ISSN: 1226-7244 (Print)
ISSN: 2288-243X (Online)
논문번호 15-04-22

j.inst.Korean.electr.electron.eng.Vol.19,No.4,610~616,December 2015
http://dx.doi.org/10.7471/ikeee.2015.19.4.610

지문 인식을 이용하여 공인인증서의 보안 요건을 만족하는 전자 신분증 시스템의 설계

Design of Electronic ID System Satisfying Security Requirements of Authentication Certificate Using Fingerprint Recognition

이 종 호*, 이 성 수**★

Chongho Lee*, Seongsoo Lee**★

Abstract

In this paper, an electronic ID system satisfying security requirements of authentication certificate was designed using fingerprint recognition. The proposed electronic ID system generates a digital signature with forgery prevention, confidentiality, content integrity, and personal identification (=non-repudiation) using fingerprint information, and also encrypts, sends, and verify it. The proposed electronic ID system exploits fingerprint instead of user password, so it avoids leakage and hijacking. And it provides same legal force as conventional authentication certificate. The proposed electronic ID consists of 4 modules, i.e. HSM device, verification server, CA server, and RA client. Prototypes of all modules are designed and verified to have correct operation.

요 약

본 논문에서는 지문 인식을 이용하여 공인인증서의 보안 조건을 만족하는 전자 신분증 시스템을 설계 및 개발하였다. 제안하는 전자 신분증 시스템은 지문 정보를 사용하여 위변조 불가, 기밀성, 무결성, 본인 인증 (=부인 방지) 등의 기능을 가진 전자서명문을 생성하고, 이를 암호화, 전송 및 검증한다. 제안하는 전자 신분증 시스템은 사용자 암호 대신에 지문을 사용하여 유출 및 탈취를 피하면서도 기존의 공인인증서와 동일한 법적 효력을 가진다. 제안하는 전자 신분증 시스템은 HSM 디바이스, 검증 서버, CA 서버, RA 클라이언트의 4개 모듈로 설계하였으며 각 모듈의 프로토타입이 정상적으로 동작하는 것을 확인하였다.

Key words : electronic ID, authentication certificate, forgery prevention, confidentiality, content integrity, personal identification, non-repudiation

* 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 22, 2015; revised Dec 28, 2015; accepted Dec 28, 2015.

Ⅰ. 서론

일상생활에서 이루어지는 거래, 계약, 신청, 승인 등의 활동에서는 이들 활동의 주체가 당사자 본인인지를 반드시 확인해야 하며, 오프라인에서는 주민등록증이나 운전면허증 등의 신분증을 확인함으로서 이루어진다. 비대면으로 이루어져서 신분증을 확인할 수 없는 온라인에서 당사자를 확인하기 위해서는 다양한 방법이 사용되며, 우리나라에서는 전자서명법[1]에 근거한 공인인증서(authentication certificate)가 많이 쓰이고 있다.

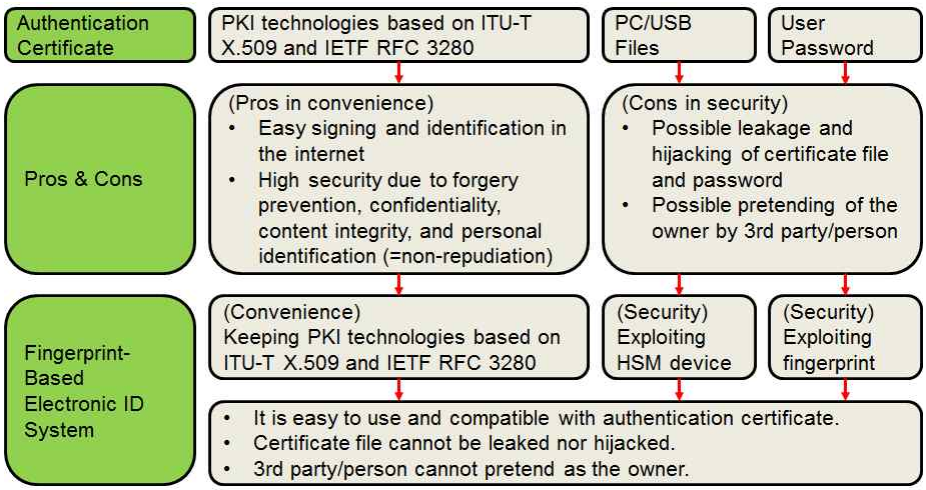

Fig. 1. Problem solving of the authentication certificate through the fingerprint-based electronic ID system
그림 1. 지문 기반 전자 신분증 시스템을 통한 공인인증서의 문제 해결

공인인증서는 위변조 불가 (forgery prevention), 기밀성 (confidentiality), 무결성 (content integrity), 본인 인증 (personal identification) (=부인 방지 (non-repudiation))의 기능을 가지기 때문에 현재 온라인에서 이루어지는 법적 행위의 상당수가 공인인증서를 요구하고 있다.

그러나 최근에 공인인증서의 유출이나 탈취가 기승을 부리면서 공인인증서를 마냥 안전한 신분 증명 수단으로 여기기는 점차 어려워지고 있다. 신분 증명을 위해서는 공인인증서 파일과 사용자 암호 두 가지를 모두 가지고 있어야 하기 때문에 하나만 탈취되었을 경우에는 안전하지만, 두 가지 모두 탈취당했을 때는 제 3자가 온라인에서 본인 행세를 하는 것을 막을 수 없게 된다.

이러한 문제점에 따라 본 논문에서는 지문 인식을 사용하여 공인인증서와 동일한 보안 요건을 모두 만족하는 전자 신분증 시스템을 제안한다.

II. 공인인증서 대체를 위한 요건

공인인증서는 공개키 (PKI: public key infrastructure) 기반의 암호화 알고리즘이 적용되고 신원 확인을 위해 비대칭키 쌍과 사용자의 신원 정보 등의 데이터를 담고 있으며, 전자서명법은 공인인증서에 당사자의 서명과 동일한 법적 효력을 부여하였다. 공인인증서는 위변조 불가, 기밀성, 무결성, 본인 인증 (=부인 방지)의 4가지 보안 요소를 가지고 있으며, 전자서명을 암호화하고 이를 검증할 수 있어야 한다[2].

공인인증서 자체에는 기술적인 문제점이 없으나, 공인인증서 파일 및 비밀번호의 물리적 유출에는 대응할 방법이 없다. 공인인증서 파일은 사용자 PC의 해킹, 피싱, 파밍 등으로 손쉽게 빼돌릴 수 있으며 USB 저장매체도 안심할 수 없다. 공인인증서 비밀번호도 키 스트로크 기록 및 화면 엿보기 등을 통해 손쉽게 빼돌릴 수 있으며 이 경우 사용자의 인지가 거의 불가능하다.

이러한 문제점을 해결하기 위해 공인인증서를 다른 전자적 수단으로 대체하는 경우, 다음과 같은 세 가지 조건이 요구된다.

(1) 공인인증서와 동일한 법적 효력: 위변조 불가, 기밀성, 무결성, 본인 인증, 부인 방지의 기능을 가진 전자서명문을 사용하고, 이 전자서명문을 암호화 및 검증할 수 있는 수단을 가져야 한다.

(2) 안전한 전자서명문 보관 수단: 기존의 공인인증서 파일을 PC나 USB 메모리에 저장하면 쉽게 유출이나 탈취당하기 쉽기 때문에 전자서명문을 안전하게 보관할 수 있어야 한다.

(3) 비밀번호를 대신할 본인 인증 수단: 기존의 공인인증서에서는 사용자가 본인인지를 인증하기 위해 최종적으로 비밀번호를 확인하고 있으나 이는 쉽게 유출이나 탈취당하기 쉽기 때문에 이를 대신할 본인 인증 수단이 필요하다.

이러한 문제점을 해결하기 위해 본 논문에서는 그림 1과 같은 방법을 사용하였다.

(1) ITU-T X.509[3] 및 IETF RFC 3280[4] 표준의

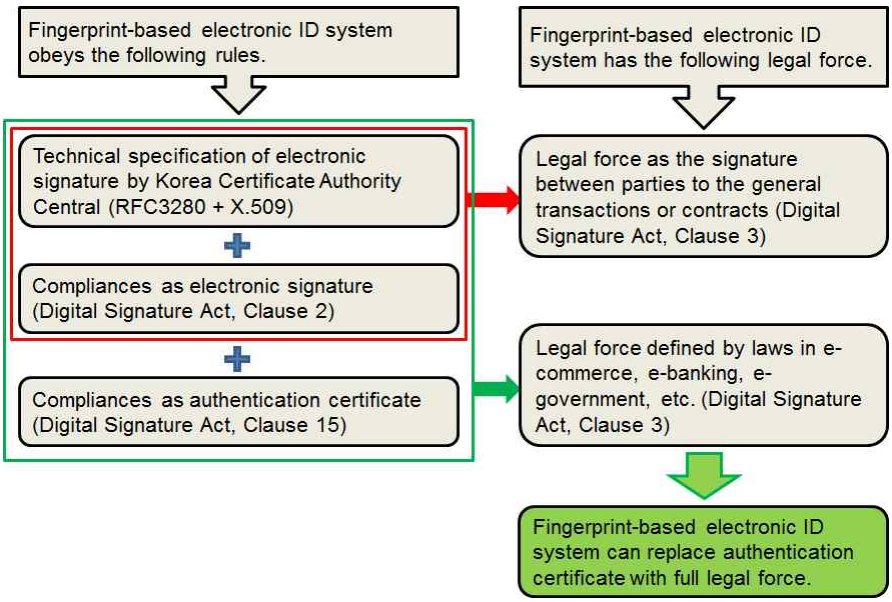

Fig. 2. Legal force of the fingerprint-based electronic ID system
그림 2. 지문 기반 전자 신분증 시스템의 법적 효력

사용: 위변조 불가, 기밀성, 무결성, 본인 인증, 부인 방지의 기능을 가진 전자서명문을 생성하고 이 전자서명문을 암호화 및 검증할 수 있다.

(2) HSM (hardware security module) 디바이스의 사용: 하드웨어적 보안이 이루어지는 HSM에서 전자서명문을 생성하고 보관하여 안전하게 관리할 수 있다.

(3) 지문 인식의 사용: 사용자가 늘 휴대하고 유출 및 탈취가 불가능한 지문을 비밀번호 대신 사용하여 안전하게 본인 인증을 수행할 수 있다.

이렇게 표준 보안 기술, HSM 디바이스, 지문 인식에 기반한 전자 신분증 시스템은 현행 공인인증서와 호환성, 보안성, 편의성을 유지하면서도 본인이 아니면 파일을 빼돌리거나 본인 행세를 할 수 없게 한다.

특히, 제안하는 전자 신분증 시스템은 그림 2와 같이 전자서명법에서 규정한 전자서명의 요건을 완벽하게 갖추고 있기 때문에 법적으로 서명 및 날인의 효력에 아무 문제가 없으며, 공인인증기관이 가입자의 신원을 확인하고 발급하기만 하면 현행 공인인증서를 대체하여 사용하는 데에도 아무 문제가 없다.

이를 좀 더 자세히 설명하면 다음과 같다. 먼저 전자서명법에서는 일반 서명 및 날인과 동일한 효력을 가지는 전자서명과, 인감과 동일한 효력을 가지는 공인인증서를 구분하여 정의하고 있다. 전자서명과 공인인증서가 갖추어야 할 법적 조건은 다음과 같다.

(1) 전자서명의 법적 조건 (전자서명법 2조)

① 전자서명생성정보가 가입자에게 유일하게 속할 것

② 서명 당시 가입자가 전자서명생성정보를 지배·관리하고 있을 것

③ 전자서명이 있은 후에 당해 전자서명에 대한 변경여부를 확인할 수 있을 것

④ 전자서명이 있은 후에 당해 전자문서의 변경여부를 확인할 수 있을 것

(2) 공인인증서의 법적 조건 (전자서명법 2조 및 15조)

① 전자서명법 2조에서 규정한 전자서명에 해당할 것

② 전자서명법 15조에서 규정한 각종 정보를 포함할 것

③ 공인인증기관에서 가입자의 신원을 확인한 후 발급할 것

실제 공인인증서를 운영하는 한국인터넷진흥원 전자서명인증센터 (KCAC)에서는 호환성을 위해 국제 표준인 ITU-T X.509 및 IETF RFC 3280을 사용하고 있으며, 이들 표준을 준수하기만 하면 위 (1)의 ①~④와 (2)의 ①~②를 만족하는 전자서명을 구현할 수 있다. 남아있는 조건인 (2)의 ③은 공인인증기관에서 해당 방식을 채택하여 운

Table 1. Comparison between the authentication certificate and the fingerprint-based electronic ID system
표 1. 공인인증서와 지문 기반 전자 신분증 시스템의 비교

Item	Authentication Certificate	Fingerprint-Based Electronic ID System
Signature Generation	PC or smartphone	HSM device
Signature Storage	computer file	HSM device
Identification Key	password	fingerprint
Ease of Use	good	good
Security Level	poor	good
Standard Compliance	X.509 and RFC 3280	X.509 and RFC 3280
Legal Force in General Transactions or Contracts	yes	yes
Legal Force Defined by Laws in e-Commerce, e-Banking, e-Government, etc.	yes	yes[1)]

1) Valid when it is issued and controlled by CA

영하기만 하면 만족된다.

즉, 본 논문에서 제안하는 지문 기반 전자 신분증 시스템은 ITU-T X.509 및 IETF RFC 3280을 만족하기 때문에 하드웨어/소프트웨어 구현 방식과 공인인증기관의 채택 여부에 관계없이 전자서명 및 전자 신분증으로 사용이 가능하며, 이를 공인인증기관에서 채택하기만 하면 현행 공인인증서를 완전히 대체할 수 있다. 표 1은 공인인증서와 지문 기반 전자 신분증 시스템을 비교한 것이다.

III. 전자 신분증 시스템의 설계

1. 시스템 구성

제안하는 지문 기반 전자 신분증 시스템은 그림 3과 같이 4개의 모듈로 구성되어 있다.

(1) HSM 디바이스: 사용자가 휴대하는 모듈로서 전자서명문의 생성 및 보관과 지문 인식을 하드웨어적 보안 기능이 탑재된 디바이스에서 수행한다.

(2) 검증 서버: 관련 표준에 따라 전자서명문을 검증하고 관련 정보를 관리하는 서버이며, HSM 디바이스와 암복호화[5][6]된 통신으로 데이터를 주고받는다.

(3) CA (certificate authority) 서버: 전자 신분증의 발급 및 관리를 수행한다. CA 서버는 실제로 다음과 같은 3개의 서버의 조합으로 이루어지며, 이들 3개의 서버는 내부적으로 서로 연동되어 동작한다.

① OCSP (Online certificate status protocol) 서버: 전자서명문의 유효성을 실시간으로 검증하는 서버이다.

② RA (registration authority) 서버: 지문 정보를 포함한 전자 신분증에 사용되는 각종 정보를 등록하며, TS 서버와 연동하여 전자 신분증을 발급한다.

③ TS (time stamp) 서버: 전자 신분증의 발급 시점을 관리하고 시점에 대한 무결성을 제공하는 서버이다.

(4) RA 클라이언트: CA 기관은 하나만 존재하여 사용자의 방문이 어려우므로, 대면 확인을 수행하고 등록을 대행하는 다수의 RA 센터가 있다. RA 클라이언트는 RA 센터에서 실제 사용자의 등록 신청을 받고 지문 정보를 취득하며 HSM 디바이스를 발급하는데 사용하는 관리 프로그램으로 CA 기관 내의 RA 서버에 연동된다.

2. 시스템 동작

제안하는 지문 기반 전자 신분증 시스템의 동작은 그림 3에 나타나있다.

(1) 사용자 등록: 사용자가 대면 신청을 통해 RA 클라이언트에서 지문을 등록하고 HSM 디바이스를 수령하면, 지문 정보 등의 관련 정보는 RA 서버로 전달된다.

(2) 전자 신분증 인증서 생성: RA 서버는 전자 신분증의 인증서를 생성하고 이를 저장한다. 이 과정에서 TS 서버와 함께 유효 기간을 부여하고 타임스탬프를 각인한다. 생성된 인증서는 다시 RA 클라이언트로 전송되어 HSM 디바이스 내에

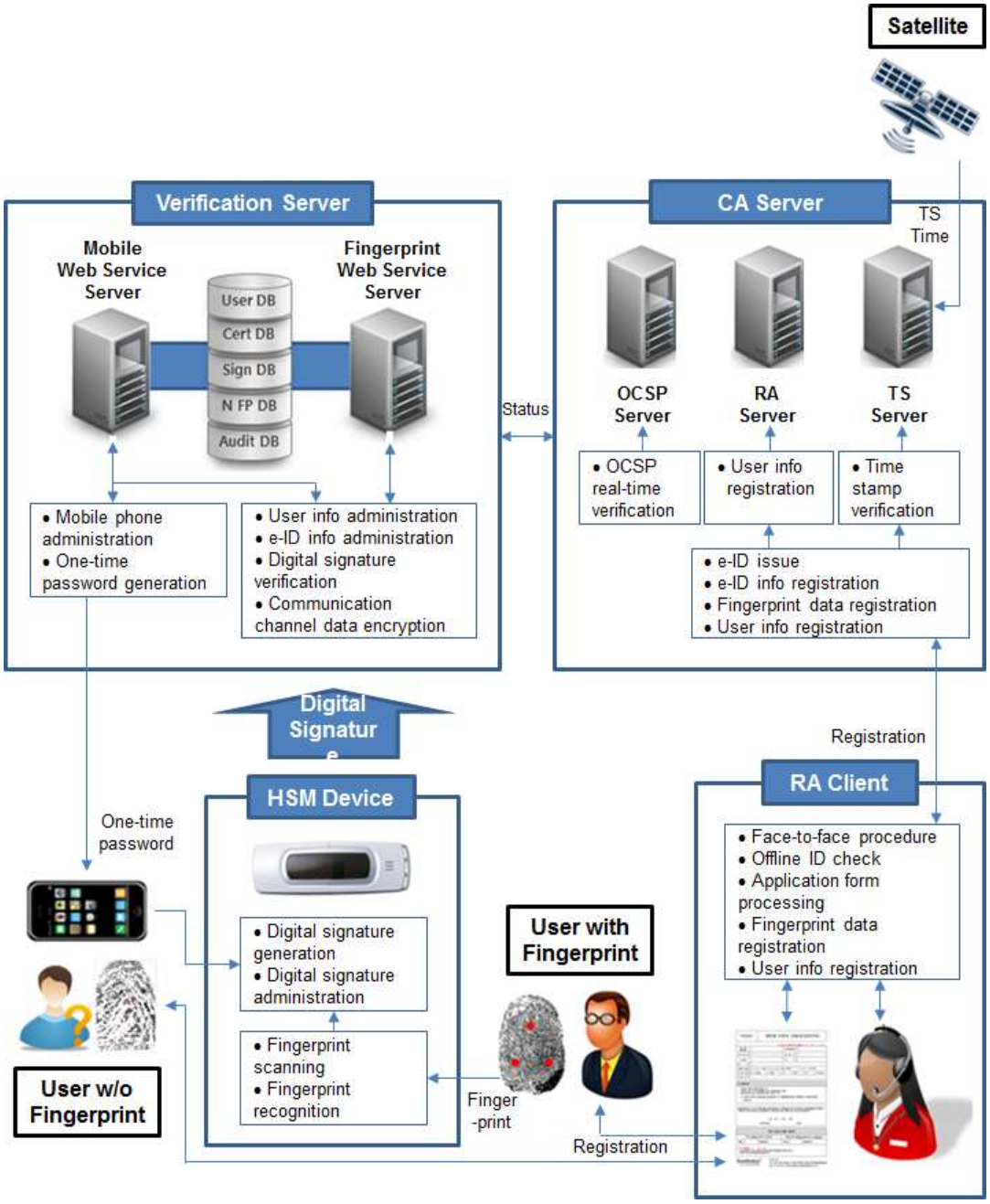

Fig. 3. Configuration of the fingerprint-based electronic ID system
그림 3. 지문 기반 전자 신분증 시스템의 구성도

저장되며, 또한 검증 서버로 전송되어 내부 DB에 저장된다.

(3) 전자서명문 생성: 사용자가 HSM 디바이스에서 전자서명을 시작하면 HSM 디바이스는 사용자의 지문을 인식하여 HSM 내부의 인증서를 사용하여 전자서명문을 생성하고 이를 검증 서버로 전송한다.

(4) 전자서명문 검증: 검증 서버는 HSM 디바이스와의 인터페이스를 담당하는 웹서버이다. 검증 서버는 HSM 디바이스로부터 전송받은 전자서명문을 검증하여 유효한 전자서명인지를 확인한다. 이 과정에서 검증 서버는 OCSP 서버를 통해 인증서가 분실, 만료, 폐기되지 않았는지를 확인한다.

(5) 지문이 없는 사용자: 질병이나 사고로 인해 지문을 사용할 수 없는 경우에는 기존의 휴대폰 인증과 비슷한 방식으로 인증을 수행한다. 사용자가 검증 서버에 휴대폰 인증을 요청하면 검증 서버는 문자 등을 통해 1회용 비밀번호를 전송한다. 사용자가 HSM 디바이스에 이를 입력하면 전

Table 2. Design of basic fields in the fingerprint-based electronic ID system
표 2. 지문 기반 전자 신분증 시스템의 기본 필드 설계

Field Name	Description	Remark
Serial Number	“Serial number” field is the serial number of the certificate issued by CA. It is used as a reference to check whether the certificate is valid, lost, aborted, or discarded. It cannot exceed 20 bytes.	It is the hardware serial number of the HSM device.
Issuer	“Issuer” field is the name of CA that issues the certificate. It should be represented in DN form. It cannot be empty. DN form should keep [KCAC.TS.DN].	
Validity	“Validity” field is the expiry date/time until which CA guarantees the validity of the certificate. Subfields “notBefore” and “notAfter” are the start time of validity and the end time of validity, respectively. Time is represented in GMT. Until 2049, UTCTime format is used. After 2050, GeneralizedTime format is used.	
Subject	“Subject“ field is the name of the certificate owner. It should be represented in DN form. It cannot be empty. DN form should keep [KCAC.TS.DN].	
Subject Public Key Info	“Subject public key info” field is the public key algorithm and information of the certificate owner. Subfield “algorithm” represents specific information of the algorithm in OID form. OID should keep [KCAC.TS.DSIG].	
Subject Private Key Info	“Subject private key info” field is the private key information of the certificate owner. It should keep PKCS#8.	
Fingerprint Data Info	“Fingerprint data info” field is the information of the hashed results of the fingerprint of the certificate owner. It cannot exceed 20 bytes. It should be processed by SHA256.	Newly adopted in this paper
Status	“Status” field is the status of the electronic ID. (Valid, InValid)	Newly adopted in this paper
Mobile Serial Number	“Mobile Serial Number” field is the IMEI serial number of the certificate owner.	Newly adopted in this paper
Mobile Data Info	“Mobile data info” field is the information of the hashed results of the IMEI serial number of the certificate owner. It cannot exceed 20 bytes. It should be processed by SHA256. It is used when the certificate owner cannot use fingerprint by disease or accident.	Newly adopted in this paper
One-Time Password	“One-time password” field is an alternative of “Fingerprint data info” field, and it is used when the certificate owner cannot use fingerprint by disease or accident. It cannot exceed 20 bytes. It should be processed by SHA256.	Newly adopted in this paper

자서명문 검증에 지문 정보 대신에 이 값을 사용하게 된다.

3. 인증서 필드 및 각 모듈의 개발

본 논문에서 제안하는 지문 기반 전자 신분증 시스템은 KCAC에서 채택한 전자서명 인증서 프로파일[7]에 따라 기본 필드를 설계하였다. KCAC의 전자서명 인증서 프로파일은 IETF RFC 3280에 따라 국내 실정에 적합하고 국제 호환성을 고려하여 설계된 것으로 기술적으로는 반드시 이 규격을 따라야 할 필요는 없으나 국내 인터넷 환경에서의 원활한 사용을 위해 이 프로파일을 따르도록 하였다. 본 논문에서 설계한 기본 필드는 표 2와 같다.

본 논문에서 제안하는 지문 기반 전자 신분증 시스템은 전체 아키텍쳐의 설계 및 개발이 완료되었으며, HSM 디바이스, 검증 서버, CA 서버, RA 클라이언트를 구성하는 각 모듈의 프로토타입도 모두 개발이 완료되었다. 각각의 모듈은 정상적으로 동작하는 것이 확인되었으며 현재 모듈간 연동 및 통합이 진행 중이다.

Ⅳ. 결론

본 논문에서는 지문 정보를 사용하여 전자서명문을 생성하고, 이를 암호화, 전송 및 검증하는 지문 기반 전자 신분증 시스템을 제안하였다. 제안하는 시스템은 사용자 암호 대신에 지문을 사용하여 유출 및 탈취를 피하면서도 기존의 공인인증서와 동일한 법적 효력을 가진다. 제안하는 시스템의 전체 아키텍처와 각 구성 모듈이 설계되었으며 설계된 각 모듈이 정상적으로 동작하였다.

References

[1] Digital Signature Act, http://www.law.go.kr/lsInfoP.do?lsiSeq=160903&efYd=20141015#0000

[2] J. Lee and S. Lee, “Development of Electronic ID Performing as Authentication Certificate Based on Fingerprint Recognition”, Proceedings of IEIE Fall Conference, CFP-020, 2015.

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

[4] IETF RFC 3280, “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile”, 2002.

[5] W. Park, “Encryption of Biometrics Data for Security Improvement in the User Authentication System”, Journal of IKEEE. vol. 9, no. 1, pp. 31-39, Apr. 2005.

[6] H. Kim, S. Kim, and K. Cho, “Design of Low-area Encryption Circuit Based on AES-128 Suitable for Tiny Applications“, Journal of IKEEE. vol. 18, no. 2, pp. 198-205, Jun. 2014.

[7] TTAS.KO-12.0012/R1, “Digital Signature Certificate Profile”, 2006.

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