INTERNATIONAL STANDARDIZED PROFILE

ISO/IEC ISP 10613-20

First edition
1998-07-01

Information technology — International Standardized Profile RA — Relaying the Connectionless-mode Network Service —

Part 20:

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 RA1111/RA1121 profiles

Technologies de l'information — Profil normalisé international RA — Relais de service de réseau en mode sans connexion —

Partie 20: Sécurité employant le protocole de sécurité de la couche réseau — Mode connexion avec protection basée SDT-PDU sur réseaux de données à commutation par paquets X.25 utilisant des appels virtuels, pour profils RA1111/RA1121

Reference number
ISO/IEC ISP 10613-20:1998(E)

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 3

4 ABBREVIATIONS 3

5 REQUIREMENTS 3

5.1 General 3

5.2 Static Conformance Requirements 3

5.3 Dynamic Conformance Requirements 4

5.4 Placement 4

ANNEX A 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
A.3.5 SA PDU Fields Generic to SA-P 8
A.3.6 SA PDU Fields Specific to Key Token Exchange SA-P 8

A.4 Features Specific to NLSP-CL 8

A.5 Features Specific to NLSP-CO 9
A.5.1 Major Capabilities (NLSP-CO) 9
A.5.2 PDUs (Connection Mode) 9
A.5.3 Modes of Connection Establishment / Release 10
A.5.4 Environment (Connection Mode) 10
A.5.5 Timers and Parameters (Connection Mode) 10
A.5.6 SDT PDU Fields (Connection Mode) 11
A.5.7 CSC PDU Fields - Generic (Connection Mode) 11
A.5.8 Example CSC PDU Content (Connection Mode) 12

ANNEX B- ADDITIONAL AGREEMENTS REQUIRED 13

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 10613-20 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 10613 consists of the following parts, under the general title *Information technology — International Standardized Profile RA — Relaying the Connectionless-mode Network Service*:

— *Part 1: Subnetwork- independent requirements*

— *Part 2: LAN subnetwork-dependent, media-independent requirements*

— *Part 3: CSMA/CD LAN subnetwork-dependent, media-dependent requirements*

— *Part 4: FDDI LAN subnetwork-dependent, media-dependent requirements*

— *Part 5: Definition of profile RA51.51, relaying the Connectionless-mode Network Service between CSMA/CD LAN subnetworks*

— *Part 6: Definition of profile RA51.54, relaying the Connectionless-mode Network Service between CSMA/CD LAN subnetworks and FDDI LAN subnetworks*

— *Part 7: PSDN subnetwork-dependent, media-dependent requirements for virtual calls over a permanent access*

— *Part 8: Definition of profile RA51.1111, relaying the Connectionless-mode Network Service between CSMA/CD LAN subnetworks and PSDNs using virtual calls over a PSTN leased line permanent access*

— *Part 9: Definition of profile RA51.1121, relaying the Connectionless-mode Network Service between CSMA/CD LAN subnetworks and PSDNs using virtual calls over a digital data circuit/CSDN leased line permanent access*

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

— *Part 11: Definition of profile RA51.53, relaying the Connectionless-mode Network Service between CSMA/CD LAN subnetworks and Token Ring LAN subnetworks*

— *Part 12: Definition of profile RA53.53, relaying the Connectionless-mode Network Service between Token Ring LAN subnetworks*

— *Part 13: Definition of profile RA53.54, relaying the Connectionless-mode Network Service between Token Ring LAN subnetworks and FDDI LAN subnetworks*

— *Part 14: Definition of profile RA54.54, relaying the Connectionless-mode Network Service between FDDI LAN subnetworks*

— *Part 15: Definition of profile RA53.1111, relaying the Connectionless-mode Network Service between Token Ring LAN subnetworks and PSDNs using virtual calls over a PSTN leased line permanent access*

— *Part 16: Definition of profile RA53.1121, relaying the Connectionless-mode Network Service between Token Ring LAN subnetworks and PSDNs using virtual calls over a digital data circuit/CSDN leased line permanent access*

— *Part 17: Definition of profile RA54.1111, relaying the Connectionless-mode Network Service between FDDI LAN subnetworks and PSDNs using virtual calls over a PSTN leased line permanent access*

— *Part 18: Definition of profile RA54.1121, relaying the Connectionless-mode Network Service between FDDI LAN subnetworks and PSDNs using virtual calls over a digital data circuit/CSDN leased line permanent access*

— *Part 19: Security employing the Network Layer Security Protocol — Connectionless-mode, for RAnn.nn profiles*

— *Part 20: 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 RA1111/RA1121 profiles*

Annex A forms an integral part of this part of ISO/IEC ISP 10613. Annex B is for information only.

Introduction

ISO/IEC ISP 10613 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 10613 consists of several parts of which this is part 20. This part of ISO/IEC 10613 specifies the security profile requirements employing the Network Layer Security Protocol (ITU-T X.273 | ISO/IEC 11577) connection-mode with SDT-PDU based protection over an X.25 packet-switched data network using virtual calls.

This part of ISO/IEC ISP 10613 extends existing RA1111 or RA1121 profiles adding security protection.

Information technology — International Standardized Profile RA — Relaying the Connectionless-mode Network Service —

Part 20:
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 RA1111/RA1121 profiles

1 Scope

1.1 General

ISO/IEC ISP 10613 is applicable to interworking units concerned with operating in the Open Systems Interconnection (OSI) environment. It specifies a combination of OSI standards that collectively provide a Network Relay function for the connection-mode Network Service.

Part 7 of ISO/IEC ISP 10613 specifies subnetwork type dependent requirements for an interworking unit when attached to an X.25 packet switched data network by a dedicated (permanent) access line and using virtual calls.

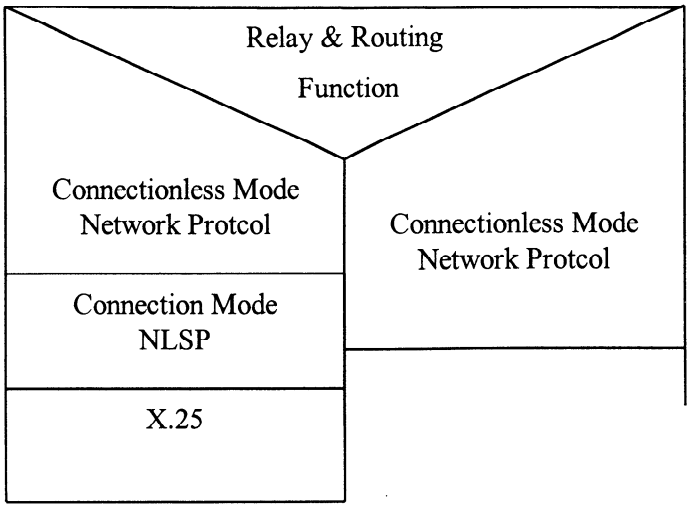
This part of ISO/IEC ISP 10613 specifies the profile requirements for the provision of security services using cryptographic techniques with Network Layer Security Protocol connection-mode and SDT-PDU based protection for use with X.25 packet switched data networks as specified in part 7 of 10613.

1.2 Position within the Taxonomy

The taxonomy of profiles is specified in ISO/IEC TR 10000-2. This part of ISO/IEC ISP 10613 supports security services for RA1111 and RA1121 profiles as specified in ISO/IEC ISP 10613 part 5.

Note: ISO/IEC TR 10000 currently does not identify security sub-profiles. Profiles based on this part of ISO/IEC ISP 10613 may be referred to as RA11n1S2, or RA11n1S2C if confidentiality is selected.

1.3. Scenario



Relay System

1.4 Security Services

The following security services are within the scope of this profile:

a) Peer entity authentication

b) Connection integrity without recovery (including replay protection)

c) Access control using security labels

Note: Where label based access control is not enforced by a system a null label may be employed.

d) Connection confidentiality (optional)

e) Traffic flow confidentiality (optional)

1.5 Security Mechanisms

This part of ISO/IEC ISP 10613 provides no assurance as to the strength of the security mechanisms employed.

This part of ISO/IEC ISP 10613 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 10613. 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 10613 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 10613 are specified in the base standards referenced (see clause 2).

4 Abbreviations

The abbreviations and acronyms used in this part of ISO/IEC 10613 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 10613.

This part of ISO/IEC ISP 10613 specifies provision of security services using the Network Layer Security Protocol connection-mode with SDT-PDU based protection.

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

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

Note: Peer entity authentication and key management using the CSC-PDU is not within the scope of this part of ISO/IEC ISP 10613. This is supported through use of the SA Protocol (see below). Only, the header part of the CSC-PDU is required to signal the mode of operation.

d) support connection integrity without recovery using the ICV field as specified in clause 13.3.3.2 and the ISN field as specified in 13.5.1 of ITU-T X.273 | ISO/IEC 11577.

e) if it claims support of connection confidentiality (sub-profile S2C), support this service though encipherment mechanisms as specified in 14.1.5(a) of ITU-T X.273 | ISO/IEC 11577.

f) support the label field, and optionally the label reference fields as specified in 13.3.4.3.6 and 13.3.4.3.7 of ITU-T X.273 | ISO/IEC 11577.

g) The SA protocol 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.

Note: The details of the SA protocol are currently outside the scope of this part of ISO/IEC ISP 10613.

h) Map the NLSP PDUs onto ISO/IEC 8208 | CCITT Rec. X.25 as though it were the network service as specified in Annex A 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 clause 11 of ITU-T X.273 | ISO/IEC 11577.

b) support NLSP-CONNECT in UN-DATA mode of connection establishment (optionally with SA-P) as specified in 8.5.4 of ITU-T X.273 | ISO/IEC 11577.

c) support NLSP-DISCONNECT in UN-DISCONNECT or UN-DATA during connection release as specified in 8.10 of ITU-T X.273 | ISO/IEC 11577.

d) support the SDT-PDU based protection of userdata as specified in 8.6.

e) support protection of all NLSP service parameters (excluding those that can be modified by in the underlying network) as specified in 5.5.1(a) 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 connection-mode protocol shall operate above the ISO/IEC 8208 | CCITT Rec. X.25 protocol and below the connectionless network protocol (ISO/IEC 8473) after the subnetwork convergence function.

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 10613)

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

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	5.2 g	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		m
CDAddr	Content field type C3 - Calling/Destination NLSP address	13.3.4.3	ParamProt: M		m

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		m
SeqNo	Sequence Number Content Field	11.3, 13.3.5.1	COInteg:O CLInteg:O		m
EncPad Send	Padding for Encipherment - Sending	11.3, 13.3.3.3	COConf:O CLConf:O		COConf: o
EncPad Rec	Padding for Encipherment - Discard on receipt	11.3, 13.3.3.3	COConf:O CLConf:O		m
SinglePad Send	Single octet general padding field - Sending	11.3, 13.3.5.2	O		o
SinglePad Rec	Single octet general padding field - Discard on receipt	11.3, 13.3.5.2	O		m
TFCPad Send	Traffic padding - Sending	11.3, 13.3.5.3	TFC:M		TFC:o
TFCPad Rec	Traffic padding - Discard on receipt	11.3, 13.3.5.3	TFC:M		m
IntegPad Send	Padding for Integrity - Sending	11.3, 13.3.5.4	COInteg:O CLInteg:O	5.3 b	COInteg: o
IntegPad Rec	Padding for Integrity - Discard on receipt	11.3, 13.3.5.4	COInteg:O CLInteg:O	5.3 b	m

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 10613

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 h	i
SNISP*	Is the protocol mapping onto CCITT Rec. X.213 | ISO 8348	5.3 Annex A	CO:O.7		m
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	m
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		i

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 c	m

A.5.3 Modes of Connection Establishment / Release

Base standard features				ISP Features	
Item	**Questions/Features**	**Refs**	**Status**	**ISP Ref.**	**Status**
UNConn	NLSP-CONNECT in UN-CONNECT	8.5.1.2	CO:O.9	5.3 b	i
UNConnSAP	NLSP-CONNECT in UN-CONNECT with SA-P	8.5.1.2	CO:O.9	5.3 b	i
UNData	NLSP-CONNECT in UN-DATA	8.5.1.2	CO:O.9	5..3 b	i
UNDataSAP	NLSP-CONNECT in UN-DATA with SA-P	8.5.1.2	CO:O.9	5.3 b	m
DUNDisc	NLSP-DISCONNECT in UN-DISCONNECT	8.10	CO:O.10	5.3 c	m
DUNData	NLSP-DISCONNECT in UN-DATA	8.10	CO:O.10	5.3 c	m

A.5.4 Environment (Connection Mode)

Base standard features				ISP Features	
Item	**Questions/Features**	**Refs**	**Status**	**ISP Ref.**	**Status**
CO1	Are the mandatory elements of IS 8348 supported?	5.2	SNISP:M		m
ConOpt1	Does the implementation provide Expedited Data?	8.7	CO:O		o
ConOpt3	Does the implementation provide Receipt Confirmation?	8.9	CO:O		o

A.5.5 Timers and Parameters (Connection Mode)

Base standard features				ISP Features	
Item	**Questions/Features**	**Refs**	**Status**	**ISP Ref.**	**Status**
T1	Is the timer between transmitting NLSP-DISCONNECT and issuing UN-DISCONNECT supported?	8.10	CO:O		o