Proceedings of the 4th WSEAS Int. Conf. on Information Security, Communications and Computers, Tenerife, Spain, December 16-18, 2005 (pp169-172)

Research on Issuing a certificate and Generating a private key of a Home-gateway

BAEHYO PARK, JAEHO YOON, JONGHYUN BAEK, SEOKLAE LEE
Information Infrastructure Protection Division, Korea Certification Authority Central
Korea Information Security Agency(KISA)
78, Garak-Dong, Songpa-Gu, Seoul
SOUTH KOREA
http://www.kisa.or.kr

Abstract: In this paper, we proposed certificate issuing and management methods for a home-gateway's public key certificate, and specified generating and storing location of a private key for a home-gateway. Home gateway's certificates are issued online or offline with an aid of the PKI entities by human user's involvement. Home-gateway without full equipment of certificate issuing and management can be assisted by home gateway administrative server. As for the generating location of a private key, a home-gateway, an administrative server, and a smart card are the choices for generating a private key as well as storing and operating the private key for authentication service of HG.

Key-Words: Home-gateway, PKI, Certificate, Private key, Issuance, Administrative server, Authentication

1 Introduction

Home-networking services need an essential device, Home-gateway(HG), which is the end point of the Internet and local network and plays a role of a controller for indoor electronic appliances. And authentication of HG is needed to communicate securely between indoor and outdoor

Authentication service of HG can be classified into "indoor and outdoor users" versus "HG", "home-networking service provider" versus "HG", and "electronic household appliance" versus "HG". Authentication of HG is the fundamental procedure before users are authenticated for digital service. Various authentication techniques such as ID/PW, symmetric key / public key authentication, and Kerberos can be applied to authentication of HG. In this thesis, authentication technique using public key certificate will be provided for authentication of HG because this authentication technique offers easiness of key distribution. Currently, there is [FIPS196][1] which NIST standardized in 1997 as a public key certificate-based authentication protocol, but there are few technology on issuance and storage of a certificate and private key. There are a certificate profile for [IPsec VPN][2] in security working group "pki4IPsec" of IETF and OpenCable[3] with digital cable broadcasting subscriber authentication and a copy protection function by CableLabs[3]. However, these specifications are not suitable for HG because it should focus on security of the private key.

In the chapter 2, this thesis explains the relationship between HG and PKI. And in the chapter of 3, the methods are suggested for issuance of HG's certificate. In the chapter 4, location of storage and generation of a private key for authentication are proposed according to HG, administrative server, and smart card. Lastly, there will be a conclusion of this thesis.

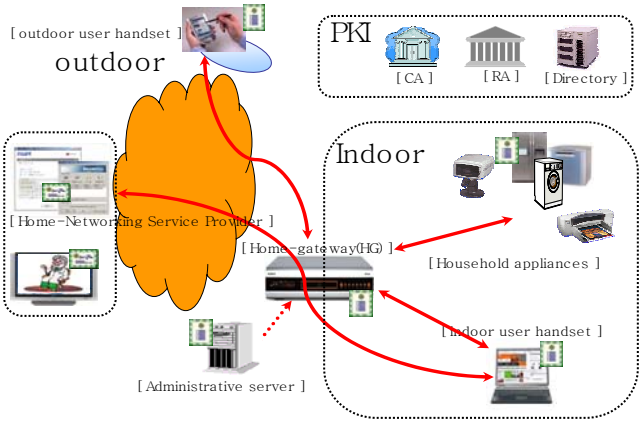

Fig 1. Participants for authenticating HG

2 Home-gateway(HG) and PKI

HG can use a public key certificate for authenticating itself because key distribution and management is getting easier as the number of HG is increasing. To achieve a public key certificate, HG needs to

communicate with PKI entities, which will be explained in this chapter. Authenticating HG, which is a kind of device, is different from authenticating human-beings in terms of non-repudiation property. Even though the authentication might be used in the same protocol, authenticating HG doesn't cover non-repudiation because it doesn't include digital signature by human-beings who has responsibility for their own signature. Thus the HG authentication makes HG be identified in the Internet and results in the secure communication channel without non-repudiation.

2.1 Participants for authenticating HG

Here are definitions for participants in authentication protocol for HG using Public key certificate in Fig.1

① Home-gateway(HG) : Device which operates as the aisle to connect the Internet and local network and controls the household appliances
② Household appliance : Devices for users' convenience at hoe such as TV, air conditioner, gas oven , etc
③ Indoor and outdoor user handset : A handset which users utilize for enjoy digital home service
④ Home-networking service provider : a server for providing various service for users such as VOD(Video on Demand), online health care, television banking, etc.
⑤ Administrative server : a server in charge of issuance of HG's certificates and management of the certificates' policy. usally operated by a digital home service operator or a local unit organization (apartment control offices)
In addition, there are PKI entities for issuance of HG's certificates. They consist of Registration Authority (RA), Certificate Authority (CA), and directories.
⑥Registration Authority (RA) : An optional entity given responsibility for performing some of the administrative tasks necessary in the registration of end entities
⑦Certificate Authority (CA) : An authority that is trusted by one or more users to create and sign PKCs (Public Key Certificate). It is important to note that the CA is responsible for the PKCs during their whole lifetime, not just for issuing them.

PKI entities should understand PKI management messages from a HG and a HG's administrative server to issue certificates and search for CRL and certificates in directory for validating a certificate.

2.2 Communication between HG and PKI entities

Direct communication between HG and PKI entities depends on calculation ability of HG, an administrative server and a manufacturer of HG. Currently, there are HGs having a degree to a general computer from ones without computational power. HG has calculation ability and memory in order to provide authentication service (key generation, request of certificate issuing and certificate validation, etc). With calculation ability, HG can use [CMP][4], acquire CRL, and proceed for verification. HG needs to deal with authentication service if HG management server does in place of HG. Also, computational power of HG becomes proportional to a degree of how much the administrative server helps HG.

3 Issuance of HG's certificate

Issuance and management of HG's certificates are necessary to authenticating HG. For this reason, currently HG applies the certificate profile and certificate management scheme in [IPsc VPN] for authentication service. A certificate request format for certificate issuance basically follows [PKCS#10][5] in case of off-line, and [CMP][4] in case of online. New value can be appended to a certificate request form according to a certificate issuance model.

3.1 Key generation

Opencable, helping the cable industry deploy interactive services over cable made specification for issuance of a settopbox's certificate. A settopbox is similar to a home-gateway in that they are the starting point of each home's network. This specification says that manufacturers issue certificates of settopboxes and put the certificates and private keys into settopboxes without any involvement of going-to-be human-users. It can give convenience to human-users. However, it has a security problem that the manufacturers can manage private keys of HG. Therefore, this thesis does not consider that manufacturers generate keys, but a home-gateway, an administrative server, or a smart card does. The chapter 4 will cover these key generators in detail.

3.2 Issuance of HG's certificate

A HG's certificate can be issued online or offline. The followings are about issuance methods of HG's certificates. A profile in a HG's certificate is basically supposed to follow [X.509][6], [RFC3280][7].

3.2.1 Online issuance

There are three methods for issuing certificates of HG online. The first method is that HG directly requests a certificate to the PKI entities on-line. A person in charge of installing HG at home or a user of HG offers information for issuing the certificate to CA in person, and CA issues HG's certificate. Because the module with which HG can deal with [CMP][4] must be appended, HG can be heavy. However, the merit is to currently apply the same PKI entities for issuance of human-beings' certificate. Also, distinguished name(DN) on the certificate can select various identification addresses such as an address or apartment name, zip code, etc where the HG are located. The second one is that HG sends the certificate request form that includes its own public key to an administrative server and then administrative server deals with issuance of the HG's certificate through communication with PKI entities. The administrative server transmits the certificate issued by CA to HG. Because HG makes only a certificate request format in this method, HG has less computational power compared to HG in the first method. DN of the certificate has the same name with the first method. In addition, the administrative server can set up DN according to the identification address of itself. The third is that the administrative server can generate a private and public key pairs instead of HG. The administrative server requests the issuance of HG's certificates and distributes these certificates to HG according to the specific relationship between HG and the administrative server.

3.2.2 Offline issuance

There are three methods for offline issuance. The first one is that a manufacturer can include a certificate issued by CA previously before HG is released. This is the most convenient to a user, but, as for this method, the DN setting which can distinguish HG must be decided by a manufacturer. For example, there can be the way that every manufacturer runs unique manufacturing serial numbers of appliances. The second one is that management server requests certificates to be issued by CA, and can distribute users when HG needs a certificate. In this case, it is also a simple way, but the DN setting which can distinguish HG must be considered by users. Every service operator has to set up a unique identification system. The third one is that a user can ask CA for issuing a certificate of HG directly. The user generates certificate request form [PKCS#10] with key pairs generated by HG and goes to CA with the request form. CA will issue a certificate of HG and the user will install the certificate in HG. In this case, there is a lot of work that the user must do directly, but the DN which is subordinate to a user may set up for the certificate of HG.

3.2.3 Certificate update, revocation and expiration

If a HG's certificate is expired, or a key is compromised, renewal, re-issuance, and revocation process for HG are needed. This process can be categorized in two ways whether the HG does direct processing as for this process or the management server substitutes for this process. The home-gateway uses [CMP] in case of on-line and deal with related authentication service. On the other hand, the management server's administrator or the user visits CA in case of off-line and deals with renewal, re-issuance, and revocation of the relevant certificate.

3.2.4 Acquisition of trust anchor certificate

Trust anchor is a CA that is directly trusted by a HG. Thus, HG should securely approach and get the value of a Root CA public key as three following methods. The first method is that the HG administrative server substitutes for PKI authentication service with management server, the management server must acquire a trust Anchor certificate safely. The HG does not need a Trust anchor acquisition related mechanism with these ways. The second one is that a HG can acquire a trust anchor certificate directly on-line. A home-networking service provider will guard human-users to learn an acquisition way of trust anchor certificate through user interface of the home-gateway such as TV. The third is that a user can receive a certificate of trust anchor off-line such as diskette by mailing and store it into the home-gateway by his or her hands.

4 Generating and securing a private key

PKI security is based on public key cryptographic safety and storage and generation safety of private keys in particular. Security problems such as a loss, theft, destruction can give a serious influence to HG in authentication service. As for location for generating and storing of the private key, it is categorized into three parts : Home-gateway, administrative server, and a smart card, which is related to safety of the authentication of home-gateway using keys directly.

4.1 Home-gateway

If HG has the computational power, it generates private and public key pairs and stores the private key in HG with encryption by a password or without encryption. If the private key is encrypted, HG must secure the encrypted key in HG's flash memory or hard disk. HG enhances safety of the password with a certificate when decrypting the encrypted key. A merit of this storage is for developers to be relatively easy to implement the key generator and storage of the keys. On the other hand, there exist risks because any sniffer programs are able to do an attack while the private key of HG is decrypted by existing software and to take important and private information of HG.

4.2 Administrative server

If HG management server generates a key, private key management can divide into two ways. The first method for private key management is to manage all these keys in a HG administrative server. When HG accesses a network, the server is to transmit the private key to HG. The private key is encrypted with a secret key which is known to HG and administrative server. The second one is that HG requests encrypting and decrypting for authentication service to the administrative server. The server has responsibility to protect private key of all users and responsibility to carry out authentication about a key use requested by HG. Technical requirements are the client software that is necessary for the server and HG. Client software utilizes PKCS#11 or MS's Crypto API as communication interface.

4.3 Smart Card

Smart card is an active token whose size is the same as a general credit card. A smart card responds to various commands, and saves variable information. Currently, a few enterprises use this function in order to implement PKI functions for HG. In this case, HG needs an physical interface with the smart card.

A smart card saves a private key to protect private key from theft or release of a password of a public key. And a few public key enterprises developed this method. The smart card carries out a function to need private key and reply the result to HG as HG using a private key password transmits requests to a smart card. HG cannot read private key by any means and it is because the private key is not supposed to go out of the smart card. The smart card does not provide a function to open a private key. The smart card provides a private key generation and verification process and can never open private key. As for the smart card, a risk related to private key use and private theft can be downsized. A unique way to use specific private key is to own a mart card having the key.

This method can give a merit of realistic security, but there is a disadvantage. First of all, the smart card has serious performance problem. Generation and verification of a RSA key needs a great deal of computational power to the smart card. For example, it takes an average of 23 seconds to generate a public and private key pairs of RSA 1024bit in case of DataKey Model 330 card, and an average of 3 minutes in case of 2048bit. (DH or a case of DSS can be practical.)

5 Conclusion

So far, this thesis suggested issuance models of HG's certificates and generating location of private keys according the issuance model. The models are mainly classified into online and offline issuance. In addition, the classification partly depends on HG's computational power, which puts influence of private key generating locations - HG, administrative server, or smart card. This suggestion gives ideas of how to implement secure home-networking service with HG's authentication to manufacturers of HG and PKI operators, etc. In the future, the research about the user interface of HG will go on in order for human-users to understand HG's authentication and secure generation of a private key.

References:

[1] NIST, FIPS196 *"Personal Identity Verification(PIV) of Federal Employees nad Contractors"*, 2005.

[2] Bonatti, C., Turner, S., *"Requirements for an IPsec Certificate Management Profile"*, IETF internet draft, 2004

[3] OpenCable, *"OpenCable System Security Specification"*, 2004

[4] Myers, M., Adams, C., Solo, D., Kemp, D., *"Internet X.509 Certificate Request Message Format"*, RFC2511, 1999

[5] RSA laboratories, *"Certification Request Syntax Standard"*, PKCS#10, 2000

[6] ITU-T, *"Information technology - Open Systems Interconnection - The Directory : Authentication Framework"*, X.509, 1997

[7] Housley, R., Polk, W., Ford, W., Solo, D., *"Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile"*, RFC3280, 2002