ATIS-1000054

ATIS TECHNICAL REPORT ON NEXT GENERATION NETWORK CERTIFICATE MANAGEMENT

TECHNICAL REPORT

Notice of Disclaimer & Limitation of Liability

The information provided in this document is directed solely to professionals who have the appropriate degree of experience to understand and interpret its contents in accordance with generally accepted engineering or other professional standards and applicable regulations. No recommendation as to products or vendors is made or should be implied.

NO REPRESENTATION OR WARRANTY IS MADE THAT THE INFORMATION IS TECHNICALLY ACCURATE OR SUFFICIENT OR CONFORMS TO ANY STATUTE, GOVERNMENTAL RULE OR REGULATION, AND FURTHER, NO REPRESENTATION OR WARRANTY IS MADE OFMERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR AGAINST INFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS. ATIS SHALL NOT BE LIABLE, BEYOND THE AMOUNT OF ANY SUM RECEIVED IN PAYMENT BY ATIS FOR THIS DOCUMENT, AND IN NO EVENT SHALL ATIS BE LIABLE FOR LOST PROFITS OR OTHER INCIDENTAL OR CONSEQUENTIAL DAMAGES. ATIS EXPRESSLY ADVISES THAT ANY AND ALL USE OF OR RELIANCE UPON THE INFORMATION PROVIDED IN THIS DOCUMENT IS AT THE RISK OF THE USER.

NOTE - The user's attention is called to the possibility that compliance with this standard may require use of an invention covered by patent rights. By publication of this standard, no position is taken with respect to whether use of an invention covered by patent rights will be required, and if any such use is required no position is taken regarding the validity of this claim or any patent rights in connection therewith. Please refer to [http://www.atis.org/legal/patentinfo.asp] to determine if any statement has been filed by a patent holder indicating a willingness to grant a license either without compensation or on reasonable and non-discriminatory terms and conditions to applicants desiring to obtain a license.

ATIS-1000054, *ATIS Technical Report on Next Generation Network Certificate Management*

Is an ATIS Standard developed by the **Security (SEC) Subcommittee** of the **ATIS Packet Technologies and Systems Committee (PTSC)**.

Published by

Alliance for Telecommunications Industry Solutions
1200 G Street, NW, Suite 500
Washington, DC 20005

ATIS-1000054

Technical Report

ATIS Technical Report on Next Generation Network Certificate Management

Alliance for Telecommunications Industry Solutions

Approved February 2013

Abstract

This document provides guidelines for managing X.509 certificates for NGN security based on the trust model defined in [ATIS-1000029] to supplement the information in [ATIS-1000034]. This TR is applicable to an 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 premise equipment (CPE)] provisioning element.

Foreword

The Alliance for Telecommunication Industry Solutions (ATIS) serves the public through improved understanding between providers, customers, and manufacturers. The Packet Technologies and Systems Committee (PTSC) develops and recommends standards and technical reports related to services, architectures, and signaling, in addition to related subjects under consideration in other North American and international standards bodies. PTSC coordinates and develops standards and technical reports relevant to telecommunications networks in the U.S., reviews and prepares contributions on such matters for submission to U.S. ITU-T and U.S. ITU-R Study Groups or other standards organizations, and reviews for acceptability or per contra the positions of other countries in related standards development and takes or recommends appropriate actions.

The mandatory requirements are designated by the word *shall* and recommendations by the word *should*. Where both a mandatory requirement and a recommendation are specified for the same criterion, the recommendation represents a goal currently identifiable as having distinct compatibility or performance advantages. The word *may* denotes a optional capability that could augment the standard. The standard is fully functional without the incorporation of this optional capability.

Suggestions for improvement of this document are welcome. They should be sent to the Alliance for Telecommunications Industry Solutions, PTSC, 1200 G Street NW, Suite 500, Washington, DC 20005.

At the time of consensus on this document, PTSC, which was responsible for its development, had the following leadership:

M. Dolly, PTSC Chair (AT&T)
V. Shaikh, PTSC Vice-Chair (Applied Communications Sciences)
W. Downum, PTSC SEC Chair (Ericsson)
Z. Zeltsan, PTSC SEC Vice-Chair (Alcatel-Lucent)
W. Downum, Technical Editor (Ericsson)
C. Underkoffler, ATIS Chief Editor

The Security (SEC) Subcommittee was responsible for the development of this document.

Table of Contents

Table of Figures

Table of Tables

Technical Report on –

ATIS Next Generation Network Certificate Management

1 Introduction

[ATIS-1000034] and [ITU-T Y.2704] identified the use of 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 premise equipment (CPE) provisioning element. This document supplements [ATIS-1000034] by providing additional guidelines for managing these X.509 certificates.

2 Scope

This Technical Report defines procedures for managing X.509 certificates used for NGN security based on the trust model defined in [ATIS-1000029] and [ITU-T Y.2701]. It provides informative information and guidance to supplement [ATIS-1000034] 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 Technical Report is applicable to an NGN using 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 premise equipment (CPE) provisioning element based on the trust model defined in [ATIS-1000029] and [ITU-T Y.2701]. This includes use of X.509 certificates between network elements of peering providers based on policy and business agreements. This document assumes that the NGN provider is the Certificate Agent (CA). Scenarios where the CA is another entity are not within the scope of this document.

NOTE: NGN Certificate Management is viewed as part of the broader topic of NGN Identity Management (IdM).

3 References

[ATIS-1000029] ATIS-1000029.2008, *Security Requirements for NGN*, November 2008.[1]

[ATIS-1000030] ATIS-1000030.2008, *Authentication and Authorization Requirements for Next Generation Network (NGN)*, November 2008.[1]

[ATIS-1000034] ATIS-1000034.2010, *Next Generation Network (NGN): Security Mechanisms and Procedures*, November 2010.[1]

[ITU-T Y.2701] ITU-T Recommendation Y.2701 (04/07), *Security requirements for NGN release 1*.[2]

[ITU-T Y.2702] ITU-T Recommendation Y.2702 (09/08), *Authentication and authorization requirements for NGN release 1*.[2]

[ITU-T Y.2704] ITU-T Recommendation Y.2704 (01/10), *Security mechanisms and procedures for NGN*.[2]

[1] This document is available from the Alliance for Telecommunications Industry Solutions (ATIS), 1200 G Street N.W., Suite 500, Washington, DC 20005. < https://www.atis.org/docstore/default.aspx >

[2] This document is available from the International Telecommunications Union. < http://www.itu.int/ITU-T/ >

[ITU-T X.509] ITU-T Recommendation X.509 (2008)/ISO/IEC 9594-8, *Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks*.[2]

4 Definitions

4.1 Terms Defined Elsewhere

This Technical Report 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.

3.1.5 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.

4.2 Terms Defined in This Recommendation

None.

5 Abbreviations & Acronyms

This TR uses the following abbreviations and acronyms:

AA	Attribute Authority
AC	Attribute Certificate
CA	Certification Authority
CPE	Customer Premise Equipment
CPE-BE	Customer Premise 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	Operation, Administration, and Management
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
SIP	Session Initiation Protocol
SLA	Service Level Agreement
SOA	Source of Authority
UICC	Universal Integrated Circuit Card

6 Reference Model

This TR assumes the use of the trust model defined in [ATIS-1000029] and [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 Agreement (SLAs).

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 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) has 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 X509], [b-IETF RFC3279] and [b-IETF RFC5280].

NGN Network Elements obtain certificates from a Certification Authority by the procedures given in section 7.1. When a certificate is exchanged as part of establishing a secure connection, the certificate contents are checked according to the procedures of section 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] CA/Browser Forum document, *Guidelines For The Issuance And Management Of Extended Validation Certificates, version 1.3,* should be taken into consideration for NGN provider issuance and management of X.509 certificates.

Each of the following sections 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 RFC2986] 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 (see following sections). 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 email 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 X.509 certificate from the information provided. See Section 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 email. The System Administrator will install the device certificate and the root certificate of the CA.

7.1.2 End User & Subscriber Certificates

End user certificates may be downloaded into the end-device through the NGN provider provisioning process. Use of PKCS#10 [b-IETF RFC2986] 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 an UICC (Universal Integrated Circuit Card) 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 section describes example certificate profiles for NGN infrastructure using X.509 version 3 Certificates . All certificates should indicate the following:

- *Version*: 3
- *Signature Algorithm*: should be one of the following:
  - sha256withRSAEncription (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 self signed certificate.

The following certificates 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 CA and follows the requirements outlined in section 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 System (DNS), the value of <Server identifier> has to be the DNS Fully Qualified Domain Name (FQDN).

The client establishing the secure connection, when using DNS, 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 Signaling Gateway: sg
- For Emergency Application Server: eas
- Etc.

Other subsystem names may be added as necessary, but should 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 at the beginning of this section. 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 X.509 v3 certificates. This certificate is signed by the device manufacturer CA, whose certificate is issued by an NGN provider's approved CA. This certificate is used to identify and provision the device with the right 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 signaling 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 at the beginning of this section. 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 CA and follows the requirements outlined at the beginning of this section. 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 section describes example certificate profiles for Peer Service Provider Certificate.

This certificate is signed by the Service Provider chosen CA and follows the requirements outlined at the beginning of this section. 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

NGN provider CA should maintain Certificate Revocation Information of the certificates that the CA issued. The NGN provider 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 X.500 Directory systems or http servers. The mechanisms to be used are determined on based on the CA's Policy (i.e., CPS, or Certification Practice Statement), 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 A
(informative)

A X.509-Based Authorization Privilege Management

A.1 Overview of X.509-based Privilege Management Infrastructure

A.1.1 PMI

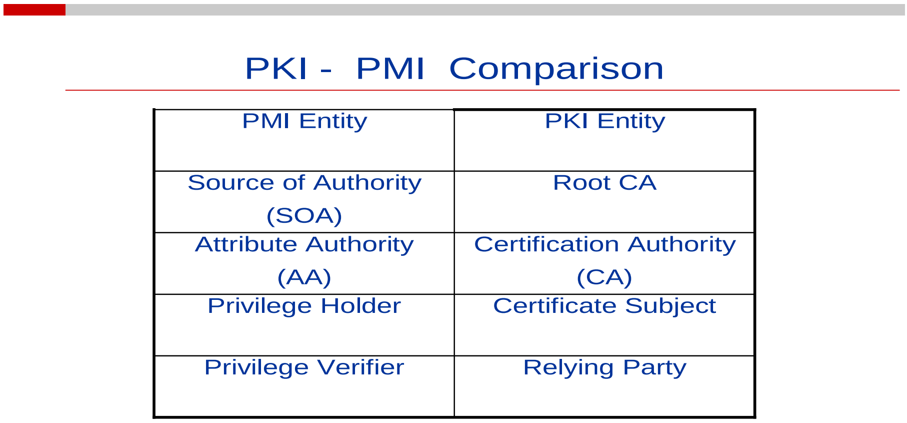
The primary purpose of a Public Key Infrastructure (PKI) is to strongly authenticate the parties communicating with each other. But authentication on its own is not sufficient in determining what the authenticated party is authorized to do once access to resource is granted. [ITU-T X.509] provides an 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.

A.1.2 PMI Functional Entities & Model

A.1.2.1 PMI Functional Entities

The PMI architecture parallels that of PKI as shown in the comparison table below.

Table A.1 - PKI and PMI Comparison

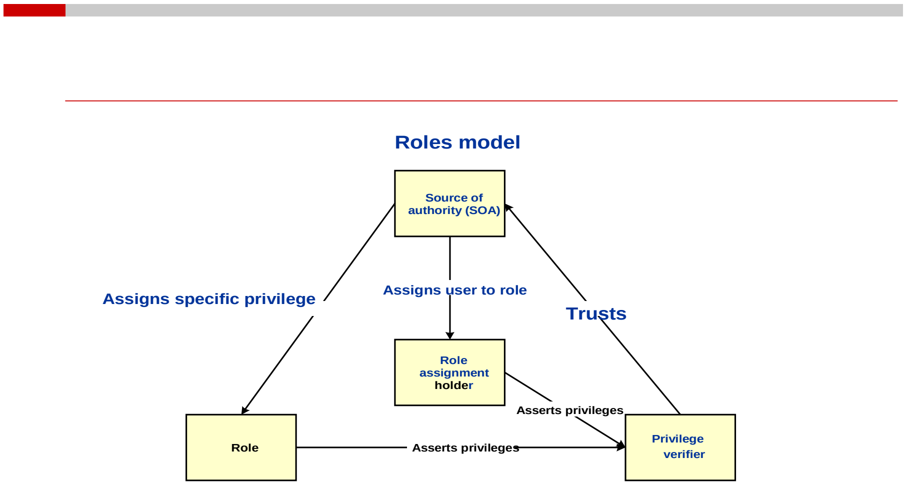


PKI - PMI Comparison

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

A.1.2.2 PMI Model

The “role assignment holder” could be a device, end user, or NE. It should be noted that PMI does not necessarily result in a separate physical infrastructure distinct from PKI, but PMI functional entities can reside in PKI ones. For instance, Source of Authority (SOA) could be part of the Certification Authority (CA).

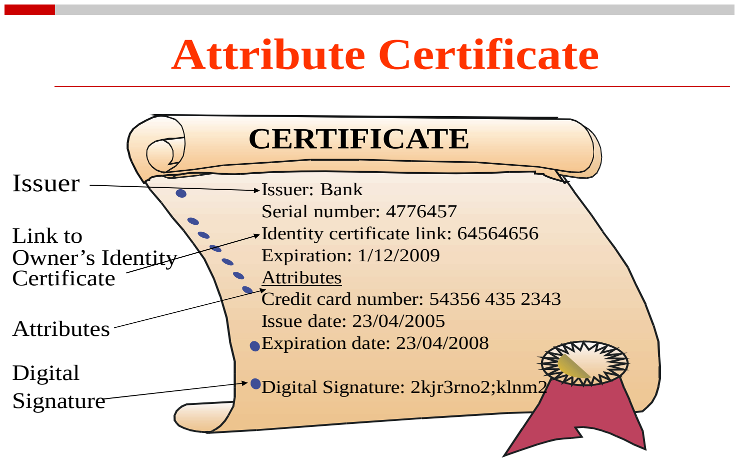


Roles model

Figure A 1 - PMI Role Model

A.1.3 Attribute Certificate

The Attribute Certificate (AC) specifies the attributes associated with the AC holder for authorization purposes.



Attribute Certificate

CERTIFICATE

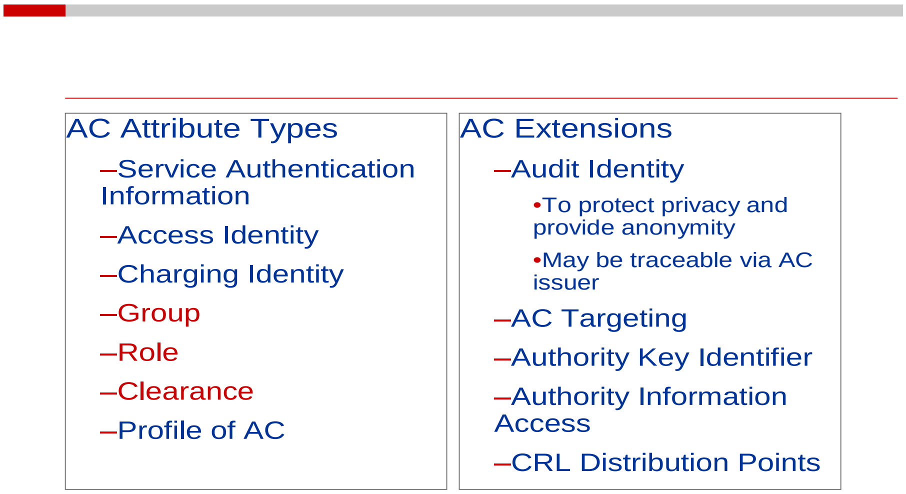
Issuer: Bank
Serial number: 4776457
Identity certificate link: 64564656
Expiration: 1/12/2009
Attributes
Credit card number: 54356 435 2343
Issue date: 23/04/2005
Expiration date: 23/04/2008
Digital Signature: 2kjr3rno2;klnm2

Figure A 2 - Example Attribute Certificate

NOTE: The AC can be used for many applications.

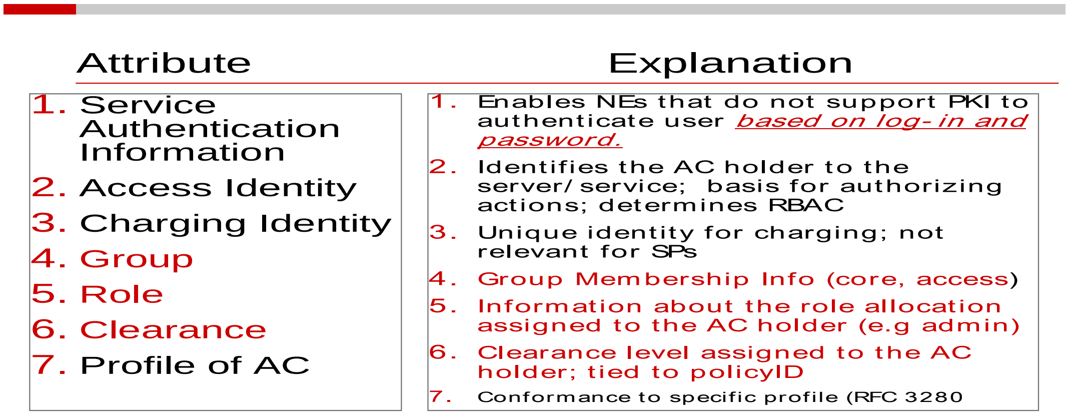
A.1.4 Attribute Certificate: Attribute Types & Extensions

Table A.2 - Attributes types and extensions



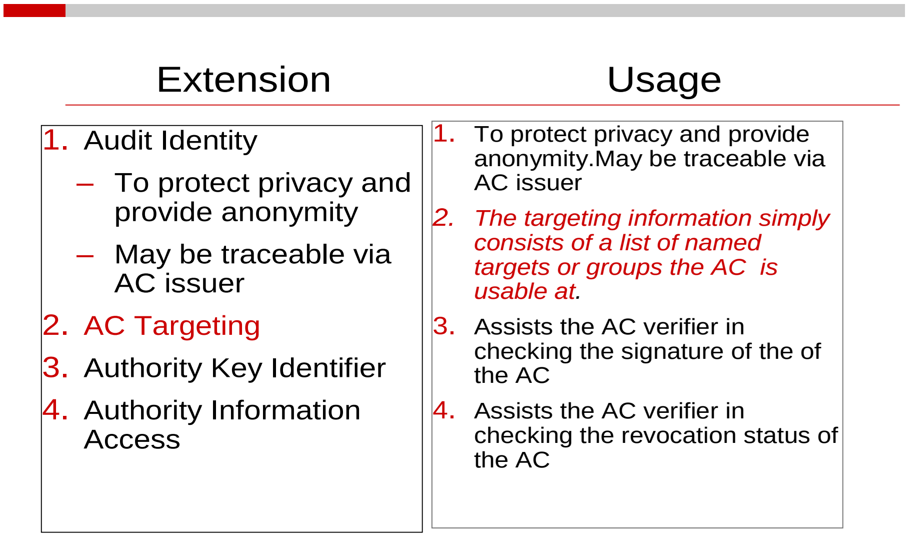
AC Attribute Types	AC Extensions
–Service Authentication Information –Access Identity –Charging Identity –Group –Role –Clearance –Profile of AC	–Audit Identity •To protect privacy and provide anonymity •May be traceable via AC issuer –AC Targeting –Authority Key Identifier –Authority Information Access –CRL Distribution Points

Table A.3 - Explanation of key attributes



Attribute	Explanation
1. Service Authentication Information	1. Enables NEs that do not support PKI to authenticate user *based on log-in and password.*
2. Access Identity	2. Identifies the AC holder to the server/service; basis for authorizing actions; determines RBAC
3. Charging Identity	3. Unique identity for charging; not relevant for SPs
4. Group	4. Group Membership Info (core, access)
5. Role	5. Information about the role allocation assigned to the AC holder (e.g admin)
6. Clearance	6. Clearance level assigned to the AC holder; tied to policyID
7. Profile of AC	7. Conformance to specific profile (RFC 3280

Table A.4 - Explanation of key extensions

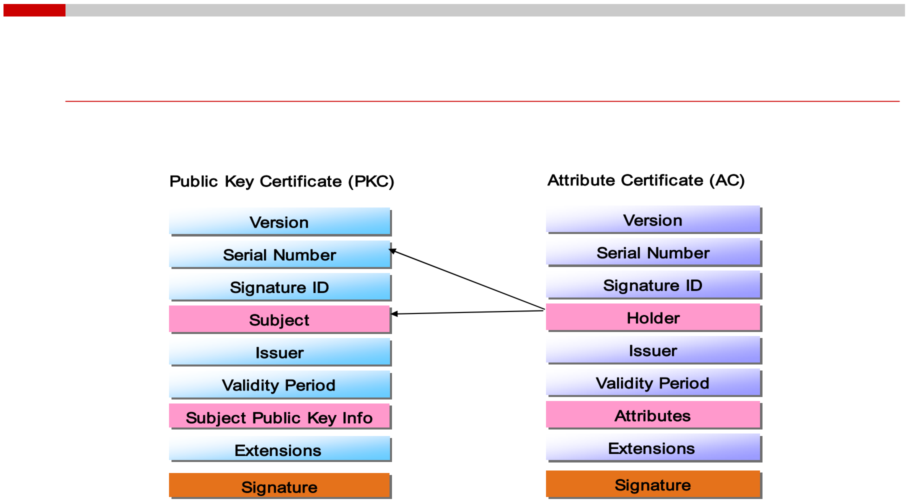


Extension	Usage
1. Audit Identity – To protect privacy and provide anonymity – May be traceable via AC issuer	1. To protect privacy and provide anonymity.May be traceable via AC issuer
2. AC Targeting	2. *The targeting information simply consists of a list of named targets or groups the AC is usable at.*
3. Authority Key Identifier	3. Assists the AC verifier in checking the signature of the of the AC
4. Authority Information Access	4. Assists the AC verifier in checking the revocation status of the AC

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 amongst the named servers/services has to reject the AC. The targeting information simply consists of a list of named targets or groups so that AC targeting can be used to prevent an NE from establishing communication links with non-authorized NEs.

A.1.5 Binding of Public Key Certificates & Attribute Certificates

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



Public Key Certificate (PKC)

- Version
- Serial Number
- Signature ID
- Subject
- Issuer
- Validity Period
- Subject Public Key Info
- Extensions
- Signature

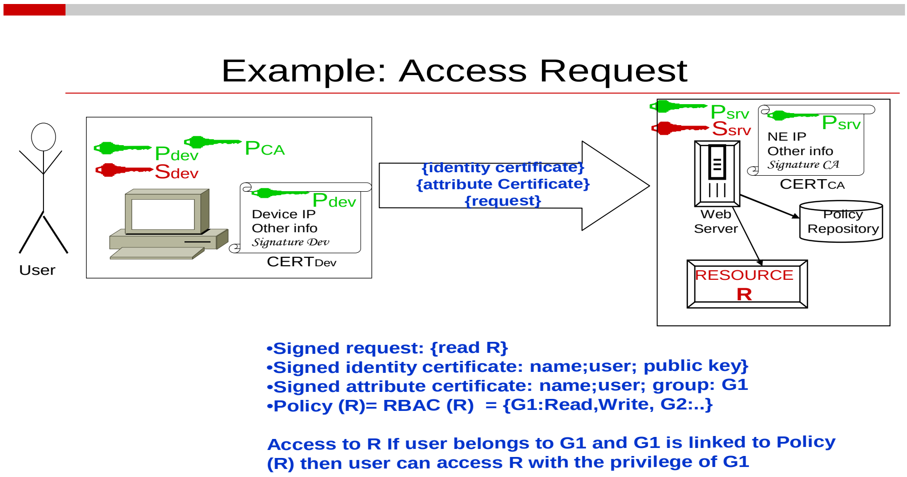
Attribute Certificate (AC)

- Version
- Serial Number
- Signature ID
- Holder
- Issuer
- Validity Period
- Attributes
- Extensions
- Signature

Figure A.3 - Binding of public key certificates and attribute certificates

A.1.6 Example of PKC & AC Usage

The example below illustrates how 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 A.4 - Example of PKC and AC usage

A.2 Applicability of PMI to NGN Security

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

1. Role Based Access Control (RBAC).

2. RBAC is usually associated with Operation, Administration and Management (OAM) access in that it defines "privileges" assigned to a user with respect to access to NEs for administrative purposes, change the root directory, etc.

3. NGN-wide uniform deployment of security algorithms.

4. 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-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 NGN.

6. End user administrative access to application servers.

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, 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 network in many areas as described in [b-ITU-T X.805] security architecture. [b-ITU- T X.805] should be used in conjunction with other standards and industry best practices for identifying and integrating PMI for NGN.

Appendix B
(informative)

B Bibliography

[b-ITU-T X.800] ITU-T Recommendation X.800, *Security architecture for Open Systems Interconnection for CCITT applications*.[2]

[b-ITU-T X.805] ITU-T Recommendation, X.805, *Security architecture for systems providing end-to-end communications*.[2]

[b-ITU-T X.810] ITU-T Recommendation X.810, *Information technology - Open Systems Interconnection - Security frameworks for open systems: Overview*.[2]

[b-ITU-T X.811] ITU-T Recommendation X.811, *Information technology - Open Systems Interconnection - Security frameworks for open systems: Authentication framework*.[2]

[b-ITU-T Y.2012] ITU-T Recommendation Y.2012, *Functional Requirements and Architecture of the NGN*.[2]

[b-IETF RFC4211] IETF RFC4211 (2005), *Internet X.509 Public Key Infrastructure Certificate Request Message Format (CRMF).*[3]

[b-W3C XKMS] W3C Recommendation (2005), *XML Key Management Specification (XKMS 2.0) version 2.0.*[4]

[b-IETF RFC2560] IETF RFC2560 (1999), *X.509 Internet Public Key Infrastructure Online Certificate Status Protocol (OCSP).*[3]

[b-IETF RFC3029] IETF RFC3029 (20010, *Internet X.509 Public Key Infrastructure Data Validation and Certification Server Protocols*.[3]

[b-IETF RFC2986] IETF RFC2986, *PKCS #10: Certification Request Syntax Specification Version 1.7*.[3]

[b-IETF RFC2315] IETF RFC2315 (1993), *PKCS #7: Cryptographic Message Syntax Standard. Version 1.5*.[3]

[b-IETF RFC5055] IETF RFC5055 (2005), *Server-based Certificate Validation Protocol*.[3]

[b-IETF RFC3279] IETF RFC3279, *Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*.[3]

[b-IETF RFC5280] IETF RFC5280, *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*.[3]

[b-IETF RFC6277] IETF RFC6277, *Online Certificate Status Protocol Algorithm Agility*[3]

[b-IETF RFC5987] IETF RFC5987, *The application/pkcs10 Media Type*.[3]

[b-IETF RFC4055] IETF RFC4055*, Additional Algorithms and Identifiers for RSA Cryptography for use in the Internet X.509 Public Infrastructure Certificate and Certificate Revocation List (CRL) Profile*.[3]

[b-IETF RFC4491] IETF RFC4491*,Using the GOST R 34.10-94, GOST R 34.10-2001, and GOST R 34.11-94 Algorithms with the Internet X.509 Public Key Infrastructure Certificate and CRL Profile*.[3]

[b-IETF RFC5480] IETF RFC5480*, Elliptic Curve Cryptography Subject Public Key Information*.[3]

[b-CA/Browser Forum] CA/Browser Forum document, *Guidelines For The Issuance And Management Of Extended Validation Certificates*, version 1.3.[3]

[3] This document is available from the Internet Engineering Task Force (IETF). < http://www.ietf.org >

[4] This document is available from the World Wide Web Consortium. < www.w3.org >