

I n t e r n a t i o n a l T e l e c o m m u n i c a t i o n U n i o n

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.

6 Reference model

This Supplement assumes the use of the trust model defined in [ITU-T Y.2701].

7 Certificate management

The NGN entities (e.g., terminal equipment, terminal equipment border element, network element and system) that are authorized to be issued certificate(s) and how the certificates are used within the NGN provider domain are subject to the NGN provider security policy. The use of certificates across peering NGN provider domains will be based on security policy established through bi-lateral or multi-lateral service level agreements (SLAs).

[ITU-T X.509] version 3 (or higher) certificate(s) may be used to facilitate the following based on the NGN provider's security policy (not limiting):

- identification of network entities (e.g., end-user terminals, network element and system);
- authentication of network entities;
- attributes and privilege management of network entities;
- establishing secure associations between communicating network entities (e.g., encryption);
- providing identification and authentication of the NGN provider to customer devices and to peering NGN providers.

All certificates of the NGN provider's network elements are issued by the NGN provider's certification authority (CA). The CA certificates (root CA certificate or its subordinate CA certificate) have to be securely delivered to, and stored by, the relying party of the CA (e.g., subscribers of the NGN provider or peering NGN providers). The certification authority is maintained by the NGN provider.

Certificates in the NGN provider's infrastructure should comply with [ITU-T X.509], [b-IETF RFC 3279] and [b-IETF RFC 5280].

NGN network elements obtain certificates from a certification authority by the procedures given in clause 7.1. When a certificate is exchanged as part of establishing a secure connection, the certificate contents are checked according to the procedures of clause 7.2.

Certificates used for setting up security associations also form the basis of end-user and device identification and authentication. For example, in the case of use of the session initiation protocol (SIP), this translates into a mapping between the certificate contents and the allowable values of originator identity for SIP requests.

The guidance and requirements provided in [b-CA/Browser Forum] should be taken into consideration for NGN provider issuance and management of ITU-T X.509 certificates.

Each of the following clauses giving certificate contents explains how the originator identity can be determined from the fields in that certificate.

7.1 Obtaining certificates

7.1.1 NGN provider's network element certificates

The NGN network element should securely generate and store a public/private key pair. Use of Public-Key Cryptographic Standard #10 (PKCS #10) [b-IETF RFC 2986] is preferred; however, other mechanisms are possible based on the NGN provider's security policy. The key generation may either be done on the device by the system administrator who then generates a certificate signing request (CSR) (e.g., PKCS #10 request) or performed separately on a secured machine that then is used to generate the CSR. If the key generation is performed on a separate machine, steps should be taken to ensure that the private key is not compromised. If the key pair is generated on a separate machine, the public/private key pair will need to be securely installed on the network

element as well as the certificate. All key generation and storage should be in compliance with the NGN provider security policy. Generation of public/private key pairs should be done using an algorithm approved by the NGN provider, to ensure sufficient randomness.

After the CSR is generated, the network element sends a CSR to the certification authority (i.e., the request can be sent automatically or by a system administrator). This request should contain a distinguishing name, the public key generated as described above, and a set of attributes, which depend on the type of network element. The CSR is sent to the certification authority (CA) using an authenticated communication channel that verifies that the request is coming from an authenticated user. Some examples of this include a signed e-mail where the signature is checked before the request is passed on to the CA, or a web form that is only accessible through some authentication method that limits access to only authorized certificate requestors. The CA verifies the signature on the CSR and builds an ITU-T X.509 certificate from the information provided. See clause 7.3 for the basic structure of NGN provider certificates. The CA then returns the certificate to the requesting system administrator. The request may occur through an HTTP request or it may be downloaded later by the system administrator, or it may be provided by e-mail. The system administrator will install the device certificate and the root certificate of the CA.

7.1.2 End-user and subscriber certificates

End-user certificates may be downloaded into the end-device through the NGN provider provisioning process. Use of PKCS #10 [b-IETF RFC 2986] is preferred; however, other mechanisms are possible based on the NGN provider's security policy. For these certificates, a CSR is generated with the end-user information and the private key, and the resulting certificate is sent to the end-user device over a secured channel that should have been authenticated by some other method.

Alternatively, memory devices such as a universal integrated circuit card (UICC) may be used to issue end-user certificates.

7.2 Certificate verification

All network elements should verify the complete certificate chain of all received certificates up to a known certification authority. If any step in this chain fails, then the certificate is considered invalid and is rejected. The network element should reject the certificate if it has expired.

7.3 Certificate contents for NGN infrastructure

This clause describes example certificate profiles for NGN infrastructure using ITU-T X.509 version 3 certificates. All certificates should indicate the following:

- Version: 3
- Signature algorithm (should be one of the following):
 - sha256withRSAEncryption (1 2 840 113549 1 1 11)
 - sha256withRSA-PSS (1 2 840 113549 1 1 10)
 - sha1withRSA (1 2 840 113549 1 1 5)
 - sha1withECDSA (1 2 840 10045 4 1)
- Public key algorithm (should be one of the following and match the signature algorithm):
 - rsaEncryption (1 2 840 113549 1 1 1)
 - ECC (1 2 840 10045 2 1)
- Key size:
 - A minimum of 2048 bits for the RSA modulus
 - A minimum of 224 bits for the EC generator.

- IssuerName: <NGN Provider>
- Subject name will contain:
 - C=<Country>
 - O=<NGN_Provider>Certificate Contents for NGN Provider CA Certificate

This certificate corresponds to the top-level certification authority for the NGN provider infrastructure. This certificate will be signed by the NGN provider CA. This can be viewed as a self-signed certificate.

The following certificate elements are marked with one or more of the following notations:

- c: critical;
- m: mandatory;
- n: non-critical.

An example format of the NGN provider CA certificate is as follows:

- Issuer name
- Subject name:
 - C=<Country>
 - O=<NGN_Provider>
 - CN= <NGN_Provider CA>
- Modulus length: 2048
- Extensions:
 - keyUsage[c,m](keyCertSign, cRLSign)
 - subjectKeyIdentifier[n,m]
 - authorityKeyIdentifier[n,m](keyIdentifier=<subjectKeyIdentifier value from CA certificate>)
 - basicConstraints[c,m](cA=true, pathLenConstraint=1).

7.3.1 Certificate contents for NGN network elements

This certificate is signed by the NGN provider's CA and follows the requirements outlined in clause 7.3. This certificate is used to authenticate elements of the NGN infrastructure and for session key generation. The validity period of this certificate is determined by the NGN provider on the basis of its policies and the issuing CA's policies. An example format of the certificate is as follows:

- Issuer name
- Subject name:
 - C=<Country>
 - O=<NGN_Provider>
 - OU=<NGN_Provider&<Sub-System Name>>
 - CN=[<Server Identifier>]
 - Issuer name.

In the above subject name, when using domain name server (DNS), the value of <Server Identifier> has to be the DNS fully qualified domain name (FQDN).

When using DNS, the client establishing the secure connection should make a DNS query to obtain the IP address of the server. The client has to verify that the CN=[<Server Identifier>], in the server certificate, matches the name used to query the DNS server.

The server establishing the secure connection, when using DNS, has to verify that the client IP address of the client matches one of the DNS entries associated with the CN, in the client certificate.

- Modulus length: 2048
- Extensions:
 - authorityKeyIdentifier[n,m](keyIdentifier=<subjectKeyIdentifier value from CA cert>)
 - subjectAltName[n,m](dNSName=<DNSName>).
 - The subjectAltName extension should be included for all servers that are capable of generating event messages. This will be the name used on the OAM&P network.
 - For all other servers, the subjectAltName extension may be included. If the subjectAltName extension is included, it has to include the corresponding name value as specified in the CN field of the subject.

In the subject name described above, the value of <Sub-System Name> may be populated with functional names or other suitable identifier defined by the NGN provider based on its policy and architectural network design. For example:

- For border element: be
- For network gateway border element: ngbe
- For IP border element: ipbe
- For call control element: cce
- For service broker: sb
- For media server: ms
- For application server: as
- For provisioning server: sasvp
- For media server resource broker: msrb
- For signalling gateway: sg
- For emergency application server: eas

Other subsystem names may be added as necessary, but each addition has to be documented.

7.3.2 Certificate content for CPE-BE

This certificate is signed by the NGN provider's CA and follows the requirements outlined in clause 7.3. This certificate is used to authenticate CPE-BEs with the NGN provider's infrastructure and may be used for session key generation. The validity period of this certificate is determined by the NGN provider on the basis of its policies and the issuing CA's policies. An example format of the certificate is as follows:

- Issuer name
- Subject name:
 - C=<Country>
 - O=<NGN_Provider>
 - OU=<NGN_Provider&<Sub-System Name>>
 - CN=[<Subscriber Account Identifier>].

The border element receiving the secure connection request from the CPE-BE has to verify that the subscriber account identifier is a valid account.

- Modulus length: 2048
- Extensions:

- authorityKeyIdentifier[n,m](keyIdentifier=<subjectKeyIdentifier value from CA cert>)
- subjectAltName[n,m](dNSName=<DNSName>).
 - The subjectAltName extension has to be included for all CPE-BEs that are capable of generating event messages. This will be the name used on the OAM&P network.
 - For all other CPE-BEs, the subjectAltName extension may be included. If the subjectAltName extension is included, it has to include the corresponding name value as specified in the CN field of the subject.

7.3.3 Device certificate contents for CPE NGN devices

CPE devices may have manufacturer-provided ITU-T X.509 v3 certificates. This certificate is signed by the device manufacturer's CA, whose certificate is issued by an NGN provider's approved CA. This certificate is used to identify and provision the device with the correct data. This certificate may also be used to authenticate the NGN provider's subscriber, and may be used for session key generation. The validity period of this certificate is determined by the NGN provider on the basis of its policies and the issuing CA's policies.

Device certificates need only include device media access control (MAC) address in the CN field as shown below:

- Subject name:
 - C=<Country>
 - O=<Manufacturer>
 - OU=
 - CN=[<Device MAC Address Identifier>].
- Modulus length: 2048
- Extensions.

The CPE provisioning element receiving the certificate has to verify that the device MAC address identifier is associated with an active customer account and only then send service provisioning data to the device.

Border elements when receiving a device certificate have to identify the customer account number associated with the device MAC address identifier and verify signalling header content before forwarding the request to call control elements.

7.3.4 Subscriber certificate contents for CPE NGN devices

This certificate is signed by the NGN provider's CA and follows the requirements outlined in clause 7.3. This certificate is used to authenticate the NGN provider's subscriber, and may be used for session key generation. The validity period of this certificate is determined by the NGN provider on the basis of its policies and the issuing CA's policies. An example format of the certificate is as follows:

- Issuer name
- Subject name:
 - C=<Country>
 - O=<NGN_Provider>
 - OU=<NGN_Provider&UserEquipment>
 - CN=[<Subscriber Account Identifier>].

The border element receiving the secure connection request from the end point device has to verify that the subscriber account identifier is a valid account.

- Modulus length: 2048
- Extensions:
 - authorityKeyIdentifier[n,m](keyIdentifier=<subjectKeyIdentifier value from CA cert>).

7.3.5 Certificate contents for NGN end-users

This certificate is signed by the NGN provider's CA and follows the requirements outlined in clause 7.3. This certificate is used to authenticate a NGN provider's end-user, and may be used for session key generation. The validity period of this certificate is determined by the NGN provider on the basis of its policies and the issuing CA's policies. An example format of the certificate is as follows:

- Issuer name
- Subject name:
 - C=<Country>
 - O=<NGN_Provider>
 - OU=<NGN_Provider&ENDUSER>
 - CN=[<Subscriber Account Identifier>&<End-User Identifier>].

The border element receiving the end-user certificate has to verify that the subscriber account identifier is a valid account.

- Modulus length: 2048
- Extensions:
 - authorityKeyIdentifier[n,m](keyIdentifier=<subjectKeyIdentifier value from CA cert>).

7.4 Expected content of service provider certificate for peering

This clause describes example certificate profiles for the peer service provider certificate.

This certificate is signed by the service provider's chosen CA and follows the requirements outlined in clause 7.3. This certificate is used to authenticate elements of the NGN infrastructure and for session key generation. The validity period of this certificate is determined by the NGN provider on the basis of its policies and the issuing CA's policies. An example format of the certificate is as follows:

- Issuer name
- Subject name:
 - CN=[<Server Identifier>].

In the above subject name, when using DNS, the value of <Server Identifier> should be the DNS fully qualified domain name (FQDN).

As a client establishing the secure connection when using DNS, the peer network border element should make a DNS query to obtain the IP address of the peering service provider server. The peer network border element should verify that the CN=[<Server Identifier>], in the server certificate, matches the name used to query the DNS server.

As a server establishing the secure connection when using DNS, the peer network border element should verify that the IP address of the peer service provider client matches one of the DNS entries associated with the CN in the client certificate.

7.5 Certificate revocation

The NGN provider's CA should maintain certificate revocation information of the certificates it issued. The NGN provider's CA should make certificate revocation information available to relying parties via using predetermined mechanisms (e.g., online certificate status protocol (OCSP) responders, CRL publishing via ITU-T X.509 directory systems or HTTP servers). The mechanisms to be used are based on the CA's policy (i.e., certification practice statement, (CPS)), which is disclosed to and agreed to by the relying parties in advance of the certificate issuance.

The NGN provider should maintain authority revocation information for the NGN provider's certification authorities. The NGN provider should make authority revocation information available to relying parties using predetermined mechanisms.

Appendix I

ITU-T X.509-based authorization privilege management

I.1 Overview of ITU-T X.509-based privilege management infrastructure


I.1.1 Privilege management infrastructure

The primary purpose of a public key infrastructure (PKI) is to strongly authenticate the parties communicating with each other. But authentication on its own is not sufficient in determining what the authenticated party is authorized to do once access to a resource is granted. [ITU-T X.509] provides an authorization mechanism called privilege management infrastructure (PMI). A PMI provides the authorization function after the authentication function has taken place, and has a number of similarities with a PKI (see below).

I.1.2 PMI functional entities and model

I.1.2.1 PMI functional entities

The PMI architecture parallels that of PKI as shown in Figure I.1.



PMI Entity	PKI Entity
Source of Authority (SOA)	Root CA
Attribute Authority (AA)	Certification Authority (CA)
Privilege Holder	Certificate Subject
Privilege Verifier	Relying Party

Figure I.1 – Comparison of PKI and PMI

I.1.2.2 PMI model

The "role assignment holder" of the PMI model could be a device, end user or NE. It should be noted that the PMI does not necessarily result in a separate physical infrastructure distinct from PKI but PMI functional entities can reside in PKI ones. For instance, the source of authority (SOA) could be part of the certification authority (CA); see Figure I.2.

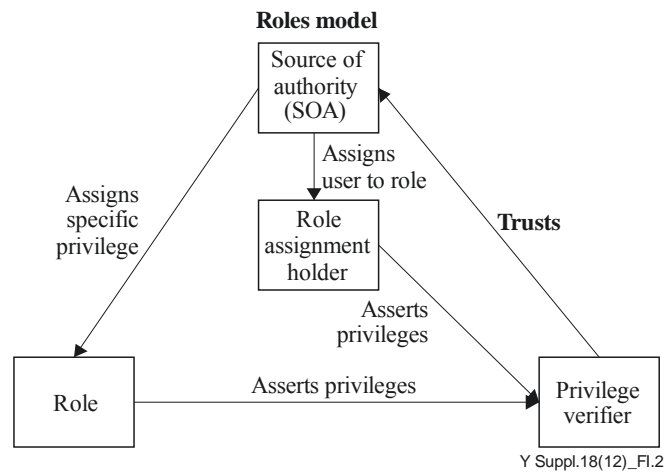


Figure I.2 – An example of the assignment of roles in the PMI model

I.1.3 Attribute certificate

The attribute certificate (AC) specifies the attributes associated with the AC holder for authorization purposes (Figure I.3). (Note that the AC can be used for many applications.) Figure I.4 highlights attribute types and extensions of the attribute certificate.

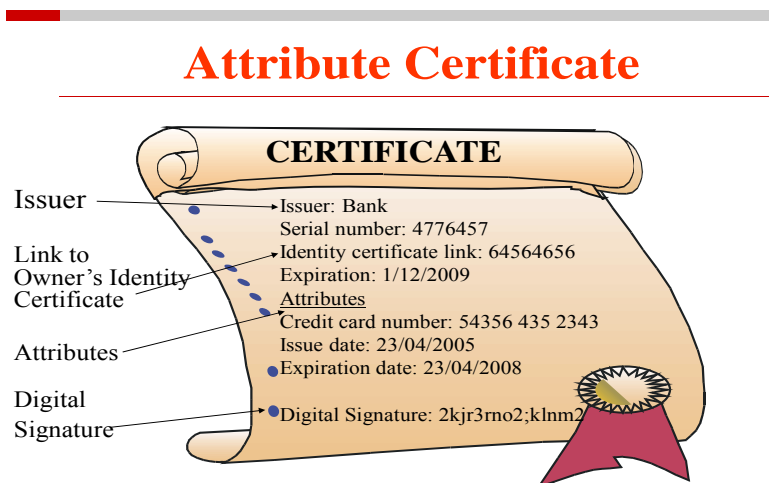


Figure I.3 – The attribute certificate

I.1.4 Attribute certificate: attribute types and extensions

AC Attribute Types	AC Extensions
<ul style="list-style-type: none">–Service Authentication Information–Access Identity–Charging Identity–Group–Role–Clearance–Profile of AC	<ul style="list-style-type: none">–Audit Identity<ul style="list-style-type: none">•To protect privacy and provide anonymity•May be traceable via AC issuer–AC Targeting–Authority Key Identifier–Authority Information Access–CRL Distribution Points

Figure I.4 – Attribute types and extensions of the attribute certificate

Figure I.5 provides a brief explanation of key attributes.

Attribute	Explanation
<ol style="list-style-type: none">1. Service Authentication Information2. Access Identity3. Charging Identity4. Group5. Role6. Clearance7. Profile of AC	<ol style="list-style-type: none">1. Enables NEs that do not support PKI to authenticate user <i>based on log-in and password.</i>2. Identifies the AC holder to the server/ service; basis for authorizing actions; determines RBAC3. Unique identity for charging; not relevant for SPs4. Group Membership Info (core, access)5. Information about the role allocation assigned to the AC holder (e.g admin)6. Clearance level assigned to the AC holder; tied to policyID7. Conformance to specific profile (RFC 3280)

Figure I.5 – Key attributes of the attribute certificate

Figure I.6 provides a brief explanation of key extensions.

Extension	Usage
<ol style="list-style-type: none"> Audit Identity <ul style="list-style-type: none"> To protect privacy and provide anonymity May be traceable via AC issuer AC Targeting Authority Key Identifier Authority Information Access 	<ol style="list-style-type: none"> To protect privacy and provide anonymity. May be traceable via AC issuer <i>The targeting information simply consists of a list of named targets or groups the AC is usable at.</i> Assists the AC verifier in checking the signature of the of the AC Assists the AC verifier in checking the revocation status of the AC

Figure I.6 – Key extensions of the attribute certificate

The target information extension may be used to specify a list of target entities the AC holder can request access to/establish secure communication with. The intent is that the AC should only be usable at the specified servers/services/NEs. An AC verifier who is not among the named servers/services has to reject the AC. The targeting information simply consists of a list of named targets or groups. AC targeting can be used to prevent an NE from establishing communication links with non-authorized NEs.

I.1.5 Binding of public key certificates and attribute certificates

The AC certificate is linked to the PKC with the serial number and subject (Figure I.7). Like the PKC, the AC is a signed certificate and together these form the basis of an architecture for authorization.

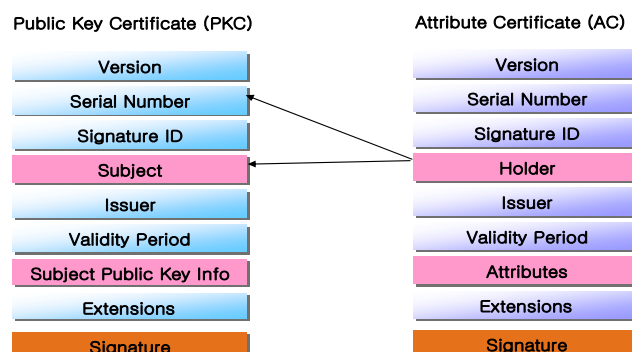
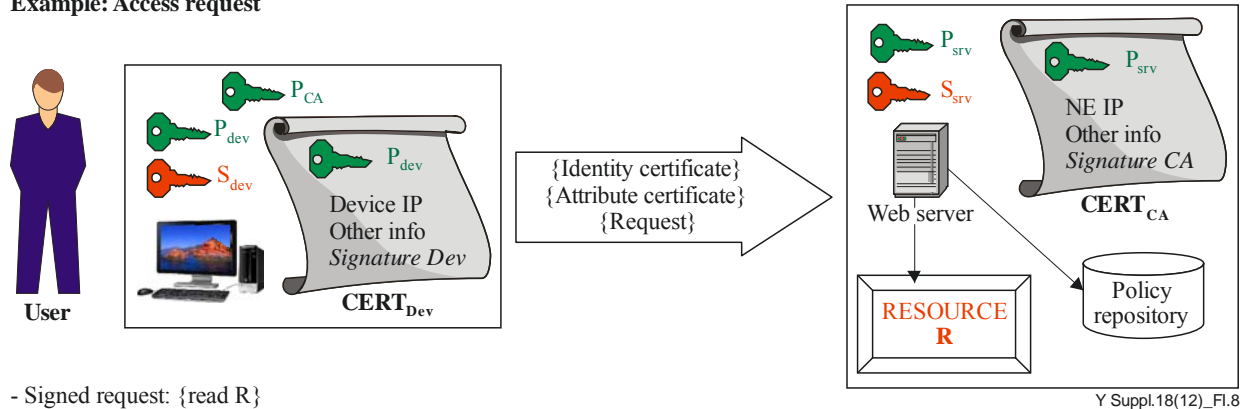


Figure I.7 – Linkages between the public key certificate and attribute certificate

I.1.5.1 Example of PKC and AC usage

Figure I.8 illustrates how the PKC and AC with RBAC based rules combine to authorize user access to a particular resource.

Example: Access request



- Signed request: {read R}
- Signed identity certificate: name; user; public key}
- Signed attribute certificate: name; user; group: G1
- Policy (R) = RBAC (R) = {G1: read, write, G2: ...}

Access to R if user belongs to G1 and G1 is linked to policy (R) then user can access R with the privilege of G1

Figure I.8 – Authorizing user access from the public key certificate and attribute certificate

I.2 Applicability of the PMI to NGN security

Potential applications of the PMI in the NGN include, but are not limited to:

- 1) Role-based access control (RBAC).
- 2) RBAC is usually associated with OAM&P access in that it defines "privileges" assigned to a user with respect to access to NEs for administrative purposes, changes the root directory, etc.
- 3) NGN-wide uniform deployment of security algorithms.
- 4) The PMI can be used to specify the various authentication, integrity and encryption algorithms an NE or group/class of NEs can use for secure NE-to-NE and inter-domain connections.
- 5) Backwards compatibility with NEs supporting log-in and password-based authentication and authorization. This feature is important as networks transition to NGNs.
- 6) End-user administrative access to application servers.

The PMI could also be used to "assign" roles to end-users/subscribers with respect to administrative access to the application servers/subscriber management systems to manage their own services. In general, the PMI will be applicable to NGN management, control and end-user processes and interactions with network elements/interfaces, services and applications. The applicable areas benefit end-to-end networks in many areas, as described in the security architecture of [b-ITU-T X.805]. [b-ITU-T X.805] should be used in conjunction with other standards and industry best practices for identifying and integrating the PMI for NGNs.

Bibliography

- [b-ITU-T X.800] Recommendation ITU-T X.800 (1991), *Security architecture for Open Systems Interconnection for CCITT applications*.
- [b-ITU-T X.805] Recommendation ITU-T X.805 (2003), *Security architecture for systems providing end-to-end communications*.
- [b-ITU-T X.810] Recommendation ITU-T X.810 (1995) | ISO/IEC 10181-1:1996, *Information technology – Open Systems Interconnection – Security frameworks for open systems: Overview*.
- [b-ITU-T X.811] Recommendation ITU-T X.811 (1995) | ISO/IEC 10181-2:1996, *Information technology – Open Systems Interconnection – Security frameworks for open systems: Authentication framework*.
- [b-ITU-T Y.2012] Recommendation ITU-T Y.2012 (2010), *Functional requirements and architecture of next generation networks*.
- [b-ITU-T Y.2702] Recommendation ITU-T Y.2702 (2008), *Authentication and authorization requirements for NGN release 1*.
- [b-IETF RFC 2560] IETF RFC 2560 (1999), *X.509 Internet Public Key Infrastructure Online Certificate Status Protocol (OCSP)*.
- [b-IETF RFC 2315] IETF RFC 2315 (1998), *PKCS #7: Cryptographic Message Syntax Version 1.5*.
- [b-IETF RFC 2986] IETF RFC 2986 (2000), *PKCS #10: Certification Request Syntax Specification Version 1.7*.
- [b-IETF RFC 3029] IETF RFC 3029 (2001), *Internet X.509 Public Key Infrastructure Data Validation and Certification Server Protocols*.
- [b-IETF RFC 3279] IETF RFC 3279 (2002), *Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*.
- [b-IETF RFC 3280] IETF RFC 3280 (2002), *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*.
- [b-IETF RFC 4211] IETF RFC 4211 (2005), *Internet X.509 Public Key Infrastructure Certificate Request Message Format (CRMF)*.
- [b-IETF RFC 5055] IETF RFC 5055 (2007), *Server-based Certificate Validation Protocol (SCVP)*.
- [b-IETF RFC 5280] IETF RFC 5280 (2008), *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*.
- [b-CA/Browser Forum] CA/Browser Forum (2010), *Guidelines For The Issuance And Management Of Extended Validation Certificates*, version 1.3.
- [b-W3C] W3C Recommendation (2004), *XML Key Management Specification (XKMS 2.0)*, version 2.0.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
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	Cable networks and 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	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Terminals and subjective and objective assessment methods
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, open system communications and security
Series Y	Global information infrastructure, Internet protocol aspects and next-generation networks
Series Z	Languages and general software aspects for telecommunication systems