네트워크를 이용한 PKI기반의 전자처방전 시스템 개발에 관한 연구

하태진* ,조경옥* ,김종우* ,김영진** ,한승조*
*조선대학교 전자 · 정보통신공학부, **데이콤

The research regarding the electronic prescription system development of the PKI base which uses the network

Tae-jin Ha* ,Kyoung-Ok Cho* ,Jong-Woo Kim*,
Young-Jin Kim** ,Seung-Jo Han*
*School of Electronic and Information Communication Eng. Chosun Univ.
**DACOM
E-mail : ha62@korea.com

요 약

현대사회는 정치, 경제, 행정, 문화 등 인류가 더불어 살아가면서 형성된 모든 영역이 정보통신 시스템을 통해 생성되고 유포되는 지식정보 기반의 사회구조로 급속히 진행되고 있고 정보화 시대가 현실화되면서 인터넷의 사용빈도도 급속히 증가하여 개인의 사생활이나 개인정보는 중요한 이슈가 되고 있는 실정이다. 네트워크와 인터넷의 발달로 많은 분야가 오프라인에서 온라인과 전자처리 방식으로 바뀌어 가고 있다. 이러한 정보통신의 변화와 개인정보의 중요성은 의료 환경에도 많은 변화를 가져오고 있다. 현재 의약분업이후 병원과 약국간의 종이 처방전 시스템에 대한 문제점이 발생되고 있다. 또한 전자처방전 시스템이 개발되어 있으나 아직 필수적인 인증 및 보안을 비롯한 각종 정보위협에 대한 대책 수립이 완전하지 않은 실정이다. 따라서 이러한 정보보호 서비스 유지 및 신뢰성을 보장해 줄 수 있는 PKI를 이용한 전자처방전 시스템을 연구하고자 한다.

1. 서 론

현재의 의료 환경은 의료시스템의 발달과 더불어 보건의료정보의 전산화가 가속화되고 있다. 그러나 가장 중요한 처방전 시스템은 구시대의 방법을 벗어나지 못하고 있다. 2000년 이후 의약분업이 실시됨에 따라 사용되는 처방전은 A4를 크기의 종이 처방전을 사용함으로써 일반인들도 쉽게 위·변조가 가능하고, 처방전의 재사용, 의료사고시 분쟁, 병원과 약국의 의료보험료 허위 청구 등 여러 가지 문제점을 야기시키고 있다.

현재 처방전 시스템을 컴퓨터와 인터넷에 접목하기 위한 많은 노력이 계속되고 있다. 그러나 기존의 인터넷은 정보공유의 목적으로 설계되었기 때문에 보안보다는 사용의 편의성과 공동작업의 효율성이 더욱 중시되면서 보안에 대한 대책이 미비하여 환자의 사생활 보호 및 의사와 환자간의 비밀보장을 위한 확실한 보안기술이 요구되고 있는 실정이다. 본 논문에서는 현재의 의료환경에 적합한 네트워크상에서 전달가능한 전자처방전 전달 시스템을 개발하여 환자들이 병원에서 내린 처방전을 일일이 약국으로 들고 가는 수고 없이 작성된 처방전을 보다 정확하게 약국에 전달하여 국민의 불편을 최소화하고 처방전 전달을 간편화하여 처방전 발행에 대한 비용을 절감하고 환자의 조제 시간 단축, 처방전 분실에 따른 불편, 처방 입력시 오류에 의한 약화사고 등 의약분업이 초래할 수 있는 각종 불편사항을 최소화할 수 있으며, 또한 전자처방전의 보안성 향상을 위해 PKI(Public Key Infrastructure)기반의 전자처방전시스템을 개발함으로써 암호키 갱신, 복구 위탁 등과 같은 키 관리, 인증서 생성 및 취소 관리, 그리고 인증 정책 관리와 같은 서비스의 제공이 가능하다. PKI에 의해서 구현되는 계층적 인증구조나 상호 인증 방식에 의하여 조직간의 안전한 데이터 통신을 위한 신뢰 관

계를 형성할 수 있게 된다.

2. 연구 배경 및 목적

2.1 현재 처방전 시스템

2.1.1 현황 및 문제점

현재 의약분업 시행으로 보건의료기관이 진료후 외래환자에게 A4규격의 종이처방전을 2매 발행하면, 환자는 이를 소지하고 약국을 전전하여야 하며 약국은 종이처방전을 받아 조제한 후 EDI청구를 위해 이를 다시 전산 입력하여 약제비를 건강보험심사평가원에 청구해야 하는 실정이다. 이러한 시스템은 현재 많은 문제점을 야기시키고 있다. 종이에 의한 처방전은 일반인들도 쉽게 위·변조가 가능하다. 또한 환자보관용 처방전을 재 사용하는 사례가 늘고 있다. 또한 의료사고 분쟁시 쉽고 빠르게 입증하기가 힘들다는 단점이 있다. 또한 약국은 처방전을 5년간 보관해야하기 때문에 보관장소 문제나, 화재나 침수 등 훼손에 대한 문제점들을 가지고 있다. 전자 처방전 시스템은 이러한 많은 문제점들을 해결할 수 있다. 그러나 정부는 인터넷으로 보낸 처방전은 위조나 해킹의 가능성이 있으며, 의료사고나 사생활 침해의 소지가 있다는 이유로 아직은 공식 인정을 유보하고 있는 실정이다.

2.1.2 개선방안

보안기술이 발달해 모든 분야에서 전자서류를 법적 문서로 인정하고 있는 현실에 부합되지 않게 전자서명된 전자처방전의 금지는 환자, 의료기관 및 약국의 불편을 초래하고 효율화를 저해하고 있다.

전자 처방전에 대한 정부의 우려를 일축하기 위하여 보다 안전하고, 편리한 전자처방전 시스템의 개발이 필요하다. 본 논문에서는 PKI를 이용하여 전자서명에 의해서 위·변조가 불가능한 전자 처방전 시스템을 설계한다. 의사의 개인키가 인감을 대신하고, 약국의 개인키가 사용여부를 날인하는 역할을 하게된다.

3. 처방전 시스템 알고리즘 제안

본 논문에서 제시하는 처방전 시스템 알고리즘에서 설명하는 전자처방전 시스템의 구성, 보호 범위와 인증에 필요한 기술을 설명하고자 한다.

3.1 전자처방전 시스템의 구성

전자처방전 시스템의 구성은 의사가 처방전을 처방하였을 때 처방전은 영구적으로 보관하여야 하며, 인터넷을 이용함으로써 보다 편리하고 간편하게 처방전을 발급 및 사용이 가능하다는 장점이 있다. 그러나 처방전을 약국에서 재사용이 가능하다는 단점도 존재하게 된다. 이를 해결하기 위하여 보호 범위와 인증할 수 있는 처방전 시스템 알고리즘을 제안한 것이 핵심이라 할 수 있다.

3.2 전자처방전의 보호 범위

의사가 처방전을 처방하였을 때 이를 보호할 수 있어야 하며, 처방전을 접수한 약국은 이를 가지고 약을 처방하였을 때 이 등록과정을 인증하여야 한다. 또한 의료 분쟁이 발생하였을 때 이를 증명할 수 있는 근거 제시할 수 있는 자료 및 개인이 어떤 약을 처방 받았는지를 알수 있도록 하여야 한다.

3.3 인증 방법

[표 2] 처방전시스템에서 사용되는 기호

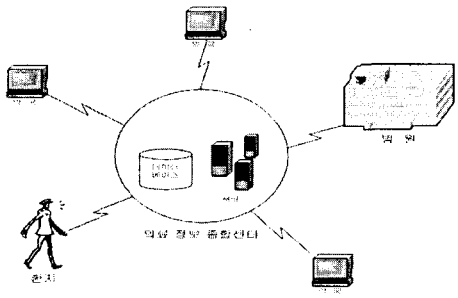
기 호	설 명
CA	의료 정보 종합 시스템
A	환자
HD	병원 의사
H	약국
Certificate A	A의 인증서(환자)
Certificate HD	HD의 인증서(의사)
Certificate H	H의 인증서(H)
M	문서(처방전)
H	Hash 알고리즘
ER	공개키 알고리즘 암호화
DR	공개키 알고리즘 복호화
E	관용키 알고리즘 암호화
D	관용키 알코리즘 복호화
KU	공개키
KR	비밀키

공개키 기반 구조인 PKI의 대표적인 알고리즘 RSA을 이용하여 서로간의 신뢰성 있는 처방전 교환과 웹 기반의 전자처방전 교환을 위한 전자처방전 시스템이다. 다음의 그림은 구현될 전자처방전의 전체적인 구성도이다.

그림[1]은 의료 정보 종합시스템에서 병원과 약국간의 연결을 담당하고 있으며, 병원과 약국에 관련된 여러 가지 사항들이 데이터베이스에 저장된다.

전자처방전이 처리되는 과정은 우선 환자가 병원에서 처방전을 발급받게 되면 의료 정보 종합 시스템은 환자의 의료 카드 번호와 환자의 인증서를 바탕으로 어떤 사용자가 처방전을 발급받게 되는지 과정을 거치게 된다. 환자의 인증이 확실하게 되면 의사는 환자에게 전자처방전을 일련번호를 부여하여 처방하게 된다. 이를 받은 환자와 의료 정보 종합 시스템의 데이터베이스에 저장되어 환자가 약국에서 약을 처방받을 경우 약국의 요청에

의료 정보 종합 시스템은 응답하게 된다. 이때 전자처방전을 받아서 처방전대로 약을 조제하였다는 사실을 확인 하여야 한다. 만약 이러한 부분이 존재하지 않는 다면 환자는 여러 군데의 약국에 가서 같은 약을 여러 번 조제를 받을 수 있을 뿐 아니라 약국에서는 한번 사용한 처방전을 재사용이 가능하기 때문이다.

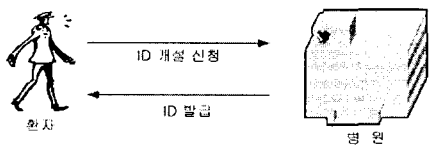


[그림 4] 시스템 기본 구성도

3.3.1 ID 개설

① 의료 정보 종합 시스템 ID 개설 신청 : 의료보험에 적용된 사실을 바탕으로 의료보험증과 신분증을 제시하여 병원에 진료카드를 작성과 동시에 의료 정보 종합 시스템의 접속 ID 및 비밀 번호를 신청한다.

② 의료 정보 종합 시스템 ID 발급 : 병원에서는 본인 확인 후 병원은 의료 정보 종합 시스템의 대리인 자격으로 의료 정보 종합 시스템의 ID 및 비밀번호를 발급한다. 개인은 발급한 ID와 비밀번호를 발급한다. 개인은 병원에서 발급한 ID와 비밀번호로 인터넷을 통하여 의료 정보 종합 시스템에 접속한 후 공개키와 비밀키를 발급받는다.



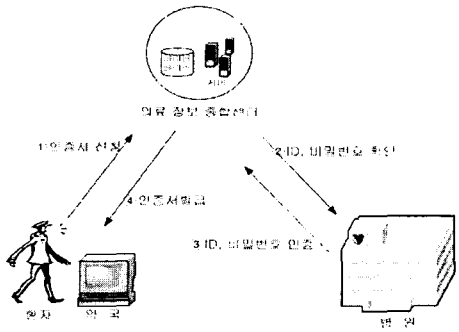
[그림 5] ID 개설

3.3.2 인증서 발급

① 환자 인증서 신청 : 병원에서 개설한 ID 및 비밀번호를 바탕으로 의료 정보 종합시스템에 인증서를 신청한다.

② ID 및 비밀번호 확인 : 병원은 병원에서 발급한 ID, 비밀번호, 개인정보가 일치하는지 여부를 의료 정보 종합시스템에 통보한다.

③ 인증서 발급 : 환자에게 병원의 자료를 바탕으로 인증서를 발급한다.



[그림 6] 인증서 발급

3.3.3 전자처방전 발급

① 병원에서는 환자의 처방전 발급시점마다 인증서와 일련번호를 의료 정보 종합센터에 전송한다. 처방전의 정보는 의료 정보 종합센터에 모든 내역이 저장되고 환자는 모든 내역을 볼 수 있다. HD(병원의사)는 문서 M(처방전, 환자개인정보)를 Hash하고 HD(병원의사)의 비밀키(KRhd)로 암호화하는 과정을 통하여 문서에 지문과 자신의 서명을 한다.

$$[\ ER_{KRa}\ \{H(M)\}\ ]$$

차후에 발생될 전송여부와 변조여부의 시비에 대비하여 Hash 된 문서(H(M))를 보관한다. 그리고 M, ERKRa{H(M)}, Certificate HD를 압축하고 세션키(Ks)를 사용하여 관용키 암호알고리즘으로 암호화 한다.

$$[\ E_{Ks}\{Z\{M\,||\,ER_{KRhd}\{H(M)\}\}\,||\,\text{Certificate HD}\,||\,\text{일련번호}\}\ ]$$

세션키(Ks)는 의료정보종합센터의 공개키(환자의 공개키)로 암호화한 후 [ERKUca{Ks}] 세션키로 암호화된문서와 같이 의료 정보 종합센터(환자)에 전송한다.

② CA(의료정보종합센터(환자))는 병원에서 전송 받은 내용을 복호화하여 정당한 문서이면 데이터베이스에 등재한다. CA는 HD(병원의사)에게서 받은 문서 중[ERKUca{Ks}]를 CA(A)의 비밀키를 사용하여 세션키(Ks)를 구한다.

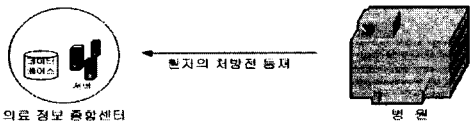
$$\{DR_{KRca}\{ER_{KUca}\{Ks\}\} = Ks\}$$

구한 세션키(Ks)를 사용하여 관용키 암호화된 부분을 복호화 한다.

$$[\ DKs\{EKs\{Z\{M\,||\,ER_{KRhd}\{H(M)\}\,||\,\text{Certificate HD}\,||\,\text{일련번호}\}\}$$

$=Z\{M||ER_{KRhd}\{H(M)\}||Certificate\ HD||일련번호\}]$

압축을 풀어내고 Certificate HD를 통하여 유효한 공개키인지 확인하여 유효하지 않으면 재전송을 요구한다.



[그림 7] 전자처방전 발급

[표 3] 처방전 발급 내역

순서	환자	의사ID	일련번호	처방전내역
1	CHO	HA	CHO0001	내과진료
2	CHO	KIM	CHO0002	피부과진료
3	CHO	HA	CHO0003	내과진료
4	CHO	CHUNG	CHO0004	치과진료

3.3.4 약 조제

① H(약국)는 A(환자)가 약을 받기위해 왔을 때 A의 개인신상정보를 입력하여 처방전을 받아본다.

② 처방전처리내역은 H(약국)의 비밀키로 암호화 한 후 CA(의료 정보 종합센터)의 공개키로 암호화하여 CA에게 전송한다.

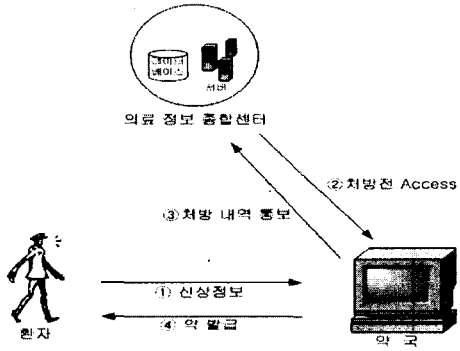
$$ER_{KUca}\{ER_{KRh}\{Certificate\ H||일련번호\}\}$$

③ CA(의료 정보 종합센터)는 H(약국)으로부터 받은 내용을 CA의 비밀키를 사용하여 복호화 한다.

$$DR_{KRca}\{ER_{KUca}\{ER_{KRh}\{Certificate\ H||일련번호\}\}$$

④ H(약국)의 공개키를 사용하여 복호화한 후 Certificat H, 일련번호를 통하여 유효한가를 확인하고 유효하지 않으면 재 전송을 요구한다.

⑤ CA(의료 정보 종합센터)는 H(약국)에서 보내온 내용이 유효하면 처방전를 처리한다.



[그림 8] 약 조제

4. 처방전 시스템 알고리즘 구현 및 시뮬레이션

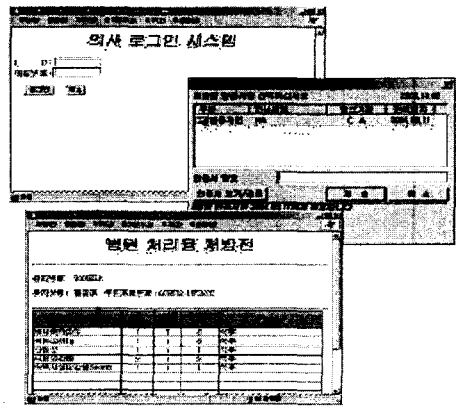
4.1 처방전 시스템 시뮬레이션 환경

- 운영체제 : Windows 2000 Server, Windows XP
- 개발언어 : ASP, MS-SQL 2000 Server
- 서 버 : SUN ULTRA 10
- 클라이언트 : 펜티엄-4

4.2 처방전 발급

① HD(병원의사)는 ID 및 비밀번호를 입력하여 로그인한 후 CA(의료 정보 종합센터)에서 발급받은 개인인증서를 제출함으로써 본인 여부를 확인할 수 있다.

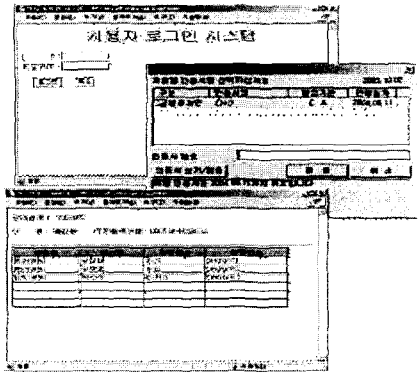
② HD(병원의사)는 A(환자)의 처방전을 작성한 후 제안된 알고리즘을 사용하여 CA(의료 정보 종합센터)에 암호화하여 전송한다.



[그림 9]

4.3 환자 개인 처방전 발급여부 확인

① A(환자)는 인터넷을 통하여 로그인후 인증서를 제출 후 HD(병원의사)가 처방한 처방전의 발급여부를 확인 할 수 있다.

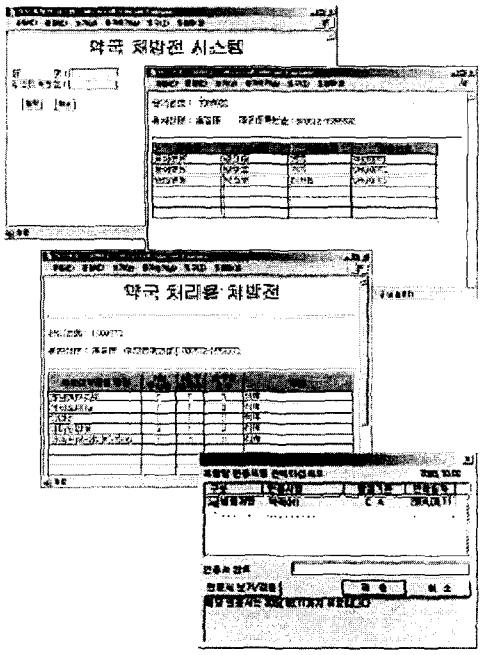


[그림 10]

4.4 약 조제

① H(약국)는 A(환자)의 개인정보를 입력함으로서 A의 처방전의 처리상태를 알 수 있고 처리하고자 하는 처방전을 선택하여 HD(병원의사)가 처방한 처방전의 내용을 확인가능하다.

② H(약국)는 처리여부를 인증서와 함께 CA(의료 정보 종합센터)에 제출함으로서 처방전의 재사용을 막을 수 있다. 또한 분쟁의 문제가 생겼을 경우 인증서를 토대로 하여 시시비비를 가릴 수 있게 된다.



[그림 11]

5. 결 론

현대 사회는 모든 것을 네트워크와 인터넷으로 처리하려고 하는 시대인 만큼 전자처방전 시스템 활성화에 있어서 가장 큰 문제인 개인정보 보호 문제를 해결하는데 초점을 두고 시스템 개발에 관한 연구를 진행하였다. 개인정보나 진료기록 같은 정보가 유출되면 개인에게 치명적일 수 있고 악용될 소지가 있다. 이에 본 연구에서는 PKI에 기반을 두고 RSA 공개키 암호방식을 이용한 시스템을 개발하였다. 제안한 시스템은 환자의 정보를 보호 및 처방전의 재사용성을 완벽하게 차단하고, 위·변조가 불가능하여 의료 분쟁의 문제가 발생하였을 때의 문제점을 쉽게 해결할 수 있게 알고리즘을 제안하였다. 또한 본 시스템을 이용하여 의료보험료 부당 청구, 환자의 불편함, 약국에서의 처방전 보관 등 여러 가지 문제점들을 해결할 수 있다.

6. 참고 문헌

[1] S. J. Han, H. S. Oh, "Design of Extended-DES cryptography," Proc- eeding of the IEEE International Symposium on Information Theory, pp.353-359, July 1995.

[2] S. J. Han, "The Improvement Data Encryption Standard(DES) Algorith- m," Proceedings of ISSSTA '96, IEEE, pp.1167-1171, Sept. 1996.

[3] S. J. Han, "Improved-DES Crypto- system Design." Journal of Kiss, Vol.24, no.1, pp.57-67, Jan. 1997.

[4] O. Goldreich and R. Ostrovsky, "Software protection and simulation on oblivious RAMs," Revised, Oct. 1995.

[5] David Aucsmith,"Tamper resistant software," Information Hiding-Procee- dings of the First International Workshop, pp.317-333, 1996.

[6] Simson garfinkel, PGP(Pretty Good Privacy), O'Reilly & Associates,Inc. 1995

[7] Housley, Russ, "Best Practices Guide for Deploying Public Key Infrastructure", Wiley, 2001.

[8] Security of Electronic money, Bank for International Settlements, 1996

본 연구보고서는 정보통신부 정보통신연구진흥원에서 지원하고 있는 정보통신기초연구지원사업의 연구결과입니다.(University fundamental Research Program supported by Ministry of Information & Communication in republic of Korea)