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.

CONTENTS

ITU-T Recommendation Q.817

TMN PKI – Digital certificates and certificate revocation lists profiles

1 Scope, purpose and application

1.1 Scope

This Recommendation is intended to promote interoperability among TMN elements that use Public Key Infrastructure (PKI) to support security-related functions. It applies to all TMN interfaces and applications. It is independent of which communications protocol stack or which network management protocol is being used. PKI facilities can be used for a broad range of security functions, such as, authentication, integrity, non-repudiation, and key exchange (ITU-T M.3016). However, this Recommendation does not specify how such functions should be implemented, with or without PKI.

PKI has emerged as an efficient, scalable method for secure authentication, for non-repudiation, and for the distribution and management of encryption keys and other security-related parameters. A PKI is based on digital certificates. ITU-T X.509 specifies the format of such certificates. X.509 digital certificates can contain any number of extensions. In order for a PKI to support interoperability among TMN elements, all such elements must be able to process the same set of certificate extensions. Ideally, all TMN elements should also exhibit the same behaviour in processing certificate extensions. In order to promote secure interoperability among TMN elements this Recommendation specifies the certificate extensions that are to be supported by a TMN PKI. It further provides default behaviours for the processing of those extensions.

In order to promote harmonization with other industries, this Recommendation is based on ITU-T X.500-series Recommendations, in particular ITU-T X.509 and PKI-related Request for Comments (RFC) 2459 from the Internet Engineering Task Force (IETF).

1.2 Purpose

The purpose of this Recommendation is to provide interoperable, scalable mechanism for key distribution and management within a TMN, across all interfaces, as well as in support of non-repudiation service over the X interface.

1.3 Application

This Recommendation applies to all Q and X interfaces of the TMN, regardless of the communication protocol. It pertains to information about public keys and revocation of public keys that is used by or exchanged among TMN elements.

Depending on application specific requirements, TMN might use predefined public keys that are distributed by means outside the scope of this Recommendation rather than use certificates.

2 Normative 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; 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.

2.1 ITU-T and ISO/IEC standards

- ITU-T M.3016 (1998), *TMN Security Overview.*
- ITU-T Q.812 (1997), *Upper layer protocol profiles for the Q3 and X interfaces.*
- ITU-T X.500 (2001) | ISO/IEC 9594-1:2001, *Information technology – Open Systems Interconnection – The Directory: Overview of concepts, models and services.*
- ITU-T X.509 (2000) | ISO/IEC 9594-8:2001, *Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks.*
- ITU-T X.680 (1997) | ISO/IEC 8824-1:1998, *Information technology – Abstract Syntax Notation One (ASN.1): Specification of basic notation.*
- ITU-T X.681 (1997) | ISO/IEC 8824-2:1998, *Information technology – Abstract Syntax Notation One (ASN.1): Information object specification.*
- ITU-T X.682 (1997) | ISO/IEC 8824-3:1998, *Information technology – Abstract Syntax Notation One (ASN.1): Constraint specification.*
- ITU-T X.683 (1997) | ISO/IEC 8824-4:1998, *Information technology – Abstract Syntax Notation One (ASN.1): Parameterization of ASN.1 specification.*
- ITU-T 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).*
- ITU-T X.736 (1992) | ISO/IEC 10164-7:1992, *Information technology – Open Systems Interconnection – Systems Management: Security alarm reporting function.*
- ITU-T X.740 (1992) | ISO/IEC 10164-8:1993, *Information technology – Open Systems Interconnection – Systems Management: Security audit trail function.*

2.2 Other standards

- IETF RFC 2459 (1999), *Internet X.509 Public Key Infrastructure – Certificate and CRL Profile.*
- IETF RFC 2251 (1997), *Lightweight Directory Access Protocol (v3).*

3 Definitions

This Recommendation uses the definitions of security services and security mechanisms as specified in ITU-T M.3016. This Recommendation further uses the definitions of elements of a Public Key Infrastructures as specified in RFC 2459.

4 Abbreviations

This Recommendation uses the following abbreviations:

ASN.1	Abstract Syntax Notation One
BER	Basic Encoding Rules
CA	Certification Authority
CRL	Certificate Revocation List
DER	Distinguished Encoding Rules
IETF	Internet Engineering Task Force

ITU-T	International Telecommunication Union – Telecommunication Standardization Sector
OID	Object Identifier
PKCS	Public Key Cryptography Standard
PKI	Public Key Infrastructure
RA	Registration Authority
RFC	Request for Comments
RSA	Rivest Shamir Adelman

5 Overview

Public Key Infrastructure (PKI) is emerging as the lowest cost, scalable solution for TMN security. This Recommendation is intended to promote interoperability among PKI components from different product suppliers and service providers, and to promote interoperability among different companies or administrations. This clause provides a high level overview of the TMN PKI.

The TMN PKI consists of the following **components**:

A **Certification Authority (CA)** produces **public key certificates** for all the TMN entities that need to have secure communications, as well as for any external entities that need to communicate securely with TMN entities. A CA also issues certificates to CAs outside the TMN. The CA issues **Certificate Revocation Lists (CRLs)** as necessary. A CRL includes the serial numbers of certificates that have been revoked (for example, because the key has been compromised or because the subject is no longer with the company) and whose validity period has not yet expired. The CA typically employs a tamper-proof computer kept under the highest security[1]. The term CA is also used to refer to an organization (rather than a device) that issues certificates as a service, usually for a fee.

The most common format of a certificate is as defined in ITU-T X.509. ITU-T X.509 defines several mandatory fields. It further provides for the addition of any number of **extensions**. Each extension is marked critical or non-critical. If an entity processing a certificate encounters a non-critical extension it does not recognize, it may ignore that extension. If an entity processing a certificate encounters a critical extension it does not recognize, it must reject the certificate. ITU-T X.509 also allows extensions to CRLs and to individual CRL entries. Interoperability in a TMN or between TMNs requires, at a minimum, full agreement on all critical extensions (if any) in certificates used in TMN applications.

A **Registration Authority (RA)** verifies the authenticity of every entity (NE, OS, WS, employee, customer, supplier, etc.) that should receive a public key certificate from the TMN's CA. The RA typically consists of a small number of security administrators with access to the CA.

An RA typically publishes a **Certification Policy Statement (CPS)** that specifies under what conditions (e.g. identity check) it would issue a certificate.

PKI includes a **directory** for the storage and distribution of certificates and CRLs. ITU-T X.500 provides the basis for the directory. ITU-T Q.812 includes a profile for the use of the X.500 Directory Access Protocol (DAP). However, directories based on the IETF PKI profile of LDAPv3 (Lightweight DAP, a subset of DAP) may be more readily available than directories based on ITU-T X.500.

[1] The requirements for physical security and system security for a tamper-proof computer are outside the scope of this Recommendation.

Each **TMN entity** would need to interact with the TMN PKI directory in order to retrieve and receive certificates of other entities as well as CRLs. It would need the capability of processing certificates and CRLs. Each TMN entity will also need the capability of constructing and processing certification paths.

The TMN PKI components need to interact through standard **protocols**. The interactions among TMN PKI components are illustrated in Figure 1.

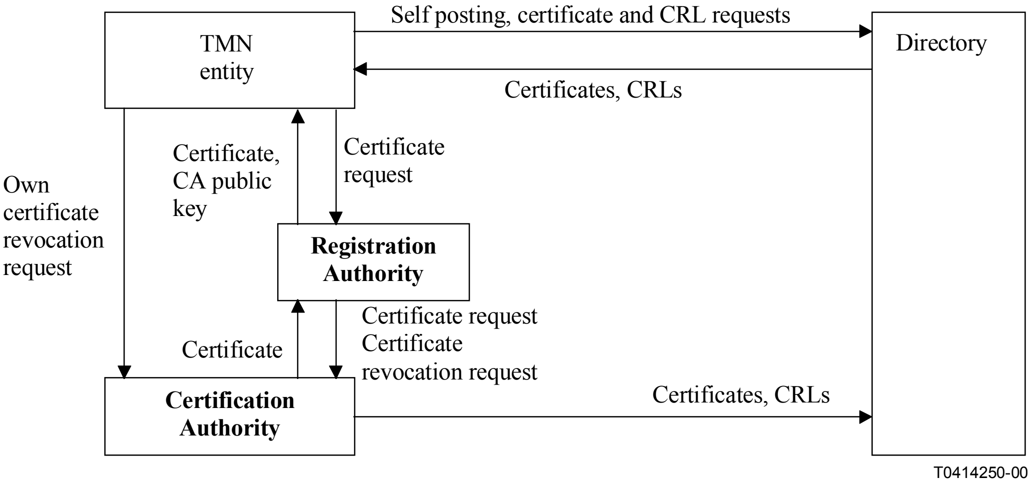

Figure 1/Q.817 – Interactions among TMN PKI components

6 Certificate extensions

The IETF PKI uses the **certificates** defined in ITU-T X.509. This format allows for any number of **extensions**. The IETF PKI includes numerous extensions, listed below. (The extensions are defined in: IETF Request for Comments 2459.) This Recommendation is based on RFC 2459, which is a normative part of this standard by reference.

This Recommendation provides a TMN-specific profile of RFC 2459 without repeating text from that RFC.

This Recommendation provides the following default guidelines for the processing of certificate extensions, each administration can choose different behaviours based on its security policy:

- If a non-critical extension that MUST be present is absent or has an invalid value, then the certificate shall be accepted and processed. At the same time the event shall be logged in a security audit trail and a security alarm shall be sent. Both the security audit trail record and the security alarm shall include a copy of the certificate, a copy of the message containing the certificate, the time the certificate was received, and the entity that detected the discrepancy.
- If a non-critical extension that should not be present, is present, then the certificate shall be accepted and processed. At the same time the event shall be logged in a security audit trail and a low-level security alarm shall be sent. Both the security audit trail record and the security alarm shall include a copy of the certificate, a copy of the message containing the certificate, the time the certificate was received, and the entity that detected the discrepancy.
- If an end-entity does not recognize a critical extension it shall not process the certificate any further. At the same time the event shall be logged in a security audit trail and a security alarm shall be sent. Both the security audit trail record and the security alarm shall include a copy of the certificate, a copy of the message containing the certificate, the time the

certificate was received, and the entity that detected the discrepancy. It shall respond to the entity sending the certificate (explicitly or implicitly by reference) with a message stating that the certificate contains an unrecognized critical extension.

- If an end-entity encounters an invalid value in a critical extension it shall not process the certificate any further. At the same time the event shall be logged in a security audit trail and a security alarm shall be sent. Both the security audit trail record and the security alarm shall include a copy of the certificate, a copy of the message containing the certificate, the time the certificate was received, and the entity that detected the discrepancy. It shall not respond to the entity sending the certificate (explicitly or implicitly by reference).

Unless noted otherwise, these extensions may be used in both CA certificates and end-entity certificates.

6.1 Authority Key Identifier

This extension is defined by and required in ITU-T X.509.

This extension is required by RFC 2459 and this Recommendation in all conformant certificates, except in a CA's self-signed certificate where it may be omitted.

This extension is always non-critical.

The keyIdentifier shall be the 160-bit SHA-1 hash BIT STRING representation of the public key (excluding tag, length, and number of unused bits). RFC 2459 provides the construction of the BIT STRING for various public key types.

6.2 Subject Key Identifier

This extension is defined by and required in X.509.

This extension is required by RFC 2459.

This extension is required by this Recommendation in all conformant CA certificates.

This extension is optional for end-entity certificates interacting over the X interface.

It shall not be used for end-entity certificates interacting only over Q interfaces.

This extension is always non-critical.

The keyIdentifier shall be the 160-bit SHA-1 hash BIT STRING representation of the public key (excluding tag, length, and number of unused bits). RFC 2459 provides the construction of the BIT STRING for various public key types.

6.3 Key Usage

This extension is defined by and required in ITU-T X.509.

This extension is optional for end-entity certificates interacting over the X interface.

This extension shall not be used for end-entity certificates interacting only over Q interfaces.

This extension shall be critical if present.

6.4 Private Key Usage Period

This extension is defined by and required in ITU-T X.509.

This extension is not recommended in RFC 2459.

This extension is optional in this Recommendation; if it is present it shall be marked non-critical.

6.5 Certificate Policies

In certificates to be used over the Q interface this extension is optional, its use is not recommended, it shall be marked non-critical.

In certificates to be used over the X interface this extension is optional, its use is recommended, it can be marked critical.

This extension is not needed for entities that interact only over the Q interface. The RA can decide on different certification policies for different TMN elements, imposing stricter policies for elements with broader access privileges. The access control function into TMN resources would then be based only on the authenticated identity of the initiator and the access privileges of that initiator, not on the certification policy for the initiator's certificate.

This extension is useful for entities interacting over the X interface; therefore all such entities should be able to process this extension. Inclusion of this extension is recommended for certificates issued to entities that are expected to interact over the X interface.

If this extension is present it shall consist of a single OID.

6.6 Policy Mapping

RFC 2459 specifies that this extension is always non-critical and it may be present only in CA certificates.

This extension is not needed for TMN CA certificates if the certificate issued only within that TMN (i.e. for Q interface interactions). End-entities that interact only over Q interfaces are not required to process this extension.

This extension may be present in CA certificates used for X interface interactions.

6.7 Subject Alternative Name

This extension is not needed for TMN interactions over the Q interface. If this extension is present it shall be marked non-critical (meaning that the subject distinguished name must be present). End-entities that interact only over Q interfaces are not required to process this extension.

This extension may be useful for some interactions over the X interface. In such cases its usage shall be as specified in RFC 2459.

6.8 Issuer Alternative Name

TMN entities are not required to process this extension. If it is present this extension shall be marked non-critical.

6.9 Subject Directory Attributes

This extension is not recommended for TMN applications. Its use is optional.

If it is present this extension shall be marked non-critical.

6.10 Basic Constraints

This extension shall be present in all CA certificates and it shall be marked critical.

This extension shall not be present in any end entity certificates.

6.11 Name Constraints

This extension may be present in CA certificates and it shall be marked critical.

This extension shall not be present in any end entity certificates.

6.12 Policy Constraints

This extension is optional. It may be marked critical or non-critical.

If the certificate is issued by one CA to another CA in the same security domain then it is recommended that this extension be marked non-critical. In this case Network Elements (NE) are not required to process this extension.

If the certificate is issued by one CA to another CA in another security domain or in another administration, then this extension shall be marked critical. Different administrations are always in different security domains, therefore gateways that support X interfaces are required to process this extension.

6.13 Extended Key Usage

This extension shall not be used for TMN applications. However, a TMN entity that supports X interface interactions may encounter this field in certificates issued by an external CA.

This extension shall not be used in certificates to be used for Q interface applications.

This extension is optional in certificates to be used for X interface applications.

If this extension is present it shall be marked critical.

6.14 CRL Distribution Points

This extension is recommended for certificates used over the X interface. This extension is optional for certificates used for Q interface transactions.

NOTE – Contributions are solicited with reference to the criticality of this extension.

6.15 Authority Information Access

This extension shall not be used in certificates intended for use over Q interfaces. It may be used in certificates intended for use over X interfaces. If it is present this extension shall be marked non-critical.

7 Certificate Revocation List (CRL) Extensions

The IETF PKI uses **CRLs** defined in the 1993 version of ITU-T X.509. It further specifies several extensions to the basic CRL. (The extensions are defined in: Request for Comments 2459.)

7.1 Authority Key Identifier

This extension shall be present and it shall be marked non-critical.

7.2 Issuer Alternative Name

This extension shall not be used for TMN Q interface transactions. It may be present in certificates used over an X interface. If it is present it shall be marked non-critical.

7.3 CRL Number

This extension shall be present and it shall be marked non-critical.

7.4 Delta CRL Indicator

This extension is optional for CRLs that support Q interface transactions. This extension is not required if the TMN administrator decides not to issue delta CRLs. Use of this extension offers the TMN administrator more flexibility in distributing CRL information. It may be present in external CRLs. If it is present this extension shall be marked critical.

7.5 Issuing Distribution Point

This extension is optional. For TMN applications the OPTIONAL field onlySomeReasons shall not be used.

It may be present in external CRLs. If it is present this extension shall be marked critical.

8 Extensions for Individual Entries in CRLs

The IETF PKI lists several extensions for **individual entries in a CRL**. (The extensions are defined in: Request for Comments 2459.)

8.1 Reason Code

This extension is optional. If it is present this extension shall be marked non-critical.

8.2 Hold Instruction Code

This extension is optional. This extension is not required in CRLs that support Q interface transactions. This extension may be present in external CRLs. If it is present this extension shall be marked non-critical.

8.3 Invalidity Date

This extension is optional. This extension is not required in CRLs that support Q interface transactions. This extension may be present in external CRLs. If it is present this extension shall be marked non-critical.

8.4 Certificate Issuer

This extension shall not be used for CRLs that support Q interface transactions. This extension may be present in external CRLs. If it is present this extension shall be marked critical.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series B	Means of expression: definitions, symbols, classification
Series C	General telecommunication statistics
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Construction, installation and protection of cables and other elements of outside plant
Series M	TMN and network maintenance: international transmission systems, telephone circuits, telegraphy, facsimile and leased circuits
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	**Switching and signalling**
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks and open system communications
Series Y	Global information infrastructure and Internet protocol aspects
Series Z	Languages and general software aspects for telecommunication systems

Geneva, 2001