J. Biomed. Eng. Res.
Vol. 24, No. 6, 533-541, 2003

진료정보 공유를 위한 IC카드 기반 병원 진찰 카드 통합 시스템 구축

박두희* · 이남용* · 이기한** · 김윤정**

숭실대학교 정보과학대학 컴퓨터학부*, 서울여자대학교 정보통신대학 컴퓨터학부**

(2003년 8월 20일 접수, 2004년 1월 6일 채택)

Implementation of A Patient Card Integrating System Using by IC Card To Share A Medical Information

D.H. Pack*, N.Y. Lee*, K.H. Lee**, Y.J. Kim**

School of Computing, College of Information Science, Soong-Sil University*,
Department of Computer Engineering, College of Information and Communication Seoul Women's University**

(Received August 20, 2003. Accepted January 6, 2004)

요 약 : 본 논문은 환자 진료정보 공유 시 환자의 개인 및 진료 정보 보호 문제점을 해결하기 위해서 여러 장의 진찰카드를 하나의 IC카드로 통합하기 위한 시스템을 개발하였다. 먼저, 진료정보 공유를 위한 최소데이터세트를 정의하였고, 이 최소데이터세트를 통합 병원 진찰 IC 카드에 구현하고 발급할 수 있는 발급 시스템을 개발했다. 환자의 개인정보 보안 및 인증을 위해서는 윈도우 2000 기반 전자서명 인증센터를 구축하고 3-DES를 적용한 IC 카드 기반의 통합 병원 진찰 IC 카드를 개발했다. 기존 병원 전산시스템과 효율적인 연동을 위한 통합 병원 진찰 IC 카드에 의한 진료접수/예약 시스템을 개발했다. 본 연구에서 개발한 통합 병원 진찰 IC 카드 시스템을 11개 병원에서 1,000명의 환자에게 적용한 결과, 시범 대상 병원들의 환자 진료 접수/예약뿐 아니라 정보 공유의 안정적 확장을 도모할 수 있는 기반을 마련할 수 있었다.

Abstract : In the paper, the health card system to integrate several cards into one card for protecting patient's privacy and security problems is proposed. Firstly, it is defined the minimal data set for integrating several patient cards into one card using IC card, and developed the issuing system to issue the integrated patient IC card. In order to secure and certificate a patient's personal information, the integrated patient IC card has applied 3-DES and the PKI certificate authority based Windows 2000 is established. The receipt and reservation system for taking care of a healthcare has developed to cooperate with the existing hospital computer system. The integrating patient IC card system proposed in this paper is implemented to 11 hospitals and used for 1,000 patients. On the result of the simulation, the proposed system can receive or reserve for a patient to take care of healthcare in the simulated hospitals and also establish the basis of the mechanism to share a medical information.

Key words : Patient card, Patient card integrating system, Certificate authority, IC card, Security

연 구 배 경

정보기술의 급격한 발전으로 의료분야의 정보화도 가속화하고 있어, 각 의료기관들은 병원업무 전반의 정보를 통합화하는 추세이다. 이러한 의료기관들의 정보화는 의료기관간 진료정보 공동활용의 가능성을 증대시키고 있다. 의료기관간에 진료정보의 공동활용에 대한 환자들의 기대감도 고조되고 있으며, 대기시간 감소 등의 효과가 기대될 뿐 아니라, 의료기관간 협진 체제의 가능성 증대를 통한 의료전달체계 확립에 기여할 수 있다는 점에서 그 필요성이 대두되고 있다[1].

현행 의료법에 따르면 진료상 목적으로 다른 의료기관의 진료정보 열람이나 사본의 송부에 대한 의무규정이 있으며(의료법 제 20조), 이는 진료정보 공동활용을 기본적으로 뒷받침해 주는 규정이다[2]. 그리고, 전산망보급확장과 이용촉진에 관한 법률에서는 정보의 공동활용을 긍정적으로 평가, 지원하고자 하는 정부의 의지를 담고 있다[3].

진료정보를 공유할 경우에 환자들은 개인정보의 무단 사용

본 연구과제는 "2003년도 서울여자대학교 교내 연구비"에 의해서 진행된 결과입니다.

통신저자 : 이기한, (139-774) 서울시 노원구 공릉 2동 126번지
서울여자대학교 정보통신대학 컴퓨터공학과 Mars Lab.
Tel. 02)970-5698, Fax. 02)970-5981
E-mail. knight@swu.ac.kr

가능성에 대한 우려가 매우 높으며, 선진국에서는 환자의 정보 보호를 위해 환자의 동의가 필수적으로 포함되도록 규정하고 있고, 우리나라의 경우에도 필수적으로 요구된다. 이러한 문제는 IC카드를 이용하면 된다[4]. 본 논문에서는 개인정보를 포함한 진찰카드 정보를 철저히 보호할 수 있는 기술로서 가장 보안 신뢰성을 가진 IC 카드를 이용하여 해결할 수 있는 방법을 제시한다.

대부분의 환자는 여러 병원들을 내원하기 때문에, 여러 장의 진찰카드를 소지한다. 병원의원 및 관련기관에서는 초진 환자의 경우에 진찰카드를 발급하기 때문에 매우 많은 환자들이 중복하여 발급받으므로서 많은 예산을 낭비하고 있고, 관리 및 유지에 많은 문제가 있다[5]. 이를 해결하기 위해선 본 논문에서는 여러 장의 진찰 카드를 하나의 카드로 통합하여 관리하는 방법을 제시한다.

현재 IC 카드를 이용한 통합 진찰카드를 추진하고 있는 서울대병원, 서울아산병원, 삼성서울병원의 현황을 조사한 결과, 표준화되지 않은 서로 상이한 플랫폼을 사용하고, 암호화 및 PKI 등의 보안 기법이 제대로 동작을 하지 못하고 있다. 따라서, 본 논문에서는 이러한 문제점을 해결하기 위해서 환자가 어느 병원을 방문하더라도 개인정보를 포함한 자신의 병력을 보호하고 각 병의원 및 종합전문요양기관에는 현재 사용하고 있는 OCS와는 별도로 분리된 시스템을 구축하여 보안 및 기존업무 진행에 차질을 발생하지 않는 표준화된 시스템을 구현하고자 한다.

진찰카드 정보 표준화

진료정보를 공유하기 위해서는 많은 부분이 표준화가 되어야 한다. 현재 사용되어지고 있는 병원진찰카드는 병원마다 환자의 개인정보 및 관련정보를 저장 방법이 서로 상이하다. 따라서, 병원 진찰카드를 통합하기 위해서는 환자의 개인정보 및 진료예약 등의 관련정보에 대한 코드 및 서식의 표준화가 이루어져야 한다.

진찰카드를 통합하는 방법은 크게 2 가지다. 먼저, 병원에서 사용되는 진찰카드의 정보를 모두 모아서 한 카드에 저장한 후에, 이 통합 진찰카드를 병원에서 사용할 때에는 해당병원에 있는 진찰카드 수납시스템이 해당 진찰카드 정보만을 추출하여서 처리하는 방법이다. 이 방법은 기존 병원 시스템을 그대로 유지하면서 진찰카드만을 교체하면 되므로 매우 경제적이다. 하지만, 진찰카드 정보를 모두 수용할 수 있는 카드의 용량이 기본이 되어야 한다. 또한, 이 통합 진찰카드를 사용하면 다른 병원에서 이 통합 진찰카드를 사용할 경우에 다른 병원에 있는 진료정보를 공유하기 위한 새로운 시스템이 도입이 되어야 하므로 엄밀하게 말하면 진정한 의미의 표준화 및 통합이라고는 볼 수 없다.

두 번째 방법은 병원에서 필요한 모든 진찰카드의 정보 중에서 최소데이터세트(minimal data set)을 추출하고 이를 통합 병원 진찰 IC 카드(Integrated Patient Data IC Card, 이하 IPIC 카드)에 저장하고 사용하는 방법이다. 이 방법은 기존 병원 진찰카드 수납시스템을 변경해야하는 단점을 가지고 있다. 하지만, 이 IPIC 카드를 사용하면 해당 병원에서도 손쉽게 다른 병원의 환자 진료정보에 접근할 수 있어서 매우 효율적인 시스템을 구축할 수 있다. 본 논문에서는 두 번째 방법을 사용하여 IPIC 카드 시스템을 구축하고자 한다.

전국의 종합전문요양기관을 방문한 705명의 환자를 대상으로 설문조사를 실시한 결과, 진료상세정보(진료기록 및 각종 검사결과 등)의 공동활용에 대부분 긍정적으로 생각하고 있으며 진료일, 진료기관, 진단명 등 진료기관 방문정보와 주민등록 사항은 68.3%, 보험사항은 64.9%등에 대한 공유에 대해서도 절반 이상의 응답자가 긍정적으로 받아들이고 있다. 진료 정보 공유를 위한 환자기본정보는 87.4%로 매우 높은 의견을 보이고 있다[1].

따라서, IPIC 카드에 수록되는 최소 진찰카드 정보 세트는 표 1과 같이 개인 정보, 장애 정보, 보험 정보, 그리고 병원 정보로 정의할 수 있다. 여기서, 개인정보 항목 및 장애정보는 현재 국내의 병원에서 사용하고 있는 일반적인 진찰카드의 정보와 ISO/TC215/WG5에서 제시하는 정보를 비교하여 꼭 필요한 최소한의 정보만을 추출해 낸 것이다[6,7]. 그리고, 의료보험정보 및 병원정보는 국내 여건에 맞추어서 필요한 정보를 추출한 것이다. 이는 ISO/TC215/WG5에는 없는 항목이다.

첫 번째 개인 정보 항목은 주로 ISO/TC215/WG5에서 제시하는 정보하는 항목들이다. 하지만, 특기 사항은 국내 여건을 감안하여 추출한 정보이다. 특기 사항은 일반 정보에는 없는 사항이지만, 병원에서 환자를 구분할 때 사용되는 정보로 꼭 필요한 정보이다. 특기 사항은 인공신장(1), 국가유공자(2)중 하나를 선택할 수 있다. 해당사항이 없는 경우에는 선택하지 않아도 된다. 화면에는 인공 신장과 국가 유공자로 보이지만, 카드나 데이터베이스에 저장될 경우 1과 2로 입력된다. 따라서 길이도 1byte로 설정하였다.

두 번째 항목은 장애정보이다. 이는 ISO/TC215/WG5에서 제시한 항목과 복지부가 제시한 항목의 최소항목을 추출한 것이다. 처방전 항목에는 없는 내용으로 현재 의료 보험 카드에 또한 이 정보가 없다. 장애인의 경우 따로 장애인 카드가 발급되기 때문이다. 이 정보를 선택적으로 선택할 수도 있지만, 반드시 일어 날 수 있는 상황으로 카드에도 공간을 할당 해 놓은 것이다. 또한 일반 의료보험 카드에도 장애정보를 입력하는 것은 국제적으로 사용되는 일반 항목으로 미래에 국제적으로 통합될 경우를 대비하여 국내정보에도 입력시켜 해당되지 않은 경우는 빈 공간으로 남겨 놓는다[6].

세 번째 항목은 의료보험 정보 항목이다. 이 항목은 국내 여건에 맞도록 조정한 항목으로 ISO/TC215/WG5에서는 정의되지 않은 항목이다. 산재보험의 정보 중에 산재 연장 승인신청일과 의료보험 취득일, 종료일의 항목이 병원에서는 공통으로 사용되고 있다. 하지만 의료보험 유효기간 항목이 있어, 프로그램으로 유효기간이 지나고 나면 사용이 불가능하게 하여 취득일과 종료일을 저장하지 않았다. 의료보험 유형은 국가가

표 1. IPIC 카드의 최소데이터 세트
Table 1. Minimal data set for IPIC Card

분류	Data 명			Data Type	Length
개인 정보	환자이름			String	10
	환자주민등록번호			String	13
	환자생년월일			String	8
	환자우편번호			String	7
	환자주소			String	60
	환자전화번호			String	14
	환자특기사항			String	1
	환자보훈번호			String	13
장애 정보	장애취득일			String	10
	장애종별			String	10
	장애등급			String	10
의료 보험 정보	증번호/산재성립번호			String	20
	조합기호/산재지정기호			String	20
	피보험자명			String	10
	피보험자관계			String	1
	산재발생일			String	10
	의료보험유효기간			String	10
	피보험자주민등록번호			String	14
	의료보험유형	보험구분	코드	유형	String 2
		국민건강보험	12	공단 공상	
		의료보호	22	보호 2종	
		산재보험	32	산재본인 100%	
		자동차보험	42	자손	
		기타	51	일반	
병원 정보	환자차트번호			String	10
	의료기관기호			String	15
	의료기관명칭			String	40
	의료기관전화번호			String	14
	의료기관 fax번호			String	14
	의료기관 E-Mail			String	35
	진료과			String	2
	진료일			String	10

정해 놓은 여러 가지 보험 유형 중에 하나를 선택할 수 있게 하였다. 그리고, 의료보험 구분은 크게 국민 건강보험, 의료보호, 산재 보험, 자동차 보험, 기타로 나눠진다. 구분되어진 보험의 유형에 관련된 코드는 현재 병원들에서 사용되고 있는 것으로 서로 다른 OCS에서도 통용되는 항목들이다.이런 유형들은 병원에서 의료비를 정산할 때 사용되는 항목으로 전체적으로 통합된 데이터로 사용되어야 한다.

마지막 항목은 병원 정보 항목이다. 병원 정보 항목은 국내 여건에 맞도록 조정한 항목이다. 이 항목의 경우 한 병원진행한다면 고정된 값으로 운영될 것이다. 하지만, 여러 병원에서 통합되어 운영되는 것으로 환자의 차트번호도 다르게 책정이 된다. 의료기관기호는 정부에서 할당한 것이며, 진료과의 경우 병원에서 운영하고 있는 더 많은 과가 있으나, 일반적으로 대부분의 병원에서 운영되고 있는 진료과를 선택하였다.

병원진찰카드 통합용 IC 카드 시스템 개발

본 논문에서는 (주)현대정보가 개발한 HCOS(Hyundai Chip Operating System)를 기반으로 한 IC 카드를 사용하여 구현한다[11].

1. 통합 병원 진찰 IC 카드 메모리 설계

IC 카드의 메모리는 위에서 정의한 IPIC 카드용 표준 최소 데이터세트를 수용하도록 그림 1과 같이 진찰카드 MF(Master File), 진찰카드 DF(Dedicated File), 그리고, 4개의 개인 정보 EF(Elementary File), 장애 정보 EF, 의료보험 정보 EF와 병

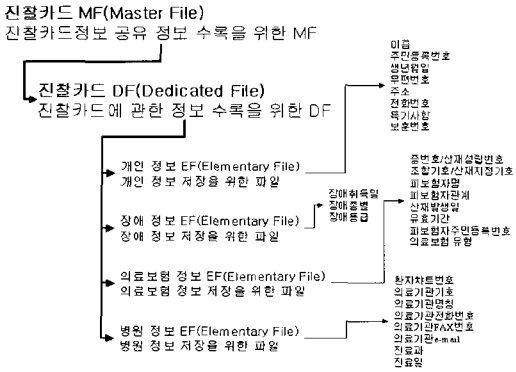

그림 1. IPIC 카드의 메모리 구조
Fig. 1. Memory Structure of IPIC card

원 정보 EF의 구조로 설계된다. MF는 IC 카드 파일 구조의 루트를 나타내는 필수 유일의 전용 파일이며, DF는 파일제어 정보 및 메모리 할당을 포함하는 파일로 EF나 DF의 모파일이 될 수 있고, EF는 동일한 식별자를 갖고 있는 데이터 또는 레코드의 집합으로 다른 EF의 모파일이 될 수 없다[8].

2. 통합 병원 진찰 IC 카드 메모리 접근 권한 및 인증 설계

IC 카드로 구현된 IPIC 카드는 표 2와 같이 여러 그룹이 사용하게 된다.

따라서, IPIC 카드를 사용하는 사용자의 권한 부여는 동일한 접근 권한을 공유하는 그룹으로 설계되어야 한다. 표 6과 같이 의료기관에 관련된 사용자는 6개의 그룹으로 생성되고, 의료기관을 이용하는 사용자는 1개의 그룹으로 생성한다. 사용자 또는 각 그룹에 대한 인증 방법으로 암호키와 개인식별번호(Personal Identification Number, 이하 PIN)를 이용한다. 각 사용자 그룹에 따른 IPIC 카드의 DF 및 EF에 대한 접근 권한을 정의했다.

3. 병원진찰카드 통합용 IC 카드 보안 인증 시스템 개발

IPIC 카드에 수록된 진찰정보에 대한 보안은 매우 중요하다. 본 연구에서 채택한 HCOS가 탑재된 IPIC 카드는 개인정보 등의 진찰카드 정보를 보안하기 위해서 패스워드에 의한 엔티티 인증, 키에 의한 엔티티 인증, 개인 정보 등의 진찰카드 정보 인증과 진찰카드 정보 암호화 등의 방법을 개발했다. 각각의 보안 체계는 다음과 같다[9]:

- 패스워드에 의한 엔티티 인증: 카드 소지자의 정당성 확인
- 키에 의한 엔티티 인증: 단말기의 정당성 확인
- 진찰카드 정보 인증: 단말기의 정당성 확인
- 진찰카드 정보 암호화: 단말기와 카드간의 정보 암호화

1) 패스워드 및 키에 의한 엔티티 인증

패스워드 및 키에 의한 엔티티 인증은 IPIC 카드 처리 단말기, PC, 병원 IPIC 카드 등의 정당성을 외부가 자신의 내부 EF에 기록되어 있는 패스워드 및 키와 동일한 패스워드 및 키를 가지고 있는가를 외부 인증 명령을 통해 확인한다. 외부는 Get Challenge 명령을 이용하여 IPIC 카드로부터 난수를 읽어와 이를 인증하려는 패스워드 및 키로 암호화한 후 암호화 값을 다시 세션 키로 MAC(Message Authentication Code)을 계산하여 그 결과를 External Authenticate 명령으로 IPIC 카드에 보내준다. IPIC 카드는 이 값과 자신이 내부에서 위와 동일한 방법으로 계산한 값과 비교하여 두 값이 서로 같으면 외부가 정당하다고 판단한다.

2) 진찰카드 정보 인증

진찰카드 정보는 외부로부터 입력된 진찰카드 정보의 정당성을 MAC를 통하여 확인한다. MAC은 IPIC 카드에 입력될 진찰카드 정보를 이용하여 만들어지는 4바이트의 진찰카드 정보로 입력 진찰카드 정보와 함께 IPIC 카드로 보내진다. IPIC 카드는 입력된 진찰카드 정보를 이용하여 외부에서 MAC을 만든 방법과 같은 방법으로 새로운 MAC을 계산하여 외부에서 입력된 MAC과 IPIC 카드가 계산한 MAC이 같은가를 비교하여 같을 때 외부에서 입력된 진찰카드 정보가 정당한 진찰카드 정보라고 판단한다.

진찰카드 정보는 외부로부터 입력된 진찰카드 정보의 정당성을 MAC를 통하여 확인한다. MAC은 IPIC 카드에 입력될 진찰카드 정보를 이용하여 만들어지는 4바이트의 진찰카드 정보로 입력 진찰카드 정보와 함께 IPIC 카드로 보내진다. IPIC 카드는 입력된 진찰카드 정보를 이용하여 외부에서 MAC을 만든 방법과 같은 방법으로 새로운 MAC을 계산하여 외부에서 입력된 MAC과 IPIC 카드가 계산한 MAC이 같은가를 비교하여 같을 때 외부에서 입력된 진찰카드 정보가 정당한 진찰카드 정보라고 판단한다.

표 2. IPIC 카드의 사용자 분류 및 접근 권한
Table 2. User classification and access control for IPIC card

항목	Hospital Group	Doctor Group	Nurse Group	Pharmacy Group	Pharmacist Group	Staff Group	Patient Group
구성원	병원	의사	간호사	약국	약사	관계자	환자
인증 프로토콜	암호키(3-DES)	PIN	PIN	암호키(3-DES)	PIN	PIN	PIN
개인정보 EF	O	△	△	O	△	O	O
장애정보 EF	O	△	△	O	△	△	△
의료보험 정보 EF	O	△	△	O	△	△	△
병원정보 EF	O	△	△	O	△	O	△

O : 읽기/쓰기 가능, △ : 읽기만 가능

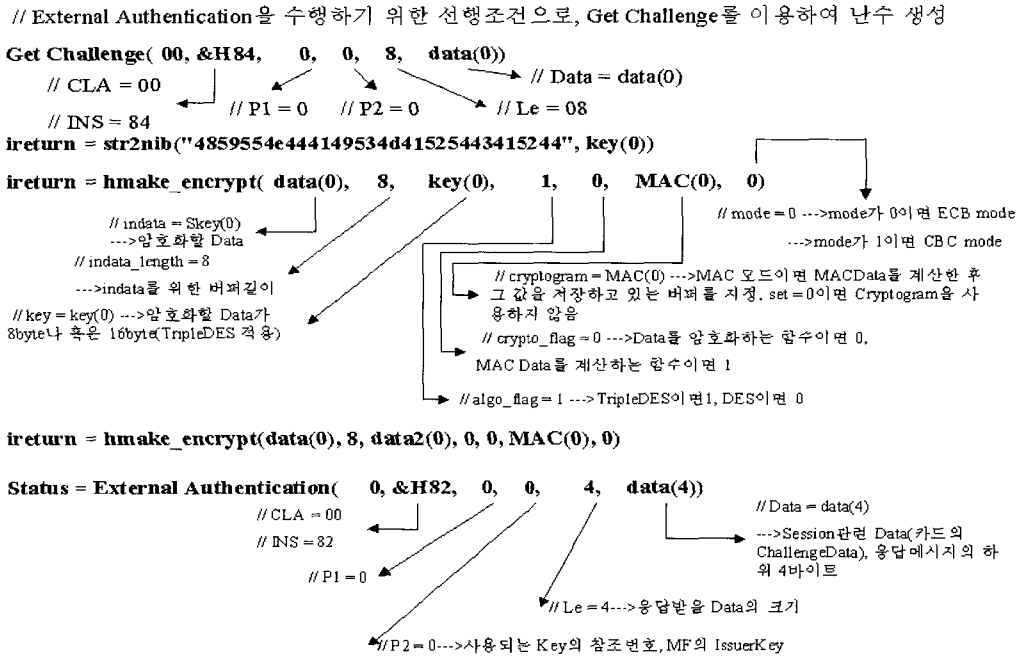

그림 2. IPIC 카드 정보 암호화
Fig. 2. Encryption of IPIC card information

3) 진찰카드 정보 암호화

단말기와 IPIC 카드사이에 입/출력되는 데이터를 보호하기 위해 사용된다. Secret File에 키/PIN을 저장하는 경우에 사용된다. 진찰카드 정보를 IPIC 카드로 전송 할 때는 다른 진찰카드 정보와 구별되는 방법을 사용한다. 이는 다음 그림 figure 2와 같이 구현했다.

4. 병원진찰카드 통합용 IC 카드 발급 시스템 개발

IPIC 카드의 발급은 먼저, 초기화 단계를 실행한다. 위에서 설계한 IC 카드 내의 메모리 구조를 HCOS가 탑재된 IC 카드로 구현할 경우 진찰카드 정보를 수록할 수 있는 메모리를 초기화하여야 한다. 메모리 초기화는 MF 생성, DF 생성, EF 생성의 순으로 진행된다. 초기화 단계를 거치고 나면 개인화 단계를 진행한다.

1) 초기화 단계

IC 카드를 초기화할 경우에 IC 카드 내에 생성되는 파일은 표 6과 같은 접근 상태(Access Condition, AC)를 따른다. 즉, MF파일 생성은 AC3(Create condition)에 적용 받고, MF외의 DF파일 생성은 AC2(Write condition)를 따른다[6].

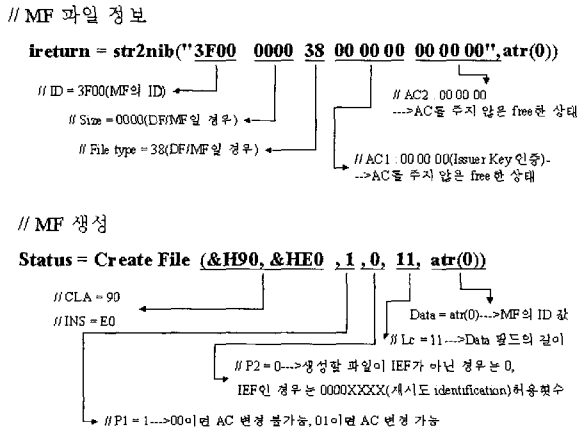

그림 3. MF 생성
Fig. 3. Creation of MF

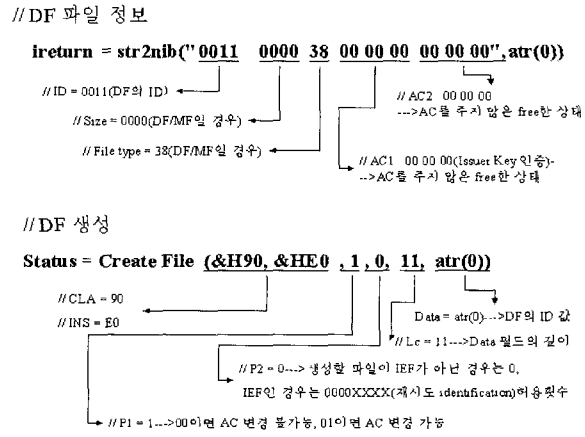

그림 4. DF 생성
Fig. 4. Creation of DF

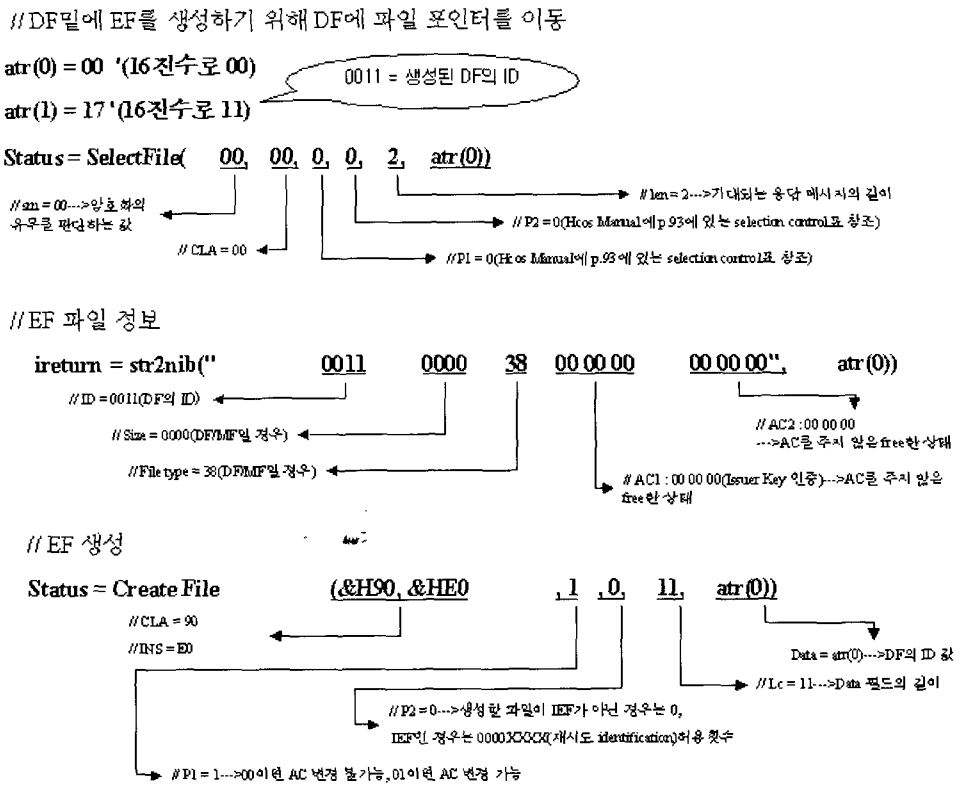

그림 5. EF 생성
Fig. 5. Creation of EF

HCOS가 탑재된 IC 카드의 MF는 Create File 명령을 이용해서 생성하며, IC 카드 내에 하나만 존재한다. MF의 ID는 ISO/IEC 1716-4에 예약된 "3F00"으로 고정되어 있다. MF의 생성은 다음 그림 3과 같이 구현된다. 일반적으로 IC카드는 하나의 MF만을 생성하도록 국제 표준으로 정의되어 있다[11,12].

DF는 MF와 같이 Create File 명령으로 생성하고, DF의 ID는 ISO 표준을 준수하거나 국가 표준에 의해서 정해진 값으로 정한다. DF의 생성은 다음 그림 4와 같이 구현된다[11,12].

EF의 생성은 MF 생성과 같은 Create File 명령을 이용하고, EF 파일 ID는 DF 생성과 같이 국제 표준 및 KS 표준을 준수한다. EF의 생성은 다음 그림 5와 같이 구현된다.

그림 6은 IPIC 카드의 초기화 단계를 위한 동작 화면이다. 이 시스템은 병원 실무자가 발급 버튼을 선택하면, 자동적으로 MF, DF, 및 4 개의 EF를 자동으로 생성한다.

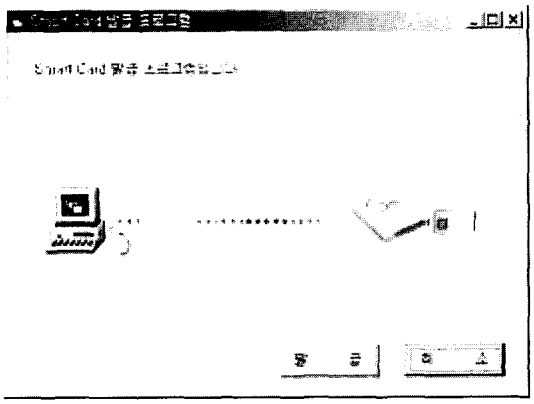

그림 6. IPIC 초기화
Fig. 6. Initialization of IPIC card

2) 개인화 단계

IPIC 카드의 초기화가 끝나고 나면, IPIC 카드에 비로소 개개인의 진찰정보를 읽고 쓸 수 있는 공간이 확보된다. 환자 개개인의 진찰정보를 IPIC 카드에 저장하는 단계를 개인화 단계라고 부르면, 본 논문에서는 그림 7과 같이 구현하였다. 본 논문에서 개발한 개인화 시스템은 개인 기본정보와 의료보험 정보, 병원 정보, 진료정보를 한번에 저장할 수 있으며, 이 정보들은 모든 병원에서 처음 방문한 환자에게 마다 기본적인 정보로 다뤄지는 정보들이다.

진찰카드 정보는 IC 카드 내에 생성된 EF에만 기록할 수 있고, Update Binary 명령어를 이용하여 수행한다. 다음 그림 8은 IPIC 카드의 병원정보 EF에 내원 병원명을 기록하기 위한 알고리즘이다.

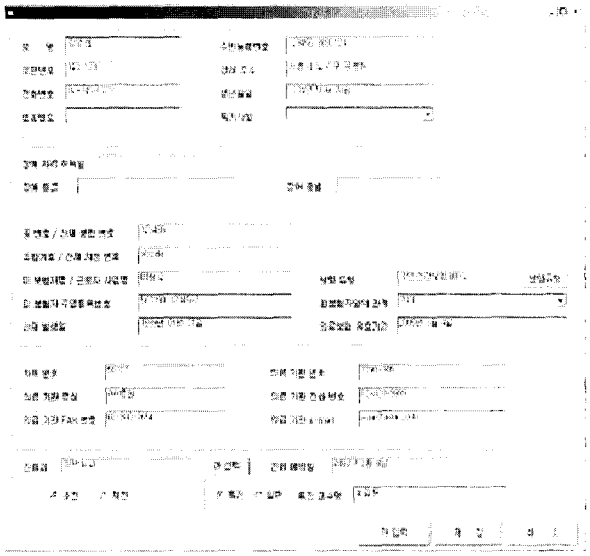

그림 7. IPIC 발급 및 정보 입력
Fig. 7. Issuing IPIC card and storing the information

```
//DF 0011선택
DF_id(0) = 00 '(16진수로 00)
DF_id(1) = 17 '(16진수로 11)          0011 = 생성된 DF의 ID
 Status = SelectFile(0, 0, 0, 0, 2, DF_id(0))

// 내원병원명을 기록하기위한 병원정보 EF 파일 선택(EF 0025선택)
  EF_id4(0) = 0
  EF_id4(1) = 36
  Status = SelectFile(0, 0, 0, 0, 2, EF_id4(0))

//내원병원명 기록하기
  str1 = info.H_info1
  data() = StrConv(str1, vbFromUnicode)
  nlen = UBound(data) + 1
  If nlen <> 0 Then
  Status = Update Binary(CLA, INS, P1, P2, Lc,   Data)
                                          // Data = 전송할 Data
                                          // nlen = EF에 갱신할 Data의 길이
```

그림 8. 병원정보EF에 병원이름저장 알고리즘
Fig. 8. Algorithm to store the hospital name at hospital information EF

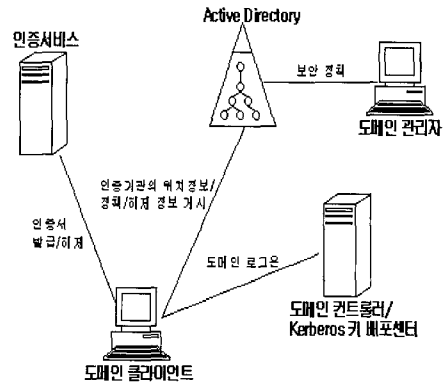

그림 9. 윈도우2000의 PKI 요소
Fig. 9. PKI component of Windows 2000

표 3. 윈도우2000이 제공하는 CA 모델
Table 3. CA model supported by Windows 2000

종류	Active Direc -tory 필요유무	내용
엔터프라이즈 루트 CA	O	최상위 수준의 CA
엔터프라이즈 하위 CA	O	다른 CA로부터 CA 인증서를 받아야 하는 CA
독립 실행형 CA	X	최상위 수준의 CA
독립실행형 하위 CA	X	다른 CA로부터 CA 인증서를 받아야 하는 CA

병원진찰카드 통합을 위한 시스템 개발

1. 통합 병원진찰 IC 카드 보안 인증을 위한 인증 센터 구축

본 논문에서는 IPIC 카드의 보안 인증을 위해서 마이크로소프트사의 윈도우 2000을 이용한 가상의 전자서명 인증센터를 구축했다. 윈도우 2000은 PKI(Public Key Infrastructure)를 지원하며 구성요소는 그림 9와 같이 인증서비스 서버, active directory, 도메인 관리자, 도메인 컨트롤러, 그리고 도메인 클라이언트로 구성된다. 윈도우 2000이 지원하는 CA 모델은 표 3과 같이 다양하다[10]. 본 논문에서는 윈도우 2000이 지원하는 CA 모델 중 엔터프라이즈 루트 CA 모델을 기본으로 전자서명 인증센터를 구축하였고, 새 인증서 요청 시 요청 정보는 요청 프로그램에서 CryptoAPI로 전달되어 CSP(Cryptographic Service Provider)에 데이터를 전달하여 공개키와 개인키를 생성한다. 이렇게 구축된 인증센터의 전자서명을 이용하면 사용자 인증 기능뿐 아니라 송수신되는 진찰카드 정보를 암호화할 수 있고, 무결성도 보장할 수 있다.

2. 병원 OCS에 연동된 통합 병원 진찰 IC 카드 진료 접수/예약 시스템 개발

개인화가 완료된 IPIC 카드를 환자들에게 배부하고, 환자가 IPIC 카드를 연동해서 사용하는 병원에 다시 내원하였을 경우 IPIC 카드를 통해서 병원 진료를 접수/예약할 수 있다. 그림 10은 IPIC 카드로 진료 접수/예약을 하는 시스템이다. 또한, 다시 병원을 재 방문하였을 경우에는 진료를 위한 항목만 활성화가 되어 진료를 등록할 수 있게 개발하였다. 그림 11은 병원 OCS에 연동된 IPIC 카드에 의한 진료 접수/예약 시스템에서 IPIC 카드의 병원정보 EF로부터 병원 정보를 읽어오는 알고리즘이다.

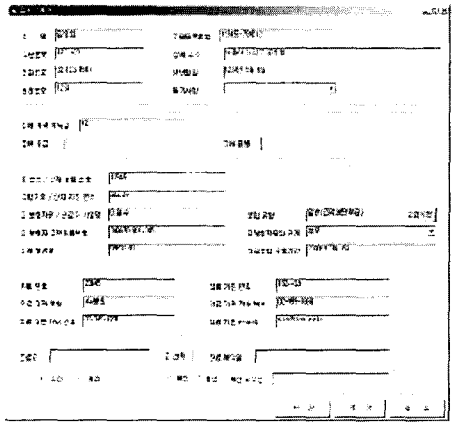

그림 10. IPIC 카드를 이용한 진료예약 시스템
Fig. 10. Medical care booking system using IPIC card

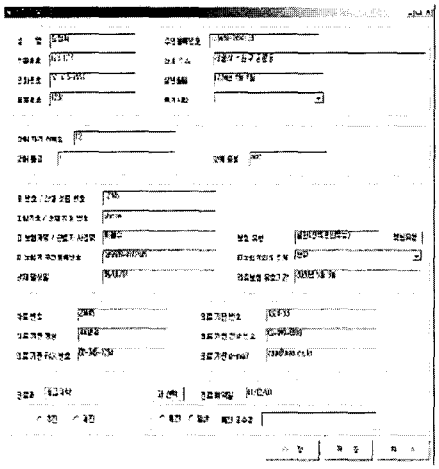

그림 12. IPIC 카드의 기본정보 수정
Fig. 12. Updating a basic information at IPIC card

마지막으로, 환자의 기본 정보는 수정될 필요가 있을 수 있다. 그림 12는 IPIC 카드의 내용을 수정하기 위한 시스템이다. 하지만, 의료보험정보와 병원정보는 수정이 불가능하며, 개인정보 중에서 주소 부분만 수정할 수 있다. 의료보험 정보는 IPIC 카드에서의 정보와 병원 OCS의 정보를 단순히 수정해서 발급이 이루어질 수 없기 때문이다. 만약 의료정보를 수정하려 한다면 새로운 사람으로 다시 등록해서 발급해야 한다. 따라서 개인정보를 바꿀 경우에는 카드의 내용과 함께 진료 받은 병원의 OCS에도 수정이 이뤄지게 된다.

결과 및 고찰

모든 병원들은 자체 OCS를 구축하고 자체 진찰카드 정보 규격을 사용하고 있다. 따라서, 단순 통합용 병원 진찰카드를 사용하는 것은 불가능하다. 모든 병원 OCS가 다른 병원의 진찰카드 정보를 수용하도록 수정하는 것은 너무나 많은 예산

```
//DF 0011선택
DF_id(0) = 00 '(16진수로 00)
DF_id(1) = 17 '(16진수로 11)
Status = SelectFile(0, 0, 0, 0, 2, DF_id(0))
// 병원 정보를 읽기위한 병원정보 EF 파일 선택(EF 0025선택)
  EF_id4(0) = 0
  EF_id4(1) = 36
  Status = SelectFile(0, 0, 0, 0, 2, EF_id4(0))
  info.H_info1 = StrConv(H_info1, vbUnicode)
Status = Read Binary(CLA, INS, P1, P2,    Le,  Data)
          // Le = 읽고자 하는 Data의 길이
```

그림 11. 병원정보EF에서 정보정보를 읽어내는 알고리즘
Fig. 11. Algorithm to read the hospital information at hospital information EF

및 노력을 초래한다. 본 논문에서 제안한 방법은 병원에서 사용하는 기본적인 진찰 정보를 바탕으로 IPIC 카드에는 표준화된 최소한의 기본적인 정보만 추출하여 병원 OCS를 간단하게 수정하므로써 연동이 손쉽게 가능하도록 설계되었다.

본 논문에서 제안한 IPIC 카드는 2001년 현재 11개 병원에서 1,000여명의 환자들에게 발급하여 사용하고 있다. 그리고, 매년 10%씩 발급량이 증가하고 있다. 하지만, 모든 환자들이 소유하기에는 제도적인 규정이 뒷받침이 되기 전까지는 많은 어려움이 있을 것으로 예상된다. 그리고, 진찰카드 정보에 대한 국가적인 차원에서 표준화에 주력하여야 할 것으로 예상된다.

본 연구는 각종 의료보험 카드나 병원 카드가 IC 카드로 대체될 경우를 대비하여 다수의 의료기관이 연계하여 하나의 보건의료용 전자카드를 사용하기 위한 발급 및 연동 시스템을 개발하였다.

환자 정보를 보호하기 위해서 전자서명 인증 센터와 3-DES를 이용하였다. 특히, IC 카드의 기본 이중 암호키 보안을 이용함으로 강력한 인증, 무결성, 정보 보호를 강화하였다. 이런 보안을 기본으로 하여 실제 병원에서 진찰 카드나 기타 의료카드를 발급하고 쓰기/읽기가 가능한 발급 시스템을 개발하였다.

본 연구에서 제시한 최소한의 진찰카드 정보의 표준화는 기존 병원 OCS의 연동을 손쉽게 해결할 수 있었다. IPIC 카드 연동 시스템은 기존 병원 OCS와 비독립적으로 연동하여 기존 업무의 흐름을 방해하지 않았다. 그리고, 신뢰성 있는 진찰정보 전달을 용이하게 함으로 환자 진료에 관한 서비스를 향상시킬 수 있었다.

참 고 문 헌

1. Korea Health Industry Development, *"The Report About Medical Information Sharing"*, 1999
2. Korea Ministry of Legislation, http://www.moleg.go.

kr/Refer/MCONLawDataView.jsp?l_lawid=01788&l_pubdt=20030806&l_pubno=06964&l_lawkdcd=A1&l_hanchk=Y
3. Korea Ministry of Legislation, http://www.moleg.go.kr/newlaw/nlab18100.hwp
4. Wrankl & Effing, Translated by Kenneth Cox, *"Smart card HandBook second edition"*, John wiely& Sons, 2000
5. Ministry of Health and Welfare, *"The Medical Statistic Annual Report"*, 1999
6. K.H.Lee, "On The Development of A Korean Medical Health IC Card", The Korean Society of Medical Informatics, vol5(2), pp.81-86, 1999
7. ISO, ISO/TC 215/WG5 N-;WD, 2000
8. K.H.Lee, *"Designing the Memory File System for Standardizing A Korean Medical Healthe IC Card"*, The Korean Society of Medical Informatics, vol5(2), pp.75-80,1999
9. Andrew Nash William Duane Celia Joseph Derek Brink, *"PKI : Implementing and Managing E-Security"*, Osborne/McGraw-Hill, 2001
10. Microsoft, *"Windows 2000 PKI"*, White paper, 1999
11. ISO/SC17 7816
12. HIT, HCOS development Manual, 2000