# The Home Device Authentication System Construction for Pervasive Home Network

Yun-kyung Lee, Deok Gyu Lee, Jong-wook Han, Jeong-nyeo Kim
*Electronics and Telecommunication Research Institute*
*138 Gajeongno, Yuseong-gu, Daejeon, KOREA**
*neohappy@etri.re.kr*

## Abstract

*The number of the home device participated in the home networking increases as the performance of the home device is improved. Accordingly, the necessity of home device authentication and authorization is enlarged for secure home network. Therefore, in this paper, we described about the home device authentication system and its construction. We implemented the CA administration, SCP(Secure Communication Protocol), home device registration procedure, home device certificate issuing procedure, home device authentication procedure, and lost device reporting process, etc. And these are simply described in this paper.*

## 1. Introduction

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. 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[1]. We think that a secure relationship among home network 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 [1].

Pervasive home network means the home network that home members (human and home devices) can connect to the home devices at anywhere, anytime through our home device authentication system. And the administration which manages certificate authority for home devices can deal with the CA at anywhere, anytime.

Device authentication ensures that only specific devices are authorized by specific authorized persons, and the security between two parties is protected 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 [2,3].



*Digital Object Identifier: 10.4108/ICST.MOBIQUITOUS2008.3858*
*http://dx.doi.org/10.4108/ICST.MOBIQUITOUS2008.3858*

So far, several mechanisms have been proposed for device authentication. Some industries suggest hardware fingerprint based approach[4,5] that extract the secret information from the unique hardware fingerprint and trust the device by verifying the secret. And CableLab[6] also provides PKI based device authentication.

In chapter 2, we describe the home device authentication system structure and the secure communication protocol which is used in the system. We describe about the process where the home device registration process, the home device certificate issuing process and home device authentication process in chapter 3. Finally, in chapter 4, the conclusion of this paper is described.

## 2. Home device authentication system based on PKI

### 2.1. The structure of home device authentication system

In this paper, the home device authentication system of the public key infrastructure is considered. There are many number of the home device participated in the home network, and the number of the mobile home device increases. Therefore home device authentication using symmetric key has a limit.

In our home device authentication system, CA issues home device certificates which 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[7,8]. 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 distributes 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 the target device requests the use of service, the authentication about the home device is made through the confirming certification after the certificate exchange between the server providing a service or the home device and target device. 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 target 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 fairness has to be guaranteed by CA or the HRA. That is, the HRA has to grantee it about the delegation server if the delegation server exists in the home. And CA has to guarantee it about the delegation server if the delegation server is shared in several homes. Figure 1 shows our home device authentication system based on public key infrastructure.

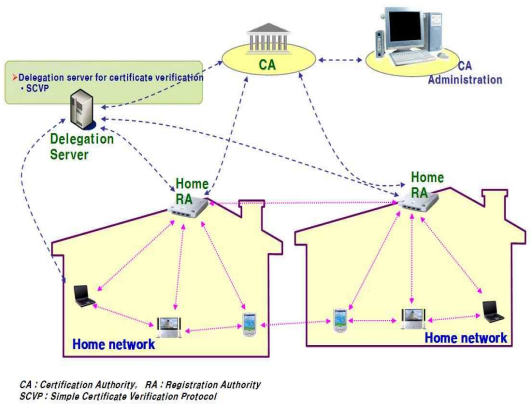


**Figure 1. The structure of our home device authentication system**

### 2.2. SCP (Secure Communication Protocol)

#### 2.2.1. 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

Digital Object Identifier: 10.4108/ICST.MOBIQUITOUS2008.3858
http://dx.doi.org/10.4108/ICST.MOBIQUITOUS2008.3858

CA issues home device certificates, the CA administration system 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, and etc. So we implement a CA administration which is certificate policy setting up system and helps us convenient policy setting up.

In the GUI(Graphic User Interface) displayer of the CA administration, if all kinds of the policies relating to the function of CA is established, policy data set up are transmitted to CA, and CA stores received policy data in database of the CA. CA administration does only the policy establishment interface and display function, and data are actually stored in the database of CA. At this time, the policy data has to be securely transmitted to CA according to the definite standard. Figure 2 briefly shows the SCP proposed in this paper.

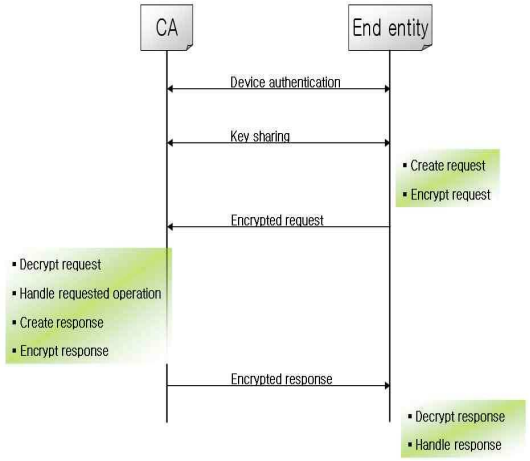


Figure 2. Brief SCP

As shown in figure 2, in SCP, CA and end entity mutually authenticate and share encryption key. And then encrypted data are transmitted with the shared key. 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 not, 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 not, 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, 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.

- end entity produces a request message, encrypts the generated 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.

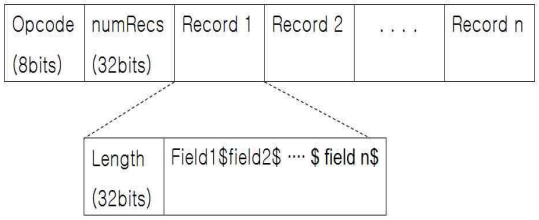


Figure 3. Packet format of SCP

On the other hand, the packet format of SCP is as shown in figure 3. 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 is 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 is constituted of the length and field data of each record and each field data are classified into a symbol '$'. 'Field' is a column of database. If the example of the upper part is used, each

*Digital Object Identifier: 10.4108/ICST.MOBIQUITOUS2008.3858*
*http://dx.doi.org/10.4108/ICST.MOBIQUITOUS2008.3858*

compositional element of a policy becomes the 'field' value.

#### 2.2.2. The use of SCP

As described in 2.2.1, SCP is 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 Home RA. In the each communication(the communication between CA and CA administration, and the communication between CA and Home RA), the same SCP packet format and protocol is used but different 'opcode' is used. Now, about two hundreds of 'opcode's are defined, implemented and used. These 'opcode's are mainly used for the communication between CA and CA administration. And some 'opcode's are used for the communication between CA and Home RA.

Figure 4 briefly shows our authentication system in the point of communication. In the figure 4, red cylindrical rod means SCP is used in a communication and orange-red color cylindrical rod means physically secure communication such as out-of-band communication or wired communication.

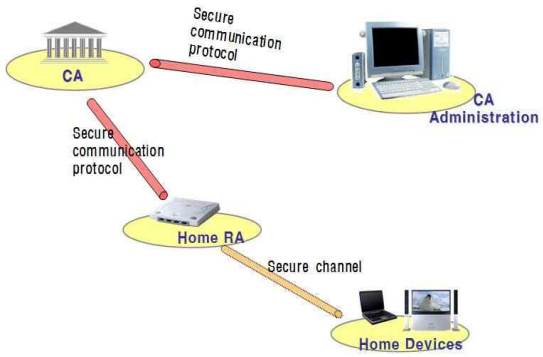


Figure 4. Our authentication system in the point of communication

## 3. Home device authentication

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

### 3.1. Home device registration process

Home device is registered to CA through Home RA. Home RA has a little more public trust than general home devices, but it must have basic security function. Home RA 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, Home RA must securely keep that data from attacker. And it is responsible for home device registration. Home gateway is mainly used as home RA device. However, the other device can become.

The registration process of home device to CA is shown in figure 5.

As shown in figure 5, in the home device registration process, if home device transmits the home device information to the Home RA, the Home RA sends combined information of this home device information and Home RA information to CA. CA stores the information which CA receives from the Home RA in a database, generates reference number and authentication code, and sends them to Home RA. In the meantime, the Home RA can transmit them to the home device or securely store in the Home RA.

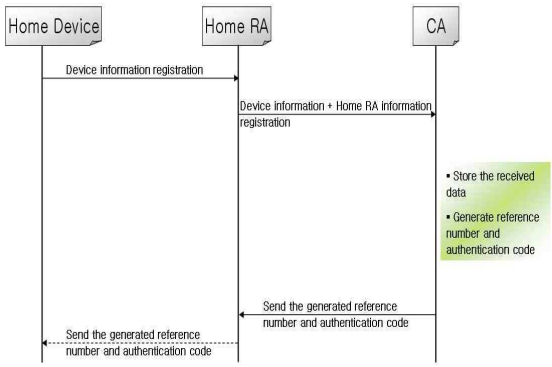


Figure 5. Home device registration process

Moreover, as described section 2.2, a communication between home device and Home RA can be physically safe communication by out-of-band communication or wired communication and a communication between Home RA and CA can be cryptographically secure communication by SCP. Reference number and authentication code which is

Digital Object Identifier: 10.4108/ICST.MOBIQUITOUS2008.3858
http://dx.doi.org/10.4108/ICST.MOBIQUITOUS2008.3858

generated by CA and transmitted to Home RA are used in home device certificate issuing process. If home device requests its certificate issue to CA, Home RA sends these values to the home device. If it doesn't, Home RA safely stores these values its database.

### 3.2. Certificate issue process

Figure 6 shows the process where the Home RA makes the certificate issue request instead of the home device. The Home RA transmits the 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 Home RA, and Home RA sends the certificate to the home device. As the same with the home device registration process, a communication between home device and Home RA can be physically safe communication by out-of-band communication or wired communication and a communication between Home RA and CA can be cryptographically secure communication by SCP.

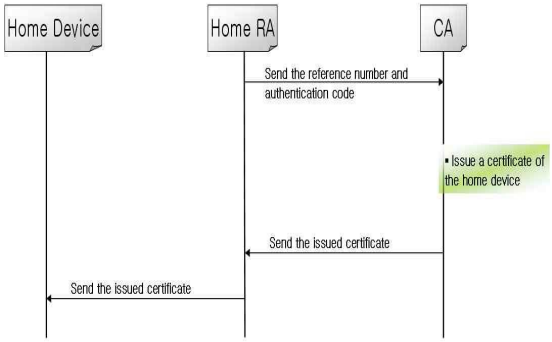


Figure 6. The issuing process of home device certificate

### 3.3. 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 propose 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 7 shows home device authentication process using delegation server. It is the authentication procedure in which home device 2 tries to use the service which the home device 1 provides. The procedure 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 sends the certificate request message of the home device 2

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

(4) The home device 1 requests certificate verification and sends its certificate $Cert_{D1}$ and received certificate $Cert_{D2}$ to the delegation server.

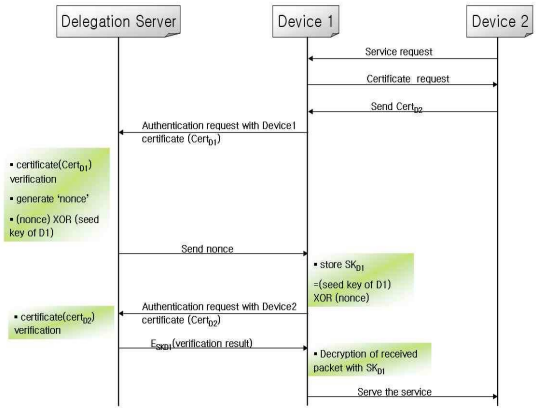


Figure 7. home device authentication process using delegation server

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

- If it is valid, the delegation server generates nonce value and stores the nonce value XOR seed key of the home device 1.
- If it is not valid, delegation server sends fail message to 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.

*Digital Object Identifier: 10.4108/ICST.MOBIQUITOUS2008.3858*
*http://dx.doi.org/10.4108/ICST.MOBIQUITOUS2008.3858*

(7) The home device 1 stores the received nonce value from the delegation server XOR its seed key. And this XOR-ed value is called $SK_{D1}$. Also, $SK_{D1}$ is new seed key of the home device1.

(8) The home device 1 request certificate validation 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 $Cert_{D2}$ isn't valid, the home device 1 disconnects the connection with the home device.

## 4. System Pictures

In this chapter, we will show our home device authentication system pictures. Our system constructs with home devices (laptop, CCTV), CA(Certificate authority) server, CA administration system, contents server, wall-pad(for user interface), delegation server etc. Figure 8 shows our system pictures.

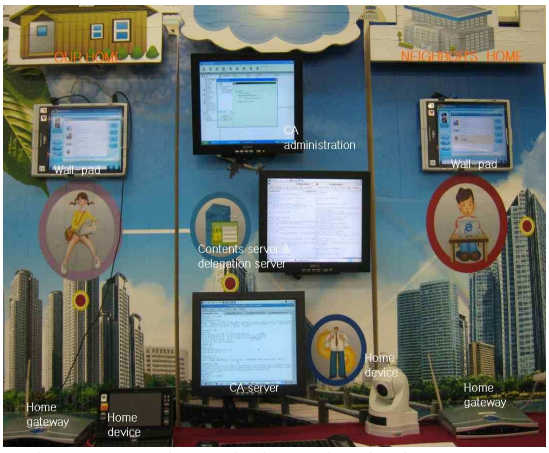


Figure 8. Our home device authentication system

In figure 8, CA administration program can be installed to laptop or PC. And figure 9 and figure 10 shows the computer screen of CA administration.

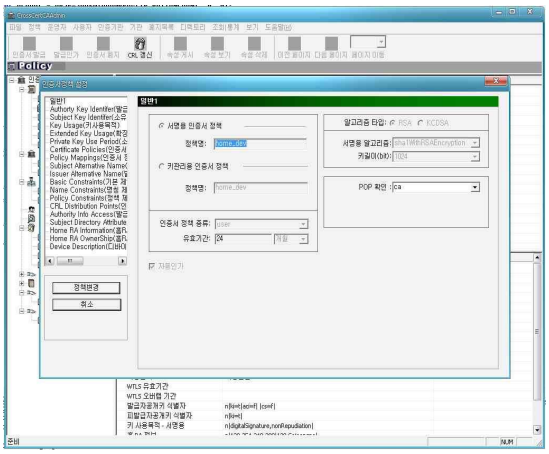


Figure 9. CA administration screen for certificate policy generation

Figure 9 shows the computer screen for certificate policy generation and figure 10 shows the computer screen for managing the registered home device list.

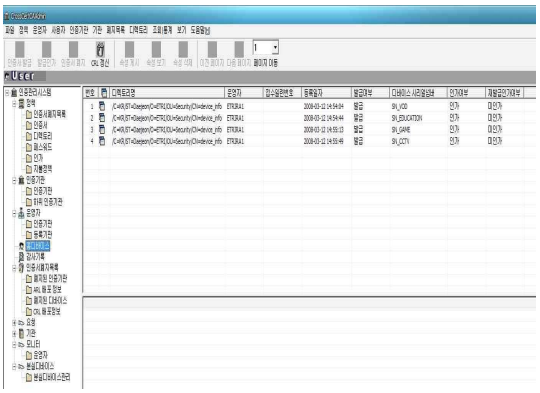


Figure 10. CA administration screen for management of registered home devices

## 5. Conclusion

In this paper, we described about the home device authentication for using secure home network. That is, the home device authentication system structure was proposed. And we proposed the communication protocol which is used in our device authentication system. This protocol is used for the communication between CA and the other home devices or CA administration. It includes mutual certificate verification, key sharing, and message encryption using shared key. Moreover, we described about the process

*Digital Object Identifier: 10.4108/ICST.MOBIQUITOUS2008.3858*
*http://dx.doi.org/10.4108/ICST.MOBIQUITOUS2008.3858*

of registering the home device to CA through Home RA and the process of home device certificate issuing through the Home RA. And, we proposed the home device authentication method between the home device for using the home service and the home device providing the home service. In this paper, moreover, we proposed the device authentication method using the delegation server to the certificate verification.

The authentication scheme proposed in this paper is not limited to the home. The authentication scheme proposed in this paper 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.

## 6. References


[1] Yun-kyung Lee, et al., "Home Network Device Authentication:Device Authentication Framework and Device Certificate Profile," LNCS 4537, July, 2007.

[2] Yeonjeong Jeong, Kisong Yoon, and Jaecheol Ryou, "A Trusted Key Management Scheme for Digital Right Management," ETRI Journal, vol.27, no.1, Feb.2005, pp.114-117.

[3] Junseok Lee, et al., "A DRM Framework for Distributing Digital Contents through the Internet," ETRI Journal, vol.25, no.6, Dec.2003, pp.423-436.

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

[5] TrustConnector2. http://phoenix.com

[6] OpenCable Security Specification. http://www.opencable.com/spedifications/, 2004.

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

[8] 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



*Digital Object Identifier: 10.4108/ICST.MOBIQUITOUS2008.3858*
*http://dx.doi.org/10.4108/ICST.MOBIQUITOUS2008.3858*