# PKI 사용자 인증을 통한 u-Healthcare 서버 로그인 시스템 설계 및 구현

윤성열, 김철중, 박석천
경원대학교 소프트웨어학부
e-mail: scpark@kyungwon.ac.kr

# Design and Implementation of u-Healthcare Server Login System by PKI user Authentication

Sung Yuol Yun, Cheol-Joong Kim, Seok Cheon Park
Division of Software, Kyungwon University

요 약

u-Healthcare란 언제 어디서나 의료 장비 및 센서 등을 이용하여 수집된 생체 정보를 유선 또는 무선의 통신수단을 이용하여 유비쿼터스를 지향하는 지능형 의료정보를 제공하는데 목적을 두고 있는 서비스이다. 각종 센서에서 수집된 생체 신호 및 의료 데이터는 그 데이터를 필요로 하는 기관 또는 병원 등에 전송되어야 하는데, 현시점에서는 하드웨어나 서비스 중심의 구현에만 집중되고 있어서 전송 시에 보안에 대한 연구가 제대로 이루어 지지 않고 있다. 또한 이와 같은 이런 정보들은 개인에게는 매우 중요한 데이터로써 외부로 노출될 시에 심각한 프라이버시 침해가 예상된다. 이를 위해 본 논문에서는 PKI 사용자 인증을 통하여 본인 여부를 확인하여 u-Healthcare서버에 로그인 하는 시스템을 설계하고 구현하였다.

## 1. 서론

u-Healthcare란 “인체의 건강관련 정보를 시간과 공간의 제약 없이(ubiquitous) 수집, 처리, 전달, 관리할 수 있게 해줌으로써 제공되는 원격지 의료서비스(Healthcare)"라고 정의할 수 있다[1].

사용자의 생체신호를 측정할 수 있는 전용 단말기로 측정하고 이를 유·무선 네트워크를 통해 u-Healthcare 서버 또는 병원으로 전송하여 치료에 필요한 데이터를 전송받는 것이 u-Healthcare의 기본 서비스이다. 이를 위해서 수집한 생체신호를 병원 또는 필요한 기관으로 전송하는 시스템이 필수적이다. 하지만 이러한 u-Healthcare 시스템은 아직 초기단계이기 때문에 센서부분이나 전송시스템 부분 등 하드웨어 및 서비스 중심의 구현에만 초점이 맞추어져 있다. 또한 이와 같은 사용자의 생체신호정보는 개인의 프라이버시에 직결되는 것으로 보안의 필요성이 매우 큰 특성을 가지고 있기 때문에 생체신호 접근 시 보안이 유지될 수 있도록 하는 연구가 필요하다[2].

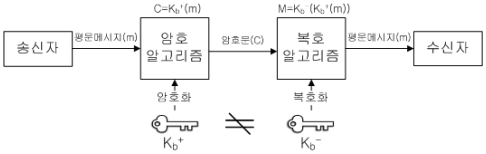
따라서 본 논문에서는 인증과, 비밀보장, 무결성, 부인방지를 만족하기 위해서 PKI(Public Key Infrastructure)를 통하여 사용자 인증과 암호화/복호화를 적용한 u-Healthcare 서버 로그인 시스템을 설계하고 구현하였다.

## 2. 공개키 암호 알고리즘

본 논문에서는 공개키 암호 알고리즘을 이용하여 PKI사용자 인증 시스템을 설계하고 구현 하였으며 인증이 완료된 송수신자끼리 키를 전송함으로써 비밀키 암호 알고리즘을 이용하여 서로간의 필요한 생체 데이터를 안전하게 전송할 수 있다.

공개키 암호 알고리즘은 연관되어 있는 두 개의 키를 이용하여 암호화하거나 복호화 하는 알고리즘이다. 즉, 하나의 키로 암호화하고 나머지 다른 하나

의 키로 이를 복호화할 수 있다. 따라서 키 쌍에서 하나의 키를 공개하고 다른 하나는 외부에 공개되지 않도록 보관한다. 이때 공개하는 키를 공개키(Public Key)라고 하며 공개하지 않고 개인이 비밀로 보관하는 키를 개인키(Private Key)라고 한다[3]. 이를 통해서 송신자와 수신자가 통신을 하기 위해서는 (그림 1)과 같은 과정을 거친다.




(그림 1) 공개키 암호 알고리즘

송신자는 수신자의 공개키(Kb+)를 통해 수신자에게 보내는 자의 메시지(m)을 암호화하고 이를 전송한다. 수신자는 이 암호문을 자신의 개인키(Kb-)로 복호화 하여 메시지를 얻는다[4].

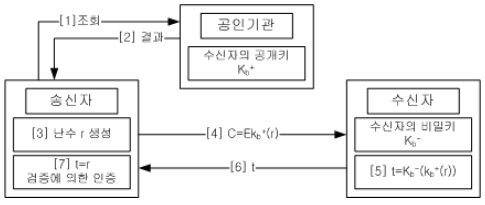
이 공개키 암호화에서는 부인 방지의 기능도 제공한다. 부인 방지란 송신자가 수신자에게 어떤 메시지를 보냈을 때 나중에 송신자가 메시지를 보내지 않았다고 부인하는 것을 방지한다는 것으로서, 송신자는 자신의 개인키로 암호화해야 공개키로 해독되므로 부인 방지 기능을 가진다. 이 부인 방지는 주로 서로가 확실한 신원이 확인되어야 하는 전자 상거래에서 쓰인다.

## 3. 인증과 PKI

### 3.1 인증

인증은 크게 두 가지 의미로 구분되어진다. 첫 번째는 전자 서명을 통하여 구현될 수 있는 사용자 인증 또는 메시지 인증을 의미하는 “Authentication"이고, 두 번째는 공개키 암호방식에서 공개키의 무결성을 보장하기 위해 인증기관이 발행하는 인증서의 의미를 갖는 ”Certification"이다.

인증(Authentication) 서비스의 필요성은 공개키 암호시스템의 사용에서부터 비롯되며, 전자상거래 환경 구축을 위해서는 인증, 무결성, 비밀성, 부인방지 등의 정보보호 서비스가 필수적으로 요구되며, 이는 전자 서명 기술을 활용함으로서 해결 가능하다. 공개키를 이용한 상대인증 방식은 (그림 2)와 같다.




(그림 2) 공개키의 의한 사용자 인증

송신자는 공인기관에 수신자의 공개키(Kb+)를 조회하여 Kb+를 획득한다. 송신자는 난수 r을 생성하고 수신자의 공개키 Kb+를 이용하여 r을 암호화한다. 그리고 암호문 C를 수신자에게 보낸다. 수신자는 자신의 비밀키(Kb-)를 이용하여 암호문 C를 복호화하고 t를 구한다. 수신자는 t를 다시 암호화 과정을 거쳐 송신자에게 보낸다. 송신자는 t의 값과 r의 값을 비교하여 같으면 수신자를 정당한 사용자로 인증한다.

### 3.2 PKI(Public Key Infrastructure)

공개키 암호기법을 이용한 전자 서명 기술은 수학적으로 그 안정성을 증명 할 수 있는 대표적인 인증(Authentication) 기법으로, 이것의 실제 적용을 위해서는 인증(Certification) 서비스가 필요하게 된다. 이를 위해서 공개키 암호방식을 이용한 전자서명 기술의 효과적인 이용이 요구되며, 공개키 암호방식을 이용한 인증방법을 구현하기 위한 기술적, 제도적 기반이 요구되는데 이를 공개키 기반구조(PKI : Public Key Infrastructure)라고 한다[7-10]. PKI를 구축함으로서 암호키 갱신, 복구 위탁 등과 같은 키 관리, 인증서 생성 및 취소관리, 그리고 인증 정책관리와 같은 서비스의 제공이 가능해진다. PKI 환경을 구축하는 주요 객체는 인증기관인 CA(Certification Authority), 인증서 저장소(Certification Repository), 최종 사용자(End User or Client) 그리고 서비스 제공 주체 등으로 구분된다.

## 4. 제안 모델 설계

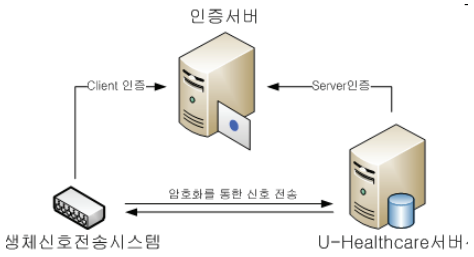
### 4.1 기존의 시스템의 문제점

기존에 공개키 알고리즘을 사용하면 송신자와 수신자 사이의 다른 알고리즘보다 비교적 안전하게 데이터를 전송할 수 있다. 하지만 송신자에게 들어온 수신자의 공개키가 정당한 수신자인지 판단할 수 있는 기반이 마련되어 있지 않다. 따라서 정당하지 못한 수신자가 송신자에게 인증되지 않은 공개키를 넘

겨주었다면, 송신자는 개인 데이터를 손쉽게 넘겨주는 결과를 초래할 수 있다. 따라서 본 논문에서는 사설 인증기관을 마련하고 JAVA언어를 통하여 SinedApplet과 RMI 프로토콜을 이용한 신뢰성 있는 통신 시스템을 구현하였다.

### 4.2 PKI를 통한 u-Healthcare 서버의 로그인 시스템 설계

본 논문에서 제안하는 모델은 인증 서버를 통하여 u-Healthcare 서버와 클라이언트 시스템(생체신호 전송시스템) 인증을 하고, 세션 정보 생성 및 데이터에 대하여 공개키 기반 TLS(Transport Layer Security)를 통하여 암호화함으로써 보안성을 강화하였다. (그림 3)은 전체 시스템의 개요도를 나타낸 것이다.




(그림 3) 전체 시스템 개요도

본 논문의 u-Healthcare 전송시스템은 시리얼포트를 통하여 생체신호를 입력받는다. 생체신호가 입력되면 인증서버에게 인증을 요청하고 공개키를 전송받는다. 공개키를 전송받은 전송시스템은 공개키를 이용하여 u-Healthcare와 상호인증을 수행하고 인증이 완료되면 비밀키를 전송받아 이를 통하여 생체신호를 암호화하여 서버로 전송한다. 여기에서 발생할 수 있는 보안 취약점을 요약하면, 각 구성요소간의 신분확인, 신호를 전송하기까지 과정에서 교환되는 제어정보에 대한 무결성 및 기밀성, 신호가 전송되는 동안에 교환되는 정보의 기밀성에 대한 보안대책이 필요하다. 따라서 보안 취약점은 u-Healthcare 서버에 공개키 기반 서버인 인증 서버를 두어 인증서를 통한 사용자인증을 확인함으로서 해결한다.

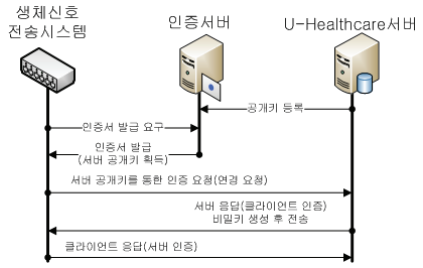
인증서를 통한 전송 보안 프로토콜은 각 참여자뿐만 아니라 하드웨어 자원에 대한 인증도 가능하여 보안성이 강화된 사용자 신분확인 서비스를 제공할 수 있다. 클라이언트의 부하를 줄이기 위해서는 키의 생성은 서버에서 이루어지게 설계하였으며 클라이언트에서는 오직 인증을 위한 공개키 암호화 및 생체신호 암호화를 위한 비밀키 암호화만을 수행하게 하였다. 다음의 (그림 4)는 u-Healthcare 서버에 로그인하는 인증 알고리즘을 나타낸 것이다.

```
Basic인증{
 MAC 어드레스 필터링을 통해 인증 수행;
 if(허가된 사용자) {u-Healthcare 서버공개키 전송;
 if(u-Healthcare서버의 공개키를 이용해
                    서버와 상호간 인증수행==Pass)
   비밀키 알고리즘을 통해 비밀키 전송;
}}

Basic전송{
 비밀키 획득후 생체신호를 암호화 전송;
 u-Healthcare 서버는 암호화된 메시지 수신후 복호화;
}
```

(그림 4) u-Healthcare 서버의 로그인 인증 알고리즘

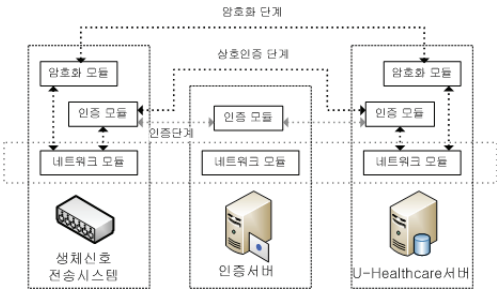
인증 절차는 (그림 5)와 같다. 먼저 클라이언트는 자신의 MAC 어드레스를 통하여 인증 서버에 인증서 발급을 요청한다. 인증 서버는 이를 통하여 클라이언트 신원을 확인하며, 정당한 사용자로 확인되면 인증서를 발급한다. 클라이언트는 이를 통해 u-Healthcare 서버의 공개키를 획득한다.




(그림 5) 인증 절차

### 5. PKI를 통한 u-Healthcare서버의 로그인 시스템 구현

전송 시스템이 생체신호측정단말기로부터 생체신호를 전달받아 인터넷망으로 전송하기 위한 시스템의 모듈 구조는 (그림 6)과 같다.

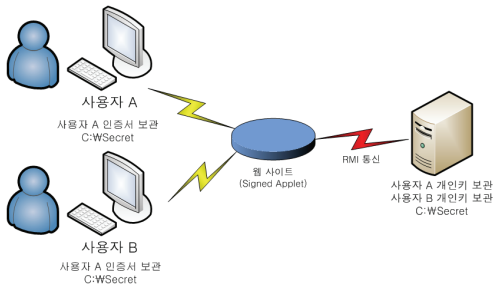



(그림 6) 전송시스템 모듈 구조

구현된 시스템은 생체신호를 암호화 모듈을 통해 암호화를 수행한 후 TCP/IP를 통해 u-Healthcare 서버로 패킷을 전송한다.

우선 인증 모듈은 클라이언트와 서버간의 공개키 알고리즘을 통한 인증을 실시하고 연결을 설정하는 단계를 수행한다. 암호화 모듈은 생체신호를 전송하기 위하여 암호화를 수행하고, 네트워크 모듈은 클라이언트와 서버간의 통신을 위한 모듈이다.

클라이언트는 자신의 MAC 어드레스를 통하여 인증 서버에게 u-Healthcare 서버의 공개키를 요청하게 된다. 인증 서버는 클라이언트의 MAC 어드레스로 클라이언트를 인증하고 u-Healthcare 서버의 공개키를 인증서에 첨부하여 전송한다. 그러나 본 논문에서 구현한 로그인 시스템은 자바의 애플릿을 기반으로 설계하였기 때문에 클라이언트의 PC에서 파일을 저장하거나 읽어올 수가 없다. 그 이유는 자바의 보안 정책 때문인데 이를 위해서 사용자 인증서를 발급하여 클라이언트 PC에 저장을 하고 인증서를 읽어오는 과정을 처리하기 위해서는 ActiveX와 같이 사용자에게 프로그램을 설치할 때 설치 할 것인지를 확인하는 메시지를 물어보는 Signed Applet의 기술을 사용해야 한다. 또한 클라이언트에 인증서를 설치하였다면 이 인증서에는 공개키가 포함되어 있는데 사용자가 웹에서 사용자 인증이 필요한 곳에 접근을 할 때 사용자가 입력한 비밀번호를 확인 하는 작업이 필요하다. 따라서 서버에는 개인키를 보관하고 있어야 하며 이와 같은 개인키를 관리하기 위해서 자바의 RMI(Remote Method Invocation) 통신 프로토콜을 이용한다. (그림 7)은 Signed Applet과 RMI를 이용하여 통신하는 것을 나타낸 그림이다.




(그림 7) Signed Applet과 RMI 구조도

## 6. 결론

u-Healthcare 서비스는 병원이나 대형 의료기관을 중심으로 발전한 의료 서비스를 언제 어디서나 편리하게 이용할 수 있는 서비스이며 현재까지 설계된 u-Healthcare 시스템은 전송이나 서비스 구현에 초점이 맞춰져 있었다. 하지만 전송되는 생체데이터는 각 개인의 중요한 정보로서 보안의 필요성이 절실히 요구된다. 이때 송신자와 수신자가 정상적인가를 확인할 수 있는 인증과정을 거쳐야 하고 데이터 또한 암호화하여 전송해야 한다. 따라서 본 논문에서는 PKI를 통하여 인증이나 기밀성 및 무결성을 구현한 u-Healthcare 서버 로그인 시스템을 제안하였다. 이를 위하여 클라이언트와 서버의 인증을 위한 인증 모듈과 암호화 모듈을 설계하였고 구현하였다.

향후 연구방향으로는 u-Healthcare 시스템의 센서에서 얻어진 중요한 생체데이터의 보안에 가장 적합한 알고리즘의 선정과 보안 모듈의 설계가 필요하다.

## 참고문헌

[1] 김희찬, “유-헬스케어와 센서”, 대한전자공학회지, 2005.

[2] e-Health 시장동향 및 활성화 방안, etri, 2004.11

[3] E.Rescorla, "Diffie Hellman Key Agreement Method," IETF RFC 2246, 1999.

[4] S.A. Thomas, "SS1&TLS Essentials : Securing the web Wiley," 2000.

[5] T. Dierks, C.Allen, "The TLS Protocol Version 1.0", EDTF RFC 2246, 1999.

[6] B. Schneier, "Applied Cryptograph," second edition John Wiley & Sons, 1998.

[7] R.Rivest, A. Shamir and L.Adelman, "A Method for Obtainging Digital Signatures and Public Key Cryptosystems," Communications of the ACM, Vol.21, No.2, pp. 120-126, 1978.

[8] Mattbew Stallings, "Cryptography and Network Security Principles and Practice," Green P.377-400, 2001.2.

[9] 칼리슬 암스 외, “보안을 위한 효율적인 방법 PKI", 인포북, 2003. 9.

[10] Russ Housley, "planning for PKI," John Wiley & Sons, 2002.