



INTERNATIONAL TELECOMMUNICATION UNION

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.834

(10/96)

SERIES X: DATA NETWORKS AND OPEN SYSTEM
COMMUNICATION

Security

**Information technology – Open systems
interconnection – Generic upper layers security:
Security exchange service element (SESE)
protocol implementation conformance
statement (PICS) proforma**

ITU-T Recommendation X.834

(Previously "CCITT Recommendation")

ITU-T X-SERIES RECOMMENDATIONS
DATA NETWORKS AND OPEN SYSTEM COMMUNICATION

PUBLIC DATA NETWORKS	X.1-X.199
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 SYSTEM INTERCONNECTION	X.200-X.299
Model and notation	X.200-X.209
Service definitions	X.210-X.219
Connection-mode protocol specifications	X.220-X.229
Connectionless-mode protocol specification	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	X.300-X.399
General	X.300-X.349
Satellite data transmission systems	X.350-X.399
MESSAGE HANDLING SYSTEMS	X.400-X.499
DIRECTORY	X.500-X.599
OSI NETWORKING AND SYSTEM ASPECTS	X.600-X.699
Networking	X.600-X.629
Efficiency	X.630-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
Systems Management framework and architecture	X.700-X.709
Management Communication Service and Protocol	X.710-X.719
Structure of Management Information	X.720-X.729
Management functions	X.730-X.799
SECURITY	X.800-X.849
OSI APPLICATIONS	X.850-X.899
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

For further details, please refer to ITU-T List of Recommendations.

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.834 was approved on 5th of October 1996. The identical text is also published as ISO/IEC International Standard 11586-5.

NOTE

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

© ITU 1997

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, except as noted in footnote 1) in Annexe A.

CONTENTS

	<i>Page</i>
1 Scope	1
2 Normative references	1
2.1 Identical Recommendations International Standards	1
2.2 Paired Recommendations International Standards equivalent in technical content	1
3 Definitions	2
4 Abbreviations	2
5 Conventions	2
6 Conformance	2
Annex A – Protocol Implementation Conformance Statement (PICS) proforma for the SESE protocol	
A.1 Notations defined for the proforma	3
A.1.1 Status column	3
A.1.2 Support column	3
A.2 PICS numbers	3
A.3 Completion of the PICS	4
A.4 Date of statement	4
A.5 Implementation details	4
A.6 ITU-T Rec. X.832 ISO/IEC 11586-3 protocol details	5
A.6.1 ITU-T Rec. X.832 ISO/IEC 11586-3 technical corrigenda implemented	5
A.7 Global statement of conformance	5
A.8 Supported APDUs	5
A.9 Supported APDU parameters	6
A.9.1 SE-Transfer (SETR)	6
A.9.2 SE-U-Absort (SEAB)	6
A.9.3 SE-P-Absort (SEPA)	6
A.9.4 Problem codes	7
A.10 Abstract syntax	7
A.11 Application Context	7
A.12 Security exchanges	7
A.12.1 Class of Security Exchange Supported	7
A.12.2 Exchange Supported	8
A.12.3 Directory Authentication Exchange (one way)	8
A.12.4 Directory Authentication Exchange (two way)	8
A.12.5 Simple Negotiation Exchange	8

Summary

This Recommendation | International Standard belongs to a series of Recommendations on Generic Upper Layers Security (GULS). It is the Protocol Implementation Conformance Statement (PICS) proforma for the Security Exchange Service Element Protocol specified in ITU-T Rec. X.832 | ISO/IEC 11586-3 and the Security Exchange described in ITU-T Rec. X.830 | ISO/IEC 11586-1, Annex C. This Recommendation | International Standard provides a description of the standardized capabilities and options in a form that supports conformance evaluation of a particular implementation.

Introduction

This Recommendation | International Standard forms part of a series of Recommendations | International Standards that provide generic upper layer security services. The parts are as follows:

- Part 1: Overview, Model 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 Service PICS Proforma.
- Part 6: Protecting Transfer Syntax PICS Proforma.

This Recommendation | International Standard constitutes Part 5 of the series.

Part 3 defines a protocol for the communication of security exchange information between open systems as part of the operation of a security mechanism. To evaluate the conformance of a particular implementation, it is necessary to have a description of the capabilities and options which have been implemented. Such a description is called a Protocol Implementation Conformance Statement (PICS). This Recommendation | International Standard includes the PICS proforma for the security exchange service element protocol specified in Part 3 and the security exchanges defined in Part 1, Annex C.