

International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Series Y
Supplement 18
(06/2012)

SERIES Y: GLOBAL INFORMATION
INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS
AND NEXT-GENERATION NETWORKS

**ITU-T Y.2700-series – Supplement on next
generation network certificate management**

ITU-T Y-series Recommendations – Supplement 18

ITU-T Y-SERIES RECOMMENDATIONS

**GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND NEXT-
GENERATION NETWORKS**

GLOBAL INFORMATION INFRASTRUCTURE

General	Y.100–Y.199
Services, applications and middleware	Y.200–Y.299
Network aspects	Y.300–Y.399
Interfaces and protocols	Y.400–Y.499
Numbering, addressing and naming	Y.500–Y.599
Operation, administration and maintenance	Y.600–Y.699
Security	Y.700–Y.799
Performances	Y.800–Y.899

INTERNET PROTOCOL ASPECTS

General	Y.1000–Y.1099
Services and applications	Y.1100–Y.1199
Architecture, access, network capabilities and resource management	Y.1200–Y.1299
Transport	Y.1300–Y.1399
Interworking	Y.1400–Y.1499
Quality of service and network performance	Y.1500–Y.1599
Signalling	Y.1600–Y.1699
Operation, administration and maintenance	Y.1700–Y.1799
Charging	Y.1800–Y.1899
IPTV over NGN	Y.1900–Y.1999

NEXT GENERATION NETWORKS

Frameworks and functional architecture models	Y.2000–Y.2099
Quality of Service and performance	Y.2100–Y.2199
Service aspects: Service capabilities and service architecture	Y.2200–Y.2249
Service aspects: Interoperability of services and networks in NGN	Y.2250–Y.2299
Numbering, naming and addressing	Y.2300–Y.2399
Network management	Y.2400–Y.2499
Network control architectures and protocols	Y.2500–Y.2599
Smart ubiquitous networks	Y.2600–Y.2699
Security	Y.2700–Y.2799
Generalized mobility	Y.2800–Y.2899
Carrier grade open environment	Y.2900–Y.2999
Future networks	Y.3000–Y.3099

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

Supplement 18 to ITU-T Y-series Recommendations

ITU-T Y.2700-series – Supplement on next generation network certificate management

Summary

Supplement 18 to ITU-T Y-series Recommendations provides guidelines for managing ITU-T X.509 certificates for NGN security based on the trust model defined in ITU-T Y.2701 to supplement the information in ITU-T Y.2704. This Supplement is applicable to any next generation network (NGN) using certificates based on the framework for public key infrastructure (PKI) and privilege management infrastructure (PMI) specified in ITU-T X.509 for identification, authentication, privilege/attribute management and/or encryption between network elements and between user end-devices and the NGN provider customer premises equipment (CPE) provisioning element.

History

Edition	Recommendation	Approval	Study Group
1.0	ITU-T Y Suppl. 18	2012-06-15	13

Keywords

Next generation network, privilege management infrastructure, public key infrastructure, security and ITU-T X.509 certificates.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). 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 publication, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this publication is voluntary. However, the publication may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the publication is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the publication is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this publication 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 publication development process.

As of the date of approval of this publication, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this publication. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at <http://www.itu.int/ITU-T/ipr/>.

© ITU 2013

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

Table of Contents

		Page
1	Scope	1
2	References.....	1
3	Definitions	1
	3.1 Terms defined elsewhere	1
	3.2 Terms defined in this Supplement	1
4	Abbreviations and acronyms	2
5	Conventions	2
6	Reference model	3
7	Certificate management	3
	7.1 Obtaining certificates	3
	7.2 Certificate verification	4
	7.3 Certificate contents for NGN infrastructure	4
	7.4 Expected content of service provider certificate for peering	8
	7.5 Certificate revocation	9
	Appendix I – ITU-T X.509-based authorization privilege management	10
	I.1 Overview of ITU-T X.509-based privilege management infrastructure	10
	I.2 Applicability of the PMI to NGN security	14
	Bibliography.....	15

Introduction

Recommendation ITU-T Y.2704 identified the use of ITU-T X.509 certificates as a means of identification, authentication, privilege/attribute management and/or encryption between network elements, and between user end-devices and the NGN provider customer premises equipment (CPE) provisioning element. This document supplements ITU-T Y.2704 by providing additional guidelines for managing these ITU-T X.509 certificates.

Supplement 18 to ITU-T Y-series Recommendations

ITU-T Y.2700-series – Supplement on next generation network certificate management

1 Scope

This Supplement defines procedures for managing ITU-T X.509 certificates used for NGN security based on the trust model defined in [ITU-T Y.2701]. It provides guidance to supplement [ITU-T Y.2704] regarding the use by the NGN of certificates based on the framework for public key infrastructure (PKI) and privilege management infrastructure (PMI) specified in [ITU-T X.509].

This Supplement is applicable to any NGN using ITU-T X.509 certificates for identification, authentication, privilege/attribute management and/or encryption between network elements, and between user end-devices and the NGN provider customer premises equipment (CPE) provisioning element, based on the trust model defined in [ITU-T Y.2701]. This includes use of ITU-T X.509 certificates between network elements of peering providers based on policy and business agreements. This Supplement assumes that the NGN provider is the certificate agent (CA). Scenarios where the CA is another entity are not within the scope of this Supplement.

NOTE – NGN certificate management is viewed as part of the broader topic of NGN identity management (IdM).

2 References

- [ITU-T X.509] Recommendation ITU-T X.509 (2008) | ISO/IEC 9594-8:2008, *Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks*.
- [ITU-T Y.2701] Recommendation ITU-T Y.2701 (2007), *Security requirements for NGN release 1*.
- [ITU-T Y.2704] Recommendation ITU-T Y.2704 (2010), *Security mechanisms and procedures for NGN*.

3 Definitions

3.1 Terms defined elsewhere

This Supplement uses the following terms defined elsewhere:

3.1.1 authentication [b-ITU-T X.811]: The provision of assurance of the claimed identity of an entity.

3.1.2 authorization [b-ITU-T X.800]: The granting of rights, which includes the granting of access based on access rights.

3.1.3 border element [ITU-T Y.2701]: Network element providing functions connecting different security and administrative domains.

3.1.4 trust [b-ITU-T X.810]: Entity X is said to *trust* entity Y for a set of activities if and only if entity X relies upon entity Y behaving in a particular way with respect to the activities.

3.2 Terms defined in this Supplement

None.

4 Abbreviations and acronyms

This Supplement uses the following abbreviations and acronyms:

AA	Attribute Authority
AC	Attribute Certificate
BE	Border Element
CA	Certification Authority
CPE	Customer Premises Equipment
CPE-BE	Customer Premises Equipment Border Element
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSR	Certificate Signing Request
DNS	Domain Name System
ECC	Elliptic Curve Cryptography
ECDSA	Elliptic Curve Digital Signature Algorithm
FQDN	Fully Qualified Domain Name
HTTP	Hypertext Transfer Protocol
IdM	Identity Management
MAC	Media Access Control
NE	Network Element
NGN	Next Generation Network
OAM&P	Operation, Administration, Maintenance and Provisioning
OCSP	Online Certificate Status Protocol
PKC	Public Key Certificate
PKCS	Public-Key Cryptographic Standard
PKI	Public Key Infrastructure
PMI	Privilege Management Infrastructure
PSS	Probabilistic Signature Scheme
RBAC	Role-Based Access Control
SIP	Session Initiation Protocol
SLA	Service Level Agreement
SOA	Source of Authority
UICC	Universal Integrated Circuit Card

5 Conventions

None.