Home Device Authentication Framework and Implementation

Yun-kyung Lee, Jong-wook Han, Deok Gyu Lee, Jeong-nyeo Kim
Information Security Division, Electronics and Telecommunications Research Institute

neohappy@etri.re.kr

Abstract

As home devices have various functions and have improved computing power and networking ability, home device authentication has become increasingly important for improving the security of home network users. Moreover, device authentication supplies user convenience for the home network service user because it can replace the user authentication required for the used home network service. In addition, the security of the home network can be strengthened if device authentication is considered in addition to the authentication and access control for the home network user. In this paper, we describe home device authentication framework and system, certificate profile for home devices, which is based on the Internet X.509 certificate, home device authentication mechanism, and our CA administration server. And also, we propose the tracing method of lost device using our home device authentication system.

1. Introduction

The development of information technology has changed our lives, even home life. The concept of a home network appeared while IT was being integrated with various home devices. Providing greater convenience, the home network connects all our home devices as a network, enabling them to communicate with each other. However, sometimes we may prefer that a particular device not be connected to our home network system. If that device is somehow connected against our wishes, the consequences may be disastrous. Hence, user authentication and authorization and home device authentication and authorization are necessary for home network services. In using a home network service, we can apply user authentication and authorization technology so that only authorized persons can use the service. However, the current authentication and authorization technology has various problems, such as the leakage of user authentication information by a user's mistake, the usage of guessable authentication information, and the discovery of new aspects of vulnerability in existing authentication methods. Thus, the user of a home network service must be guaranteed from security through a credible device. This type of security involves home device authentication as well as user authentication and authorization. Furthermore, the nature of the home network, with its combination of wired and wireless network devices, means that the possibility of unauthorized access is very high for particular devices. Hence, there is a great need for device authentication.

The home device means all devices which participate in the home networking. It can be a supplier of some home services or be user of that. To provide greater convenience, the home network connects all our home devices through a network, enabling them to communicate with each other. We think that a secure relationship among home devices is crucial because the home network service is becoming more convenient. The role of the user in a home network service is minimized and the services provided by the network of devices are maximized [6]. Device authentication ensures that only specific devices are authorized by specific authorized persons, and the security between two parties is ensured as long as the unauthorized device is not used. Furthermore, device authentication is a mandatory technology that enables the automatic provision of emerging context-aware services through device cooperation without user intervention; and DRM systems also need device authentication [3,4].

Several mechanisms have been proposed for device authentication not home device authentication. Some industries suggest a hardware fingerprint-based approach [7,8] in which the trustworthiness of the device is established through verification of secret information extracted from a unique hardware fingerprint. Bluetooth [9] and Zigbee [10] provide a device authentication mechanism based on a shared symmetric key, and CableLab [1] provides a public key infrastructure (PKI)-based mechanism. Especially, CableLab [1] provides device authentication method, but it only authenticates home gateway by using X.509 version 3 certificate. A personal certificate authority (CA) provides a localized PKI model [2, 11]. However, to the best of our knowledge, these mechanisms are unsuitable for our home device authentication framework[12].

We now describe a framework of home device authentication and its implementation. In section 2, we discuss our home device authentication framework and in section 3, we propose home device certificate profile. In section 4, we propose secure communication protocol. In section 5, we describe home device authentication mechanism. In section 6, we give an example of tracing method for lost home device. Finally, in section 7, we present our conclusions.

2. Home device authentication system

2.1. Home device authentication framework

We propose a PKI-based home device authentication mechanism. The mechanism covers intra-home device authentication and inter-home device authentication. We considered a public CA instead of a personal CA [2, 11]. The use of a personal CA may have been suitable if we had only considered device authentication in an intra-personal area network (PAN) or intra-home network. However, because we considered inter-home network, the public CA was more suitable. Figure 1 shows our home device authentication framework.

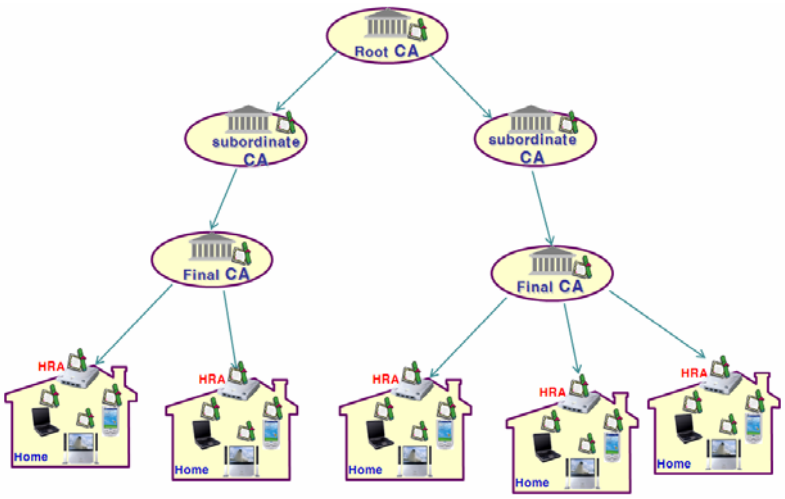

Fig.1. Home device authentication framework

In figure 1, our home device authentication framework has a hierarchical PKI structure. That is, a root CA manages the framework's subordinate CAs, and the CAs manage other subordinate CA, home devices and home registration authority (HRA). Final CA is a subordinate CA, but it has not its subordinate CA. It only controls home devices (including HRA). The HRA is a home device with sufficient computing power for public key operation and for communication with other home devices and user interface equipment (such as a monitor or keypad.). The HRA, which also functions as a regular registration authority (RA) has more authority and requirements.

Figure 1 shows various home devices connected to a home network. These devices, which can communicate with each other and have basic computing ability, including the following: an Internet-microwave, an Internet-refrigerator, a digital TV such as IPTV, an Internet-washing machine, a PDA, a notebook computer, a wall-pad, a PC, and a cellular phone. Many home devices are used in everyday life and more will soon be developed.

2.2. Home device authentication system architecture

In our home device authentication system, CA issues home device certificates, belongs to many number of homes and has some responsibilities; the first responsibility is to protect its private key from disclosure, the second responsibility is to verify the information in a certificate before it is issued, the third responsibility is to ensure that all certificates and CRLs it issues conform to its profile, the fourth responsibility is to accurately maintain the list of certificates that should no longer be trusted, the fifth responsibility is to distribute its certificates and CRLs, and the sixths responsibility is the maintenance of sufficient archival information to establish the validity of certificates after they have expired[13, 14]. So, the CA must be a trusted party in our home network system. It needs to be controlled by a nonprofit organization. Also, we put a HRA(Home Registration Authority) and it works as RA(Registration Authority) and helps the issuing of home device certificates. HRA can be home gateway, and other devices which have some computing ability and some interfaces to communicate with other home devices. If the new home device is registered, HRA verifies the registration information of the device and requests the issuing of the home device's certificate to CA. If CA issues the certificate of the device and sends it to the HRA, HRA

sends the certificate to the device. When HRA sends certificate to the device, HRA can use various methods; out-of-band transmission method and wired-transmission methods, etc.

When a home device requests a service which supplied by other device, the authentication between two devices is needed. It is performed through certificate verification of them. After the success of the mutual authentication process, between the home device providing a service and the home device requesting a service. At this time, devices which there is a difficulty in the public key operation, ask for the verification of a certificate to the delegation server. The delegation server informs a result after the certificate verification to the device. If the delegation server can be entrusted with a complex calculation, the verification time and energy in the home device can be reduced. But, the security and trust has to be guaranteed by CA or the HRA. That is, the HRA has to guarantee that of the delegation server if the delegation server exists in the home. And CA has to guarantee that of the delegation server if the delegation server is shared in several homes. Figure 2 shows our home device authentication system based on public key infrastructure. And it consists of CA, CA administration server, delegation server, HRA, many home devices.

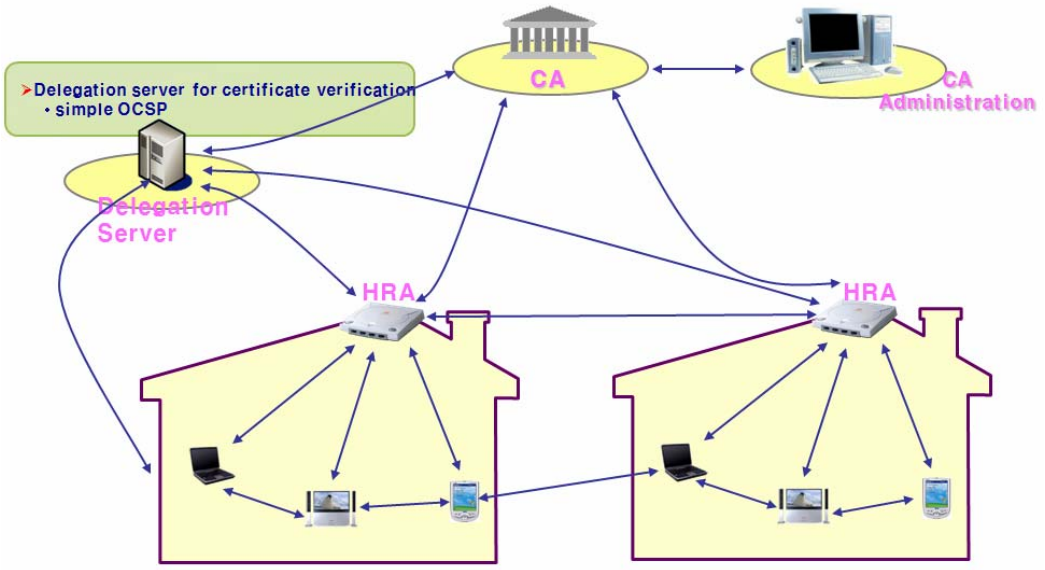

Figure 2. The structure of our home device authentication system

3. Home Device Certificate Profile

Our home device certificate follows the form of an Internet X.509 version 3 certificate [13,14]. More specifically, it is the same as the X.509 version 3 certificate with a few added, extensions for home device authentication. Our home device certificate authenticates home devices but the Internet X.509 certificate authenticates humans, enterprises, servers, routers, and so on. The popular X.509 certificate – provides a good basis for our home device certificate; moreover, it facilitates the implementation of our home device authentication framework and expedites the spread of the mechanism. Table 1 and 2 show our home device certificate profile.

Table 1. Basic device certificate profile

version
serialNumber
signature
issuer
validity
* subject
subjectPublicKeyInfo
* extensions
signatureAlgorithm
signature

In Table 1, the subject and extensions fields signed with '*' are different from those of the X.509 version 3 certificate. Table 2 shows a brief home device certificate. The home device certificate uses only five extensions of the X.509 certificate [13,14] and three additional extensions. In table 2, 'n' means a non-critical extension, 'c' means a critical extension, 'm' means a mandatory extension, and 'o' means an optional extension. We defined the additional three extensions (namely the HRAInfo, HRAOwner and devDesc extensions) as non-critical optional extensions for compatibility with existing PKI solutions.

Table 2. Brief home device certificate

Subject name form	C=<Country> O=<Home Device Manufacturer> OU=<Product Name> CN=<Home Device Recognition Information>
Validity Period	10 years
Extensions	authorityKeyIdentifier [n,m] subjectKeyIdentifier [n,o] keyUsage [c,m] (sign:digitalSignature, nonRepudiation) (key management: keyEncipherment) basicConstraints [n,o] cRLDistributionPoints [n,o] HRAInfo [n,o] HRAOwner [n,o] devDesc [n,o]

We now describe the home device certificate fields that differ from the X.509 version 3 certificate fields.

3.1. Signature

The signature field contains an algorithm identifier, and it identifies the digital signature algorithm used by the certificate issuer to sign the certificate. It is a copy of the signature algorithm contained in the signature algorithm field. In the X.509 version 3 certificate, the RSA algorithm is recommended. However, in the home device certificate, both the elliptic curve digital signature algorithm and RSA algorithm are recommended.

3.2. Subject

Fundamentally, the subject field of our certificate follows that of the X.509 version 3 certificate. The subject field of the CA certificate is the same as that of the X.509 version 3

certificate. However, the subject field of the end-device certificate is slightly different. The organization referred to in the X.500 naming attributes must be the device manufacturer, and the common name attribute must be a device recognition number such as a device serial number, or a device MAC address. The following expression is an example of the X.500 naming attributes of the home device certificate:

C={country}, O={device manufacturer}, OU={product name}, CN={device recognition number}

In this example, the product name means a kind of device which is the owner of the device certificate. For example, a refrigerator, a PDA, a Laptop computer or a Television can be a product name.

3.3. HRA Information Extension

The HRA information extension describes the location of the HRA related to the device. The location of the HRA is filled with an IP address of the HRA and the postal address of the home. If a home device is lost and the CA is notified of the loss, this extension can help in the retrieval of the lost device.

In this extension, IPAddr attribute will become more meaningful value when IPv6 address structure is used and all things can have an IP address.

The ASN.1 syntax for the HRA information extension is as follows:

```
HRAInfo ::= SEQUENCE {
        IPAddr          iPAddress OPTIONAL,
        PostAddr        UTF8String OPTIONAL}
        iPAddress       ::= OCTET STRING
```

3.4. HRA Ownership Extension

The HRA ownership extension is the extension field for describing the owner information of the HRA. This extension field becomes the method of knowing the owner of the HRA. In addition, when this field receives a service by using the home device certificate, it assumes legal and moral responsibility.

This extension has a ‘hRA’ attribute which shows whether it is an HRA device and ‘RealName’ attribute which shows the real name of the HRA owner. The ASN.1 syntax for this extension is as follows:

```
HRAOwner ::= SEQUENCE {
hRA             BOOLEAN   DEFAULT TRUE,
RealName        UTF8String  OPTIONAL}
```

3.5. Device Description Extension

The device description extension identifies the basic function of the home device. This extension offers four device characteristics: ‘device control’, ‘home appliance’, ‘simple UI media’ and ‘PCs’. The four device description choices are described as follows:

The **device control** characteristic indicates whether a device may be used to control home devices by remotely, that is by a remote controller.

The **home appliance** characteristic indicates whether a device may be a home appliance, such as a refrigerator, a washing machine, a microwave, or an audio equipment.

The **simple UI media** characteristic indicates whether a device may have simple user interface equipment, such as a wall pad, a portable media player or a DMB player, and so on. These devices lack the powerful computing ability of PCs but they have a basic computing capability and a simple user interface.

The **PC** characteristic indicates whether a device may be a PC, a notebook computer, or PDA.

This extension, which has the basic functions of computing power and communication ability with a device can be used in the home device access control.

4. SCP (Secure Communication Protocol)

4.1. Definition of SCP

Before the home device authentication based on public key infrastructure is done, the certificate issuing process about the home device is needed. And before CA issues home device certificates, the CA administration server must set up policies including the issuing of certificate and the issued certificate management, the CA management, registered home device management, lost device management, operators of CA administration system management, etc. So we implement a CA administration server which helps us convenient policy setting up.

In the GUI(Graphic User Interface) displayer of the CA administration server, if all kinds of the policies relating to the function of CA is established, that data are transmitted to CA, and CA stores received policy data in database of the CA. CA administration server is only the interface for CA's policy establishment and displays the policies. Data are actually stored in the database of CA. At this time, the policy data has to be securely transmitted to CA according to our supposed method (that is SCP). Figure 3 briefly shows the SCP proposed in this paper.

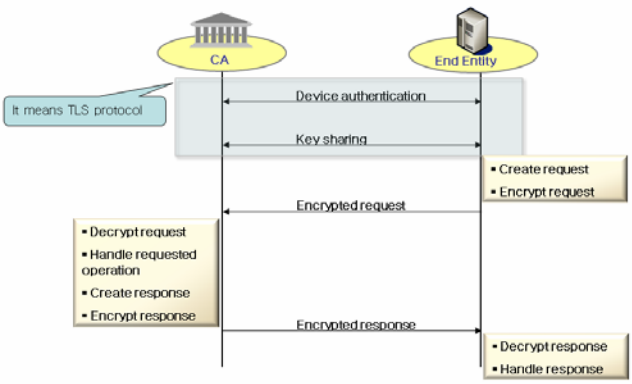

Figure 3. Brief SCP

As shown in figure 3, in SCP, CA and end entity mutually authenticate and share encryption key. And then encrypted data with the shared key are transmitted. SCP operates as follows;

(1) End entity sends its certificate and request message about CA's certificate to CA

(2) CA verifies the end entity's certificate.

- If it is valid, CA sends its certificate to the end entity.

- If it is invalid, CA disconnects with the end entity.

(3) End entity verifies the CA's certificate.

- If it is valid, end entity transmits the negotiation startup request message for the encryption algorithm and key to CA.

- If it is invalid, end entity disconnects with the CA.

(4) CA generates the session key.

- CA encrypts the generated key and encryption algorithm with public key of the end entity.

- CA sends the encrypted data to the end entity.

(5) End entity decrypts the received data with its private key(it is the pair of its public key and it was generated during the issuing process of its certificate), so it knows the session key and encryption algorithm which will use in communication between CA and it. This session key and algorithm will be used if their communication doesn't disconnect over the predetermined time.

- The end entity produces a request message, encrypts the message with the session key and algorithm, and then sends the encrypted request message to CA

(6) CA decrypts the received message, processes the request, generates the response message about the request, encrypts the generated response, and then sends the encrypted message to end entity.

(7) End entity decrypts the received message, and then processes the decrypted response message.

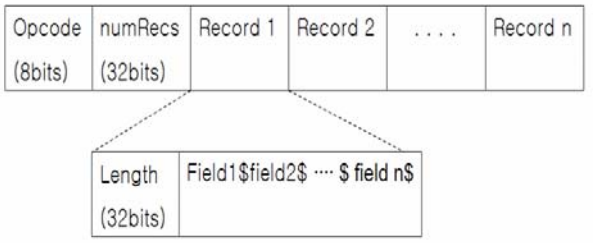

Figure 4. Packet format of SCP

On the other hand, the packet format of SCP is as shown in figure 4. There is the 'opcode' of 8-bit length which is the value showing the kind of the communications message between CA and end entity and is promised in advance. After that, 'numRecs' of 32-bit length successively come out. 'numRecs' is the number of 'record' fields. At this time, the meaning

of a 'record' is a row of database. For example, when the nine policies of certificate are stored in the database of CA, if a end entity sends a request, which asks the kind of certificate policies, to CA, then CA responds with nine successive records to the request of end entity. Moreover, each 'record' consists of 'length' and 'field'. A 'field' value is the data of each record and each 'field' data are classified into a symbol '$'. And 'field' is a column of database. If the example of the upper part is used, each compositional element of a policy becomes the 'field' value.

4.2. The use of SCP

As described in 4.1, SCP is a secure protocol which is used in communication between CA and CA administration in order to establish all kinds of the policies relating to certificate and the function set-up of CA. Also, in the certificate issuing process including the certificate issuing request, SCP is used in a communication between CA and HRA. In the each communication (the communication between CA and CA administration server, and the communication between CA and HRA), the same SCP packet format and protocol is used but different 'opcode' is used. About two hundreds of 'opcode's are defined and are implemented. These 'opcode's are mainly used for the communication between CA and CA administration server. And some 'opcode's are used for the communication between CA and HRA.

Figure 5 briefly shows our authentication system in the point of communication. In the figure 5, long-dotted line means SCP is used in a communication and short-dotted line means physically secure communication such as out-of-band communication or wired communication.

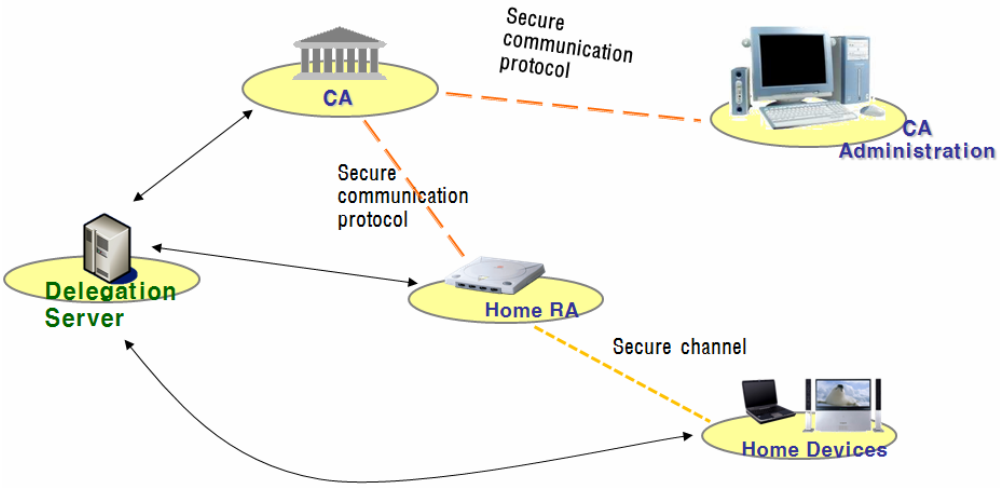

Figure 5. Our authentication system in the point of communication

5. Home Device Authentication Mechanisms

To authenticate home device, first of all, home device registration process to CA is needed. And then, CA or HRA confirms the information about registered home device and CA issues certificate to the device. In this section, we describe registration process of home device, certificate issuing process, and home device authentication process through the issued certificate.

5.1. Home device registration process

Home device is registered to CA through HRA. HRA has a little more public trust than other home devices, but it must have basic security function. HRA has the convenient user interface and communication means in order to communicate with other home devices. Moreover, because information relating to the other home device is saved, HRA must securely keep that data from attacker. And it is responsible for home device registration. Home gateway is mainly used as HRA device. However, the other device can become.

The registration process of home device to CA is shown in figure 6.

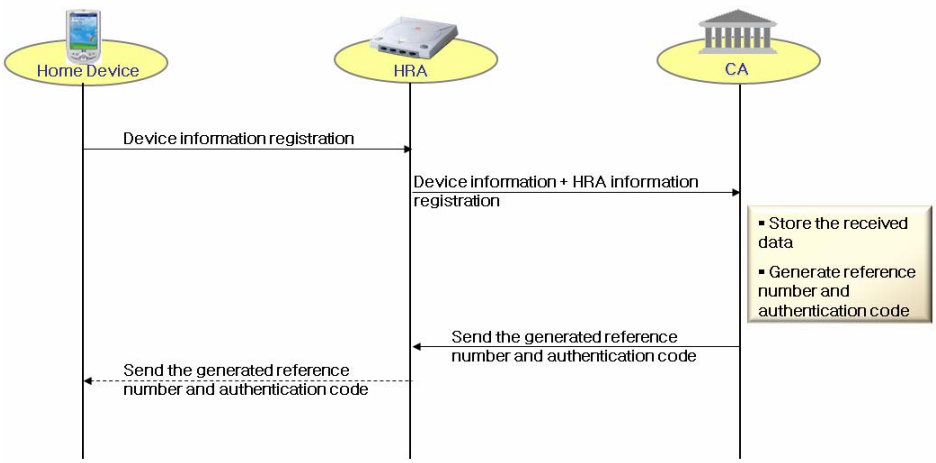

Figure 6. Home device registration process

As shown in figure 6, in the home device registration process, if home device transmits the home device information to the HRA, the HRA sends combined information of this home device information and HRA information to CA. CA stores the information which CA receives from the HRA in a database, generates reference number and authentication code, and sends them to HRA. In the meantime, the HRA can transmit them to the home device or securely store in the HRA.

Moreover, home device and HRA can be physically secure communication by out-of-band communication or wired communication and a communication between HRA and CA can be cryptographically secure communication by SCP. Reference number and authentication code which is generated by CA and transmitted to HRA are used in home device certificate issuing process. If home device requests its certificate issuing to CA, HRA sends these values to the home device. If it doesn't, HRA safely stores these values its database.

5.2. Certificate issuing process

Figure 7 shows the process where the HRA makes the certificate issuing request instead of the home device. First of all, The HRA generates a key pair (public key and private key) of the home device. The HRA transmits the generated public key of the home device, reference number and authentication code in its own database to CA. CA confirms these values. And the CA takes out the home device information based on these values from its database and issues the home device certificate. At this time, the certificate policy which set in advance through the CA administration is used. The issued certificate is transmitted to the HRA, and

HRA sends the certificate to the home device. As the same with the home device registration process, a communication between home device and HRA can be physically secure communication by out-of-band communication or wired communication and a communication between HRA and CA can be cryptographically secure communication by SCP.

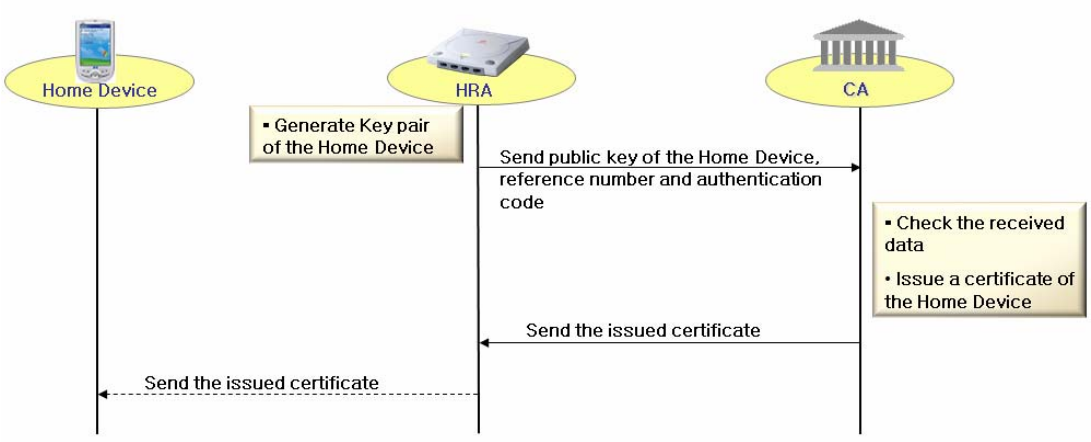

Figure 7. The issuing process of home device certificate

5.3. Home device authentication process

The authentication about a home device is necessary when the home device tries to use the home network service. All home devices could provide and receive the home network service. But some home devices don't have computing ability for public key operation. So we proposed delegation server. Delegation server performs the function of verifying the certificate instead of home devices. As the performance of this server, the time to be required to the home device authentication can decrease. This server can exist in each home or can share several homes. Or each CA can manage several delegation servers for the home devices which are registered the CA. Moreover, home devices which have the enough computing ability for public key operation can entrust certificate verification to delegation server or directly performs it.

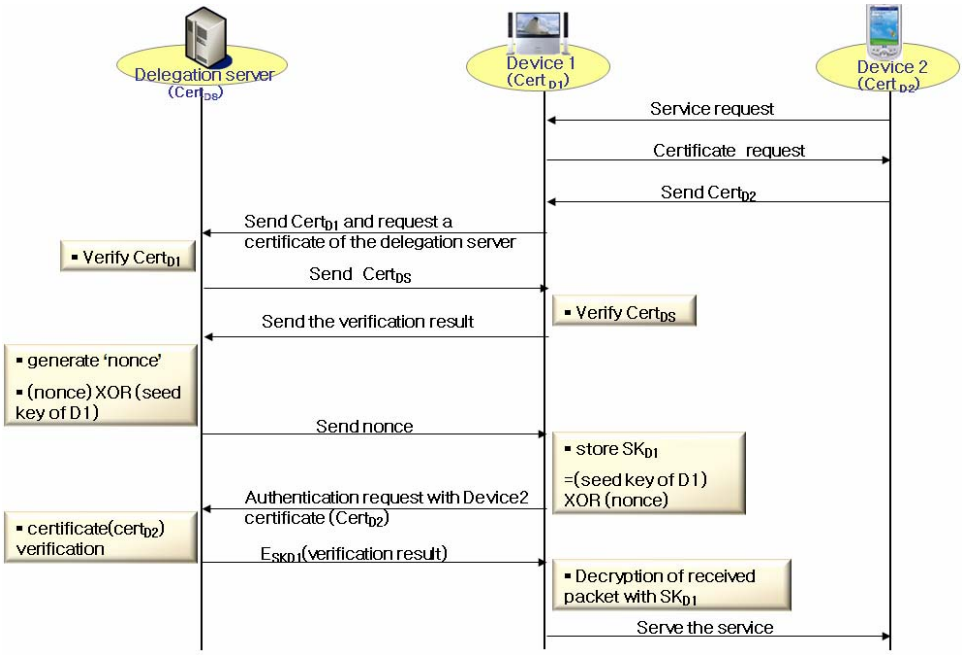

Figure 8. Home device authentication process using delegation server

Figure 8 shows home device authentication process using delegation server. It is the authentication procedure in which home device 2 tries to use the service which is supplied by the home device 1. The device authentication procedure using delegation server is as follows;

(1) Home device 2 requests the use of the service which is provided by home device 1.

(2) The home device 1 requests the certificate of home device 2.

(3) The home device 2 sends its certificate $Cert_{D2}$ to the home device 1.

(4) The home device 1 sends its certificate $Cert_{D1}$ to the Delegation server. And request a certificate of the delegation server

(5) Delegation server verifies the certificate of the home device 1($Cert_{D1}$).

- If it is valid, the delegation server sends its certificate $Cert_{DS}$ to the home device 1.
- else, the delegation server sends the verification result(fail) to the home device 1 and terminates the session.

(6) If home device 1 receives a certificate of the delegation server, then verifies the certificate.

- If it is valid, home device 1 sends the verification result (success) to the delegation server.
- else, home device 1 sends the verification result (fail) to the delegation server, and terminates the session.

And then, home device 1 notifies home device 2 “disapproving the request of service”.

(7) Delegation server generates nonce value and stores the nonce value XOR seed key of the home device 1.

- we assume the delegation server know all seed keys of home devices which are under the responsibility of the delegation server.

(6) The delegation server sends the generated nonce value to the home device 1.

(7) The home device 1 computes XORing between the received nonce value from the delegation server and its own seed key. And then it securely store that XOR-ed value(SK_{D1}). Also, SK_{D1} is new seed key of the home device1.

(8) The home device 1 requests the verification of $Cert_{D2}$ to the delegation server.

(9) The delegation server verifies $Cert_{D2}$, encrypts the verification result of $Cert_{D2}$, and sends it to the home device 1.

(10) The home device 1 decrypts the received message from the delegation server, checks the verification results.

- If $Cert_{D2}$ is valid, the home device 1 supplies its service to the home device 2.
- If $Cert_{D2}$ is invalid, the home device 1 notifies home device 2 “disapproving the request of service”. And then it terminate the session between home device 1 and home device 2.

6. Tracing method of lost device

Figure 9 shows the tracing method of lost devices. As shown in figure 9, the tracing of a lost device is possible by using the home device certificate as follows:

(1) If device A is lost, notify the CA of the loss. The CA then records the loss.

(2) Anyone who finds device A may bring it home and try to use it or register it with HRA2 as a home device.

(3) A home device verifies the certificate of device A through the CA or HRA2 requests the issuance of the certificate of device A.

(4) The CA knows device A is used at home2 through the HRAInfo field in the certificate of the device and then verifies the certificate of device A or the certificate of HRA2.

(5) The CA informs HRA1 that device A is used at home2

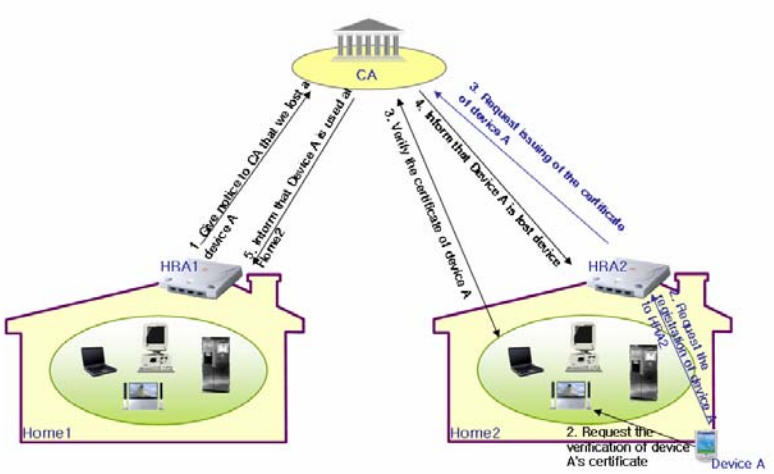

Figure 9. Tracing method of a lost device using device certificate

7. Conclusion

Home device authentication is essential for a home network security and user convenience. We propose a PKI-based home device authentication method and describe the process of home device registration and the issuance of the home device certificate. Our home device certificate profile is based on the Internet X.509 version 3 certificate. And we propose the communication protocol which is used in our device authentication system. This protocol is used for the communication between CA and CA administration server or HRA. It includes mutual certificate verification, key sharing, and message encryption using shared key. Moreover, we describe about the process of registering the home device to CA through Home RA and the process of home device certificate issuing through the Home RA.

Our home device certificate differs from an Internet X.509 version 3 certificate in some fields of the certificate. The differing fields are the subject, the HRA information extension, the HRA ownership extension, and the device description extension. The subject field of the home device certificate includes information pertaining to the kind of device, the device manufacturer, and the device identity. The HRA information extension includes the postal address of the home, which is subordinated by the HRA, and IP address of the HRA. Our method enables us to locate lost home devices, and to relate the HRA with the home device. The HRA ownership extension includes representative information for the use of a simple home network service based solely on device authentication. Finally, the device description extension includes information on the computing power of the device and access to home services. This extension is useful in device access control.

Moreover, the proposed home device certificate can be used for home device authentication. We have also shown that it can be used to trace lost devices. The home device certificate has potential for wide application besides the examples presented in this paper. In short, the home device authentication with the home device certificate enhances user convenience and creates a more secure environment for the home network. Moreover, our proposed authentication scheme is not limited to the home. This scheme is also applicable to an office or the country. And, in the home device authentication system proposed in this

paper, if home device authorization concept is added, the more secure and convenient home network system can be implemented.

8. References

[1] OpenCable Security Specification. http://www.opencable.com/specifications/, 2004.

[2] C. Gehrmann, K. Nyberg, C. Mitchell, "The Personal CA-PKI for a personal area network", IST Mobile and Wireless Telecommunications Summit 2002, pp. 31-5.

[3] J. Lee, S. Hwang, K. Yoon, C. Park, J. Ryou, "A DRM Framework for Distributing Digital Contents through the Internet," ETRI Journal, vol.25, no.6, Dec.2003, pp.423-436.

[4] Yeonjeong J., Kisong Y., and Jaesheol R., "A Trusted Key Management Scheme for Digital Right Management," ETRI Journal, vol.27, no.1, Feb.2005, pp.114-117.

[5] G.Wang and G. Cho, "Compromise-Resistant Pairwise Key Establishments for Mobile Ad hoc Networks," ETRI Journal, vol.28, no.3, June 2006, pp.375-378.

[6] Y. Lee, D. Lee, J. Han, T. Kim, "Home Network Device Authentication:Device Authentication Framework and Device Certificate Profile," The computer Journal, Oxford University Press, 2008.

[7] Device Authentication. http://www.safenet-inc.com

[8] Trust Connector2. http://phoenix.com

[9] Bluetooth Core Specification v1.0, December 2004, http://www.bluetooth.org/spec/, 2004

[10] ZigBee Specification v1.0, December 2004, http://www.zigbee.org/en/spec_download/

[11] Intermediate specification of PKI for heterogeneous roaming and distributed terminals," IST-2000-25350-SHAMAN, March, 2003.

[12] J. Hwang, H. Lee, J. Han, "Efficient and User Friendly Inter-domain Device Authentication/ Access control in Home Networks," In Proc. 2nd International Conference on Embedded and Ubiquitous Computing, LNCS 4096, Aug., 2006.

[13] Planning for PKI: Best Practices Guide for Developing Public Key Infrastructure," John Wiley & Sons, Inc. 2001.

[14] R. Housley, W. Polk, W.Ford, D. Solo, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List(CRL_ Profile, "RFC 3280, April, 2002. Baldonado, M., Chng, C.-C.K., Gravano, L., Paepcke, A.: The Standard Digital Library Metadata Architecture. Int. J. Digit. Libr. 1(1997) 108-121.

Authors

Yun-kyung Lee received her M.S. degree in Electrical Engineering from POSTECH(Pohang University of Science and Technology), Korea in 2001. Since 2001, she has been with Information Security Technology Division in Electronics and Telecommunications Research Institute(ETRI). She researches user authentication and authorization method in home network, and user authentication method with anonymity.

Jong-wook, Han received the MS and Ph.D degrees in the Dept. of electronic engineering from Kwangwoon University, Seoul, Korea, 1n 1991 and 2001, respectively. Since 1991, he has been with Information Security Technology Division in Electronics and Telecommunications Research Institute(ETRI), His research interests include home network security and optical security.

Dr. Deok Gyu Lee received his Ph.D. degree in Graduate School of Computer Science from Soonchunhyang University, Korea. He is now a post-doc of R&D Institute, ETRI(Electronics and Telecommunication Research Institute), Korea. Dr. Lee has published many research papers in international journals and conferences. Dr. Lee has served as Chairs, program committee for many international conferences and workshops; Chair of ISA'08, DMUC'07, and PC member of IS'07, TRUST'07, ASWAN'07 and so on. Dr. Lee' s research interests include Key Management, signature schemes, Broadcast Encryption, Contents Security, Wireless Security, Ubiquitous Computing, Home Network, etc. He is a member of the KICS, KIISC, KMS, and IEICE.

Jeong-Nyeo Kim received her M.S. degree and Ph.D. in Computer Engineering from Chungnam National University, Rep. of Korea, in 2000 and 2004, respectively. She studied at computer science from the University of California, Irvine, USA in 2005. Since 1988, she has been a principal member of engineering staff at the Electronics and Telecommunications Research Institute (ETRI), where she is currently working as a team leader of the Knowledge-based Information Security Research Team. She researches network security and secure operating system, and distributed security middleware.