Journal of The Health Care and Life Science(ISSN 2383-4552) Vol.9, No.2, pp.213-220, Dec. 2021
https://doi.org/10.22961/JHCLS.2021.9.2.213

DRM기반 의료취약지 진료만족도 조사 연구

이경화*
송호대학교 보건행정과

A study on Satisfaction with Treatment in Medically vulnerable areas based on DRM

Kyeung-Hwa Lee*
Department of Health Administration, Songho University

요약 의료취약지에 거주하는 농촌 주민들에게 적절한 의료서비스를 제공하고, 이를 통한 보건의료자원의 불균형을 해소하기 위한 정책이 필요하다. 일반적으로 해당 주민들에게 의료서비스 확보를 위하여 설문 방법을 활용하며, 조사자와 참여자간의 설문문형과 개인정보를 디지털 컨텐츠로 배포 및 수집하기 위해 보안 정책이 필요하다. 제안한 논문에서는 조사자의 설문문형과 참여자의 개인정보를 안전하게 관리하기 위한 방안으로 DRM(Digital Rights Management)기술을 도입하며, 기존의 License Server가 모든 도메인들에게 라이센스를 발행, 갱신, 취소하는 문제점을 개선하기 위하여 패밀리도메인으로 묶은 DM만이 인증서를 발급받은 후 라이센스 관리를 수행하는 DRM기반 설문조사 정책에 편리성을 제공한다.

Abstract A policy is needed to provide appropriate medical services to rural residents living in medically vulnerable areas and to resolve imbalances in health and medical resources through this. In general, a survey method is used to secure medical services to the residents, and a security policy is needed to distribute and collect the questionnaire type and personal information between the investigator and the participant as digital contents. The proposed thesis introduces DRM (Digital Rights Management) technology as a way to safely manage the questionnaire type of the investigator and the personal information of the participants, and improves the problem that the existing License Server issues, renews, and cancels licenses to all domains. In order to do this, it provides convenience to the DRM-based survey policy that only DMs bundled with the family domain performs license management after the certificate is issued.

Key Words DRM(Digital Rights Management), LS(License Server), DM(Domain Manager), healthcare

1. 서 론

의료취약지에 거주하는 농촌 주민들에게 적절한 의료서비스를 제공하기 위해서는 지역 간 보건의료자원의 불균형을 해소하고 공공보건의료 부문의 취약성을 해결하는 것이 필요하다.

공공보건의료기관은 국가나 지방자치단체에 의해 설립된 국·공립병원과 정부부처에 소속되어 있는 특수법인 형태의 병원 그리고 각 시·군·구에 설치되어 있는 보건소, 보건지소 그리고 보건진료소를 말하며, 현재 우리나라의 공공보건의료기관은 보건소 252기관을 포함하여 총 3,740개 기관이 있다[9]. 그 중 농어촌의 공공보건기관 이용률은 4.3%로 일반 병의원 이용률이 83.5%인 것에 비하면 턱없이 낮은 실정이다[10]. 이는 농어촌에 거주하는 주민들이 질병치료 시 '적합한 의료기관을 찾기 어렵다'는 응답이 16.5%로 2013년보다 2배 늘어났고, 주로 이용하는 의료기관은 병(의)원이 83.5%, 종합병원이 10.8%, 특히 보건소(지소) 이용률이 3.0%에 불과해 공공보건기관에 대한 농어촌지역 주민들의 이용률이 높지 않은 것으로 분석된다[10].

본 논문은 2021년도 송호대학교 교내연구비 지원에 의해서 수행되었음.
*Corresponding Author : Kyeung-Hwa Lee(Songho Univ.)
Email: nam1q2w3e4@naver.com
Received December 01, 2021 Revised December 09, 2021 Accepted December 20, 2021

제안한 논문에서는 해당 의료취약지에 거주하는 주민들을 대상으로 설문을 통하여 의료서비스의 요구사항을 분석하고자 하며, 자료조사자의 설문문형과 참여자의 개인정보를 안전하게 보호하기 위한 전략으로 DRM(Digital Right Management) 기술을 설계하며, 기존의 License Server의 과도한 트래픽 및 오류 개선을 위하여 설문대상 군집을 패밀리도메인으로 묶은 후 DM(Domain Manager)권한을 위임받아 해당 도메인들에게 라이센스를 발행, 갱신, 취소하는 정책을 갖음으로써 비용적 측면과 트래픽 등의 문제를 해결하고 설문조사 정책에 편의성을 제공한다.

2장의 관련연구에서는 기존의 DRM시스템에 대하여 설명하며, 3장의 패리밀도메인 설계를 통한 설문형 콘텐츠를 설계하며, 4장에서 결론을 통한 적용 방안 및 향후 연구에 대하여 정의한다.

2. 관련연구

2.1 환자 만족도와 충성도

의료취약지역을 대상으로 설문을 통하여 의료서비스에 대한 질적 수준을 조사할 필요가 있으며, 이를 위하여 기존의 의료서비스의 질적 평가와 평가를 통한 기대이론에 대하여 조사하였다.

환자만족은 그 자체가 의료서비스의 질 평가에 중요한 기준이 되고 있으며, 환자의 치료순응도 및 병원 재이용 의사, 타인에게 권유의사와도 관련되는 등 다양한 측면에서 그 중요성이 강조되고 있다[12]. 또한 환자만족도는 기대수준이 중요한 요소로서 작용하며 개인적인 차들을 고려하여야 한다고 보고되고 있다[11].

Salancilk 과 Feller[13]는 의료서비스의 만족은 의료기관으로부터 받은 진료의 여러 가지 질에 관한 개인의 평가라고 정의하였으며, Linder pelz[14]는 환자만족도를 의료서비스를 구성하는 여러 가지 요소들에 대한 긍정적 평가라고 하였다.

Linder pelz[14]는 환자만족을 환자의 의료속성에 대한 믿음과 그에 대한 환자의 긍정적 태도 및 평가로 구성된다는 가치-기대 모형(value-expectation model)으로 정의하고, 환자만족을 측정하는 구성차원으로 ①접근성/편리성, ②자원의 활용 가능성, ③진료의 지속성, ④의료의 효과 또는 결과, ⑤재정, ⑥인간적인 태도, ⑦정보수집, ⑧정보의 제공, ⑨주변 환경의 쾌적함, ⑩의료의 질 또는 능력 등 10가지를 제시하였다[13].

환자 만족에 영향을 미치는 요인에 관한 선행연구를 살펴보면, 기존의 환자 만족도 연구에 대한 내용 분석을 통하여 의사-환자 간 매너(interpersonal manner), 기술적인 질(technical quality), 접근성/편리성(accessibility/convenience), 경제성(finances), 효능/결과(efficacy/outcomes), 지속성(continuity of care), 물리적 환경(physical environment), 유효성(availability)의 8가지 구성요소를 제시하였다. 고객의 사회인구학적 요인, 신체적 상태, 정신적 상태, 의료에 대한 태도와 기대, 의료를 제공하는 조직의 구조적 특성, 의료의 기술적 측면, 의료의 결과 등을 환자만족도 구성요인으로 제시한 바 있다. 그 밖의 환자만족 요인에 관한 기존 문헌들에서도 의사의 진료수준과 친절성, 간호사의 간호능력과 친절성, 일반직원의 친절성, 병원시설 및 장비의 수준, 편의시설, 대기시간, 이용절차의 편리성, 진료비 수준 등이 주로 언급되고 있으며, 고객의 사회인구학적 특성과 기대수준이 통제변수로서 작용하고 있는 것으로 보고되고 있다[15-18].

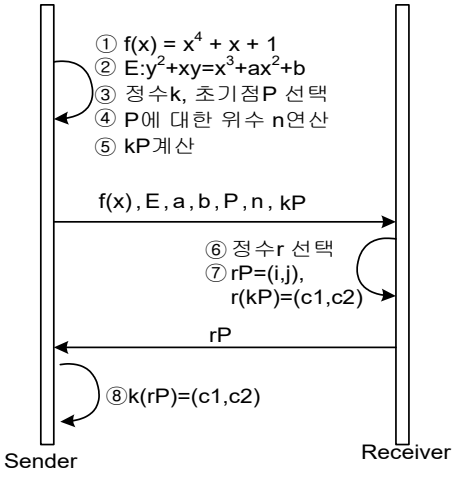
2.2 SPK(Shared Private Key)와 DRM(Digital Rights Management) 시스템

본 절에서는 설문을 위한 조사자와 참여자간의 라이센스에 관련된 개체들간의 안전한 자료 전송을 위하여 공유비밀키(SPK : Shared Private Key) 알고리즘의 설계와 정당한 사용권한을 라이센스 발급과정을 통하여 위임받는 DRM에 대하여 정의한다.

2.2.1 공유비밀키

라이센스 발급을 위한 개체인 Publisher, Provider, LS(License Server), clearing house, DM(Domain Manager)간의 안전한 정보 전송을 위해 공개키 알고리즘을 이용한 SPK(Shared Private Key)에 대하여

정의 한다. 또한, 제안한 기법인 DM과 DM의 라이센스 관리대상으로 설정된 MAC들 간의 라이센스 발급, 갱신, 취소 과정에도 거래 주체자 들간의 안전한 정보전송을 SPK를 이용한다.



[Fig. 1] create of Shared Private Key
[그림 1] 공유비밀키 생성

디지털 콘텐츠를 이용하기 위해 당사자간에는 DRM CA로부터 인증서를 발급받는다. 이때, 인증서의 내용 중 공개키 값을 통하여 거래 당사자간에 전송받을 문서를 암호화하여 전송받을 수 있게 된다. 제안한 논문에서는 제 3의 불법적인 도청을 배제하기 위하여 거래 당사자간에 공유비밀키를 생성하여 사용한다. [그림 1]은 $F_2^m ECC$알고리즘을 이용한 공유비밀키 생성 과정을 표현한 것이다.

다수의 거래 당사자를 Sender와 Receiver로 정의한다. Sender는 우선 감축불가 다항식 f(x)와 타원곡선 E를 선택하고, 타원곡선 E의 벡터 a, b를 결정한다. 또한, 타원곡선 위의 한 점을 초기점 P로 선택하고 초기점 P에 대한 위수(order) n을 구한다. 비밀키 k만큼 덧셈 연산한 kP를 계산한 후, 타원곡선 E, 감축 불가 다항식 f(x), 벡터 a, b, 초기점 P, 위수 n, 공개키 kP를 Receiver에 전송한다. Receiver는 전송받은 감축 불가 다항식 f(x)와 타원곡선 E를 이용해 Receiver의 비밀키 r만큼 덧셈 연산한 Receiver의 공개키 rP를 Sender에 전송하고, Sender의 공개키 kP를 비밀키 r만큼 덧셈 연산한 공유 비밀키(SPK : Shared Private Key) r(kP)로 정의한다. 이후에 거래하고자 하는 당사자간에는 Sender와 Receiver의 고유한 SPK를 이용한 안전한 디지털 정보를 보장받을 수 있다.

2.2.2 DRM 시스템

디지털 컨텐츠는 특성상 쉽게 온라인을 통한 컴퓨터를 이용하여 쉽고, 빠르게 복사할 수 있고 또한, 복제품은 원본과 질적인 차이 없이 사용할 수 있다는 문제점으로부터 저작권 보호를 위한 법적 제도 및 실질적 기술의 필요성도 점차 증가되어 법적으로도 정비되어 가는 추세이다. 제안한 논문에서는 라이센스를 발급 받을 주체를 사용자 인증과 디바이스 인증 중 MAC값을 기반으로 한 디바이스 인증 즉, 도메인을 기반으로한 라이센스 관리절차와 DM을 이용해 MAC들에게 라이센스를 재 배포(super-distribution)하는 방법에 대하여 설명한다.

1) DRM 식별자

디지털 콘텐츠에 사용되어지는 인증기법은 크게 두 가지로 구분할 수 있다. ID/Password, 인증서의 공개 키, 이메일 주소 정보, 지문, 홍채 등의 생체 정보를 통한 사용자 인증과 해당 디바이스에 프로그램을 설치하고자 할 경우에 행하여지는 디바이스 인증 즉, 도메인 인증이 다음이다. 또한, 디바이스 인증은 세 가지로 구분할 수 있다. IMEI(International Mobile Equipment Identification)과 IMSI(International Mobile Subscriber Identity)는 국제이동 단말기 식별번호로 전 지구적 이동통신 시스템(GSM : Global System for Mobile communications) 이동 단말기로 형식은 서로를 고유하게 식별할 수 있도록 이동 단말기에 할당된 식별번호인 형식 승인코드, 최종조합코드 및 일련번호를 포함하여 15자리로 구성되어있다. 또한, MAC(Media Access Control) 값이 있는데, MAC값은 네트워크 카드의 48비트 하드웨어 주소를 말하며 모든 네트워크 카드가 고유한 주소값을 갖는다. 따라서 제안한 논문에서는 MAC을 이용한 도메인 인증을 기준으로 설명한다. 또한, 제안한 논문에서 SPK를 이용한 디

바이스 인증은 IMEI와 IMSI에도 적용이 가능하다.

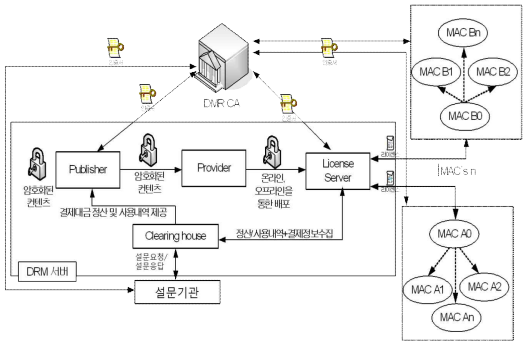
2) 도메인 재 배포 시스템

LS와 도메인들 간에 안전한 라이센스를 요청 및 발급하기 위한 절차를 두 가지 방법으로 나눌 수 있다. 먼저, 인증된 도메인(authorized domain) 기법은 기존에 발급할 라이센스를 마스터 디바이스 키 목록에 저장해 놓고 저장된 디바이스는 도메인이 추가될 때마다 목록에 있는 키를 하나씩 할당하는 방법으로 할당한 키가 부족하면 인증된 도메인을 다시 LS에 등록하고 마스터 디바이스 키 목록을 재 생성해야 하는 문제점을 지니고 있다. 둘째로, 패밀리 도메인(family domain)을 들 수 있는데, 이는 콘텐츠 제공자의 계약사항과 조건에 따라 라이센스를 서버로부터 발급 받아 유한개의 사용권한을 얻을 수 있는 방법을 말한다.

이 두 가지 방법은 모두 재 배포의 의미를 갖는다. 즉, 정의된 라이센스 서버로부터 초기의 라이센스 발급 권한을 획득한 디바이스로부터 추가되어지는 디바이스에 MAC값을 이용하여 서버측에 라이센스를 요청하는 방법을 의미한다. 제안한 논문에서는 LS로부터 권한을 위임 받은 DM이 라이센스를 발급, 갱신, 취소할 수 있는 재 배포 기법을 갖는다.

3. 본 론

제안한 DRM의 구조는 [그림 2]와 같다.



[Fig. 2] DRM system block diagram
[그림 2]. DRM 시스템 구성도

첫째, DRM CA(Certification Authority)는 각각의 객체인 Publisher(출판업자), Provider(콘텐츠 배포 서버), LS(License Server), DM(Domain Manager)인 MAC0, 설문기관에게 정당한 거래자임을 확인하기 위한 인증서를 발급 및 관리한다. 둘째로 금융기관은 패밀리 도메인 매니저인 MAC0으로부터 콘텐츠를 이용할 수 있는 설문을 지급 받아 Publisher에게 수익을 전달하며, 셋째로, MAC0은 DRM서버로부터 라이센스 관리 권한을 얻은 후 디지털 콘텐츠를 이용할 수 있도록 패밀리 MAC들에게 라이센스를 발급 및 관리한다. 넷째로, DRM서버에서는 디지털 콘텐츠를 생성한 후 암호화하여 제공하는 Publisher, Publisher로부터 받은 디지털 콘텐츠를 배포하기 위한 Provider, 사용자 정보를 입력받아 사용자가 요청한 콘텐츠를 제공할 수 있도록 사용권한을 제공하는 정책을 맡고, 허가된 사용자에게 라이센스를 부여하여 콘텐츠를 안전하게 제공하는 역할을 하는 클리어링 하우스, License를 MAC들에게 발급하기 위한 정책을 담당하는 LS로 구분할 수 있다. 다섯째, 위의 개체들 간에 정보를 전송하기 위하여 거래 대상간의 SPK를 통해 안전한 정보 공유를 수행한다.

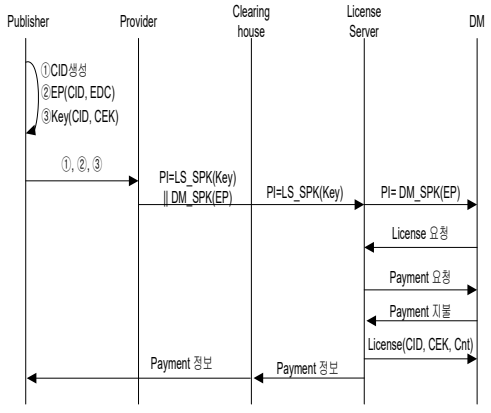
제안 논문에서는 각 장을 통하여 기존과 차별화 된 패밀리 도메인 생성 및 관리방법에 대하여 정의 한다. 첫째, LS로부터 DM 권한을 지닌 MAC0가 DRM CA로부터 인증서를 발급 받은 후 하위의 MAC들에게 콘텐츠 사용권한인 라이센스를 발급한다. 둘째, LS로부터 라이센스 관리 권한을 위임받은 DM은 패밀리 MAC들에게 라이센스를 신규발급, 갱신, 취소의 권한을 지닌다. 특히, DM은 두 가지 방법을 통해 MAC들을 관리한다. 첫째, 유효기간이 만료된 콘텐츠나 특별한 조건에 의해 사용권한을 상실한 MAC의 경우에는 폐기한 MAC들을 재사용할 수 없도록 제한 한다. 둘째, DM으로부터 올바른 권한을 지닌 MAC이 고장으로 인해 교체 되었을 경우 올바른 사용권한을 License 재 발급 과정을 통하여 지속할 수 있다.

3.1 DRM 구성요소

본 절에서는 Publisher로부터 콘텐츠를 사용하고자 하는 DM에게 콘텐츠를 포함한 라이센스 발급 권한을 위임받는 과정에 대해 설계한다. Publisher는

컨텐츠를 안전하게 디지털 창작물로 생성한 후에 컨텐츠 암호화키(CEK : Content Encryption Key)를 이용하여 암호화된 컨텐츠를 생성한다. 후에 Provider에 전송하는 역할을 한다. 또한, Clearing house를 통하여 해당 콘텐츠를 사용한 댓가를 지불받는다. Provider는 Publisher로부터 전송되어온 디지털 콘텐츠를 도메인(MAC's)에게 전송하기 위한 콘텐츠 배포서버인 LS에게 전송한다.

[그림 3]은 DRM의 흐름도를 설명한 그림이다. 먼저, Publisher는 발급하고자 하는 ①컨텐츠의 식별번호(CID : Content ID)를 생성한다. ②EP(CID, EDC)에서 EP(Encrypted Package)의 요소인 EDC(Encrypted Digital Content)를 CID를 포함하여 생성한다. ③Key(CID, CEK)에서 Key는 해당 컨텐츠(CID)의 암호화된 문서를 해독하기 위한 용도의 CEK(Content Encryption Key)로 구분하여 Provider에게 전송한다. Provider는 PI(Provider Information)인 ③은 License Server와의 SPK(Shared Private Key)로 암호화 하여 Key정보를 전송하며 ②는 DM(Domain Manager)와의 SPK로 EP를 전송한다. 후에, DM은 Payment과정을 수행함으로써 LS로부터 License(CID, CEK, Cnt)를 통하여 발급 받음으로써 패밀리 도메인 매니저로의 기능을 수행할 수 있다. 이 과정에서 Cnt는 패밀리 도메인에게 라이센스를 요청한 하위의 MAC들의 수량으로 Cnt의 수량에 따라 Payment의 정보가 변경될 수 있다.



[Fig. 3] DRM flow chart
[그림 3]. DRM 흐름도

3.2 DM(Domain Manager) 시스템 설계

제안한 DRM시스템은 기존의 LS를 통한 정형적인 라이센스 발급 과정을 패밀리 도메인 매니저인 DM에게 위임함으로써 LS에서 처리해야하는 업무를 줄여줌과 동시에 모든 개체가 인증기관으로부터 인증서를 발급받아야 하는 문제점을 DM에게까지만 발급함으로써 비용 절감에서의 효율성을 강화하였다. 또한, 패밀리 도메인의 요소인 MAC들의 컨텐츠 사용 권한을 체계화 하였다. 즉, 유효기간등에 의해 사용이 중지되어야 하는 MAC들의 사용제한 기법과 디바이스의 교체에 따른 새로운 MAC들에 대한 올바른 사용권한 지속을 함께 설계함으로써 최적화된 DRM시스템을 기대할 수 있다.

3.2.1 DM(Domain Manager) 등록

본 절에서는 LS에 DM을 등록하고, 또한 라이센스를 발급받고자 하는 MAC들의 수량을 파악하여 LS에 라이센스를 요청하는 과정을 설계한다. 또한, LS는 DM의 환경에 HT(History Table)의 설치를 통하여 도메인(MAC's)에게 발급한 라이센스를 통하여 사용권한에 대한 검증을 수행한다.

[그림 4]는 LS에 DM이 라이센스 발급 권한을 위임받기 위해 등록하는 과정으로 자신의 도메인 정보인 MAC0과 라이센스 발급 수량인 Cnt를 상호 SPK를 암호화과정을 통해 전송한다. 후에, LS는 SPK를 이용하여 DM의 라이센스 권한을 수량과 함께 재 전송한다.

[Fig. 4] DM to LS
[그림 4]. LS에 DM등록

3.2.2 라이센스 발급

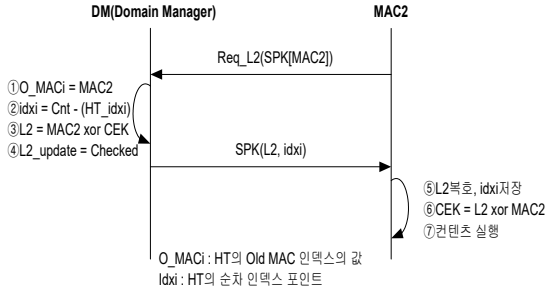
패밀리 도매인 매니저로 LS에게 등록을 마친 DM은 초기의 라이센스 발급을 원하는 도메인(MAC's)의 수량(Cnt)을 파악하여 해당 라이센스를 LS로부터

지급 받았다. 또한, DM은 [그림 5]와 같은 HT을 생성한다. HT의 구성요소는 크게 idx, License, MAC's로 구분한다. idx는 초기에 LS에게 요청한 라이센스의 수량과 순차번호를 의미한다. License정보의 CID(Content ID)는 제품의 식별번호를 의미하며, CEK(Content Encryption Key)는 암호화된 컨텐츠를 MAC환경에서 실행할 수 있도록 하는 복호키를 의미한다. 또한, MAC's의 O_MAC은 라이센스를 발급받고자 하는 MAC의 정보로 초기의 MAC값은 O_MAC(Old MAC)에 등록되며 갱신과정과 삭제과정 시에는 N_MAC(New MAC)의 값으로 갱신한다. 또한, 해당 MAC의 값이 차후에 발생할 갱신과 삭제의 경우를 대비하여 MAC값이 변경된 경우 update에 checked함으로써 MAC의 현재 값을 N_MAC으로 update 한다.

idx	License		MAC's		
	CID	CEK	O_MAC	update	N_MAC
1	survey	54640...x121	00030D4398F4	☐	00030D4398F4
2	survey	54640...x122	33430D4398FD	☑	33430D4398FF
3	survey	54640...x123	29392291DDF2	☐	none
4	survey	54640...x124		☐	
⋮					
n	survey	54640...x12n		☐	

[Fig. 5] Register history table
[그림 5]. HT(Histroy Table) 등록

[그림 6]은 MAC2가 DM에게 라이센스를 요청하는 과정을 보이는 그림이다. MAC2는 DM에게 SPK를 이용하여 MAC2 값을 암호화한 후 L2(License 2)를 요청한다. DM에서는 공유비밀키인 SPK를 복호화 한후에 ①O_MACi에 MAC2의 값을 등록한다. N_MAC은 초기에 O_MAC값과 같은 주소를 등록한다. ②idxi = Cnt - (HT_idxi)는 MAC으로부터 라이센스 요청이 있을 경우 DM가 License Server에게 요청한 컨텐츠의 수량(Cnt)에서 DM이 관리하는 MAC's의 수량(HT_idxi)를 빼줌으로서 HT에서 MAC의 index값을 정의할뿐만 아니라 사용가능한 라이센스의 남은 수량까지 확인할 수 있다. ③L2=MAC2 xor CEK는 DM에게 보내온 MAC2의 값에 디지털 컨텐츠를 복호할 수 있는 CEK를 xor연산하여 L2를 MAC2에게 발급한다. 이때, 정형화된 CEK에 의해 MAC2의 값을 변조한다면 디지털 컨텐츠에서는 복호화 키와 일치하지 않음으로 CEK의 해독이 불가능하게된다. ④L2_update=Checked는 차후에 발생할 갱신과 삭제의 과정에서 반드시 필요한 과정이다. 즉, 기존에 사용한 MAC값인 O_NAC과 차후에 변경된 MAC값인 N_MAC을 HT에 등록한다. DM에서 생성한 MAC2의 라이센스(L2)를 HT의 idxi와 함께 SPK를 이용하여 MAC2에게 전송해 준다. MAC2는 ⑤의 과정에서 SPK를 이용하여 L2를 복호하며, 차후에 재 발행과 삭제의 위치값인 idxi를 저장한다. ⑥CEK = L2 xor MAC2는 MAC에서 ③의 과정을 역암호화 하여 디지털 컨텐츠를 사용할 수 있는 CEK를 획득한다. ⑦의 과정에서는 CEK를 이용하여 디지털 컨텐츠를 실행할 수 있다.

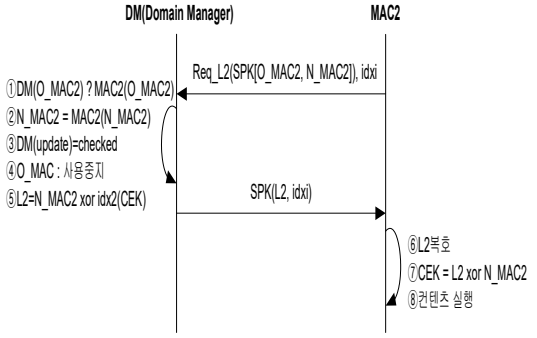


[Fig. 6] Issue license to MAC2
[그림 6]. MAC2에게 라이센스 발급

3.2.3 라이센스 갱신

상위 LS로부터 인증권한을 위임받은 DM은 패밀리로 그룹화한 MAC's을 안전하게 관리하여야 함을 원칙으로 한다. 본 절에서는 특정 MAC의 물리적 주소인 MAC2값이 변경된 후 DM에게 라이센스 갱신 요청 및 처리과정을 설계한다. 또한, 갱신 과정에서는 패키징된 컨텐츠는 기존의 저장된 매체의 것을 이용함을 원칙으로 한다. 먼저, 갱신을 요청하는 MAC2는 변경전의 MAC2값(O_MAC2)와 변경된 MAC2값(N_MAC2)를 상호 공유비밀키로 암호화하여 HT의 idxi값을 포함하여 라이센스(L2)를 DM에게 요청한다. DM은 5단계를 통해 재 갱신

과정을 처리한다. ①DM(O_MAC2) = MAC2(O_MAC2)는 DM의 HT의 O_MAC2와 MAC2로부터 전송된 MAC2(O_MAC2)의 일치여부



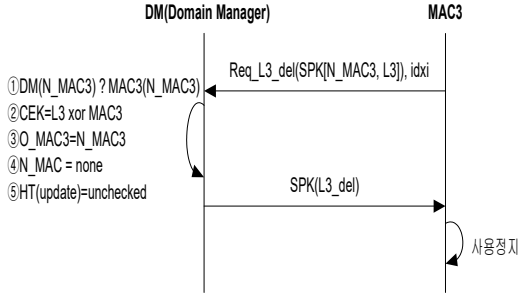
[Fig. 7] License Update to MAC2
[그림 7]. MAC2에게 라이센스 갱신

를 확인한다. 만약 일치하지 않으면 MAC2의 신분을 불신하여 거절하게 되며, 일치할 경우는 다음 단계를 수행한다. ② N_MAC2 = MAC2(N_MAC2)는 MAC2로부터 전송되어온 N_MAC2를 HT의 N_MAC2로 갱신하다. ③ DM(update) = checked는 HT에 N_MAC2를 새로 갱신하였다는 의미의 뜻으로 update를 checked 하며 ④O_MAC2:사용중지 는 기존의 MAC2의 MAC값을 사용할 수 없도록 중지시킨다. ⑤ L2=N_MAC2 xor idx2(CEK)는 HT에 등록한 MAC2의 값에 기존의 CEK를 xor 연산한 후 L2를 생성한다. 결국, DM은 새로운 L2를 생성하여 SPK를 이용해 MAC2에게 재 전송한다. MAC2는 ⑥L2복호 과정을 SPK를 통하여 역암호화(복호화)한 후에 ⑦CEK=L2 xor N_MAC2과정인 새로 교체한 자신의 N_MAC2의 값과 DM으로부터 전송된 L2를 xor 연산함으로써 해당 컨텐츠를 사용할 수 있는 CEK를 얻을 수 있다. ⑧컨텐츠 실행 과정은 CEK를 통한 패키징된 컨텐츠를 복원함으로서 해당 장치에서 사용할 수 있다[그림 7].

3.2.4 라이센스 취소

DM은 LS로 부터의 라이센스 관리 권한을 위임받은 후 발급, 갱신, 취소의 과정을 수행함으로써 사용권한이 있는 도메인인 MAC′s에게 컨텐츠 사용을 허가한다.

[그림 8]은 DM의 관리 중 라이센스 취소과정에 대한 설명이다. MAC의 유효기간등의 이유에 의하여 사용권한을 취소할 경우에 대한 과정으로 MAC3는 DM에게 사용 취소를 요청한다. 물론, 의도적인 부정사용을 DM의 위치에서 HT의 N_MAC값의 검증을 통해서도 가려낼수도 있음은 기본이다. 먼저, MAC3



[Fig. 8] License revocation to MAC3
[그림 8]. MAC3에게 라이센스 취소

는 DM에게 취소요청을 자신의 인덱스인 idxi를 통해 N_MAC3와 초기에 발급받은 CEK를 역암호화한 L3를 공유비밀키를 이용하여 전송한다. DM은 ①의 과정을 통하여 HT의 N_MAC3와 MAC3로부터 전송된 N_MAC3를 비교하여 신분을 확인한다. ②CEK=L3 xor MAC3의 과정을 통하여 HT의 CEK값과 비교함으로써 한번의 검증과정을 더 거치게 된다. ③O_MAC3=N_MAC3를 통하여 N_MAC3의 값을 O_MAC3의 값으로 대체함으로써 ④의 N_MAC의 값을 none으로 변환한다. 따라서, 실제로 MAC3는 현재 사용하고 있는 MAC3의 값인 N_MAC3값을 사용할 수 없음으로 정의한다. 결국, 모든 MAC들의 N_MAC들의 값이 있을 경우, DM은 랜덤하게 MAC들의 라이센스를 요청함으로써 사용권한이 없는 MAC들을 가려낼 수 있다. 마지막으로 ⑤HT(update)=unchecked로 설정함으로써 다른 MAC들이 사용할 수 있도록 권한을 포기하게 된다. 즉, 패밀리 도메인의 정의인 해당 수량만큼 라이센스를 발급할 수 있는 DM이 필요한 MAC들에게 MAC3가 취소한 권한을 위임할 수 있다.

4. 결 론

제안한 논문에서는 의료 취약지를 대상으로 보건소와 민간병원 방문환자들의 특성 및 고객만족도에 미치는 영향요인을 비교 분석하기 위하여 DRM기반의 설문조사를 설계하였다.

제안한 DM의 독립적 기능을 강화한 DRM설계는 기존의 패밀리 도메인을 이용한 재 배포(super-distribution)의 문제점인 도메인의 트래픽 증가와 추가되는 도메인의 수량으로 인한 NDK값의 끝없는 업데이트, 도메인키의 도난 시 발생할 수 있는 도용 등의 단점을 강화한 기법이다. 즉, 초기에 License Server로부터 라이센스 관리의 권한을 위임받은 패밀리 도메인 관리자인 DM은 인증기관으로부터 인증서를 발급받은 후 패밀리 도메인 그룹인 MAC's에게 License Server를 대행하여 라이센스를 신규발급, 갱신, 취소할 수 있는 독립적 라이센스 발급 기관의 기능을 제공한다.

향후 연구과제로는 현재까지 정착되어지지 않은 DRM시스템 기반의 설문을 시스템으로 구축함 후 서비스 함으로써 설문자와 참여자의 설문문항 콘텐츠 및 개인정보를 안전하게 관리할 수 있는 환경 구축을 목적으로 한다.

References

[1] C-G Park , "Mutual authentication protocol and encryption method design for digital content protection ", *Soongsil University Graduate School,* 2005.

[2] Y-T Shin, "Digital copyright management technology ", *Information & Resources,* 2007.

[3] G-G Jo, "DRM technology and information protection", *Information Technology Trends,* 2005.

[4] Korea Computer Center, *"Discovery of public project plans for DRM activation",* 2005.

[5] Bogdan C. Popescu, Bruno Crispo, Andrew S. Tanenbaum, Frank L.A.J. Kamperman, "A DRM Security Architecture for Home Networks", *ACM Workshop DRM* '04, pp.1-10, October 25.

[6] Windows Media Rights Management, http://www.microsoft.com/windows/windowsmedia

[7] Open Mobile Alliance, "DRM Architecture", OMA-DRM-ARCH-V2_0-20 040820-C, Draft Version 2.0-20 August 2004, http://www.openmobilealliance.org

[8] Fraunhofer Institute, "Light Weight DRM(LWDRM)", http://www.lwdrm.com

[9] Ministry of Health and Welfare , "Operation Status of Public Health Centers and Health Branches in 2016", *Ministry of Health and Welfare Policy Paper,* 2017.

[10] Rural Development Administration , "2016 Agricultural and Fishermen Welfare Survey Report", *Rural Development Administration Policy,*, 2017.

[11] G-H Kim, "Analysis of Determinants of Satisfaction by Patient Types in Hospitals ", *Yonsei University Master's Thesis,* 2005.

[12] G-I H, H-E Park, "A Study on Patient Satisfaction as an Outcome Indicator . *Journal of the Adult Nursing Association.* Vol.12, no.1, pp.29-39, 2001.

[13] Salancilk G. R., Feller J. P., "An examination of need satisfaction models of job satisfaction", *Administrative Science Quartery*, pp.176-179, 1977.

[14] Linder-Peltz, S., "Toward of theory of patient satisfaction", *Social science & medicine,* Vol.16, no.5, pp.577-582, 1982.

[15] C-H Kang, "A study on the effect of key factors in health care service quality on customers' intention to reuse :Focusing on medical institutions in Busan and Gyeongnam area", *Ph.D., Inje University above thesis,* 2012.

[16] O-S Park. "A Study on Factors Affecting Medical Institution Selection Criteria ", *Inje University Ph.D. thesis,* 2013.

[17] G-J Lee, "Analysis of Factors Influencing Hospital Revisit Using Data Mining : Focusing on outpatient satisfaction", *Journal of Health Administration,* Vol.13, no.3, pp.21-34, 2003.

[18] S-H Lee, et., 'Analysis of Patient Satisfaction Survey Status of Domestic General Hospitals', *Journal of the Korean Medical QA Society,* Vol.5, no.1, pp.42-57, 1998.