



INTERNATIONAL TELECOMMUNICATION UNION

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.832

(04/95)

**DATA NETWORKS AND OPEN SYSTEM
COMMUNICATIONS
SECURITY**

INFORMATION TECHNOLOGY –

OPEN SYSTEMS INTERCONNECTION –

**GENERIC UPPER LAYERS SECURITY:
SECURITY EXCHANGE SERVICE
ELEMENT (SESE) PROTOCOL SPECIFICATION**

ITU-T Recommendation X.832

(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.832 was approved on 10th of April 1995. The identical text is also published as ISO/IEC International Standard 11586-3.

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

	<i>Page</i>
1 Scope	1
2 Normative references	1
2.1 Identical Recommendations International Standards	1
3 Definitions	2
4 Abbreviations	2
5 Overview of the protocol	2
5.1 Service provision	2
5.2 Use of underlying services	2
6 Elements of procedure	3
6.1 APDUs used	3
6.2 Transfer procedure	3
6.3 User-initiated abort procedure	3
6.4 Provider-initiated abort procedure	3
7 Structure and encoding of SESE APDUs	4
7.1 Generic APDU specification	4
7.2 Abstract syntax construction	6
8 Mapping to underlying services	6
8.1 General	6
8.2 Mapping to ACSE services	7
9 Conformance	7
9.1 Statement Requirements	7
9.2 Static Requirements	7
9.3 Dynamic Requirements	7
Annex A – SEPM state tables	8
A.1 General	8
A.2 Conventions	8
A.3 Tables	8
Annex B – Basic SESE application context definition	11
B.1 Application Context Name	11
B.2 Application Service Elements	11
B.3 SESE APDU Mappings	11
B.4 PDV concatenation constraints	11
B.5 PDV embedding constraints	11
B.6 Procedural constraints	12
B.7 Presentation context constraints	12

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 specifies the protocol provided by the Security Exchange Service Element (SESE). The SESE is an application-service-element (ASE) which facilitates the communication of security information to support the provision of security services within the Application Layer of OSI.

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.