



INTERNATIONAL TELECOMMUNICATION UNION

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Q.815

(02/2000)

SERIES Q: SWITCHING AND SIGNALLING

Specifications of Signalling System No. 7 – Q3 interface

Specification of a security module for whole message protection

ITU-T Recommendation Q.815

(Formerly CCITT Recommendation)



Documents

Document Sharing Hub

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 a security module for whole message protection

Summary

This ITU-T Recommendation specifies an optional security module to be used with ITU-T Recommendation Q.814, Specification of an Electronic Data Interchange Interactive Agent, that provides security services for whole Protocol Data Units (PDUs). In particular, the security module supports non-repudiation of origin and of receipt, as well as whole message integrity.

Source

ITU-T Recommendation Q.815 was prepared by ITU-T Study Group 4 (1997-2000) and approved under the WTSC Resolution 1 procedure on 4 February 2000.

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	2
2.1	Normative references.....	2
2.2	Informative references.....	3
3	Definitions	3
4	Abbreviations	4
5	Conventions.....	4
6	Q.815 details.....	4
6.1	Security Module Message Types.....	4
6.1.1	Message Integrity Service	4
6.1.2	Non-Repudiation of Origin Service	5
6.1.3	Non-Repudiation of Receipt Service.....	5
6.2	General Characteristics.....	5
7	General Syntax	5
7.1	Hashed Messages.....	5
7.1.1	Object Identifiers Referenced by Hashed Messages	6
7.1.2	Value Information for Hashed Messages	6
7.2	Signed Messages	6
7.2.1	Object Identifiers Referenced by Signed Messages.....	6
7.2.2	Value Information for Signed Messages.....	7
7.3	IA Receipt Message.....	7
7.3.1	Object Identifiers Referenced by IA Receipt Messages.....	7
7.3.2	Value Information for IA Receipt Messages.....	8
7.4	Stase-Rose PDU	8
	Annex A – ASN.1 Production Module.....	8
	Appendix I – Non-normative references	10
	Appendix II – The SHA-1 Message Digest Algorithm	10
II.1	Introduction	10
II.2	Bit strings and integers	11
II.3	Operations on words.....	11
II.4	Message padding	12
II.5	Functions used.....	13
II.6	Constants used	13
II.7	Computing the message digest	13



Documents

Document Sharing Hub

II.8	Alternate method of computation.....	14
II.9	Comparison of methods.....	14