



INTERNATIONAL TELECOMMUNICATION UNION

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Q.817

(01/2001)

SERIES Q: SWITCHING AND SIGNALLING

Q3 interface

TMN PKI – Digital certificates and certificate revocation lists profiles

ITU-T Recommendation Q.817

(Formerly CCITT Recommendation)

ITU-T Q-SERIES RECOMMENDATIONS
SWITCHING AND SIGNALLING

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.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.

ITU-T Recommendation Q.817

TMN PKI – Digital certificates and certificate revocation lists profiles

Summary

This Recommendation explains how Digital Certificates and Certificate Revocation Lists can be used in the TMN and provides requirements on the use of Certificate and Certificate Revocation List extensions.

Source

ITU-T Recommendation Q.817 was prepared by ITU-T Study Group 4 (2001-2004) and approved under the WTSA Resolution 1 procedure on 19 January 2001.

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 Assembly (WTSA), 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 WTSA 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 ITU.

CONTENTS

Page

1	Scope, purpose and application	1
1.1	Scope.....	1
1.2	Purpose.....	1
1.3	Application.....	1
2	Normative references	1
2.1	ITU-T and ISO/IEC standards	2
2.2	Other standards	2
3	Definitions	2
4	Abbreviations.....	2
5	Overview	3
6	Certificate extensions.....	4
6.1	Authority Key Identifier	5
6.2	Subject Key Identifier	5
6.3	Key Usage.....	5
6.4	Private Key Usage Period.....	5
6.5	Certificate Policies	6
6.6	Policy Mapping.....	6
6.7	Subject Alternative Name	6
6.8	Issuer Alternative Name	6
6.9	Subject Directory Attributes	6
6.10	Basic Constraints	6
6.11	Name Constraints.....	6
6.12	Policy Constraints	7
6.13	Extended Key Usage.....	7
6.14	CRL Distribution Points	7
6.15	Authority Information Access	7
7	Certificate Revocation List (CRL) Extensions	7
7.1	Authority Key Identifier	7
7.2	Issuer Alternative Name	7
7.3	CRL Number.....	7
7.4	Delta CRL Indicator.....	8
7.5	Issuing Distribution Point	8
8	Extensions for Individual Entries in CRLs	8



ITU-T Q.817 (01/2001)

Documents

Document Sharing Hub

iii