



INTERNATIONAL TELECOMMUNICATION UNION

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Q.814

(02/2000)

SERIES Q: SWITCHING AND SIGNALLING

Specifications of Signalling System No. 7 – Q3 interface

**Specification of an electronic data interchange
interactive agent**

ITU-T Recommendation Q.814

(Formerly CCITT Recommendation)

SIGNALLING IN THE INTERNATIONAL MANUAL SERVICE	Q.1-Q.3
INTERNATIONAL AUTOMATIC AND SEMI-AUTOMATIC WORKING	Q.4-Q.59
FUNCTIONS AND INFORMATION FLOWS FOR SERVICES IN THE ISDN	Q.60-Q.99
CLAUSES APPLICABLE TO ITU-T STANDARD SYSTEMS	Q.100-Q.119
SPECIFICATIONS OF SIGNALLING SYSTEMS No. 4 AND No. 5	Q.120-Q.249
SPECIFICATIONS OF SIGNALLING SYSTEM No. 6	Q.250-Q.309
SPECIFICATIONS OF SIGNALLING SYSTEM R1	Q.310-Q.399
SPECIFICATIONS OF SIGNALLING SYSTEM R2	Q.400-Q.499
DIGITAL EXCHANGES	Q.500-Q.599
INTERWORKING OF SIGNALLING SYSTEMS	Q.600-Q.699
SPECIFICATIONS OF SIGNALLING SYSTEM No. 7	Q.700-Q.849
General	Q.700
Message transfer part (MTP)	Q.701-Q.709
Signalling connection control part (SCCP)	Q.711-Q.719
Telephone user part (TUP)	Q.720-Q.729
ISDN supplementary services	Q.730-Q.739
Data user part	Q.740-Q.749
Signalling System No. 7 management	Q.750-Q.759
ISDN user part	Q.760-Q.769
Transaction capabilities application part	Q.770-Q.779
Test specification	Q.780-Q.799
Q3 interface	Q.800-Q.849
DIGITAL SUBSCRIBER SIGNALLING SYSTEM No. 1	Q.850-Q.999
PUBLIC LAND MOBILE NETWORK	Q.1000-Q.1099
INTERWORKING WITH SATELLITE MOBILE SYSTEMS	Q.1100-Q.1199
INTELLIGENT NETWORK	Q.1200-Q.1699
SIGNALLING REQUIREMENTS AND PROTOCOLS FOR IMT-2000	Q.1700-Q.1799
BROADBAND ISDN	Q.2000-Q.2999

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

Specification of an electronic data interchange interactive agent

Summary

This ITU-T Recommendation defines the technical specification of a session layer protocol module called Electronic Communications Interactive Agent. This may be used as an interface reference point in a TMN model for the asynchronous exchange of data between peer application entities. The Interactive Agent (IA) supports the exchange of near real time Electronic Data Interchange (EDIFACT or ASC X12 EDI) transactions. In addition, this ITU-T Recommendation defines the architecture, design, structure, and process-flow for both *normal*¹ and *high priority*² business functions utilizing Transport Layer Security (TLS).

Source

ITU-T Recommendation Q.814 was prepared by ITU-T Study Group 4 (1997-2000) and approved under the WTSC Resolution 1 procedure on 4 February 2000.

¹ *Normal Priority* – An example of a Normal Priority Business Function is an Order Request Transaction

² *High Priority* – An example of a High Priority Business Function is an interactive inquiry transaction

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications. The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Conference (WTSC), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSC Resolution 1.

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.

NOTE

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

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementors are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database.

© ITU 2001

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.

CONTENTS

Page

1	Scope	1
2	References	1
2.1	Normatives references	1
2.2	Informative references	1
3	Definitions	2
4	Abbreviations	2
5	Conventions	2
6	Architecture and Service Characteristics	3
6.1	Architecture	3
6.2	Service characteristics	5
6.2.1	Elements of Service	5
6.2.2	Classifications of Elements of Service	6
7	Data Flow	6
8	IA Messages	7
8.1	Message Format Definitions	7
8.2	Message Syntax Definitions	7
8.2.1	Basic Message	7
8.2.2	IA Status/Control Message	8
8.2.3	Enhanced Message	8
8.3	IA Status Message Detail Format	8
8.3.1	First Octet	8
8.3.2	Second Octet	8
8.3.3	Third and Fourth Octets	8
8.3.4	Special Test Message	9
8.3.5	Invalid Message	9
9	Client Specifications	9
9.1	Determine IP Destination Address	9
9.2	Connect to Server	9
9.2.1	Allocate TLS Data Structure and Memory	10
9.2.2	Open Socket	10
9.2.3	Send TLS Client Hello	10
9.2.4	Send Client's Certificate to Server	10
9.2.5	Client Key Exchange	10
9.2.6	Send Client Certificate Verify	10
9.2.7	Change Cipher Specs	11



9.2.8	Send Client Finished	11
9.3	Send Application Data to Server	11
9.4	Transmission Logging	11
9.5	Client Disconnect	11
10	Server Specifications	12
10.1	Initialize Server.....	12
10.2	Accept Connection from Client.....	12
10.3	Message Read Setup.....	12
10.3.1	Allocate TLS Data Structure and Memory	13
10.3.2	Bind TLS Data Structure to the Socket.....	13
10.3.3	Send TLS Server Hello	13
10.3.4	Send Server's Certificate to Client	13
10.3.5	Server Key Exchange	13
10.3.6	Send Client Certificate Request	13
10.3.7	Send Server Hello Done.....	13
10.3.8	Execute Change Cipher Specs.....	13
10.3.9	Send Server Finished.....	13
10.4	TLS Read Processing	13
10.5	Server Disconnect.....	14
10.6	Parsing the Received Message	14
10.7	Transfer Data to Immediate User (Translator/Security Module)	14
10.8	Receipt Logging	15
11	Operational requirements	15
11.1	Security.....	15
11.2	Digital Certificates.....	15
11.3	Flow Control.....	16
12	Port Assignments.....	16
Annex A – ASN.1 Production Module.....		17
Annex B – Design Considerations.....		17
B.1	Multi-processing/Multi-threading	17
B.2	Non-Persistent Versus Persistent Connections.....	17
B.3	Resumable TLS Sessions	18
Annex C – Error Handling/Recovery		18
Appendix I – Non-normative references		18

Introduction

This ITU-T Recommendation defines the specifications for an Electronic Data Interchange Interactive Agent (IA). The IA supports the exchange of Electronic Data Interchange transactions between peer entities. It maps EDI transactions into the transport layer. More specifically, it interfaces with Transport Layer Security (TLS) to request the establishment and termination of secure (i.e. supporting peer entity authentication, integrity, and privacy) TCP sessions and secure transport of EDI messages. The IA further provides basic flow control functionality.



ITU-T Recommendation Q.814

Specification of an electronic data interchange interactive agent

1 Scope

This ITU-T Recommendation provides a specification for the Electronic Data Interchange Interactive Agent (IA). The IA supports the interchange of Electronic Data Interchange (EDIFACT/ASC X12 EDI) transactions over a Transmission Control Protocol/Internet Protocol (TCP/IP) network utilizing Transport Layer Security (TLS). This ITU-T Recommendation specifies the general architecture of the IA, the syntax of the message formats to be used, the encoding rules for the messages and the applicable security transformations.

2 References

2.1 Normatives references

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; all users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published.

- ITU-T Recommendation Q.815 (2000), *Specification of a security module for whole message protection*.
- ITU-T Recommendation X.509 (1997) | ISO/IEC 9495-8:1998, *Information technology – Open Systems Interconnection – The Directory: Authentication framework*.
- ITU-T Recommendation X.680 (1997) | ISO/IEC 8824-1:1998, *Information technology – Abstract Syntax Notation One (ASN.1): Specification of basic notation*.
- ITU-T Recommendation X.681 (1997) | ISO/IEC 8824-2:1998, *Information technology – Abstract Syntax Notation One (ASN.1): Information object specification*.
- ITU-T Recommendation X.682 (1997) | ISO/IEC 8824-3:1998, *Information technology – Abstract Syntax Notation One (ASN.1): Constraint specification*.
- ITU-T Recommendation X.683 (1997) | ISO/IEC 8824-4:1998, *Information technology – Abstract Syntax Notation One (ASN.1): Parameterization of ASN.1 specifications*.
- ITU-T Recommendation X.690 (1997) | ISO/IEC 8825-1:1998, *Information technology – ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)*.

Internet Society/Internet Engineering Task Force:

- RFC 2246, *The TLS Protocol Version 1.0*.

2.2 Informative references

- Directory Implementors Guide (Version 12) (1999).