KIPS Tr. Comp. and Comm. Sys.
Vol.2, No.12 pp.511~516 pISSN: 2287-5891

http://dx.doi.org/10.3745/KTCCS.2013.2.12.511

A Study on the Next Generation Identification System of Mobile-Based using Anonymous Authentication Scheme

Jeong Hyo Park† · Yong Hoon Jung†† · Moon Seog Jun†††

ABSTRACT

The cases of identification forgery and counterfeiting are increasing under the current identification system, which was established based on social conditions and administrative environments over 20 years ago. This leads to an increase of various criminal acts including illegal loan using fake ID and a number of damages caused out of good intentions that result in interference with the operations of public organizations. In addition, according to the advancement of information society, privacy protection has emerged as an important issue. However, ID card exposes individuals' personal information, such as names, resident registration numbers, photos, addresses and fingerprints, and thus the incidents associated with illegal use of personal information are increasing continuously. Accordingly, this study aimed at examining the issues of ID card forgery/ counterfeiting and privacy protection and at proposing a next-generation identification system to supplement such weaknesses. The top priority has been set as prevention of forgery/ counterfeiting and privacy protection in order to ensure the most important function of national identification system, which is user identification.

Keywords : National ID Card, Privacy, Prevent Forgery, Anonymous Authentication Scheme, The Next Generation Identification Means

익명 인증기법을 이용한 모바일 기반 차세대 본인확인수단에 관한 연구

박 정 효† · 정 용 훈†† · 전 문 석†††

요 약

20여년 이전의 사회적 여건과 행정환경을 전제로 만들어진 현행 신분증은 매년 위·변조 사례가 증가하고 있다. 이에 따라, 신분증 위·변조로 인한 불법대출 등 각종 범죄행위가 증가하고, 공공기관의 업무지장이 초래되는 등 많은 선의의 피해가 발생하고 있다. 또한, 정보화 사회가 진전되면서 프라이버시 보호가 매우 중요해지고 있다. 하지만 주민등록증은 이름, 주민등록번호, 사진, 주소, 지문 등 사용자의 개인정보가 그대로 노출되어 개인정보 도용사고가 지속적으로 증가하고 있다. 이에 따라, 본 논문에서는 주민등록증의 위·변조 및 프라이버시 보호의 문제점을 살펴보고 이를 보완할 수 있는 차세대 본인확인수단을 제안한다. 이는 국가신분증의 가장 중요한 기능인 사용자 본인확인에 충실하기 위해 위·변조 방지 및 프라이버시 보호를 최우선 목표로 하였다.

키워드 : 국가신분증, 프라이버시, 위·변조 방지, 익명 인증기법, 차세대 본인확인수단

1. 서 론

주민등록증은 주민등록법에 의해 시장, 군수, 구청장이 만 17세 이상인 신청 국민에게 발급하는 증명서로, 지급결제, 인터넷뱅킹 등 본인확인수단으로 광범위하게 사용되고 있다.

현재의 주민등록증은 이름, 사진, 주민등록번호, 주소, 지문 등 사용자 개인의 프라이버시 정보가 표면에 그대로 노출되어 있어, 사용자의 개인정보를 이용한 불법대출 등 각종 범죄에 악용되고 있다.

이러한 문제점을 개선하고자 1997년 "전자주민카드 등록법" 개정 추진, 1999년 "전자주민카드 제도 추진계획" 발표, 2013년 "전자주민등록증 발급계획" 발표 등 정부가 주도적으로 전자신분증 도입을 추진해오고 있다.

현재 전자신분증을 도입하고 있는 해외 여러 국가들은 비접촉식 스마트카드 기능의 IC(Integrated Circuit)칩에 사용

† 정 회 원 : 숭실대학교 컴퓨터통신학과 박사수료
†† 준 회 원 : 숭실대학교 컴퓨터학과 박사
††† 종신회원 : 숭실대학교 컴퓨터학부 정교수
논문접수 : 2013년 9월 30일
심사완료 : 2013년 11월 26일
* Corresponding Author : Jeong Hyo Park(helios914@ssu.ac.kr)

자 정보 및 바이오 정보 그리고 발급 카드의 정보 등을 포함하고 있다.

하지만 이러한 정보들을 보호하기 위한 보안 기능을 포함하고 있음에도 불구하고, 전자신분증 복제, 도용, 개인정보 유출 등의 위험을 그대로 가지고 있으며, 개인정보의 안전한 저장 및 사용, 사용자 인증을 포함한 정보보안의 문제 또한 크게 부각되고 있다.

이러한 문제점들을 해결하기 위해 본 논문에서는 익명 인증기법을 이용하여 온라인 및 오프라인에서 사용자 본인확인시 사용자 정보 노출을 최소화하고 보다 안전하게 보호할 수 있는 방안을 제시한다.

본 논문은 총 5장으로 구성되어 있다. 제2장에서는 주민등록증 대체수단의 필요성에 대해 기술한다. 제3장에서는 익명 인증기법을 이용한 모바일 기반 차세대 본인확인수단을 제안하고 이용 상세절차를 기술한다. 제4장에서는 국내·외 전자신분증 관련 표준과 비교하여 연산횟수 및 처리속도의 효율성을 분석한다. 마지막으로 제5장에서는 결론을 제시하고 향후 연구과제 및 방향에 대해 기술한다.

2. 주민등록증 대체수단의 필요성

2.1 주민등록증 위·변조 사례 증가

현행 주민등록증은 쉽게 위·변조가 가능하여 범죄에 많이 사용되고 있으며, 매년 주민등록증 위·변조 검거사례가 증가하고 있다. 이러한 위·변조된 주민등록증을 이용한 범죄행위로 선의의 피해자가 발생되거나 공공기관의 업무에 지장이 초래되는 일도 빈번하게 발생하고 있다.

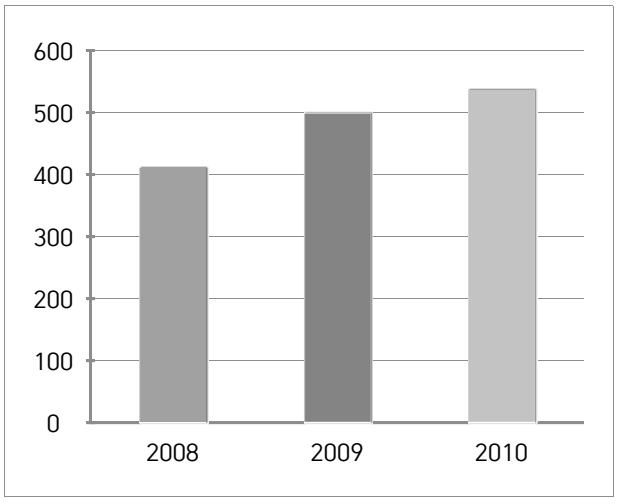

Fig. 1. Arrest Status of National Identification Card Fogery (Police Resources in 2011)

Fig. 1는 2011년 10월 기준 경찰청이 집계한 “주민등록증 위·변조 사건 사례” 통계를 나타내고 있다. 경찰청이 공개한 이 자료에 따르면 주민등록증 위·변조 사건은 2008년 410건에서 2009년 499건, 2010년 536건으로 최근 3년간 30.7% 증가했다. 그러나 주민등록증 위·변조 사례가 발견되지 않거나 발견되어도 여러 가지 이유로 고발되지 아니한 경우를 포함하면 실제 위·변조 사례는 더 많을 것으로 추정된다.

이러한 주민등록증의 문제점들을 보완하기 위해, 플라스틱 주민등록증을 도입하면서 여러 보안기술(홀로그램, 미세문자 등)을 채택하였으나, 복사·변조 기술이 계속 발전함에 따라 현행 주민등록증 형태로는 위·변조 주민등록증의 유통에 대응하는데 한계가 있는 실정이다.

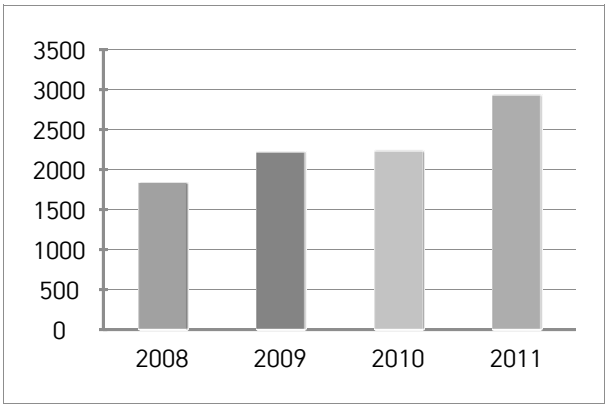

Fig. 2. Social security law violations and arrests Status (Police Resources in 2012)

Fig 2.는 2012년 10월 기준 경찰청이 집계한 “주민등록법 위반 및 검거현황” 자료에 따르면 2008년부터 2012년 8월까지 주민등록법을 위반했다가 검거된 사람이 1만 1천428명으로 집계됐다. 주민등록법 위반 행위는 다른 사람의 주민등록증을 부정하게 사용하는 행위, 거짓 주민등록번호를 만들어 본인 또는 다른 사람의 재산상 이익을 위해 사용하는 행위, 주민등록증와 관련한 거짓 사실을 신고하는 행위 등이 모두 포함된다.

주민등록법을 위반해 검거된 사람은 2008년에는 1천821명이었지만 2009년 2천209명, 2010년 2천227명, 2011년 2천924명으로 가파른 증가세를 보이고 있다.

국민 기본 신분증으로서 주민등록증의 가장 기본적이며 중요한 기능이 신분 확인, 즉 본인여부 확인인데 다수의 위·변조 사례가 나타나 이러한 기능수행에 지장을 초래하고 있으며, 국가 신분증 제도의 신뢰도가 떨어지고 있는 것은 매우 큰 문제이다.

2.2 프라이버시 보호 취약

정보화 사회가 진전되면서 프라이버시 또는 사생활 보호가 매우 중요한 요소로 자리 잡고 있다. 특히, 최근 개인정보 유출 사건이나 피해사례가 사회적으로 논란이 되면서 이 부분에 대한 국민들의 관심이 매우 높아져 있고 일부에서는 피해의식까지 호소하고 있다. 이러한 사고의 원인으로는 이름, 주민등록번호, 주소, 지문 등이 주민등록증 표면에 노출되어 있다는 점이다.

Fig. 3. National Identification Card

Fig. 3는 현행 주민등록증에서 이름, 사진, 주민등록번호, 주소, 지문 등 사용자 개인의 프라이버시 정보들이 그대로 노출되어 있음을 보여준다.

주민등록번호와 지문의 외부 기재는 지난 1983년 종이 주민등록증의 도입 이전부터 채택된 것이다. 사실 재질 부분만을 제외한다면 현행 주민등록증은 23년 전인 1983년 당시의 사회적 여건을 전제로 고안된 것이며, 오늘의 사회 환경이나 가치 기준에서 보면 미흡할 수밖에 없다.

우리사회가 정보화 사회로 진전되면서 주민등록번호가 여러 가지의 개인정보를 통합하는 키로서의 역할을 하고 있으며, 주민등록번호 도용 피해가 잇따라 제기되면서, 주민등록번호와 지문의 노출은 꼭 개선되어야 한다는 의견이 지속적으로 제기되고 있다.

2.3 정보화 사회로의 급속한 변화 및 활용도 저하

국가신분증 제도가 기능해야 할 사회적, 행정적 환경은 이미 과거와 크게 달라져 있어 새로운 국민생활 패턴에 맞는 제도와 서비스 설계가 필요해지고 있다.

그간 주민등록증은 민원 처리나 각종 증명서 발급, 금융거래 등의 경우에 오프라인에서 신분을 확인하는 용도로 주로 사용되어 왔다.

그러나 국민생활은 이미 종래의 오프라인 영역을 크게 넘어 온라인 영역으로 전개되고 있다. 온라인 영역의 대표적인 서비스로는 각종 증명서 발급, 인터넷 뱅킹, 각종 지급결제 등을 사용하고 있으며, 온라인 또는 사이버 공간을 통한 국민생활의 비중은 앞으로 더욱 커질 것이다. 현행 주민등록증은 정보화 사회의 진전으로 급속히 확대되는 온라인 공간에서의 활용도가 없다. 그러나 각종 오프라인 창구에서 신분확인 기능은 여전히 중요한 역할이지만, 이러한 역할만으로 주민등록증의 소지·활용가치는 계속 저하될 수밖에 없을 것이다.

3. 익명 인증기법을 이용한 모바일 기반 차세대 본인확인수단

차세대 본인확인수단은 기존의 플라스틱 형태의 구조 즉, 하드웨어 토큰방식이 아닌 소프트웨어 토큰방식으로 설계되어 있다.

이는 국내 스마트폰 가입자 수가 3,330만명('13.1월 기준)을 넘어 지속적으로 증가하고 있으며, 사용자의 67.7%가 하루 일과 시간중 8시간 이상을 몸에 지니고 있는 생활습관을 반영한다.

또한, 소프트웨어 토큰방식의 본인확인수단이 분실되어도 즉시 갱신 및 폐지가 가능하여, 사용자의 이용편의성과 저장매체의 안전성을 높였다.

3.1 차세대 본인확인수단 발급

차세대 본인확인수단은 국내·외 전자신분증과 물리적 구조가 같다. 하지만 주민등록증과 같은 고유식별번호 사용으로 인한 위험을 감소시키기 위해, 익명 인증기법을 이용하여 고유식별번호가 아닌 익명식별번호를 생성하여 사용한다.

이는 사용자 요청에 의해 즉시 변경이나 폐기가 가능하며, 기존 주민등록번호 13자리가 아닌 512자리 임의의 숫자를 사용함으로써 무단 및 추측 생성 등 악의적인 시도를 미연에 방지할 수 있다.

사용자가 차세대 본인확인수단을 발급받기 위해서는 발급기관에 직접 방문하여 발급기관 담당자와 직접 대면과정을 통해 본인확인 후 발급 신청해야 한다. 발급 상세과정은 다음 Table 1과 같다.

Table 1. The next generation identification system of the issuance process

· **STEP 1 (사용자→발급기관)** : ID, PW, PIN
· **STEP 2 (발급기관)** : ASN ≤ 512bits
※ ASN(Anonymous Serial Number) : 익명식별번호
· **STEP 3 (발급기관)** : USER_INFO = (EI ‖ SI)
※ EI(Essential Information) : 성명, 주민등록번호, 주소, 지문, 발행번호, 공인인증서 등 필수 정보
※ SI(Selective Information) : 혈액형, 소유자의 물리적 특징 등 선택 정보
· **STEP 4 (발급기관)** : H_{PW} = H(PW)
· **STEP 5 (발급기관)** :
E-ID=E_{HPW}{USER_INFO ‖ ASN ‖ ID}
※ E-ID(Electronic-Identification) : 차세대 본인확인수단인 전자신분증

Table 2. The certification of the issuance process

· **STEP 1 (사용자)** : ID, PW
· **STEP 2 (사용자→발급기관)** : E_{RA-PU}{ID, PW}
· **STEP 3 (발급기관)** : D_{RA-PR}{ID, PW}
· **STEP 4 (사용자)** : U_{PR}, U_{PU}
· **STEP 5 (사용자)** :
CSR = E_{KEY}(U_{PU}, USER_INFO)
· **STEP 6 (사용자→발급기관)** : E_{RA-PU}{CSR, KEY}
· **STEP 7 (발급기관)** : D_{RA-PU}{CSR, KEY}
· **STEP 8 (발급기관→인증기관)** :
REQ=E_{CA-PU}{CSR, KEY}
· **STEP 9 (인증기관)** : D_{CA-PR}{REQ}, D_{KEY}{CSR},
USER_CER=E_{CA-PU}{CA_{PU}, U_{PU}, USER_INFO}
· **STEP 10 (인증기관→발급기관)** :
E_{RA-PU}{USER_CER}
· **STEP 11 (발급기관→사용자)** :
D_{RA-PR}{USER_CER}

전자신분증에 추가 인증수단으로 특수목적용 인증서 중 본인확인용 공인인증서를 반드시 추가 발급받아야 한다. 이는 현재 공인인증서에 없는 서비스이므로 본 논문에서 추가적으로 세부사항을 정의하였다.

본인확인용 인증서 발급 절차는 다음 Table 2과 같다.

3.2 모바일 기기에 차세대 본인확인수단 등록

오프라인으로 발급받은 차세대 본인확인수단은 모바일 기기에 등록이 가능하다. 단, 소프트웨어 토큰방식이므로 안전한 저장매체(HSM, USIM 등)에 보관 및 이용하여야 한다.

등록하는 상세 과정은 다음 Table 3과 같다.

Table 3. The next generation identification system of the enrollment process

- **STEP 1 (사용자→모바일)** : ID, PW
- **STEP 2 (모바일→발급기관)** : IDT=E_{RA-PU}{ID, PW}
- **STEP 3 (발급기관)** : D_{RA-PR}{IDT}
- **STEP 4 (발급기관→모바일)** : AUTH=E_{U-PU}{ID, PW, Timestamp}
- **STEP 5 (모바일)** : D_{U-PR}{AUTH}
- **STEP 6 (모바일→발급기관)** : EN=E_{RA-PU}{ID, PW, Timestamp, SN}, SIG=E_{U-PR}{H(EN)}, USER_CER
- **STEP 7 (발급기관)** : D_{RA-PR}{EN}
- **STEP 8 (발급기관→인증기관)** : REQ=E_{CA-PU}{H(EN)', SIG, USER_CER}
- **STEP 9 (인증기관)** : D_{CA-PR}{REQ}, H(EN)' == D_{U-PU}{SIG}
- **STEP 10 (인증기관→발급기관)** : Result
- **STEP 11 (발급기관→모바일)** : Result

3.3 차세대 본인확인수단 갱신

차세대 본인확인수단 역시 기존 주민등록증과 같이 일정 기간 이후 갱신이 필요하며, 갱신 방법은 모바일 기반에서 이루어지게 된다. 오프라인 대면확인 과정에서 입력한 갱신용 비밀번호를 사용하여 사용자를 인증하며, 이는 단순한 사용자의 정보뿐만 아니라 모바일 자체의 정보를 활용하여 추측공격에 대한 안전성을 높였다.

상세 갱신과정은 다음 Table 4과 같다.

3.4 이용자 요청에 의한 차세대 본인확인수단 폐기

모바일 기반 차세대 본인확인 수단은 분실 및 도난 위험이 있으므로, 사용자가 원하는 즉시 폐기가 가능하도록 제안한다. 상세 폐기 절차는 다음 Table 5과 같다.

4. 성능 분석

본 논문에서 제안하는 모바일 기반 차세대 본인확인수단은 전자여권 표준인 BAC(Basic Access Control), PA (Passive Authentication), AA(Active Authentication) 규격을 기반으로 구성되어 있다.

Table 4. The next generation identification system of the update process

- **STEP 1 (사용자)** : ID, PW, USER-CERT, PIN
- **STEP 2 (모바일)** : NEW=E_{RA-PU}{ID,PIN}, NSIG=E_{U-PR}{H(NEW)}
- **STEP 3 (모바일→발급기관)** : E_{RA-PU}{NEW, NSIG, USER_CER}
- **STEP 4 (발급기관)** : D_{RA-PR}{NEW, NSIG, USER_CER}
- **STEP 5 (발급기관→인증기관)** : E_{CA-PU}{NSIG, USER_CER}
- **STEP 6 (인증기관)** : D_{CA-PR}{NSIG, USER_CER}
- **STEP 7 (인증기관→발급기관)** : H'==D_{U-PU}{NSIG}
- **STEP 8 (발급기관)** : D_{RA-PR}{NEW}
- **STEP 9 (발급기관→모바일)** : ID'=ID+nounce, ASN'=ASN≤512bits
- **STEP 10 (모바일)** : UPDATE(ID', ASN')

Table 5. The next generation identification system of the disposal process

- **STEP 1 (사용자→컴퓨터)** : ID, PW, USER_CERT, PIN
- **STEP 2 (컴퓨터)** : DELETE=E_{RA-PU}{ID, PIN}
- **STEP 3 (컴퓨터→발급기관)** : DELETE, DSIG=E_{U-PR}{H(DELETE)}, USER_CERT
- **STEP 4 (발급기관→인증기관)** : E_{CA-PU}{DSIG, USER_CER}
- **STEP 5 (인증기관)** : D_{CA-PR}{DSIG, USER_CER}
- **STEP 6 (인증기관→발급기관)** : H'==D_{U-PR}{DSIG}
- **STEP 7 (발급기관)** : D_{RA-PR}{DELETE}, USER_INFO 삭제
- **STEP 8 (발급기관→컴퓨터)** : DELETE RESULT

이에 따라, 본 장에서는 차세대 본인확인수단과 전자여권 표준의 암·복호화, 난수생성, 서명 생성 및 검증 등에 대한 항목들에 대하여, 연산횟수 및 처리시간의 효율성을 비교·분석하였다.

Table 6는 차세대 본인확인수단이 기존 전자여권 표준에 비하여 연산횟수를 최소화하고 있음을 알 수 있다. 또한 암·복호화, 난수생성, 서명 생성 및 검증에서 전자여권 표준과

Table 6. The number of operations between electronic identification and readers(number)

Compare the number of operations	The number of operations between electronic identification and readers(number)				
	encrypt	decrypt	random generate	signature generate	signature verify
BAC	2	2	4	2	2
PA	1	1	3	1	1
AA	2	1	4	1	1
Proposed	1	1	2	1	1

Table 7. The time of processing between electronic identification and servers(ms)

Compare the processing time	The time of processing between electronic identification and servers(ms)	
	E-passport standard	the next generation identification means
1 time	0.536	0.542
10 times	3.601	3.500
100 times	33.192	32.891
200 times	84.804	84.214
300 times	170.210	156.216
400 times	223.653	206.033
500 times	360.173	314.425

비교하여 동일한 안전성을 보장하면서도 최소 연산횟수로 동작함을 알 수 있다.

Table 7는 사용자의 애플리케이션과 발행기관 서버 사이의 총 처리시간을 측정하였다. 단, 처리시간 비교 과정에서 동시처리(그룹인증 등)에 관한 사항은 논외로 하고, 순차적으로 처리한 시간만을 고려하여 측정하였다.

비교 횟수가 증가함에 따라 연산시간의 효율성은 격차가 더욱 벌어졌으며, 이는 차세대 본인확인수단에서 암·복호화, 서명 생성 및 검증 횟수 등을 최소로 한 결과를 보여준다.

5. 결 론

본 논문을 작성하는데 있어, 국가신분증의 가장 중요한 기능 중 하나인 사용자 본인확인에 충실하기 위해 위·변조 방지, 프라이버시 보호 강화를 최우선 목표로 하여, 온라인 및 오프라인에서 사용되는 전자신분증을 모바일 환경에서 차세대 본인확인수단으로 이용할 수 있도록 등록, 갱신, 폐기 절차를 제안하였다.

기존 플라스틱 주민등록증과 관련하여 제기된 프라이버시 취약 논란을 근본적으로 해소하기 위하여, 이름, 주민등록번호, 주소, 지문 등은 외부에 노출되지 않도록 소프트웨어 토큰방식의 익명 인증기법을 사용하였으며, 온라인상에서 빠른 식별처리를 위해 연산횟수 및 처리시간의 효율성을 높였다.

이는 빠른 본인식별 시간으로 민원처리 속도가 빨라지고, 무엇보다 온-오프라인상 본인확인 절차의 개선으로 각종 행정민원 처리나 공공서비스 이용이 보다 용이해 질 것이다.

이에 따라, 행정의 효율도 크게 증대될 것으로 기대된다.

향후 주민등록증에 여타 부가서비스를 탑재하는 경우에는 그로인한 편의 증대도 기대할 수 있을 것이다.

참 고 문 헌

[1] YoungHo Park, ByungUn Kong, KyungHyune Rhee, “Design of an Authentication System Based on Personal Identity Verification Card”, Journal of Korea Multimedia Society Vol.13, No.8, August, 2011.

[2] Jongho Mun, changhwan Lee, Keyn Kwon, Kwangwoo Lee, Dongho Won, “Consideration to introducing Electronic-ID”, Korea Computer Congress Vol.38, 2011.

[3] Jung Hyo Park. “The Design and Implementation of Anonymous Authentication Method based on Smart-Card”, Master’s thesis, Soongsil University, 2010.

[4] Ho Jung Lee. “A Study on Improved-electronic Identity Document Service Protocol”, Master's thesis, Hanyang University, 2009.

[5] Kil Young Oh, “Battle Front : Issues and Implications of Electronic Resident Registration Card”, Democratic Legal Studies Association, pp.305-332, 2011.

[6] HyungHyo Lee, Heeman Park, SangRae Cho, SeungHun Lee, “A Propose of New National Identification Number System Providing privacy Protection for online and offline environment”, Journal of the Korea Information Security, Vol.20, 2010.

[7] BSI, “Common Criteria Protection Profile - Machine Readable Travel Document with ICAO Application, Basic Access Control”, BSI-PP-0017, Version 1.0, 18th August, 2005.

[8] BSI, “Advanced Security Mechanisms Machine Readable Travel Documents- Extended Access Control(EAC)”, Version 2.05, TR-03110, 2010.

[9] NIST, “Special Publication 800-78-1 : Cryptographic Algorithms and Key Sizes for Personal Identity Verification”, August, 2007.

[10] NIST, “Special Publication 800-78-2 : Interfaces for Personal Identity Verification -Part2 : End Point PIV Card Application Card Command Interface”, September, 2008.

[11] NIST, “Special Publication 800-78-2 : Interfaces for Personal Identity Verification -Part3 : End Point PIV Card Application Card Command Interface”, September, 2008.

[12] NIST, “Special Publication 800-78-2 : Interfaces for Personal Identity Verification -Part4 : End Point PIV Card Application Card Command Interface”, September, 2008.

박 정 효

e-mail : helios914@ssu.ac.kr

2001년 숭실대학교 컴퓨터학과(학사)

2009년 숭실대학교 정보보안학과(석사)

2011년~현 재 숭실대학교 컴퓨터통신학과 박사수료

관심분야 : anonymous authentication, multi-factor authentication, diversity authentication techniques

정 용 훈

e-mail : s0178@ssu.ac.kr
2004년 숭실대학교 전자계산원(학사)
2006년 숭실대학교 컴퓨터학과(석사)
2010년 숭실대학교 컴퓨터학과 박사
관심분야 : anonymous authentication, multi-factor authentication, multimedia security

전 문 석

e-mail : mjun@ssu.ac.kr
1981년 숭실대학교 컴퓨터학과(학사)
1986년 University of Maryland 전산과 (석사)
1989년 University of Maryland 전산과 (박사)
1989년 Morgan State University(전산수학과 조교수)
1991년~현 재 숭실대학교 컴퓨터학부 정교수
관심분야 : 정보보호, 전자여권, 전자상거래, 암호학