INTERNATIONAL TELECOMMUNICATION UNION

ITU-T X.833

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

(04/95)

DATA NETWORKS AND OPEN SYSTEM COMMUNICATIONS

SECURITY

INFORMATION TECHNOLOGY – OPEN SYSTEMS INTERCONNECTION – GENERIC UPPER LAYERS SECURITY: PROTECTING TRANSFER SYNTAX SPECIFICATION

ITU-T Recommendation X.833

(Previously "CCITT Recommendation")

FOREWORD

ITU (International Telecommunication Union) is the United Nations Specialized Agency in the field of telecommunications. The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of the ITU. Some 179 member countries, 84 telecom operating entities, 145 scientific and industrial organizations and 38 international organizations participate in ITU-T which is the body which sets world telecommunications standards (Recommendations).

The approval of Recommendations by the Members of ITU-T is covered by the procedure laid down in WTSC Resolution No. 1 (Helsinki, 1993). In addition, the World Telecommunication Standardization Conference (WTSC), which meets every four years, approves Recommendations submitted to it and establishes the study programme for the following period.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC. The text of ITU-T Recommendation X.833 was approved on 10th of April 1995. The identical text is also published as ISO/IEC International Standard 11586-4.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

© ITU 1996

All rights reserved. No part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from the ITU.

ITU-T X-SERIES RECOMMENDATIONS

DATA NETWORKS AND OPEN SYSTEM COMMUNICATIONS

(February 1994)

ORGANIZATION OF X-SERIES RECOMMENDATIONS

Subject area	Recommendation Series
PUBLIC DATA NETWORKS	
Services and Facilities	X.1-X.19
Interfaces	X.20-X.49
Transmission, Signalling and Switching	X.50-X.89
Network Aspects	X.90-X.149
Maintenance	X.150-X.179
Administrative Arrangements	X.180-X.199
OPEN SYSTEMS INTERCONNECTION	
Model and Notation	X.200-X.209
Service Definitions	X.210-X.219
Connection-mode Protocol Specifications	X.220-X.229
Connectionless-mode Protocol Specifications	X.230-X.239
PICS Proformas	X.240-X.259
Protocol Identification	X.260-X.269
Security Protocols	X.270-X.279
Layer Managed Objects	X.280-X.289
Conformance Testing	X.290-X.299
INTERWORKING BETWEEN NETWORKS	
General	X.300-X.349
Mobile Data Transmission Systems	X.350-X.369
Management	X.370-X.399
MESSAGE HANDLING SYSTEMS	X.400-X.499
DIRECTORY	X.500-X.599
OSI NETWORKING AND SYSTEM ASPECTS	
Networking	X.600-X.649
Naming, Addressing and Registration	X.650-X.679
Abstract Syntax Notation One (ASN.1)	X.680-X.699
OSI MANAGEMENT	X.700-X.799
SECURITY	X.800-X.849
OSI APPLICATIONS	
Commitment, Concurrency and Recovery	X.850-X.859
Transaction Processing	X.860-X.879
Remote Operations	X.880-X.899
OPEN DISTRIBUTED PROCESSING	X.900-X.999

CONTENTS

Summary

This Recommendation | International Standard belongs to a series of Recommendations which provide a set of facilities to aid the construction of OSI Upper Layer protocols which support the provision of security services. This Recommendation | International Standard defines the protecting transfer syntax, associated with Presentation Layer support for security services in the Application Layer.

Introduction

This Recommendation | International Standard forms part of a series of Recommendations | International Standards, which provide(s) a set of facilities to aid the construction of Upper Layers protocols which support the provision of security services. The parts are as follows:

- Part 1: Overview, Models and Notation;
- Part 2: Security Exchange Service Element Service Definition;
- Part 3: Security Exchange Service Element Protocol Specification;
- Part 4: Protecting Transfer Syntax Specification;
- Part 5: Security Exchange Service Element PICS Proforma;
- Part 6: Protecting Transfer Syntax PICS Proforma.

This Recommendation | International Standard constitutes Part 3 of this series.

INTERNATIONAL STANDARD

ITU-T RECOMMENDATION

INFORMATION TECHNOLOGY – OPEN SYSTEMS INTERCONNECTION – GENERIC UPPER LAYERS SECURITY: PROTECTING TRANSFER SYNTAX SPECIFICATION

1 Scope

1.1 This series of Recommendations | International Standards defines a set of generic facilities to assist in the provision of security services in OSI applications. These include:

a) a set of notational tools to support the specification of selective field protection requirements in an abstract syntax specification, and to support the specification of security exchanges and security transformations;

b) a service definition, protocol specification and PICS proforma for an application-service-element (ASE) to support the provision of security services within the Application Layer of OSI;

c) a specification and PICS proforma for a security transfer syntax, associated with Presentation Layer support for security services in the Application Layer.

1.2 This Recommendation | International Standard defines the protecting transfer syntax, associated with Presentation Layer support for security services in the Application Layer.

2 Normative references

The following Recommendations and International Standards contain provisions which, through reference in this text, constitute provisions of this Recommendation | International Standard. At the time of publication, the editions indicated were valid. All Recommendations and Standards are subject to revision, and parties to agreements based on this Recommendation | International Standard are encouraged to investigate the possibility of applying the most recent edition of the Recommendations and Standards listed below. Members of IEC and ISO maintain registers of currently valid International Standards. The Telecommunication Standardization Bureau of the ITU maintains a list of currently valid ITU-T Recommendations.

2.1 Identical Recommendations | International Standards

– ITU-T Recommendation X.200 (1994) | ISO/IEC 7498-1:1994, *Information technology – Open Systems Interconnection – Basic Reference Model: The Basic Model*.

– ITU-T Recommendation X.216 (1994) | ISO/IEC 8822:1994, *Information technology – Open Systems Interconnection – Presentation service definition*.

– ITU-T Recommendation X.226 (1994) | ISO/IEC 8823-1:1994, *Information technology – Open Systems Interconnection – Connection-oriented presentation protocol: Protocol specification*.

– ITU-T Recommendation X.680 (1994) | ISO/IEC 8824-1:1995, *Information technology – Abstract Syntax Notation One (ASN.1): Specification of basic notation*.

– ITU-T Recommendation X.681 (1994) | ISO/IEC 8824-2:1995, *Information technology – Abstract Syntax Notation One (ASN.1): Information object specification*.

– ITU-T Recommendation X.682 (1994) | ISO/IEC 8824-3:1995, *Information technology – Abstract Syntax Notation One (ASN.1): Constraint specification.*

– ITU-T Recommendation X.683 (1994) | ISO/IEC 8824-4:1995, *Information technology – Abstract Syntax Notation One (ASN.1): Parameterization of ASN.1 specifications*.

– ITU-T Recommendation X.690 (1994) | ISO/IEC 8825-1:1995, *Information technology – ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER).*

- ITU-T Recommendation X.803 (1994) | ISO/IEC 10745:1995, *Information technology – Open Systems Interconnection – Upper layers security model*.
- ITU-T Recommendation X.830 (1995) | ISO/IEC 11586-1:1995, *Information technology – Open Systems Interconnection – Generic upper layers security: Overview, models and notation*.

3 Definitions

3.1 This Recommendation | International Standard makes use of the following terms defined in ITU-T Rec. X.200 | ISO/IEC 7498-1:

- transfer syntax.

3.2 This Recommendation | International Standard makes use of the following terms defined in ITU-T Rec. X.216 | ISO/IEC 8822:

- abstract syntax;
- presentation context;
- presentation data value.

3.3 This Recommendation | International Standard makes use of the following terms defined in ITU-T Rec. X.803 | ISO/IEC 10745:

- security association;
- security transformation.

3.4 This Recommendation | International Standard makes use of the following terms defined in ITU-T Rec. X.830 | ISO/IEC 11586-1:

- presentation-context-bound security association;
- single-item-bound security association;
- externally-established security association;
- initial encoding rules;
- protecting presentation context;
- protecting transfer syntax.

4 Abbreviations

GULS	Generic Upper Layers Security
OSI	Open Systems Interconnection
PDU	Protocol-data-unit
PDV	Presentation data value
PICS	Protocol implementation conformance statement

5 General overview

The concept of a protecting transfer syntax was introduced in ITU-T Rec. X.830 | ISO/IEC 11586-1. This Specification defines a generic protecting transfer syntax. This Specification can be used, in conjunction with particular security transformation definitions, to generate particular protecting transfer syntaxes, tailored to satisfy particular application protection requirements.

NOTE – The generic protecting transfer syntax may also prove useful in providing data compression for non-security-related purposes, however such use is outside the scope of this Specification.

The generic protecting transfer syntax is based upon the security transformation model described in ITU-T Rec. X.830 | ISO/IEC 11586-1. The purpose of a protecting transfer syntax is to provide a standard means for representing, for transfer purposes, the following information items:

- the transformed item resulting from applying the encoding process of a security transformation to a representation of an unprotected item which is to be protected;

– protected static and dynamic parameters of a security transformation, which achieve protection by being processed in the encoding process of a security transformation (along with the representation of the unprotected item);

– unprotected static and dynamic parameters of a security transformation;

– on the first PDV of a protecting presentation context, or a protected PDV sent outside a presentation context, either:

  a) in the case of a presentation-context-bound or single-item-bound security association, an identifier of the security transformation;

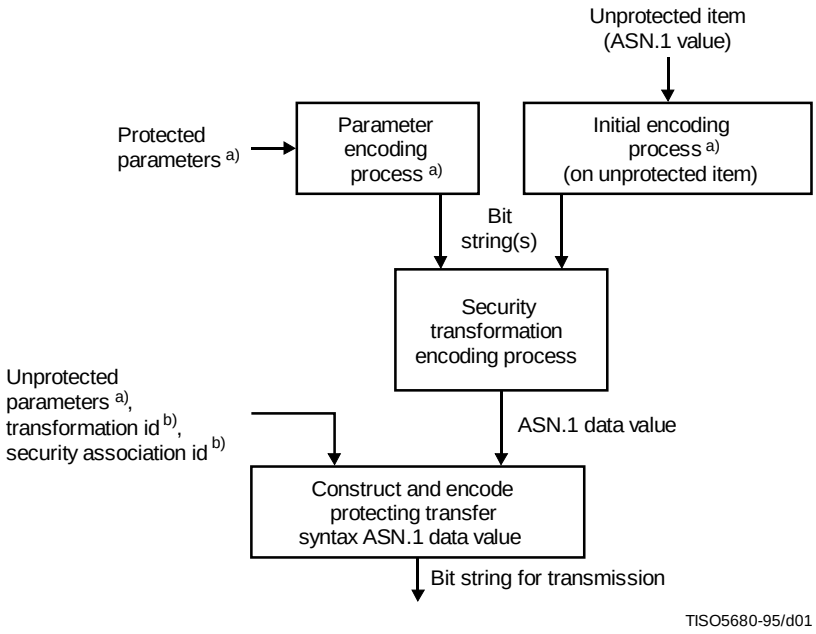
  b) in the case of an externally-established security association, an identifier of that security association.

Use of a protecting transfer syntax is negotiated by the presentation protocol or announced in an ASN.1 EXTERNAL or EMBEDDED PDV construct. It can be applied to any abstract syntax, which may be specified using ASN.1 or by other means. Object identifiers for negotiating or announcing protecting transfer syntaxes are addressed in clause 9.

A protecting transfer syntax is a context-sensitive transfer syntax, i.e. state is retained within encoders and decoders.

5.1 Model of a protecting transfer syntax

Figure 1 illustrates, in finer detail than in ITU-T Rec. X.830 | ISO/IEC 11586-1, the operations associated with a protecting transfer syntax at an encoding system (the corresponding operations at a decoding system follow naturally).



a) If applicable.
b) These two encoding processes may be combined.

Figure 1 – Protecting transfer syntax construction at encoding system

5.2 Initial encoding rules

The initial encoding process (in the encoding system) and corresponding decoding process (in the decoding system) map between an abstract syntax and an unprotected syntax. The rules applied to this process are known as the initial encoding rules.

NOTE – For an ASN.1-based abstract syntax, this mapping will typically employ some variant of the ASN.1 encoding rules.

Single-valued encoding rules (e.g. the ASN.1 Canonical Encoding Rules or Distinguished Encoding Rules) should be applied where the transformation is a function of data which may also be sent separately, particularly when used via a relay system.

The initial encoding rules for use in a protecting transfer syntax are established as follows:

a) if the security transformation in use provides for conveying an identifier of a specific set of encoding rules as a static (protected or unprotected) parameter, and if this parameter is present in the applicable first-PDV field, then these encoding rules are used; otherwise

b) the encoding rules indicated by the &initialEncodingRules field of the applicable security transformation definition are used.

5.3 Security transformation

The security transformation to be employed is determined in either of two ways:

a) when the PDV transfer relates to a presentation-context-bound or single-item-bound security association, the security transformation identifier is conveyed in the transfer syntax structure along with the first PDV in that security association;

b) when the PDV transfer relates to an externally established security association, the security transformation identifier is an attribute of that security association.

The rules of a security transformation indicate how a bit string of user data and a set of protected parameter values are to map to an ASN.1 value for transfer purposes.

5.4 Syntax structure

A protecting transfer syntax defines the data structure used to convey the output of the encoding process of a security transformation, plus unprotected parameters and identifiers of the security transformation or security association (as applicable). The data structure transferred has a different variant for each of the cases:

a) the first PDV of a protecting presentation context in a presentation-context-bound security association, or the one PDV in a single-item-bound security association;

b) the first PDV of a protecting presentation context, or a protected PDV sent outside a presentation context, in the case of an externally established security association;

c) a subsequent PDV in a protecting presentation context.

6 Data structures for a protecting transfer syntax

The set of data structures used by a protecting transfer syntax is defined by the ASN.1 type SyntaxStructure in the following ASN.1 module. The SyntaxStructure type is parameterized by the object set ValidSTs, which is a set of SECURITY-TRANSFORMATION objects. When a value for ValidSTs is supplied, together with the corresponding security transformation specifications, the SyntaxStructure type becomes a complete syntax specification for a specific protecting transfer syntax.

```
GenericProtectingTransferSyntax {joint-iso-ccitt genericULS (20)
        modules (1) genericProtectingTransferSyntax (7) }
DEFINITIONS AUTOMATIC TAGS ::=
BEGIN

EXPORTS
        SyntaxStructure {};

IMPORTS
        notation
            FROM ObjectIdentifiers {joint-iso-ccitt
            genericULS (20) modules (1) objectIdentifiers (0) }
        SECURITY-TRANSFORMATION, ExternalSAID
            FROM Notation notation;

SyntaxStructure {SECURITY-TRANSFORMATION: ValidSTs}::=  CHOICE
{
        firstPdvExplicit      FirstPdvExplicit {{ValidSTs}},
        -- To be used on the first PDV of a protecting presentation
        -- context, or a protected PDV sent outside a presentation
        -- context, in the case of a presentation-context-bound or
        -- single-item-bound security association.
```

```
        firstPdvExternal      FirstPdvExternal {{ValidSTs}},
        -- To be used on the first PDV of a protecting presentation
        -- context, or a protected PDV sent outside a presentation
        -- context, in the case of an externally established
        -- security association.
        subsequentPdv         SubsequentPdv {{ValidSTs}}
        -- To be used on a subsequent PDV in a protecting
        -- presentation context.
}
FirstPdvExplicit {SECURITY-TRANSFORMATION: ValidSTs}::= SEQUENCE
{
        transformationId  SECURITY-TRANSFORMATION.&sT-Identifier
                ({ValidSTs}),
        staticUnprotParm
            SECURITY-TRANSFORMATION.&StaticUnprotectedParm
                ({ValidSTs}{@transformationId})
                OPTIONAL,
        dynamicUnprotParm
            SECURITY-TRANSFORMATION.&DynamicUnprotectedParm
                ({ValidSTs}{@transformationId})
                OPTIONAL,
        xformedData  SECURITY-TRANSFORMATION.&XformedDataType
                ({ValidSTs}{@transformationId})
}
FirstPdvExternal {SECURITY-TRANSFORMATION: ValidSTs}::= SEQUENCE
{
        externalSAID          ExternalSAID,
        dynamicUnprotParm
            SECURITY-TRANSFORMATION.&DynamicUnprotectedParm
                ({ValidSTs}) OPTIONAL,
            -- Actual member of ValidSTs is as implied
            -- by externalSAID
        xformedData  SECURITY-TRANSFORMATION.&XformedDataType
                ({ValidSTs})
            -- Actual member of ValidSTs is as implied
            -- by externalSAID
}
SubsequentPdv {SECURITY-TRANSFORMATION: ValidSTs}::= SEQUENCE
{
        dynamicUnprotParm
            SECURITY-TRANSFORMATION.&DynamicUnprotectedParm
                ({ValidSTs}) OPTIONAL,
        xformedData  SECURITY-TRANSFORMATION.&XformedDataType
                ({ValidSTs})
            -- Actual member of ValidSTs is implied
            -- by presentation context
}
END
```

7 Incorporation into underlying protocol

When conveyed directly in a presentation PDU (as specified in ITU-T Rec. X.226 | ISO/IEC 8823-1) or when embedded in an EXTERNAL or EMBEDDED PDV ASN.1 construct (as specified in ITU-T Rec. X.680 | ISO/IEC 8824-1), the appropriate value of the SyntaxStructure type is encoded using the encoding rules implied by the transfer syntax object identifier, if any (see clause 9), or, by default, using the ASN.1 Basic Encoding Rules.

When used in conjunction with the direct option of the PROTECTED or PROTECTED-Q notation described in ITU-T Rec. X.830 | ISO/IEC 11586-1, the ASN.1 for the SyntaxStructure type is imported into the ASN.1 for the surrounding protocol, hence is encoded using the encoding rules determined for that protocol.

8 Synchronization procedures

All state information shall be preserved when, in accordance with the session service specification, a synchronization point is established. State information shall be restored when a resynchronization takes place.

NOTES

1 This Specification specifies "state restoration" on resynchronization. The equivalent operation without presentation context restoration is not provided in this Specification.

2 Resynchronization to a minor synch point may result in the sending entity being unsure as to whether the receiving entity received and acted upon all recent dynamic parameter changes. If this can occur, on resynchronization the sending entity should re-establish dynamic parameter settings to the correct value.

9 Object identifier assignment

The following object identifier is assigned to the protecting transfer syntax defined in this Specification:

{joint-iso-itu-t genericULS (20) generalTranferSyntax (2)}

Use of this object identifier does not require that a specific set of encoding rules be used to encode the SyntaxStructure ASN.1 value, but ASN.1 Basic Encoding Rules will be used by default:

Additional object identifiers are assigned to the protecting transfer syntax defined in this Specification for use when a specific set of encoding rules must be used to encode the SyntaxStructure ASN.1 value. Any one of the standard ASN.1 encoding rules specifications (e.g. those defined in ITU-T Rec. X.690 | ISO/IEC 8825-1) may be stipulated. The following convention is employed. The object identifier commences with the following prefix:

{joint-iso-itu-t genericULS (20) specificTranferSyntax (3) ... }

The remaining field values are the same values that follow the prefix:

{joint-iso-itu-t asn1 (1) ... }

in the case of the regular ASN.1 encoding rules.

NOTE – As examples, the object identifier {joint-iso-itu-t genericULS (20) specificTranferSyntax (3) ber (1)} stipulates that Basic Encoding Rules be employed while the object identifier {joint-iso-ccitt genericULS (20) specificTranferSyntax (3) ber-derived (2) distinguished-encoding (1)} stipulates that Distinguished Encoding Rules be employed.

10 Conformance

A system claiming conformance to this standard, when using the protecting transfer syntax as identified by the ASN.1 object identifier for the “GenericProtectingTransferSyntax” module given in clause 6, shall support the applicable ASN.1 and any associated stipulations.