WPKI를 이용한 모바일 의료 인증 시스템 구현

오근탁* · 구제영·김용호· 이윤배

*조선대학교 대학원 전자계산학과

WPKI Using for Mobile Medcial Authentication System Embodiment

Keun-Tack Oh* · Jae-Young· Ku yung-Ho· Kim Yun Bae Lee**

*Chosun University

E-mail : osc@effff.chol.com

요 약

오늘날 원격의료가 새롭게 부각되는 것은 정보통신기술의 발달이 원격의료를 뒷받침해 주고 있기 때문이기도 하면서 새로운 의료서비스에 대한 제공자와 수요자들의 인식전환이 이루어지고 있기 때문이라고 할 수 있다. 매우 빠르게 발전하고 있는 진단과 치료기술을 이러한 의료를 필요로 하는 사람들에게 제공하는 접근성의 보장 문제를 해결할 수 있는 대안으로 WPKI를 이용한 모바일 환경 의료인증 시스템을 제안 하고자 한다.

ABSTRACT

There are two reasons that the remote medical is newly embossed. One is the development of the info-comm unications technology that is possible to the remote diagnosis. Another is changing the thinking about the ne w medical services for the offerers and consumers. Therefore, we suggest the WPKI mobile-environmental re mote diagnosis system. The system could apply more efficient connetion with the very fast developing diag nosis and medical treatment.

여

키워드

Key Worlds:communication, WPKI, Remote Medical Authentication System

Ⅰ. 서 론

의료정보는 단순한 텍스트형의 데이터뿐만 아니라 방사선 사진에 이르기까지 광범위한 데이터가 있으며 이 데이터를 이용하는 사람이 많다. 그리고 이 데이터들이 의미론적으로 상호 연결되어 있어서 복잡하며 이 데이터로 지원해야할 목적도 다양하며 광범위 하다. 특히 이 분야에서는 진료정보가 신속 정확하게 전달되기 위해서는 통신매체도 중요하지만 더욱 중요한 것은 데이터의 안전성 문제이다. 그러므로 이러한 보호 문제를 포함한 보안 문제를 해결하기 위한 제반 장치가 마련되지 않는다면 중요한 환자를 위한 개인의 데이터의 안전성을 기대 할 수 없게 된다[1].

의료 현장에서는 일반적인 비정상적인 내용만 기록 되므로 어떤 데이터가 환자의 기록에서 발견되지 않을 때는 이상이 없는 것을 뜻할 수도 있고 이러한 데이터가 이용될 수 없거나 수집되지 않는 것을 뜻할 수도 있다[2]. 데이터의 안전한 전송을 보장하기 위해서는 상대방을 확인함과 동시에 정보의 복제에 의한 정보의 누출이나 손상을 방지하는 대책이 절실하다. 즉 전송 당사자들에 대한 인증을 수행하고 데이터에 부정이 없다는 것을 증명 하는 구조가 갖추어져 있어야 하며 이러한 데이터 들이 다른 사람들에게 노출되어 손상을 입는 일이 없이 기밀성을 보장하는 암호화 및 복호화가 필요하다[3]. 본 논문에서는 모바일 원격 의료 정보 시스템을 구현하는 경우 발생할 수 있는 보안 위협에 대처할 수 있는 모바일 인증 시스템을 제안하고 구현하였다. 시스템은 무선 네트워크를 기반으로 한 WAP(Wireless Application Protocol)과 PDA를 통해 임상에 필요한 데이터를 참조하고, 실시간으로 환자에게 처방을 할 수 있는 시스템을 기반으로 하였다. 인증 시스템의 구조는 유선 상에서는 RSA기반의 X.509 v3 인증서를, 무선 상에서는 ECC 기반의 WTLS 및 X.509를 이용하였다.

Ⅱ. 본 론

무선인터넷을 기반으로 하는 무선 의료정보 시스

템은 기존의 유선 환경의 의료정보 시스템에서 제공하기 힘들었던 이동성(mobility), 편재성(ubiquity), 그리고 이로부터 발생하는 위치 기반 서비스(Location Based Service) 제공이 가능한 여러 가지 이점이 있다. 이와 함께 무선인터넷 서비스의 요구 사항으로써 상호 운영성(interoperability), 확장성(scalability), 효율성(efficien-cy), 신뢰성(reliability) 및 보안성(security)을 고려하여야 한다[1]. 특히 무선 인터넷에서의 정보보호는 전송계층 및 응용계층에서 접근이 이루어져야하고 무선 환경의 제약사항을 고려하여야 한다. WAP(Wireless Application Protocol)방식인 경우, 무선 게이트웨이로 인해 종단 간 보안을 제공하기 어렵다는 문제가 있으며 이를 해결 할 수 있도록 해야 한다. 또한 원격 의료정보시스템 환경에서 다양한 응용 서비스를 제공하기 위해 독립적인 어플리케이션 운영기능을 제공해야 한다. 무선 플랫폼 상의 WAP 게이트웨이에서의 보안의 취약점이라든지, 종단 간 보안 문제를 해결하는 방안중의 하나인 J2ME환경에서의 지원 플랫폼 자체에서의 보안 기능을 이용하여 응용 계층에서의 WPKI
(Wireless Public Key Infrastruc-ture) 구조를 새로이 만들어 사용 할 수 있다.

2.2모바일 의료정보 설계

본 장에서는 모바일 의료정보 시스템의 설계과정에 대해 유선PKI와 무선 PKI의 차이점을 통하여 모바일 의료정보시스템에 적합한 무선 환경에 최적화된 WPKI기술설계에 대해 설명 한다.

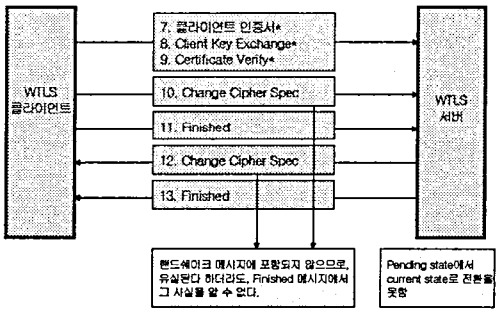
1)USER Interface
무선 환경의 모듈에 접근하기 위해서는 무선환경용 PIN(Personal Identification Number)을 입력받도록 하며 PIN 검증을 통해 인증된 사용자만이 무선 환경의 정보를 접근하고 설정 할 수 있는 인터페이스를 제공한다. PIN정보는 사용자 인증과 무선 환경의 정보의 암/복호 화에 이용된다. 또한 정당하지 않는 사용상의 무선 환경의 사용을 방지하기 위해 LOCK기능을 제공한다.

2) 모바일 환경의 정보관리
모바일 의료정보는 크게 사용자 신상정보(User Profile Information), 영상정보(PACS Image Information) 및 인증서정보(Certificate Information)로 나눌 수 있다.

User Profile Information
사용자 신상정보는 사용자 이름과 담담의사 이름과 같은 사용자 개인정보와 담당환자의 병명을 전달받기 위해 설정하는 의사코드가 있다

PACS Image Information
환자의 이상 유무를 확인하기 위해서는 영상정보와 환자의 이력카드 정보가 저장하고 있다

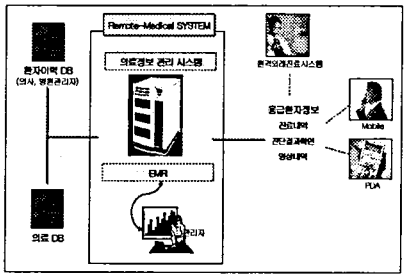
Certificate Information
인증서 정보에는 CA인증루트에 개인 인증서가 저장되어 관리된다.



[그림1]무선 환경에서의 보안

3. 제안 시스템

3.1 의료정보 시스템의 구성



[그림2]모바일에서의 원격 진료 시스템 구성

WAP을 기반으로 한 원격 의료정보시스템은 (그림 2)와 같은 구조를 가진다. 새로운 환자를 입력하면 DB 서버에 저장이 되고, Web server를 통하여 각각 필요한 의사, 간호사의 PC에 전송된다. 그리고 처방전이나 X-ray 촬영 등의 새로운 데이터를 입력하면 바로 서버에 전송되어 저장된다.

3.2 정보보호를 위한 인증 기법

이러한 환경에서 원격 의료 정보시스템의 WPKI의 전체적인 가상 시나리오를 설명하면 (그림3)과 같은 시나리오를 가질 수 있다.

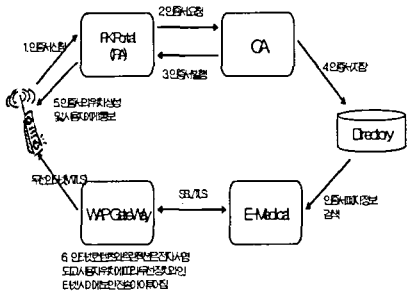
시나리오

①인증요청
- 사용자가 환자 목록을 검색한 후 환자를 선택한 경우
- 환자이름 및 병명 Request를 pc로 전송

②Redirection
-CP에서 WAP Phone을 거쳐 Direct Link Page로 Redirection한다.
-이때 CP에서 전송되는 Information은 CPID, Transaction NO, Transaction Data& Time, 환자 이력을 얻어올 CP의 URL등을 포함한다.

③환자병명 및 영상 요청 ④ 응급 환자정보응답
-Direct Link Page에서 CP로부터 환자정보와 이력 및 영상 접근정보를 가져온다.
-모바일 접근 정보라는 것은 CP에서 환자정보와 영상정보를 사져 올 것인지를 결정하는 모바일 의료정보의 접근에 관한 정보 이다.

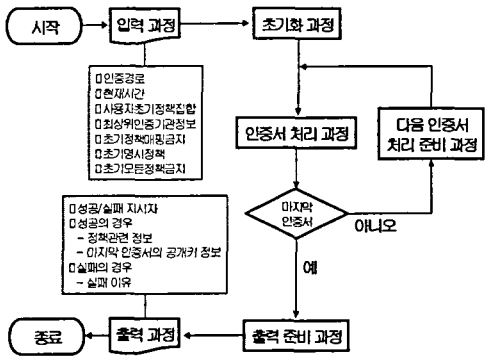
⑤인증요청 암호화 및 전자 서명된 결제정보
-환자의 이상 유무를 판독하고 지시를 내린 정보를 암호화 하고 전자서명하기 위해 모바일 의료정보 시스템 모듈이 실행된다.
-모바일 의료정보의 실행은 담당의사의 비밀번호 확인, 의료정보시스템의 접근(off-line에 설정된 정보를 가져옴), 전자서명의 암호화 수행, Enveloped Data Return의 순서대로 진행된다.
(그림 3)에서 보는바와 같이 모바일 의료정보 시스템의 시나리오는 WAP G/W 인증서이며 WTLS 서버 인증용(minicert)은 WAP 게이트웨이에 발급되고 무선으로 단말기에 전송한다. 사용자 및 서비스 서버 인증서 WTLS 클라이언트 인증용(X.509 cert) 단말기에는 URL만 저장하고 WTLS 서버가 인증 시 디렉토리 에서 가져온다. 전자서명용 (x.509 cert) 단말기에는 URL만 저장하고 응용 서버가 서명 검증 시 해당 directory에서 가져온다.



[그림3]모바일 인증시스템 시나리오

3.4 WPKI 구현 문제점 및 해결 방안

인증서 검증과정은 통신하고자 하는 상대방, 즉 타깃의 공개키 인증서 및 공개키가 올바른지를 검증하기위해서는 검증자 자신의 신뢰 CA와 타깃 사이의 인증경로가 존재하고 이 인증경로가 올바른 것인지를 확인하기 위한 경로 설정 및 검증 작업을 수행해야 한다. 이 방법을 해결하기 위해 단말기에서는 RSA와 ECC를 동시 지원하고 서버는 *WTLS* 및 *X.509* 인증서를 복수 발행하여 해결하였다.



[그림4] 인증서 검증 흐름도)

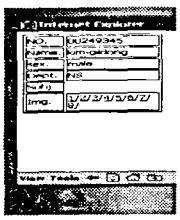
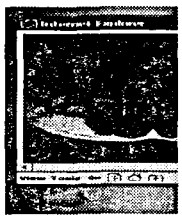
인증서 경로검증은 신뢰당사자의 입력 값을 기반으로 인증서를 검증하기 위해 초기화과정을 거친다. 초기화과정의 결과 값을 통해 인증경로의 첫 번째 인증서부터 인증서처리과정을 수행한다. 만약, 처리된 인증서가 마지막 인증서라면 출력준비과정을 거쳐 신뢰당사자에게 검증한 인증서의 경로검증 결과를 제공한다. 만약, 처리된 인증서가 마지막 인증서가 아니라면, 다음 인증서처리준비과정을 수행한 후 인증경로의 두 번째 인증서를 처리한다. 이러한 절차는 인증경로의 마지막 인증서까지 반복된다. CA 인증서의 무결성 확인이 어려우므로 [그림 8]과 같이 단말기에 데이터를 전송할 때 CA 인증서를 전송 설치한다. X.509 CRL 방식의 CRL 목록을 이용한 인증서 검증이 어려우므로 서버는 Short-lived 인증서를 사용하고 유무선 연동을 고려하여 다음과 같은 사항을 추가하였다.

유선 : RSA기반의 X.509 v3 인증서
무선 : ECC 기반의 WTLS 및 X.509

3.5 제안 시스템의 구현

WAP을 기반으로 하는 원격의료정보시스템은 XML , Mobile JAVA를 이용하여 펜티엄 III

1GHz, WINDOWS 2000 SERVER 환경에서 구현되었다. (그림11)은 모바일 인증 시스템을 기반으로 한 원격 의료정보시스템의 실행 결과를 나타낸 것이다.

<환자인적사항> <영상이미지1>

<영상이미지2>

[그림5]원격 의료 인증 프로그램 결과 화면

V. 결 론

디지털화가 급격히 이루어지고 있는데 개인 사생활, 국가 안보, 경제 질서 등 위협요인을 제거 안전하고 신뢰할 수 있는 통신 환경을 구축할 수 있는 수단으로 보안 기술의 중요성이 강조되고 있다. 원격 의료 정보 시스템의 확산을 위해서는 종합적인 추진 체계의 확립과 법적, 제도적인 장치, 기술 변화에 대한 대응이 이루어져야만 안심하고 사용할 수 있는 통신 환경이 구축될 수 있다. 본 논문 에서는 무선 인터넷 환경에서 전자서명 기법을 사용할 수 있는 시스템을 설계하는데 주안점을 두었고 XML 문서와의 상호 연동 가능성과 전자서명 시스템과 상호 작용 성을 높일 수 있다. 따라서 유선 인터넷 환경에서 사용하던 XML 전자 서명의 장점을 그대로 사용하는 장점을 가지고 있다. 무선 환경의 의료정보 시스템이 활성화되기 위해서는 보안 문제 해결이 필수적이며 현재 추진되고 있는 WPKI 연동을 통한 사용자 인증 및 신뢰성 있는 정보 교환이 이루어 져야 한다. 무선 단말기는 연산속도 및 메모리의 제한으로 유선 환경과는 차별적인 보안 대책이 필요하며 이를 위해 본 논문에서는 알고리즘 수행 속도가 빠르고 작은 키 사이즈로 높은 암호화 강도를 제시 하였다. 향후 연구과제는 WPKI 서비스와의 연동을 필요로 하며 모바일 플랫폼에서의 인증서 사용이 가능하도록 단말기의 지원 등 해결해야 할 과제가 많다. 무선 환경의 의료인증 시스템을 위해서 기존의 PACS 이미지를 현재 새롭게 대두되고 있는 HL7규격에 맞는 연구가 진행 되어야 하겠다.

5. 참고문헌

[1]Marchin Metter, "WAP enabling existing HTML applications", IEEE AUIC, Jan 31, 2000.
[2]Certicom, complete WAP Security
[3] 무선 공개키 기반구조 표준,WAP-217-wpki-20010 424-a
[2]Rick Bender, "Kentucky Field Inspection PDA Application" , IPEC,Conf2002, 2002.
[3] Jo & S 기획 저, "모바일 프로그래밍", 2002.
[4] 홍준호 외 2인 공저, "about WAP" 2001.
[5] 백철화, "원격진료의 발전 및 실례",
[6] http://www.cs.ncl.ac.kr/old/people/wyell.hanna/home.formal/.
[7] WAP White Paper, AU-System Radio. FEb.1999
[8] WAP White Paper, WAP Forum, June 1999.
[9]WapForum :WAP Transport layer End-to-end Security WAP-187-TransportE2
ESec, "Jun-2001.
[9] S.K. Miller, "Facing the challenge of wireless security", Computer.org, pp16-18, 2001.