International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1112

(11/2007)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Telecommunication security

Device certificate profile for the home network

ITU-T Recommendation X.1112

ITU-T X-SERIES RECOMMENDATIONS

DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

PUBLIC DATA NETWORKS	
Services and facilities	X.1–X.19
Interfaces	X.20–X.49
Transmission, signalling and switching	X.50–X.89
Network aspects	X.90–X.149
Maintenance	X.150–X.179
Administrative arrangements	X.180–X.199
OPEN SYSTEMS INTERCONNECTION	
Model and notation	X.200–X.209
Service definitions	X.210–X.219
Connection-mode protocol specifications	X.220–X.229
Connectionless-mode protocol specifications	X.230–X.239
PICS proformas	X.240–X.259
Protocol Identification	X.260–X.269
Security Protocols	X.270–X.279
Layer Managed Objects	X.280–X.289
Conformance testing	X.290–X.299
INTERWORKING BETWEEN NETWORKS	
General	X.300–X.349
Satellite data transmission systems	X.350–X.369
IP-based networks	X.370–X.379
MESSAGE HANDLING SYSTEMS	X.400–X.499
DIRECTORY	X.500–X.599
OSI NETWORKING AND SYSTEM ASPECTS	
Networking	X.600–X.629
Efficiency	X.630–X.639
Quality of service	X.640–X.649
Naming, Addressing and Registration	X.650–X.679
Abstract Syntax Notation One (ASN.1)	X.680–X.699
OSI MANAGEMENT	
Systems Management framework and architecture	X.700–X.709
Management Communication Service and Protocol	X.710–X.719
Structure of Management Information	X.720–X.729
Management functions and ODMA functions	X.730–X.799
SECURITY	X.800–X.849
OSI APPLICATIONS	
Commitment, Concurrency and Recovery	X.850–X.859
Transaction processing	X.860–X.879
Remote operations	X.880–X.889
Generic applications of ASN.1	X.890–X.899
OPEN DISTRIBUTED PROCESSING	X.900–X.999
TELECOMMUNICATION SECURITY	X.1000–

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

ITU-T Recommendation X.1112

Device certificate profile for the home network

Summary

ITU-T Recommendation X.1112 proposes a certificate profile for authenticating the device in the home network. It also describes how authentication works between devices in the home network with a secure home gateway. In addition, this Recommendation describes the certificate profile standard for home network devices using ITU-T Recommendation X.509 as the basic reference for the device certificate profile. Finally, this Recommendation describes the certificate management procedures for the home device certificate in the home network.

Source

ITU-T Recommendation X.1112 was approved on 13 November 2007 by ITU-T Study Group 17 (2005-2008) under the ITU-T Recommendation A.8 procedure.

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 Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure e.g. interoperability or applicability) and compliance with the Recommendation 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 Recommendation is required of any party.

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, 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/.

CONTENTS

ITU-T Recommendation X.1112

Device certificate profile for the home network

1 Scope

The framework for device certification in the home network can generally be categorized into two models, one of which is the internal issuing model wherein all home device certificates including a self-signed certificate (i.e., certification authority certificate) and an end-entity certificate (i.e., home device certificate) are issued by an internal certification authority (CA) in the home network. Usually, an internal CA can be a secure home gateway with the capability for generating a key pair and issuing a certificate. Therefore, the secure home gateway can issue a CA certificate as well as home device certificates. Moreover, the secure home gateway can have a device certificate which is issued by an external certification authority for use in external home services. In particular, this home gateway device certificate can be used for authentication between the home gateway and home network service provider as defined in [ITU-T J.192].

The other model is the external issuing model wherein all home device certificates are issued by an external CA.

This Recommendation defines the CA certificate profile and the device certificate profile in the first model particularly that wherein the home security gateway acts as the internal CA. These profiles are used for device authentication in the general home network environment.

This Recommendation also defines the procedure for device certificate management.

2 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. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T J.190] ITU-T Recommendation J.190 (2002), *Architecture of MediaHomeNet that supports cable-based services*.

[ITU-T J.192] ITU-T Recommendation J.192 (2004), *A residential gateway to support the delivery of cable data services*.

[ITU-T Q.1701] ITU-T Recommendation Q.1701 (1999), *Framework for IMT-2000 networks*.

[ITU-T Q.1711] ITU-T Recommendation Q.1711 (1999), *Network functional model for IMT-2000*.

[ITU-T Q.1761] ITU-T Recommendation Q.1761 (2004), *Principles and requirements for convergence of fixed and existing IMT-2000 systems*.

[ITU-T X.500] ITU-T Recommendation X.500 (2005), *Information technology – Open Systems Interconnection – The Directory: Overview of concepts, models and services*.

[ITU-T X.501] ITU-T Recommendation X.501 (2005), *Information technology – Open Systems Interconnection – The Directory: Models*.

[ITU-T X.509] ITU-T Recommendation X.509 (2005), *Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks*.

[ITU-T X.520] ITU-T Recommendation X.520 (2005), *Information technology – Open Systems Interconnection – The Directory: Selected attribute types*.

[ITU-T X.680] ITU-T Recommendation X.680 (2002), *Information technology – Abstract Syntax Notation One (ASN.1): Specification of basic notation*.

[ITU-T X.800] ITU-T Recommendation X.800 (1991), *Security architecture for Open Systems Interconnection for CCITT applications*.

[ITU-T X.803] ITU-T Recommendation X.803 (1994), *Information technology – Open Systems Interconnection – Upper layers security model*.

[ITU-T X.805] ITU-T Recommendation X.805 (2003), *Security architecture for systems providing end-to-end communications*.

[ITU-T X.810] ITU-T Recommendation X.810 (1995), *Information technology – Open Systems Interconnection – Security frameworks for open systems: Overview*.

[ITU-T X.1111] ITU-T Recommendation X.1111 (2007), *Framework of security technologies for home network.*

[ITU-T X.1121] ITU-T Recommendation X.1121 (2004), *Framework of security technologies for mobile end-to-end data communications*.

[IETF RFC 2511] IETF RFC 2511 (1999), *Internet X.509 Certificate Request Message Format*.

[IETF RFC 3280] IETF RFC 3280 (2002), *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*.

3 Definitions

3.1 OSI reference model security architecture definitions

The following terms are defined in [ITU-T X.800]:

a) authentication;

b) authentication information;

c) authorization;

d) encipherment;

e) integrity;

f) key;

g) key management.

3.2 Public-key and attribute certificate frameworks definitions

The following terms are defined in [ITU-T X.509]:

a) authority;

b) certification authority (CA);

c) CA certificate;

d) certificate revocation list (CRL);

e) certificate serial number;

f) certificate user;

g) certificate validation;
h) certificate path;
i) end-entity;
j) hash function;
k) private key;
l) public key;
m) public key infrastructure (PKI);
n) self-signed certificate;
o) trust.

3.3 Framework of security technologies for home network definitions

The following terms are defined in [ITU-T X.1111]:

a) administrator of home network;
b) device certificate;
c) home device;
d) home user;
e) remote terminal;
f) remote user;
g) secure home gateway.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations:

AKI Authority Key Identifier
ASN.1 Abstract Syntax Notation One
CA Certification Authority
CMP Certificate Management Protocol
CMS Cryptographic Message Syntax
CN Common Name
CPU Central Processing Unit
CRL Certificate Revocation List
DN Distinguished Name
LAN Local Area Network
MAC Message Authentication Code
OID Object Identifier
OSI Open Systems Interconnection
PC Personal Computer
PDA Personal Data Assistant
PIN Personal Identification Number
PK Public Key

PKI	Public Key Infrastructure
RA	Registration Authority
RSA	Rivest, Shamir, Adleman (algorithm for public-key cryptography)
SAN	Subject Alternative Name
SHA	Secure Hash Algorithm
SKI	Subject Key Identifier
SSL	Secure Socket Layer
TLS	Transport Layer Security
UTF	Universal Transformation Format

5 Conventions

None.

6 Framework for home network device certification

Authentication of the presented identity of a person or device will be one of the most important functions of home network security. In general, authentication in the home network can be classified into user authentication and device authentication. In providing a device authentication, device certification can be used.

The framework for device certification in the home network can generally be categorized into two models: one is the internal issuing model wherein all home device certificates including a self-signed certificate (i.e., CA certificate) and an end-entity certificate (i.e., home device certificate) are issued by an internal CA in the home network. Usually, an internal CA can be a secure home gateway with the capability of generating a key pair and issuing a certificate. Therefore, the secure home gateway can issue a CA certificate as well as home device certificates. Moreover, the secure home gateway can have a device certificate issued by an external certification authority for use in external home services. This home gateway device certificate can be used for authentication between the home gateway and home network service provider as defined in [ITU-T J.192].

The other model is the external issuing model wherein all home device certificates are issued by an external CA. For this model, [ITU-T J.192] defines the device certificate profile for authentication between a cable TV service provider and a set-top box.

This Recommendation only deals with the first model particularly that wherein the home security gateway acts as the internal CA (the other model is dealt with in [ITU-T J.192]).

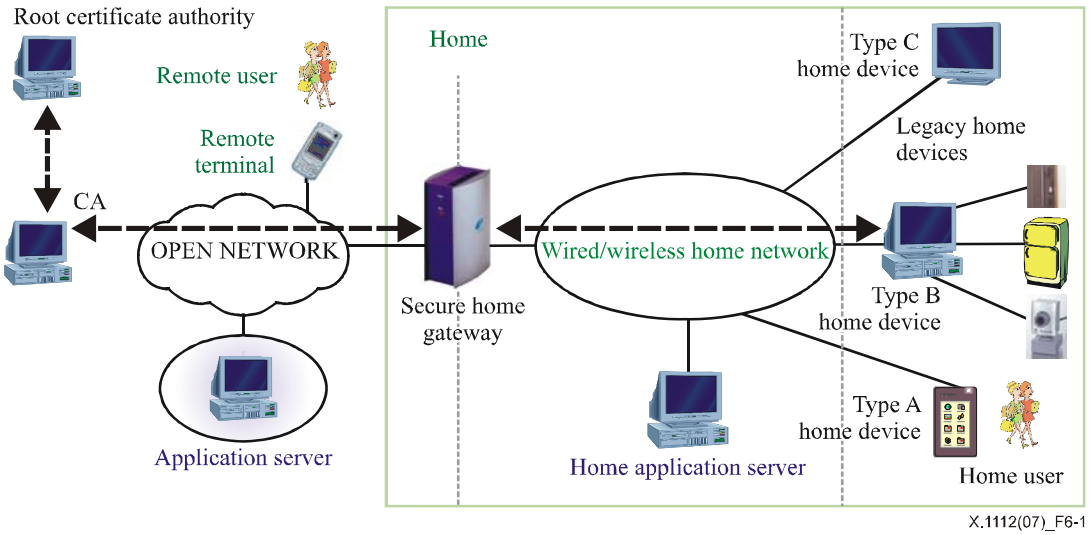

Figure 6-1 – Device authentication model for the secure home network

7 Certificate profile for the home network device

This clause describes the home network device certificate profile that complies with [ITU-T X.509] and [IETF RFC 3280]. For the home network device authentication, a unique identifier that can identify each device in the home network is needed. Specifically, a home device certificate will be required as a unique trust element when used in the home network. The home network service provider can identify the valid home network device using the device certificate.

7.1 Basic certificate fields

7.1.1 Version

This field describes the version of the encoded certificate to distinguish a PKI certificate format.

The version of the certificates must be a version 3 (value is 2) in the home device certificate in accordance with clause 7 of [ITU-T X.509].

```
Version ::= INTEGER {v1(0), v2(1), v3(2) }
```

7.1.2 Serial number

The serial number must be a unique positive integer assigned by a given CA to each certificate (i.e., the issuer name and serial number identify a unique certificate).

Given the uniqueness of the above requirements, serial numbers can be expected to contain long integers. Certificate users must be able to handle serial number values of up to 20 octets. Conformant CAs must not use serial number values longer than 20 octets.

7.1.3 Signature

This field contains the algorithm identifier for the algorithm and hash function used by the CA to sign the certificate.

The algorithm identifier is used to identify a cryptographic algorithm. The OBJECT IDENTIFIER (OID) component identifies the algorithm (i.e., sha-1WithRSAEncryption, id-dsa-with-sha1, etc.).

7.1.4 Issuer

The issuer field identifies the entity that signed and issued the certificate. The issuer field must contain a non-empty X.500 distinguished name (DN). The issuer field is defined as X.501 type Name.

In this Recommendation, all certificate fields that used DN must comply with [ITU-T X.500] and [ITU-T X.501].

7.1.5 Validity

The certificate validity period is the time interval during which the CA warrants that it will maintain information about the status of the certificate.

The field defined in clause 7 of [ITU-T X.509] is represented as a SEQUENCE of two dates: the date on which the certificate validity period begins (*notBefore*) and the date on which the certificate validity period ends (*notAfter*).

```
Validity ::= SEQUENCE {
        notBefore    time,
        notAfter     time }
```

Both *notBefore* and *notAfter* may be encoded as *UTCTime* or *GeneralizedTime*.

7.1.6 Subject

The Subject field identifies the device associated with the public key stored in the subject public key field. The value of the subject field in one certificate shall match the value of the issuer field in the subsequent certificate in the certification path. The subject field must contain a non-empty X.500 distinguished name (DN) and must also be defined as X.501 type Name.

7.1.7 Subject public key info

This field defined in clause 7 of [ITU-T X.509] is used to carry the public key and identify the algorithm with which the key is used (e.g., RSA, DSA, ECDSA, etc.).

```
SubjectPublicKeyInfo ::= SEQUENCE {
        algorithm        AlgorithmIdentifier,
        subjectPublicKey BIT STRING }
```

The *AlgorithmIdentifier* structure must comply with [ITU-T X.509].

7.2 Extensions

The home device certificate may be used to minimize certificate extensions for the lightweight validation properties since many of the home devices have limited computing power.

In this Recommendation, authority key identifier, subject key identifier, key usage, and basic constraints extensions are used for the home device certificate and must be compliant with [ITU-T X.509].

All other certificate extensions, if any, must be marked as non-critical.

7.2.1 Authority key identifier

The authority key identifier extension defined in clause 8.2.2.1 of [ITU-T X.509] provides a means of identifying the public key corresponding to the private key used to sign a certificate.

```
AuthorityKeyIdentifier ::= SEQUENCE {
        keyIdentifier             [0] KeyIdentifier OPTIONAL,
        authorityCertIssuer       [1] GeneralNames OPTIONAL,
        authorityCertSerialNumber [2] CertificateSerialNumber OPTIONAL}
        (WITH COMPONENTS {..., authorityCertIssuer PRESENT,
                authorityCertSerialNumber PRESENT} |
         WITH COMPONENTS {..., authorityCertIssuer ABSENT,
                authorityCertSerialNumber ABSENT})
```

The *keyIdentifier* form or *authorityCertIssuer* and *authoritySerialNumber* form must be used for identifying the issuer's public key.

The *keyIdentifier* form can be used to select CA certificates during path construction. The *authorityCertIssuer*, *authoritySerialNumber* pair can only be used to provide preference to one certificate over others during path construction.

The *AuthorityKeyIdentifier* extension must include the *subjectKeyIdentifier* from the issuer's certificate with the exception of root certificate. The *keyIdentifier* is composed of the 256-bit hash of the value of the BIT STRING *subjectPublicKey* field of the issuer's certificate.

This extension must be present in home device certificates and must always be non-critical. It may also be present in CA certificates.

7.2.2 Subject key identifier

The subject key identifier extension provides a means of identifying a certificate containing a particular public key. To facilitate certification path construction, this extension must appear in all conforming CA certificates.

```
SubjectKeyIdentifier ::= KeyIdentifier
```

For CA certificates, the subject key identifiers should be derived from the public key. The *keyIdentifier* is composed of the 256-bit hash of the value of the BIT STRING *subjectPublicKey*.

This extension must be present in CA certificates and must always be non-critical.

7.2.3 Key usage

The key usage extension defined in clause 8.2.2.3 of [ITU-T X.509] specifies the purpose (e.g., encipherment, signature, certificate signing) of the subject public key contained in the certificate.

```
KeyUsage ::= BIT STRING {
          digitalSignature (0), contentCommitment (1),
          keyEncipherment  (2), dataEncipherment  (3),
          keyAgreement     (4), keyCertSign       (5),
          cRLSign          (6), encipherOnly      (7),
          decipherOnly     (8) }
```

The key usage extension must be present not only in CA certificates but also in home device certificates. For CA certificates, the *keyCertSign* and *cRLSign* bits must be asserted. For home device certificates, the *digitalSignature* bit must be asserted. Since an RSA key can be used in both signature verification and key management, the *digitalSignature* bit and *keyEncipherment* bit can be asserted.

This extension must be present in both CA certificates and home device certificates, and must always be critical in this Recommendation.

7.2.4 Basic constraint

The basic constraint extension defined in clause 8.4.2.1 of [ITU-T X.509] identifies whether the subject of the certificate is a CA as well as the maximum depth of valid certification paths.

```
BasicConstraintsSyntax ::= SEQUENCE {
        cA                  BOOLEAN DEFAULT FALSE,
        pathLenConstraint   INTEGER (0..MAX) OPTIONAL }
```

This extension must be present in CA certificates but not in home device certificates, and must be present as a critical extension in CA certificate containing public keys used to validate the digital signature on certificates. The *cA* field must be set to TRUE in CA certificate.

This extension may appear in home device certificates as a non-critical extension.

7.3 Security considerations

The security considerations for secure home network services are as follows:

- The key length of the home device certificate must be 2048 bits or more in the case of RSA algorithm. However, RSA key length of 1024 bits only can be used for home devices without computational capability for controlling a 2048-bit key length certificate such as Type B or Type C home device.
- When using the other signature algorithm, the key length must be determined to be the same strength as the 2048-bit RSA key.
- The sufficient validity of the home device certificate should be more than 10 years.
- If the encryption key is used for secure communication between the secure home gateway and home devices, it could be renewed regularly.
- The secure home gateway should securely generate and manage a home device certificate and private key for home devices without computational capability.
- Since the possibility of a collision search attack on SHA-1 (160 bits) was raised for example in ([b-CRYPTO 2005]), this Recommendation recommends a 224-bit or more hash algorithm for the device certificate.

8 Certificate management for device certificate in the home network

The home gateway should be the certification authority for device certificate management in the home network.

The certificate management procedures for device certificates consist of the procedure for device certificate issuance, procedure for device certificate revocation, and procedure for device certificate validation.

8.1 Procedures for device certificate issuance

There are two kinds of procedure for device certificate issuance: one is the out-of-band issuance procedure and the other is the online issuance procedure. Many home devices such as Type B home devices and Type C home devices cannot have any computational power for certificate management and key generation except secure home gateway and Type A home devices, which have sufficient capability for certificate management and key generation. Therefore, such kinds of devices should need an administrator's involvement for certificate issuance.

When issuing a device certificate, all home devices should have some interfaces for certificate issuance, key pair generation, certificate and private key storage. Implementation method for the home device interface is not covered by the scope of this Recommendation. In case of online issuance procedure, certificate management protocol (CMP) should be used for device certificate management in the home network.

8.1.1 Procedures for device certificate issuance for the secure home gateway

When issuing a secure home gateway certificate, the out-of-band issuance procedure by the home network administrator and procedure for online certificate issuance will be used.

Before an issuance procedure, however, the administrator should have a registration code such as reference number, authorization code from CA or registration authority (RA) for the secure offline registration procedure. The registration code will be used in the procedure for device certificate issuance.

When an issuance procedure is performed by the administrator, he or she should send the registration code to an external CA for issuing a certificate. A secure home gateway requests a device certificate to the external CA, and then the device certificate for the secure home gateway

will be issued by external CA. The information used for the issuance procedure may be protected properly by a secure channel such as secure socket layer (SSL), transport layer security (TLS), etc.

8.1.2 Procedure for device certificate issuance per device

When issuing an end-entity device certificate, the secure home gateway should have a CA for issuing home device certificates. This mediation issuance method requires the registration procedure of a device when a device certificate is issued by a secure home gateway. The device certificate for Type A home devices such as remote controller, personal computer (PC), or personal data assistant (PDA) can be issued based on both online issuance procedure and offline issuance procedure. However, the device certificate for Type B, C home devices should be issued based on the offline issuance procedure. For a non-computational capability home device such as Type B or Type C home devices, the secure home gateway should generate a key pair and issue a device certificate instead of these home devices. Moreover, there is a need for an out-of-band transmission of the private key and device certificate from the home gateway to the home devices for device authentication among them. The out-of-band transmission method for the private key and device certificate is not covered by the scope of this Recommendation, however.

8.2 Procedure for device certificate revocation

In the home network environment, device certificate revocation rarely occurs because the device certificate has long validity and certificate management is also confined to its own home network only. In some cases, e.g., private key compromise, missing or stolen home device, etc., however, device certificate revocation is required for device certificate management in the home network environment. The online certificate revocation procedure and out-of-band certificate revocation procedure can be used for device certificate revocation. Devices with computational capability (i.e., Type A home device) can be used in the CMP for online certificate revocation. For the out-of-band certificate revocation procedure, an administrator should take charge of device certificate revocation instead of devices without computational capability (i.e., Type B or C home device).

8.3 Procedure for device certificate validation

[ITU-T J.192] sets the term of validity of a certificate to more than 20 years to match the lifecycle of a device. In other words, there may be no certificate validity check for a device authentication in the cable network. Unlike a cable network, however, the longevity of the device certificate will not be a long validity (i.e., more than 20 years). Therefore, an effective certificate status validity method is required for home device certificate validation, e.g., online certificate status protocol or offline validation methods. The certificate status verification server can verify a device certificate status using an online certificate status protocol. In addition, CRL can be used for a device certificate validation if the internal CA issues CRL periodically.

When a CRL is used for the device certificate validation, the CRL profile and management procedure will be required. The CRL profile and management procedure should also comply with [ITU-T X.509].

9 Use cases for the device certificate

There are four typical use cases of a device certificate: 1) between the remote terminal and secure home gateway, 2) between the application server and secure home gateway, 3) between home devices and secure home gateway, and; 4) among home devices. For the external internet service from the home device to the external application server, a home device should be authenticated first with the secure home gateway with its own device certificate; the secure home gateway should then be authenticated with the external application server using the home gateway certificate issued by the external CA. These use cases can be basically applied to various application protocols for supporting secure home network services.

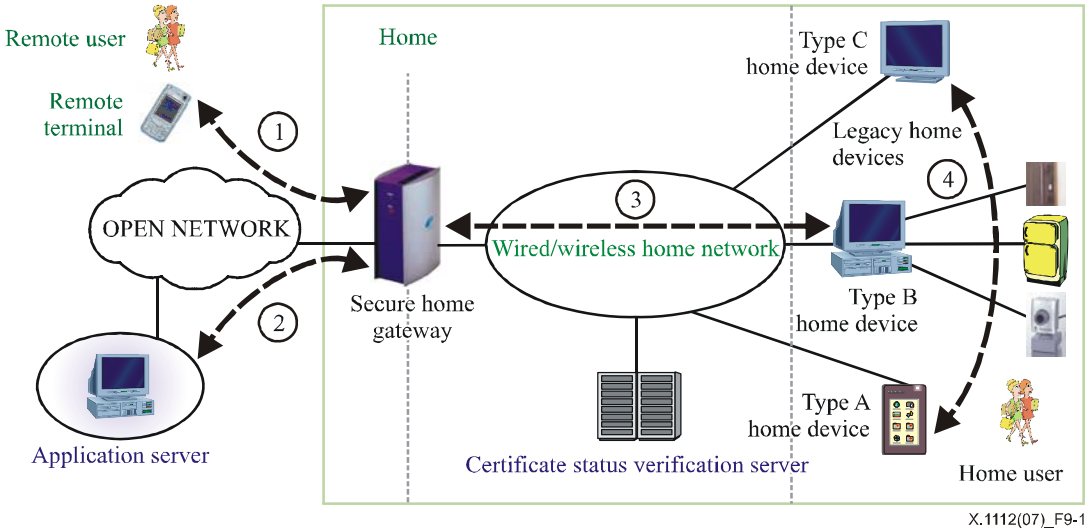

Figure 9-1 – Device authentication use case based on general home network model for security

10 Message format for certificate management

The message format for the issuance and revocation of a certificate is fundamentally based on [IETF RFC 2511], although it can be modified to fit the home network service.

Appendix I

Examples of the home device certificate profile

(This appendix does not form an integral part of this Recommendation)

These examples of home device profile comply with X.509 and J.192 profiles.

I.1 CA certificate profile (self-signed certificate)

In the CA certificate profile, the product name and its unique identification information of the secure home gateway are used for the subject name. This CA certificate can be issued when the secure home gateway is shipped.

	Contents
Subject name form	C=<Country> [O =<Manufacturer Name>] OU=<Product Name> CN=<Identification Information>
Signed by	Self-Sign
Validity period	More than 10 years
Key length	2048 bits (RSA)
Extensions	authorityKeyIdentifier [n, o] subjectKeyIdentifier [n, m] keyUsage [c, m] (keyCertSign, cRL Sign) basicConstraints [c, m]

- **`UTF8String` or `PrintableString`** can be used for the DN string in the home device certificate profile.
- For the identification information in CN, the unique information to be assigned to each device should be used, e.g., serial number, device MAC address, etc.

I.2 Home device certificate profile

In the home device certificate, the product name and its unique identification information of the home device are used for the subject name. When issuing a device certificate to a certain home device, CA (i.e., home security gateway) should retrieve that information from the device. In case of online issuance, the home device contains the information in the CMS message. The retrieval method for offline issuance is not covered by the scope of this Recommendation, however.

	Contents
Subject name form	C=<Country> [O =<Manufacturer Name>] OU=<Product Name> CN=<Identification Information>
Signed by	CA
Validity period	More than 10 years
Key length	Over 1024 bits (RSA)
Extensions	authorityKeyIdentifier [n, m] subjectKeyIdentifier [n, o] keyUsage [c, m] (digitalSignature) (RSA: digitialSignature and/or keyEncipherment) basicConstraints [n, o]

- The ASN.1 types **`UTF8String`** or **`PrintableString`** [ITU-T X.680] can be used for the DN string in the home device certificate profile.
- For the identification information in CN, the unique information to be assigned to each device should be used, e.g., serial number, device MAC address, etc.

Bibliography

[b-CRYPTO 2005] *Advances in Cryptology – CRYPTO 2005*, 25th Annual International Cryptology Conference, Santa Barbara, California, USA, 14-18 Aug. 2005.

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	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, 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

Printed in Switzerland
Geneva, 2008