공개키 기반의 홈디바이스 인증시스템 구축

이윤경* · 한종욱*

*한국전자통신연구원

Home Device Authentication System Construction based on PKI

Yun-kyung Lee* · Jong-wook Han*

*Electronics and Telecommunication Research Institute

E-mail : neohappy@etri.re.kr

요 약

본 논문에서는 홈디바이스 인증체계 및 인증서 발급, 인증방법에 관하여 기술하였다. 홈네트워크에 참여할 수 있는 홈디바이스의 수가 많아짐에따라 공개키 기반의 홈디바이스 인증구조가 더욱 필요할 것이므로 본 논문에서는 공개키 기반의 홈디바이스 인증 시스템에 관하여 기술하였다. 또한 CA 관리의 편의를 위해 CA Administrator를 두어 CA 관리 인터페이스를 구축한 방법에 관하여 기술하였다.

ABSTRACT

In this paper, we described about the home device authentication framework, certificate issuing process and home device authentication method. since the home device authentication scheme of the public key infrastructure would be more needed as the number of home device can participate in the home network increased, we described about the home device authentication system of the public key infrastructure. Moreover, we described about the construction method of CA adminstration interface for convenient CA administration.

키워드

홈디바이스 인증, 공개키 기반, CA, Secure Communication Protocol

Ⅰ. 서 론

홈디바이스란 홈네트워킹에 참여하여 서비스를 제공하거나 제공받는 모든 디바이스를 의미한다. 홈디바이스가 고급화되고, 반도체 기술의 발달로 저가로 다양한 기능 구현이 가능해짐에 따라 홈네트워크는 더욱 활성화 될 것이다. 따라서 홈네트워크에서의 보안은 더욱 중요성이 커질 것이다.

다양한 유무선 네트워크가 사용되고 있는 홈네트워크의 특성상, 주변 홈네트워크의 디바이스를 이용하여 불법적인 접근이 이루어질 가능성이 높으므로 자신의 홈네트워크에서만 사용할 수 있도록 소유하고 있는 디바이스에 대해 신뢰성을 부여할 필요가 있다[1]. 또한 향후 홈서비스는 사용자 개입을 최소화하고, 디바이스들간의 협업으로 사용자에게 서비스를 제공하는 형태로 진화할 것이므로 디바이스 상호인증을 통한 안전한 협업 관계 구축이 더욱 중요한 필수요소가 될 것이라 본다[1].

디바이스 인증은 특정 인증받은 디바이스들만이 통신에 참여할 수 있음을 확인해준다는 점에서 필요하고, 인가받지 않은 디바이스가 사용되지 않는 한 둘 간의 안전한 통신이 보장된다. 또한 이와는 별도로, 디바이스 인증은 사용자 개입이 없이 자동으로 서비스를 제공하는 context-aware 서비스에서 필수적인 기능이고, 또한 DRM 시스템에서도 디바이스 인증이 필요하다[2].

2장에서는 본 논문에서 제안하는 공개키 기반의 홈디바이스 인증시스템 구조와 이 구조에서 사용하는secure communication protocol에 관하여 기술하고, 3장에서는 홈디바이스 등록과정, 홈디바이스가 인증서를 발급받는 과정 및 홈디바이스를 인증하는 과정에 관하여 기술한다. 마지막으로, 4장에서는 이 논문의 결론을 기술한다.

II. 공개키 기반 홈디바이스 인증 시스템

2.1. 홈디바이스 인증시스템 구조

본 논문에서는 공개키 기반의 홈디바이스 인증시스템을 고려한다. 홈네트워크에 참여하는 홈디바이스의 수가 많아지고, 이동식 홈디바이스의 수가 증가하고 있으므로, 대칭키 기반의 홈디바이스 인증에는 한계가 있기 때문이다.

본 논문의 홈디바이스 인증 시스템은 공개키 기반의 홈디바이스 인증을 다룬다. 홈디바이스 인증서를 발급하는 CA를 댁외에 두고, 이 CA는 자신이 발행한 인증서에 대한 검증 및 관리책임을 진다. 그리고 홈 내에 RA의 기능을 하는 디바이스(주로 홈 게이트웨이가 될 것이다.)인 HRA를 두어 홈디바이스들에 대한 인증서 발급을 돕는다. HRA는 새로운 홈디바이스가 등록되면 이 디바이스에 대한 확인작업을 거쳐 외부 인증기관에 홈디바이스 인증서 발급을 요청한다. 외부 인증기관이 해당 홈디바이스의 인증서를 발행하여 HRA에 배포하면 HRA는 이를 받아서 해당 홈 디바이스에 인증서를 전송한다. HRA가 홈디바이스로 해당 인증서를 전송할 때 out-of-band 혹은 유선으로 연결된 매체를 통하는 방법 등 다양한 방법을 이용할 수 있다.

홈디바이스에 대한 인증은 해당 디바이스가 서비스 이용을 요청할 때, 서비스를 제공하는 서버 혹은 홈디바이스와 해당 디바이스 사이의 인증서 교환후 인증서 확인을 통해 이루어진다. 이때, 컴퓨팅능력이 떨어져서, 공개키 연산에 어려움이 있는 디바이스들은 delegation server에 인증서의 확인을 부탁하고, delegation 서버는 certificate verification 결과를 해당 디바이스에 알려주는 방법으로 상대 디바이스에 대한 인증을 수행할 수 있다.

본 논문에서 제안하는 공개키 기반의 홈디바이스 인증시스템은 그림 1과 같은 구조를 지닌다.

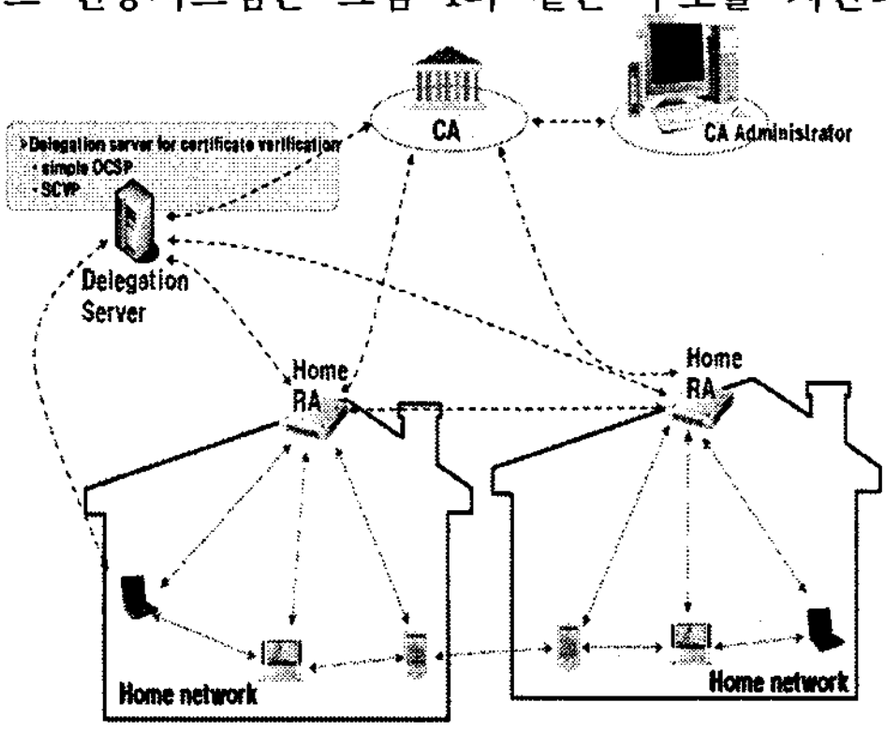

그림 1. 홈디바이스 인증 시스템 구조

2.2. SCP(Secure Communication Protocol)

2.2.1. SCP의 정의

공개키 기반의 홈디바이스 인증을 할 때, 선행되어야 할 사항이 홈디바이스에 대한 인증서 발급이다. 인증서를 발급하기에 앞서 CA의 관리자가 CA에 인증서 발급 및 인증서 관리, CA 관리 등에 관한 정책을 설정하는 과정이 필요하다. 이러한 정책설정을 편리하게 하기 위해서 CA administrator라고 하는 인증서 정책 설정 시스템을 구현하였다. CA administrator의 GUI(Graphic User Interface) 화면에서 CA의 기능과 관련된 각종 정책을 설정하면 설정된 정책 데이터가 CA로 전송되고, CA는 전송 받은 정책 데이터를 CA의 데이터베이스에 저장한다. CA administrator는 정책 설정 인터페이스 및 디스플레이 기능만을 하고, 실제 데이터들은 CA의 데이터베이스에 저장된다. 이때, CA와 CA Administrator 사이의 데이터 전송시 안전한 경로로, 정해진 규격에 맞춰 전송될 필요가 있는데, 이를 위해서 SCP(secure communication protocol)을 정의하였다. 그림2는 본 논문에서 제안하는 SCP를 간략하게 보여준다.

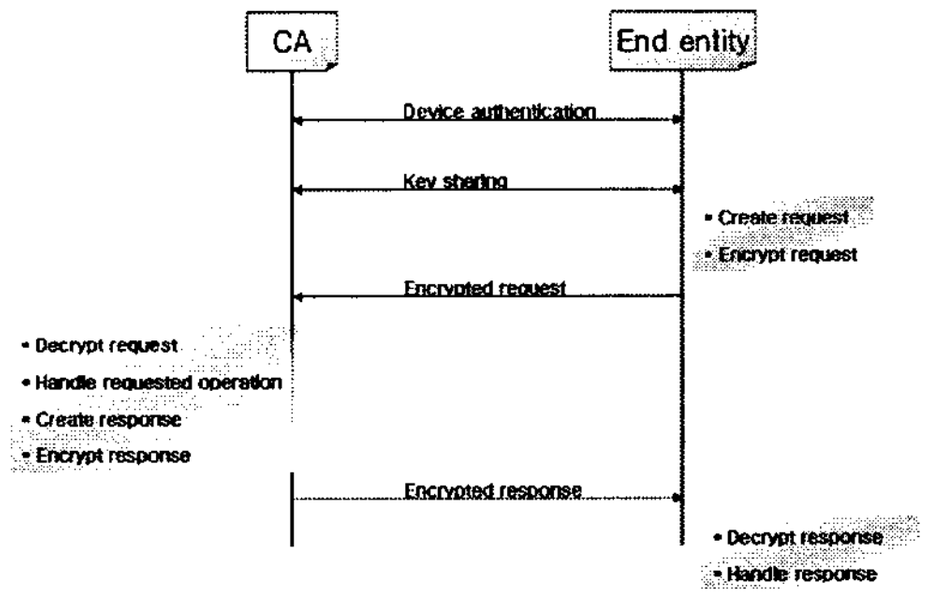

그림 2. SCP 프로토콜

그림 2에서 알 수 있듯이 SCP 프로토콜은 CA와 end entity 사이에 상호인증을 한 후, 이들 사이에 나눠가진 키로 서로 암호화를 하여 데이터를 전송한다. SCP 프로토콜은 다음과 같은 순서를 따른다.

(1) end entity의 인증서와 CA 인증서를 요구하는 메시지를 CA에 전송한다.

(2) CA는 end entity 인증서를 검증한 후, 신뢰할 수 있는 인증서일 경우 CA의 인증서를 end entity에 전송한다.

(3) End entity는 CA의 인증서를 검증한 후, 신뢰할 수 있는 인증서일 경우 상호 통신시 사용할 키와 암호 알고리듬에 대한 협상 시작요청 메시지를 CA에 전송한다.

(4) CA는 상호 통신에서 사용할 키를 생성하고, 사용할 알고리듬에 대한 정보도 함께 end entity의 공개키로 암호화하여 end entity로 전송한다.

(5) End entity는 본인의 비밀키로 복호화하여앞으로 통신에 사용할 세션키와 암호 알고리듬 정보를 알게 된다. 이 세션은 CA와 end entity간 통신이 일정시간 이상 끊어지지 않는다면 지속될 것이다.

- end entity가 request 메시지를 생성하고 공유된 키와 알고리듬을 이용하여 암호화 한 후, 암호화된 request 메시지를 CA로 전송한다.

(6)CA는 request 메시지를 복호화 한 후, request를 처리하고, 이에 대한response를 생성한 후 이 메시지를 암호화하여 end entity에 전송한다.

(7) End entity는 response를 받아서 복호화 한 후 이를 처리한다.

한편, SCP의 패킷 구조는 그림 3과 같다. CA와 end entity간 통신 메시지의 종류를 나타내는, 미리 약속된 값인 8비트 길이의 opcode가 있고, 그 뒤로 32비트의 record의 숫자가 따라온다. 그 뒤로 record들이 차례로 나오게 된다. 이때, record의 의미는 데이터베이스의 한 행에 해당하는 값

이다. 예를 들어 CA의 데이터베이스에 9가지의 인증서 정책이 저장되어 있을 때, end entity에서 인증서 정책종류를 보내달라는 opcode를 CA로 보내면, CA는 이에 대한 응답으로 9개의record 값들을 차례로 보내게 된다. 또한 각 record는 각 레코드의 길이(length)와 필드 값들로 구성되어 있고, 각 필드 값들은 세미콜론으로 구분된다. 각 필드는 데이터베이스의 칼럼에 해당하는 값으로, 위의 예를 이용하면, 각 정책의 구성 요소들에 해당 하는 값이 field 값이 된다.

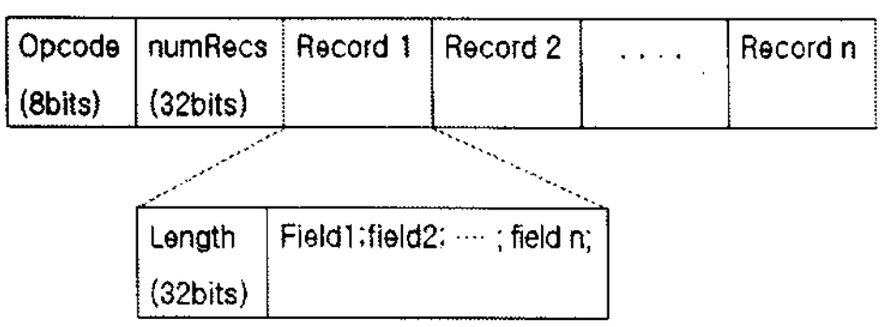

그림 3. SCP 패킷구조

2.2.2. SCP의 적용

SCP는 앞서 2.2.1.에서 기술한 CA의 기능 설정 및 인증서와 관련된 각종 정책을 설정하기 위해서 CA와 CA administrator 사이의 통신에 사용되는 안전한 프로토콜이다. 또한 SCP는 인증서 발급 요청을 포함한 인증서 발급과정에서 CA와 Home RA간 통신에 사용되기도 한다. 이때, CA와 CA administrator간, CA와 Home RA간 사용되는 SCP의 구조와 프로토콜은 동일하지만 사용되는 opcode 값은 달라진다. 그림 4는 인증시스템에서 사용되는 통신프로토콜을 보여준다. 붉은색으로 원통막대는 통신에 SCP가 사용됨을 나타내고, 주황색 원통막대는 out-of-band 혹은 유선연결 등의 물리적인 안전성이 확보된 상황에서 통신하는 것을 나타낸다.

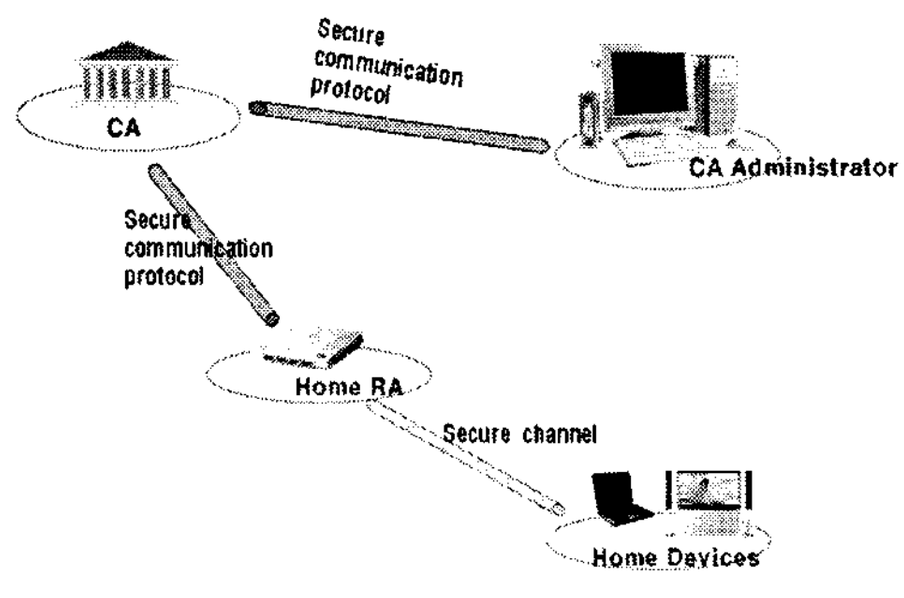

그림 4. 인증 시스템에서 사용되는 통신 방법

III. 홈디바이스 인증

홈디바이스를 인증하기 위해서는 홈디바이스를 CA에 등록하고, 등록된 홈디바이스에 대한 확인 작업을 거쳐 인증서를 발급하는 선행과정이 필요하다. 본 장에서는 홈디바이스를 CA에 등록하는 과정, 인증서 발급과정 및 발급된 인증서를 이용하여 홈디바이스를 인증하는 과정에 관하여 기술하고자 한다.

3.1. 홈디바이스 등록 과정

홈디바이스는 Home RA를 거쳐 CA에 등록된다. Home RA는 홈에 존재하는 하나의 디바이스로써, 다른 홈디바이스보다 약간의 권한을 더 많이 갖는다. 즉, 일반 디바이스에 비해 조금 더 많은 공신력을 가진다. Home RA는 댁내의 디바이스들 중 제법 편리한 사용자 인터페이스를 갖고 있고, 다른 홈디바이스들과 통신할 수 있는 통신 수단을 갖고 있어야 한다. 또한 다른 홈디바이스들과 관련된 정보들을 저장하고 있어야 하므로 외부 공격으로부터 이들 데이터를 안전하게 보관할 수 있어야 한다. 그리고 HRA는 홈디바이스의 등록 및 관리의 책임을 진다. 이러한 Home RA 디바이스로는 주로 홈게이트웨이를 이용하지만, 다른 디바이스가 될 수도 있다.

홈디바이스를 CA에 등록하는 과정은 그림5에 나타나 있다.

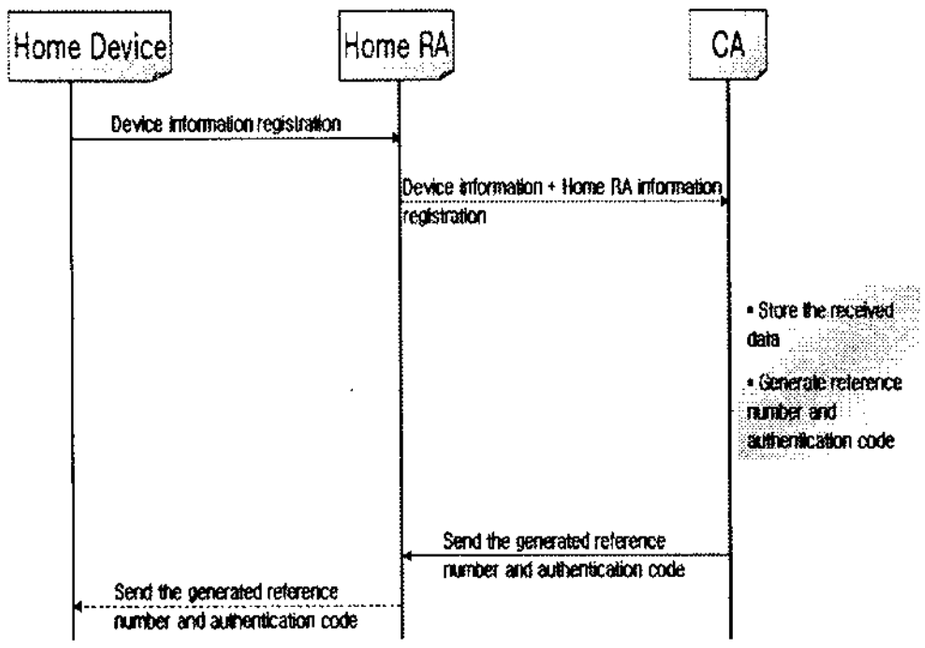

그림 5. 홈디바이스 등록 과정

그림 5에서 볼 수 있듯이, 홈디바이스 등록 과정은 홈디바이스가 home RA에 홈디바이스 정보를 전송하면 Home RA는 이 정보와 Home RA 정보를 통합하여 CA로 전송한다. CA는 Home RA로부터 받은 정보를 데이터베이스에 저장하고, 참조번호와 인가코드를 생성한 후 이 값들을 Home RA로 전송한다. 한편, Home RA는 CA로부터 받은 참조번호와 인가코드를 홈디바이스에 전송할 수도 있고, Home RA에서 안전하게 저장하고 있을 수도 있다. 또한 2.2.절에서 기술한 바와 같이 홈디바이스와 Home RA간 통신은 out-of-band 혹은 유선의 연결 등의 물리적 안전성에 기반한 통신을 하게 되고, Home RA와 CA간 통신은 SCP를 이용한 암호학적 안전성에 기반한 통신을 하게 된다.

홈디바이스 등록시 CA가 생성하여 전달하는 참조번호와 인가코드는 홈디바이스 인증서 발급에 사용하게 될 값으로, 홈디바이스가 직접 인증서 발급요청을 할 경우 Home RA는 CA에게서 받은 이 값들을 홈디바이스에 전송하고, Home RA가 인증서 발급요청을 홈디바이스를 대신하여 하게 될 경우 Home RA는 이 값들을 자신의 데이터베이스에 저장하게 된다.

3.2. 인증서 발급 과정

그림 6은 Home RA가 홈디바이스를 대신하여 인증서 발급요청을하는 과정을 보여준다. Home RA는 자신의 데이터베이스에 저장된 참조번호와 인가코드를 CA로 전송하고, CA는 Home RA가 보내온 참조번호와 인가코드를 확인한 후, 이 값들을 기반으로 홈디바이스 정보를 CA의 데이터베이스에서 꺼내어 홈디바이스 인증서를 발급한다. 이때 인증서 정책은 CA administrator를 통해서 미리 세팅된 정책을 이용하게 된다. 발급된 인증서는 Home RA로 전송되고, 이를 받은 Home RA는 인증서를 홈디바이스에 보낸다. 통신 채널은 홈디바이스 등록과정과 동일한 형태로, Home RA와 CA간 통신은 SCP를 이용한 암호학적 안전성에 기반한 통신을 하고, 홈디바이스와 Home RA간 통신은 out-of-band 혹은 유선의 연

결 등의 물리적 안전성에 기반한 통신을 한다.

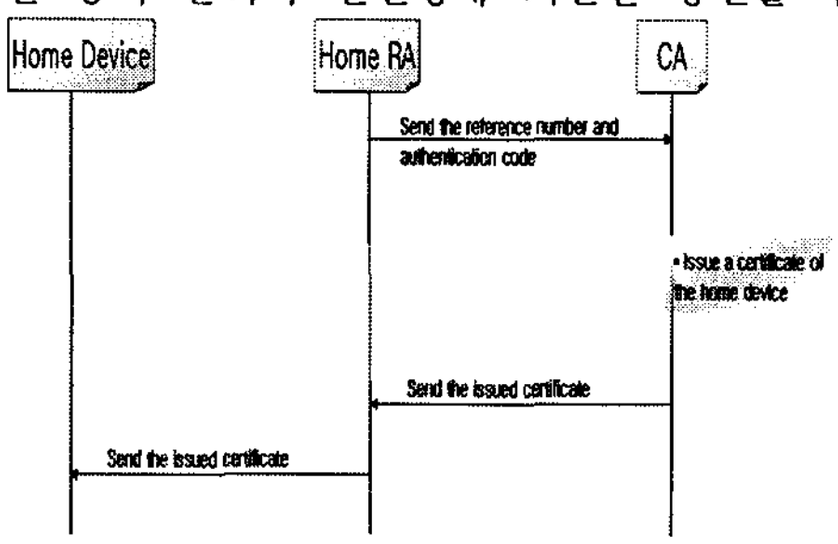

그림 6. 홈디바이스 인증서 발급과정

3.3. 홈디바이스인증 과정

홈디바이스가 홈네트워크 서비스를 이용하고자 할 때 해당 디바이스에 대한 인증이 필요하다. 모든 홈디바이스는 홈네트워크 서비스를 제공할 수 있고, 제공받을 수 있지만, 모든 홈디바이스가 공개키 연산을 할 수 있는 컴퓨팅 능력을 갖고 있는 것은 아니기 때문에Delegation Server의 개념을 제안하게 되었다. Delegation server는 홈디바이스를 대신하여 상대방 디바이스의 인증서를 검증하는 기능을 수행하는데, 이 서버의 성능이 좋을수록 홈디바이스 인증에 소요되는 시간이 줄어들 수 있다. 이 서버는 각 홈에 한 대씩 있을 수도 있고, 여러 개의 홈이 공유하도록 할 수도 있다. 또는 각 CA마다 몇 대씩 두어 관리하는 형태가 될 수도 있을 것이다.

또한 컴퓨팅 능력이 뛰어난 홈디바이스들은 상대방 디바이스 인증서의 검증을 delegation server에 위탁할 수도 있고, 본인이 직접 할 수도 있을 것이다. 그러나, 이 논문에서는 Delegation server를 이용할 경우 홈디바이스의 인증과정만을 기술하고자 한다. 홈디바이스 2가 홈디바이스1이 제공하는 서비스를 이용하고자 할 때의 인증과정으로, 이 과정을 기술하면 다음과 같다.

(1) Home Device2가 Home Device1에 서비스를 요청한다.

(2) Home Device1은 Home Device2의 인증서 요청 메시지를 보낸다.

(3) Home Device2는 Home Device1에 자신의 인증서 $Cert_{D2}$를 보낸다.

(4) Home Device1은 자신의 인증서와 함께 Delegation server에게 인증서 verification 요청이 있음을 알린다.

(5) Delegation Server는 Home Device1의 인증서를 확인하고, 유효한 인증서일 경우 nonce를 생성하고, 이 nonce와 Home Device1의 seed key를 XOR 연산하여 저장한다.

- 이때, Delegation server는 자신이 맡은 디바이스들의 seed key에 관한 정보를 미리 알고있다고 가정한다.

(6) Delegation Server는 생성한 nonce 값을 Home Device1에 전송한다.

(7) Home Device1은 Delegation Server로부터 받은 nonce와 자신의 seed key를 XOR 하여 저장하고 이 값을 SK_{D1}이라 칭한다. 또한 이 키가Home Device1의 새로운 seed key가 된다.

(8) Home Device1은 Home Device2에게서 받은 인증서를Delegation Server에 전송하여 인증서 검증을 요청한다.

(9) Delegation server는 Home Device1에게서 받은 Home Device2의 인증서를 검증한다.

(10) Delegation Server는 인증서 검증 결과를 SK_{D1}으로 암호화하여 Home Device1으로 전송한다.

(11) Home Device1은 delegation server로부터 받은 메시지를 복호화하여 인증서 검증 결과를 확인 한 후, Home Device2의 인증서가 유효하면 Home Device2에 서비스를 제공하고, 유효하지 않으면 Home Device2에 서비스를 제공하지 않고, Home Device2와의 연결을 끊는다.

Ⅳ. 결 론

본 논문에서는 안전한 홈네트워크를 이용하기 위한 홈디바이스 인증에 관하여 기술하였다. 즉, 홈디바이스 인증시스템 구조를 제안하고, 이 시스템에서 사용하는 통신프로토콜도 제안하였다. 이 프로토콜은 주로 CA와 다른 디바이스간 통신에 사용되고, 이들 사이의 안전한 통신을 위해서 인증서 확인 및 키 교환 과정, 교환된 키를 이용한 메시지 암호화 과정을 포함한다. 또한 Home RA를 통해서 홈 디바이스를 CA에 등록하는 과정 및 홈디바이스가 Home RA를 통해서 인증서를 발급받는 과정에 관하여 기술하였다. 그리고, 홈서비스를 이용하고자 하는 홈디바이스와 홈서비스를 제공하는 디바이스 사이의 인증 방법을 제안하였다. 이 논문에서는 공개키 연산을 할 수 있을 만큼의 충분한 컴퓨팅 파워가 없는 경우 delegation server를 두어 상대방 디바이스 인증서의 유효성을 검증할 수 있는 디바이스 인증구조를 제안하였다.

본 논문에서 제안한 인증구조는 home에 국한되지 않고, 사무실이나 도시 내에서, 더욱 확장하여 국가 내에서 사용할 수 도 있으리라 본다. 그리고 본 논문에서 제안한 홈디바이스인증체계에서 홈디바이스 인가를 더한다면, 더욱 안전하고 편리한 홈네트워크시스템을 구현할 수 있으리라 본다.

참고문헌

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

[2] Yeonjeong Jeong, et al., "A Trusted Key Management Scheme for Digital Right Management," ETRI Journal, vol.27, no.1, Feb.2005.