ISSN: 1226-7244 (Print)
ISSN: 2288-243X (Online)
논문번호 15-04-23
158

j.inst.Korean.electr.electron.eng.Vol.19,No.4,617~624,December 2015
http://dx.doi.org/10.7471/ikeee.2015.19.4.617

스마트폰과 근거리 무선 통신을 이용한 성인 인증 시스템의 개발

Implementation of Adult Authentication System Using Smartphone and Near-Field Communication

이 종 호*, 이 성 수**★

Chongho Lee*, Seongsoo Lee**★

Abstract

In this paper, an adult authentication system based on authentication certificate was designed and implemented using smartphone and near-field communication. It has three advantages. First, it achieves easy, convenient, and fast authentication by using smartphone and near-field communication. Second, it achieves extremely high security and reliability by exploiting authentication certificate. Third, it achieves extremely low risk of personal information leakage by generating and sending only virtual identification code. Finally, it has a proper legal basis by Digital Signature Act. It consists of adult authentication module, near-field communication control module, policy server module, and database server module. A prototype of the proposed system was designed and implemented, and it was verified to have correct operation.

요 약

본 논문에서는 스마트폰과 NFC 통신을 이용한 공인 인증서 기반의 성인 인증 시스템을 설계 및 개발하였다. 제안하는 성인 인증 시스템은 스마트폰과 NFC 통신을 기반으로 하여 쉽고 간편하고 빠르게 인증할 수 있으며, 공인 인증서 기술을 기반으로 하여 보안성 및 신뢰성이 매우 높고, 가상 신원 확인 코드만 생성하고 전송하여 개인 정보 유출의 위험이 매우 낮으며, 전자서명법에 기반하여 적절한 법적 근거를 가지고 있다. 제안하는 성인 인증 시스템은 성인 인증 모듈, NFC 제어 모듈, 정책 서버 모듈, DB 서버 모듈로 구성되며, 프로토타입을 설계하고 구현하여 정상적으로 동작하는 것을 확인하였다.

Key words : adult authentication, authentication certificate, smartphone, NFC, virtual ID

* PKI Security Institute, ISolutec Corporation
** School of Electronic Engineering, Soongsil University
★ Corresponding author: sslee@ssu.ac.kr, 02-820-0692

※ Acknowledgment
"This work (Grants No. C0239158) was supported by Business for Academic-Industrial Cooperative Establishments funded Korea Small and Medium Business Administration in 2014."
Manuscript received Dec 14, 2015; revised Dec 28, 2015; accepted Dec 28, 2015.

Ⅰ. 서론

청소년이 담배, 술, 성인용품과 같은 청소년 유해물에 접근하거나 술집, 클럽, 숙박업소와 같은 청소년 유해 업소에 출입하는 것이 사회적 문제로 대두되고 있다. 청소년보호법은 이러한 경우에 업주를 엄격하게 처벌하고 있어서 대부분의 업주는 성인이라는 것을 인증하기 위해 주로 육안으로 판별하거나 신분증을 확인하고 있다. 그러나 육안 판별의 경우에는 성인 옷차림이나 화장 등을 통해 청소년과 성인의 구별이 어려운 경우가 많다. 대안으로 주로 사용되는 신분증 확인

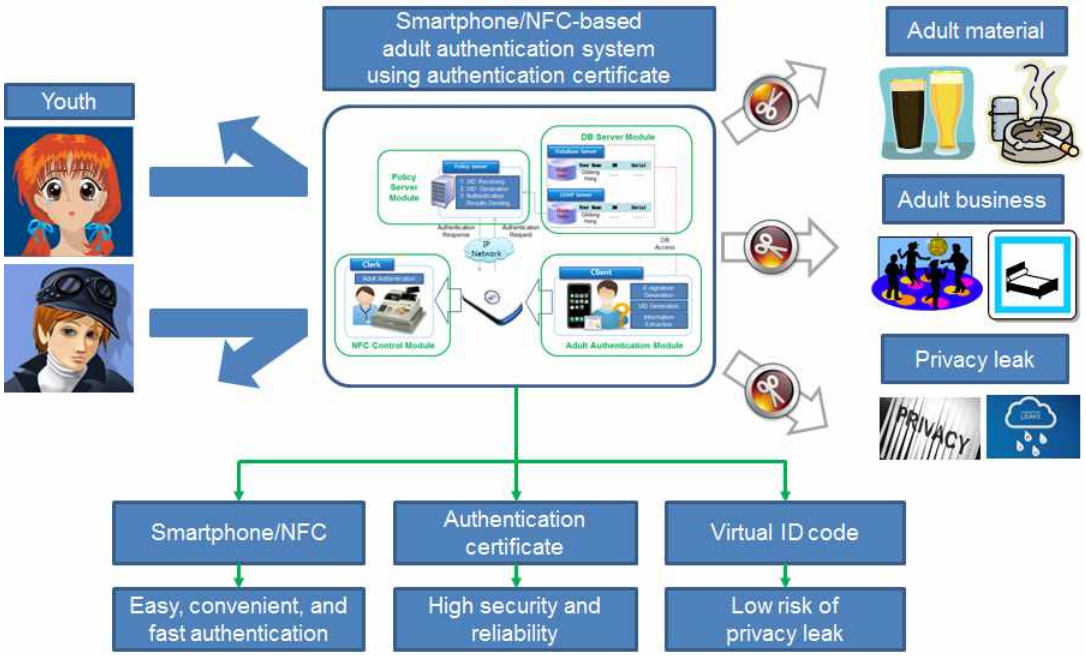

Fig. 1. Overview of the proposed adult authentication system
그림 1. 제안하는 성인 인증 시스템의 개요

의 경우에도 개인정보보호법의 엄격한 규정에 저촉될 수 있으며 개인 정보 유출의 위험이 있다. 또한 많은 여자 고객 등이 스토킹 등을 우려하여 신분증 확인을 꺼리며, 신분증 미소지자가 의외로 많아 손님과의 마찰이 자주 발생하고 있다. 심지어는 습득한 신분증에 자신의 사진을 붙이거나 타인의 신분증을 사용하는 사례도 심심치 않게 발생하고 있다. 이러한 이유로 인해 정확하고 손쉬운 성인 인증 수단의 개발이 절실하다.

공인인증서 (authentication certificate)는 온라인상에서 신원 확인, 전자 서명, 부인 방지 등의 기능을 수행하며, 전자서명법에 의해 강력한 법적 근거를 가지고 있다[1]. 따라서 이러한 공인인증서를 성인 인증 시스템에 적용하면 위에서 열거한 문제점을 모두 해결할 수 있다. 이 경우, 온라인에서만 사용하는 공인인증서를 오프라인에서 사용할 수 있도록 하는 기술이 필요하다.

본 논문에서는 스마트폰과 근거리 무선 통신 (NFC: near-field communication)[2]을 이용한 공인인증서 기반의 성인 인증 시스템을 그림 1과 같이 제안한다. 이 시스템은 스마트폰과 NFC 통신을 기반으로 하여 쉽고 간편하고 빠르게 인증할 수 있으며, 공인인증서 기술을 기반으로 하여 보안성 및 신뢰성이 매우 높고, 가상 신원 확인 코드 (VID: virtual ID)만 생성하고 전송하여 개인 정보 유출의 위험이 매우 낮으며, 전자서명법에 기반하여 적절한 법적 근거를 가지고 있다. 또한 기존의 하드웨어를 대부분 그대로 사용하고 소프트웨어만 추가하면 되기 때문에 확산 보급 및 유지 보수가 용이하다는 장점이 있다.

최근에 스마트폰과 NFC 통신을 이용하여 전자결제를 수행하는 서비스가 개발되었으나 업체가 자체적으로 발급한 전자서명문을 사용하므로 성인 인증에 대한 법적 근거가 부족하다. 이에 반하여 본 시스템은 정부가 성인에 한하여 발급하는 공인인증서를 사용하기 때문에 성인 인증에 대한 법적 논란을 원천적으로 차단할 수 있다.

II. 시스템 구성

본 논문에서 제안한 성인 인증 시스템은 그림 2와 같이 성인 인증 모듈, NFC 제어 모듈, 정책 서버 모듈, DB 서버 모듈로 구성되며, 각 모듈의 역할은 다음과 같다.

① 성인 인증 모듈: 스마트폰에 저장된 공인인증서로부터 개인 식별 정보인 VID를 생성하며, 스마트폰 앱의 형태로 구현된다.

② NFC 제어 모듈: NFC 리더기를 제어하는 모듈로서, 스마트폰과 NFC 리더기 사이에 NFC 통신을 통해 데이터를 주고받으며, NFC 리더기와

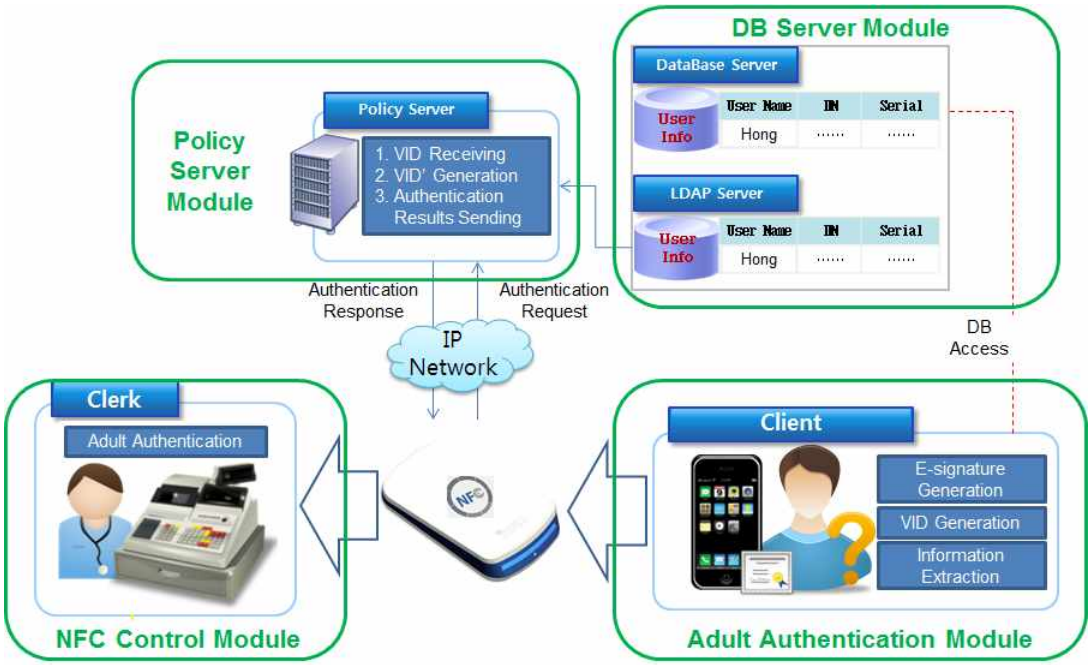

Fig. 2. Modules and configuration of the proposed adult authentication system
그림 2. 제안하는 성인 인증 시스템의 모듈 및 구성

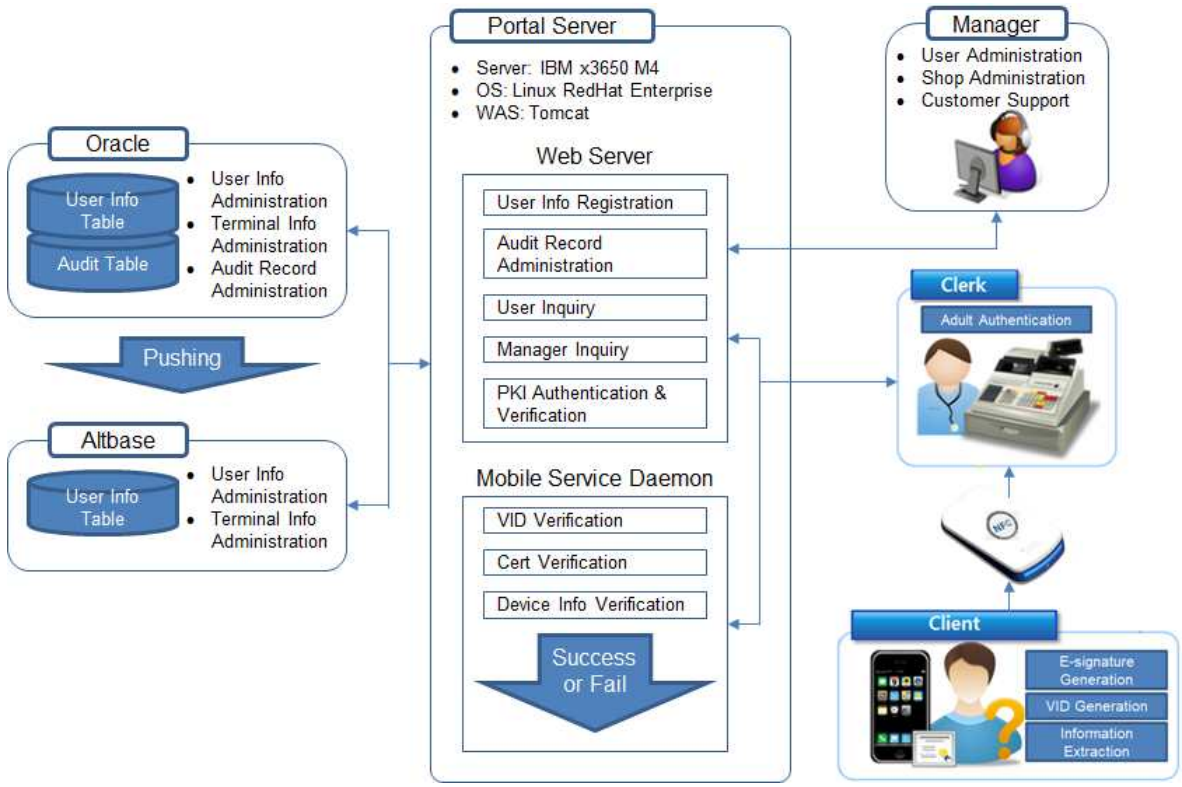

Fig. 3. Operation flow of the proposed adult authentication system
그림 3. 제안하는 성인 인증 시스템의 동작 흐름

서버 사이의 네트워크 통신도 수행한다.

③ 정책 서버 모듈: 사용자의 신원 확인 검증을 실시간으로 수행하며, 사용자 등록, 가맹점 등록, 감사 기록 조회 등의 부가 기능도 수행한다.

④ DB 서버 모듈: 사용자 신원 확인 정보, 사용자 일반 정보, 감사 기록을 저장 및 관리한다.

제안하는 성인 인증 시스템은 그림 3과 같이 동작하며, 구체적인 동작 흐름은 다음과 같다.

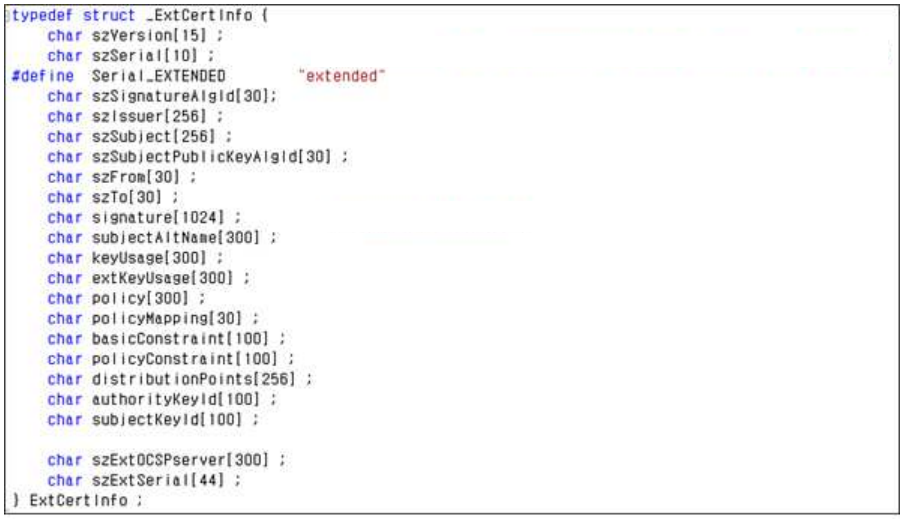

Fig. 4. Field structure in the authentication certificate
그림 4. 공인인증서 내의 필드 구조체

① 구매자가 성인 인증 시스템에 가입할 때 공인인증서로부터 생성된 가상 신원 확인 코드인 VID를 제출하고, 이는 DB 서버에 저장된다.
② 구매자는 매 결재마다 본인의 스마트폰에 저장된 공인인증서를 이용해 성인 인증에 사용할 정보 데이터인 VID'를 생성한다.
③ 구매자가 스마트폰을 판매자의 NFC 리더기에 대면 스마트폰은 VID'를 전송한다.
④ NFC 리더기는 스마트폰에서 수신된 VID'를 네트워크를 통해 정책 서버로 전송한다.
⑤ 정책 서버는 DB 서버로부터 구매자가 가입 시에 미리 제출한 VID 값을 호출하고, 이번에 수신된 VID'와 일치하는지를 판단한다.
⑥ 정책 서버는 네트워크를 통해 검증 결과를 NFC 리더기에 전송한다.
⑦ NFC 리더기는 수신된 검증 결과를 구매자와 판매자 모두에게 알린다.

III. 각 모듈의 설계 및 구현

1. 성인 인증 모듈

성인 인증 모듈은 스마트폰에 저장된 공인인증서로부터 개인 식별 정보인 VID를 생성하며, 스마트폰 앱의 형태로 구현된다.

국내에서 사용하고 있는 공인인증서는 X.509[3] 표준을 따르며, 외부 공개를 위한 인증서 파일(SignCert.der)과 PKCS#11[4] 표준 기반의 패스워드 암호화 된 개인키 파일 (SignPri.key)로 구성되어 있다. 공인인증서로부터 필요한 정보 필드를 추출하기 위해서는 먼저 SignCert.der를 인코딩한 후, 이 데이터를 다시 Hex 코드로 변환하여 그림 4의 필드 구조체에 대입한다.

공인인증서 개인키 파일에는 난수 값인 R이 주입되어 있는데, 이 난수 값은 개인을 확인할 수 있는 식별번호로 사용된다. 여기에 대한 기술 규격은 IETF RFC 4683[5]에 정의되어 있다.

본 논문에서는 민감한 개인정보의 유출을 방지하기 위해 공인인증서에서 추출한 정보를 그대로 사용하지 않고, 여러 개의 필드를 조합해서 식 (1)과 같이 가상 식별 번호인 VID를 생성한 후 이를 암호화한다. 여기에서 h는 해쉬 함수[6], IDN은 주민등록번호와 같은 식별번호, R은 공인인증서 내의 난수이다.

$$VID = h(h(IDN, R)) \quad (1)$$

스마트폰 앱에서는 사용자 정보 등록 및 성인 인증이 수행되며, 동작 흐름은 다음과 같다.

(1) 사용자 정보 등록 과정
① 기본 정보를 입력하고 공인인증서를 선택하면 사용자 등록에 필요한 인증서 정보를 추출한다.
② 스마트폰 앱에서 전자서명 및 암호화 라이브러리에 의해 등록 데이터를 생성한다.
③ 등록 데이터는 NFC 리더기를 통해 정책 서버로 전송되고 등록이 끝나면 메시지를 수신한다.

(2) 성인 인증 과정
① 사용자 정보 등록이 끝난 후, 성인 인증이 필

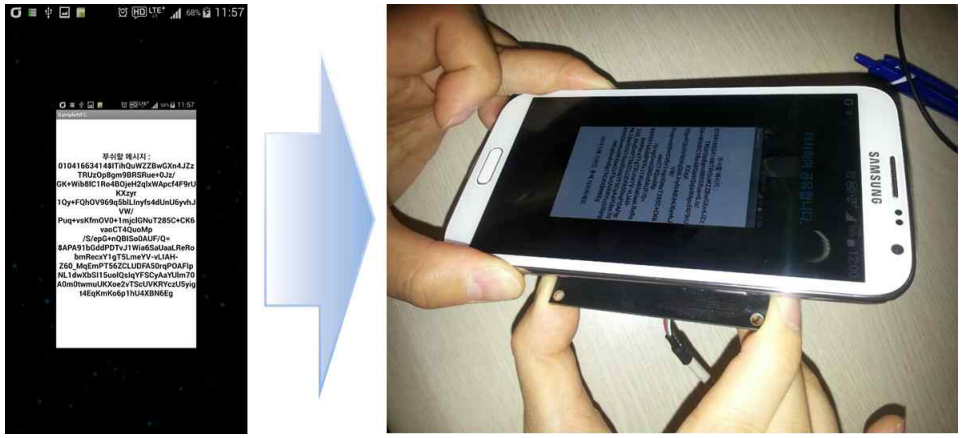

Fig. 5. Execution result of adult authentication
그림 5. 성인 인증 수행 결과

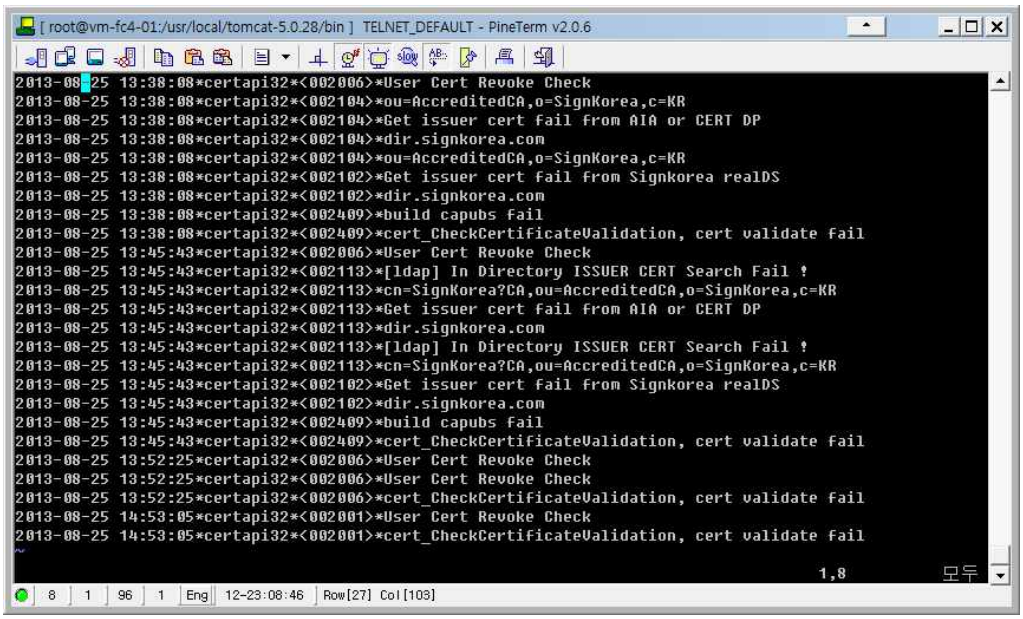

Fig. 6. Validity check of authentication certificate
그림 6. 공인인증서 유효성 검증

요할 때 공인인증서를 선택한다.

② 성인 인증에 필요한 데이터만 추출하여 암호화한 후 NFC 리더기로 데이터를 전송한다.

2. NFC 제어 모듈

NFC 제어 모듈은 스마트폰과 NFC 리더기 사이에 NFC 통신을 통해 데이터를 주고받으며, NFC 리더기와 서버 사이의 네트워크 통신도 수행한다. NFC 통신에서는 NDEF (NFC Data Exchange Format) 메시지의 형태로 데이터를 전달하며, 이를 위해 SNEP (Simple NDEF Exchange Protocol) 프로토콜로 데이터를 주고받을 수 있는 API (Application program interface)를 개발하였다. 개발된 API를 사용하여 NFC를 통해 VID가 제대로 전송되고 성인 인증이 정상적으로 수행됨을 그림 5와 같이 확인하였다.

3. 정책 서버 모듈

정책 서버 모듈은 사용자의 신원 확인 검증을 실시간으로 수행한다. 또한 사용자 등록, 가맹점 등록, 감사 기록 조회 등의 부가 기능도 수행한다. 본 논문에서는 전자를 실시간 성인 인증 서비스, 후자를 관리자 서비스로 나누어 구현하였다.

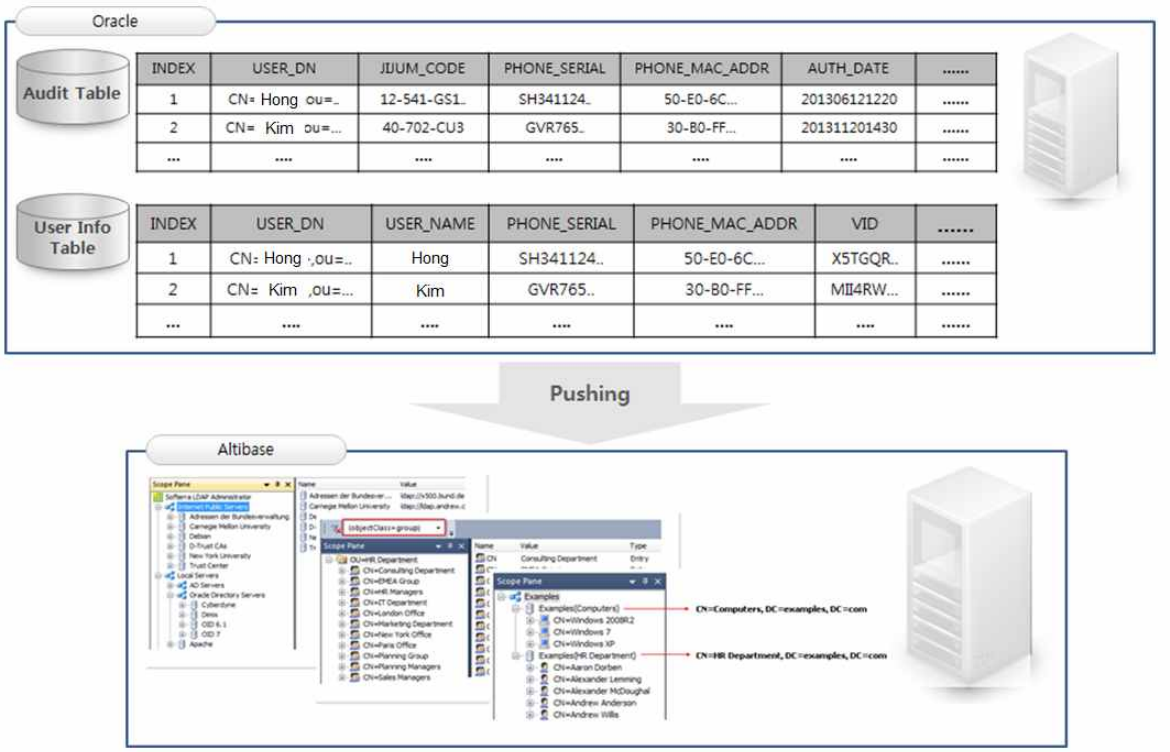

Fig. 7. DB structure
그림 7. DB 구조

(1) 실시간 성인 인증 서비스
① 사용자의 성인 인증 데이터 비교 검증
② 사용자의 스마트폰 인증
③ 사용자 정보 변경 및 감사 기록 저장
④ 데이터 복호화 처리
⑤ DB 연동
(2) 관리자 서비스
① 최초 사용자 정보 등록
② 사용자 서비스 이용 지점 조회
③ 사용자 정보 변경 및 삭제
④ 사용자 조회 및 감사 기록 조회
⑤ DB 연동

사용자가 처음 공인인증서 등록을 할 때에는 이 공인인증서의 유효성을 확인해서 폐기 또는 분실된 것이 아닌지 확인해야 한다. 이를 위해 공인인증기관의 서버와 통신하여 그림 6과 같이 인증서 유효성 검증을 수행하여야 한다.

4. DB 서버 모듈

DB 서버 모듈은 사용자가 등록한 신원 확인 정보인 VID, 사용자 정보, 감사 기록을 저장 및 관리한다. DB 구조는 그림 7과 같으며, 시스템의 부하를 최소화하기 위해 실시간 성인 인증 서비스용 DB와 관리자 서비스용 DB로 나누어 구현하였다. DB 스키마는 표 1과 같이 구성하였다.

5. 구현 결과

본 논문에서는 제안한 성인 인증 시스템을 검증하기 위해 스마트폰, NFC 리더기, PC, 서버를 사용한 테스트 환경을 구축하였으며, 스마트폰 앱, 서버 프로그램, DB 프로그램, NFC 제어 프로그램, 가맹점 프로그램, 관리자 프로그램 등을 개발하여 이들이 모두 서로 연동되어 정상적으로 동작하였으며, 실제 가맹점에서의 성인 인증 시스템 운영에 필요한 다양한 시나리오를 모두 만족하는 것을 확인하였다.

이러한 시스템이 실제로 활용되기 위해서는 동작 속도도 중요하다. 측정 결과 NFC 리더기에서 VID를 송수신하는 시간은 300ms 이내, 정책 서버에서 신원을 확인하는 시간은 200ms 이내, DB에서 데이터를 검색하는 시간은 300ms 이내로 실제 사용에 큰 문제가 없는 수준이다.

Table 1. DB schema (a) User info table (b) Audit info table (c) Smarphone info table (d) Shop info table
표 1. DB 스키마 (a) 사용자 정보 테이블 (b) 감사 정보 테이블 (c) 스마트폰 정보 테이블 (d) 가맹점 정보 테이블

(a)

Column	Data Type	Attribute	Description	Initial Value
INDEX	integer	not null	index number	null
USER_CERT_DN	varchar2(64)	pk	certificate dn	null
CN_NAME	varchar2(32)	not null	certificate cn name	null
VID_VALUE	varchar2(256)	not null	b64encoding(hash)	null
PHONE_SERIAL	varchar2(32)	not null	smartphone serial number	null
PHONE_MAC_ADDR	varchar2(32)	not null	smartphone MAC address	null
PHONE_NUMBER	varchar2(32)	not null	smartphone phone number	null

(b)

Column	Data Type	Attribute	Description	Initial Value
INDEX	integer	not null	index number	null
USER_CERT_DN	varchar2(64)	pk	certificate dn	null
CN_NAME	varchar2(32)	not null	certificate cn name	null
AUTH_DATE	sysdate	not null	authentication request date	null
JIJUM_CODE	varchar2(64)	not null	shop code	null
SUCCESS_FAIL	char(1)	not null	authentication success or failure	null
PHONE_SERIAL	varchar2(32)	not null	smartphone serial number	null
PHONE_MAC_ADDR	varchar2(32)	not null	smartphone MAC address	null
PHONE_NUMBER	varchar2(32)	not null	smartphone phone number	null

(c)

Column	Data Type	Attribute	Description	Initial Value
PHONE_NUMBER	varchar2(11)	not null	smartphone phone number	null
DEVICE_ID	varchar2(200)	not null	smartphone serial number	null
PHONE_TYPE	varchar2(1)	null	OS (Android, IOS)	null

(d)

Column	Data Type	Attribute	Description	Initial Value
CHAIN_ID	varchar2(50)	not null	shop ID	null
CHAIN_NAME	varchar2(20)	not null	shop name	null
CHAIN_ADDRESS	varchar2(1000)	not null	shop address	null
CHAIN_PHONE	varchar2(20)	not null	shop phone number	null

Ⅳ. 결론

본 논문에서는 청소년의 유해물 접근 및 유해업소 출입을 차단하기 위해 스마트폰과 NFC 통신을 이용한 공인 인증서 기반의 성인 인증 시스템을 설계 및 개발하였다. 제안하는 성인 인증 시스템은 성인 인증 모듈, NFC 제어 모듈, 정책 서버 모듈, DB 서버 모듈로 구성되며, 프로토타입을 설계하고 구현하여 정상적으로 동작하는 것을 확인하였다.

References

[1] J. Lee, “Applications and Problems of Authentication Certificate in Smart Environment”, Internet & Security Focus, pp. 23-53, Mar. 2013.

[2] Y. Jung, S. Lee, H. Oh, and T. Jeon, “Research on the Influence of Absorbing Sheet for Electrical Performance of NFC Antenna”, Journal of IKEEE, vol. 16, no. 3, pp. 167-172, Sep. 2013.

[3] ITU-T Recommendation X.509, “Information Technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks”, 2012.

[4] OASIS PKCS#11, “Cryptographic Token Interface Base Specification, Interface Profiles, Current Mechanisms Specification, and Historical Mechanisms Specification”, 2014.

[5] IETF RFC 4683, “Internet X.509 Public Key Infrastructure Subject Identification Method”, 2006.

[6] B. Kim and I. Shin, “Implementation of Authentication Algorithm for CDMA Digital Mobile Communication System”, Journal of IKEEE, vol. 3, no. 2, pp. 204-214, Dec. 1999.

BIOGRAPHY

Chongho Lee (Member)

2002: BS degree in Computer Engineering, Howon University.
2004: MS degree in Computer Engineering, Soongsil University.
2004~2005: S/W Developer, Assistant Manager in Ksign Corporation
2005~2012: Department Manager in ITNade Corporation
2012~Now: CEO in ISolutec Corporation
<Main Interest> PKI Security

Seongsoo Lee (Life Member)

1991: BS degree in Electronic Engineering, Seoul National University.
1993: MS degree in Electronic Engineering, Seoul National University.
1998: PhD degree in Electrical Engineering, Seoul National University.
1998~2000: Research Associate, University of Tokyo.
2000~2002: Research Professor, Ewha Womans University.
2002~Now: Professor in School of Electronic Engineering, Soongsil University.
<Main Interest> HEVC, Low-Power SoC Design, Multimedia SoC Design, Battery Management