is Access Control supported?	5.2	O		o
TFC Send	Is traffic Flow Confidentiality Supported for sending	5.2	O	5.3 b	o
TFC Rec	Can the system discard any traffic padding (including STD PDUs without any userdata) on receipt			5.3 b	m
ParamProt*	Is protection of all NLSP service parameters supported	5.5.1a	O.2	5.2 e	i (see note 3 below
UserDatProt	Is protection of NLSP Userdata supported	5.5.1b	O.2	5.2 e	m
NoProt*	Is no protection supported	5.5.1c	O		o
SdtBase*	Is any SDT PDU based encapsulation function supported?	5.5.3.	CO:O.3 CL:M ParamProt: M	5.3 a	m
NoHead	Is any no header encapsulation function supported?	5.5.3	CO:O.3 CL:X ParamProt: X	5.3.a	i
SA-P*	Is any in-band SA-P supported?	5.4.1	O	5.2 f	o (see note 2 below)
LabMech*	Is the label mechanism supported	6.2g, 6.4.1.1e 6.4.2.1f	SdtBase:O		o
SDTMech*	Is the standardised SDT PDU based encapsulation functions supported	11	SdtBase:O	5.3 a	m
NoHeadMech	Is the standardised No Header encapsulation function supported	12	NoHead:O	5.3 a	i

Note: 1) It is mandatory that a system can discard traffic padding

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

2) Use of the SA-P is not recommended except in specific environments where it is known that the subnetworks utilised provide a reliable communications service.

3) Protection of NLSP service parameters is considered unnecessary as similar protection can be achieved by placing the NLSP protocol below a CLNP protocol layer which itself contains protected address etc. information.

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	5.2 b	m
SA*	Is the Security Association PDU supported on transmission / receive?	5.4.1, 13.4	SA-P:O		i

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

Base Standard Features				ISP Features	
Item	**Questions/Features**	**Refs**	**Status**	**ISP Ref.**	**Status**
SdtPID	PID field value 1000 1011 in each SDT PDU	13.3.2.1	SDT:M		m
SdtLI	Length Indicator field in each SDT PDU	13.3.2.2	SDT:M		m
SdtPDUType	PDU Type field with value 01001000 in each SDT PDU	13.3.2.3	SDT:M		m
SdtContLen	Content Length in each SDT PDU	13.3.4.1	SDT:M		m
DataType	Data Type field in each SDT PDU	13.3.4.2	SDT:M		m
UserData	Content field type C0 - Userdata	13.3.4.3	SDT:O		m
CSAddr	Content field type C2 - Calling/Source NLSP address	13.3.4.3	ParamProt: M		i
CDAddr	Content field type C3 - Calling/Destination NLSP address	13.3.4.3	ParamProt: M		i

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

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

Base Standard Features				ISP Features	
Item	**Questions/Features**	**Refs**	**Status**	**ISP Ref.**	**Status**
Synch	Crypto synchornisation	11.3, 13.3.3.1	O		o
ICV	ICV field	11.3, 13.3.3.2	COInteg: M CLInteg:M	5.2 c	m
SeqNo	Sequence Number Content Field	11.3, 13.3.5.1	COInteg:O CLInteg:O	5.2 c	o
EncPad Send	Padding for Encipherment - Sending	11.3, 13.3.3.3	COConf:O CLConf:O	5.3 b	CLConf: o
EncPad Rec	Padding for Encipherment - Discard on receipt	11.3, 13.3.3.3	COConf:O CLConf:O	5.3 b	m
SinglePad Send	Single octet general padding field - Sending	11.3, 13.3.5.2	O	5.3 b	o
SinglePad Rec	Single octet general padding field - Discard on receipt	11.3, 13.3.5.2	O	5.3 b	m
TFCPad Send	Traffic padding - Sending	11.3, 13.3.5.3	TFC:M	5.3 b	TFC:o
TFCPad Rec	Traffic padding - Discard on receipt	11.3, 13.3.5.3	TFC:M	5.3 b	m
IntegPad Send	Padding for Integrity - Sending	11.3, 13.3.5.4	COInteg:O CLInteg:O	5.3 b	CLInteg: o
IntegPad Rec	Padding for Integrity - Discard on receipt	11.3, 13.3.5.4	COInteg:O CLInteg:O	5.3 b	m

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

A.4 Features Specific to NLSP-CL

A.4.1 Major Capabilities (NLSP-CL)

	Base Standard Features			ISP Features	
Item	**Questions/Features**	**Refs**	**Status**	**ISP Ref.**	**Status**
CLConf*	Is connectionless confidentiality supported?	5.2	CL:O.5	1.3	o
CLInteg*	Is connectionless integrity supported?	5.2	CL:O.5	1.3	m
DOA	Is Data Origin Authentication supported?	5.2	CL:O.5	1.3	m

A.4.2 Initiator/Responder (Connectionless Mode)

	Base Standard Features			ISP Features	
Item	**Questions/Features**	**Refs**	**Status**	**ISP Ref.**	**Status**
CLXmtProt	Is the implementation capable of transmitting protected connectionless data units?	7.6	CL:O.6		m
CLRcvProt	Is the implementation capable of accepting incoming protected connectionless data units?	7.7	CL:O.6		m
CLXmt	Is the implementation capable of transmitting unprotected connectionless data units?	7.6.1	NoProt:M		o
CLRcv	Is the implementation capable of accepting incoming unprotected connectionless data units?	7.7.1	NoProt:M		o

A.4.3 Environment (Connectionless Mode)

	Base Standard Features			ISP Features	
Item	**Questions/Features**	**Refs**	**Status**	**ISP Ref.**	**Status**
CL1	Are the mandatory elements of IS 8348AD1 supported?	5.2	CL:M		m

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

A.4.4 SDT PDU Fields (Connectionless Mode)

Base Standard Features				ISP Features	
Item	**Questions/Features**	**Refs**	**Status**	**ISP Ref.**	**Status**
SdtSA-ID	SA-ID field transmitted in each SDT PDU?	13.3.2.4	CL:M		m
StdSA-IDlen	Length of SA-ID field			5.3 c	4 octets

A.5 Placement

ISP Features				
Item	**Questions/Features**	**Refs**	**Status**	**Support**
NLSPPos1	NLSP over CLNP	5.4 c	i	Yes No
NLSPPos2	CLNP over NLSP over CLNP	5.4 a	o.1	Yes No
NLSPPos3	CLNP over NLSP	5.4 d	i	Yes No
NLSPPos4	Dynamic	5.4 b	o.1	Yes No

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Annex B
(Informative)
Additional Agreements Required

This ISP does not specify those parameters directly related to the choice of cryptographic algorithm. The selection of algorithm may be subject to national regulations and export restrictions. Advice on cryptographic algorithms may be obtained from the user's national security authority or other body or association which represents the user's community of interest.

Before interworking with other parties agreements need to be established on the following additional parameters:

a) The algorithm (cryptographic or hashing) used to generate the ICV field and the required length of the ICV field.

b) If the ISN field is supported: the ISN field length and sequencing algorithm

c) If confidentiality is supported: the encipherment algorithm employed including mode of operation, crypto-synchronisation and block size as relevant.

d) If security labelling is supported, the label defining authorities recognised.

e) SA management mechanism including key management.

These parameters may be registered as an "Agreed Set of Security Rules".

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

--`,,```,,,,````-`-`,,`,,`,`,,`---

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

© ISO/IEC

ICS 35.100.05

Descriptors: data processing, information interchange, network interconnection, open systems interconnection, network layer, data transmission, services, profiles.

Price based on 11 pages

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS

Not for Resale