Journal of Korea Multimedia Society Vol. 14, No. 8, August 2011(pp. 1029-1040)

전자신분증 기반의 개인 신분확인을 위한 인증시스템 설계

박영호[†], 공병운[††], 이경현[†††]

요 약

스마트카드 기반의 전자신분증은 오프라인과 온라인 신분확인을 위한 대표적인 개인 신분확인 수단으로, IC칩에 카드소유자의 신분확인 정보와 암호기법이나 전자인증서 관리를 위한 암호화 모듈을 포함하게 된다. 개인 식별정보에 대한 빠른 접근성과 신뢰성 및 보안성으로 인해 주요자산에 대한 접근통제를 위해 전자신분증을 도입하려는 공공기관이나 기업들이 증가하고 있다. 본 논문에서는 전자신분증을 이용한 접근통제에서 개인 신분확인을 위한 인증시스템의 구현방안에 대해 제안하고, 효과적인 인증시스템의 운영을 위한 기능적 요구사항들에 대해 논의한다. 이를 위해 본 논문에서는 Personal Identity Verification 시스템 모델을 대상으로 하여 연구하였다.

Design of an Authentication System Based on Personal Identity Verification Card

Young-Ho Park[†], Byung-Un Kong[††], Kyung-Hyune Rhee[†††]

ABSTRACT

Electronic identity (e-ID) card based on smartcard is a representative identity credential for on-line and off-line personal identification. The e-ID card can store the personal identity information securely, so that the information can be accessed fast, automated identity verification and used to determine the cardholder's authorization to access protected resources. Due to such features of an e-ID card, the number of government organizations and corporate enterprises that consider using e-ID card for identity management is increasing. In this paper, we present an authentication framework for access control system using e-ID cards by discussing the threat environment and security requirement against e-ID card. Specifically, to accomplish our purpose, we consider the Personal Identity Verification system as our target model.

Key words: e-ID(전자신분증), Personal Identification(개인식별), Authentication(인증), Access Control (접근통제)

※ 교신저자(Corresponding Author) : 이경현, 주소 : 부산광역시 남구 대연3동 부경대학교 IT융합응용공학과 1305호(608-737), 전화 : 051) 629-6247, FAX : 051) 626-4887, E-mail : khrhee@pknu.ac.kr
접수일 : 2010년 11월 29일, 수정일 : 2011년 5월 14일
완료일 : 2011년 6월 28일
[†] 준회원, 부경대학교 IT융합응용공학과
(E-mail : pyhoya@pknu.ac.kr)
[††] 정회원, 부경대학교 대학원 정보시스템협동과정
(E-mail : kong2177@paran.com)
[†††] 종신회원, 부경대학교 IT융합응용공학과
※ 이 논문은 2011년도 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임(No. 2011-0012849).

1. 서 론

개인 신원식별과 인증기술은 주요 자산에 대한 접근통제와 정보보호를 위한 가장 기본적인 수단이며, 최근 정보서비스 기술이 우리의 일상생활과 밀접한 환경으로 변화함에 따라 개인 또는 개체 인증의 중요성이 더욱 부각되고 있다. 이처럼 IT기술의 발전과 서비스 환경의 변화에 따라 다양한 형태의 인증 메커니즘을 제공하기 위해 여러 형태의 인증 방법들을 조합한 효율적이고 안전한 다중요소 개인 인증(Multi-factor Authentication) 서비스의 필요성이 대두되었으며, 온라인과 오프라인에서 개인의 신원을 확인할 수 있는 대표적인 수단으로 스마트카드 기반의 전자신분증(Electronic Identity Card)이 있다.

전자신분증은 정부기관, 기업 등의 신뢰기관이 발급하는 공인된 신분증으로서, 기존의 오프라인에서 사용되는 신원 확인 정보를 대체하여 더욱 안전하고 신뢰성 있는 개인 신분확인을 가능하게 할뿐만 아니라 온라인 환경에서도 일관성 있게 사용할 수 있다는 이점이 있다. 더욱이 전자신분증은 전자화되고 자동화된 사용자의 식별과 인증 및 디지털 서명에 사용될 수 있으며 인증 절차와 서비스를 효율적으로 제공하는 것을 목적으로 하고 있다.

카드 기반의 개인 신분증명은 편리성과 대중성으로 인해 가장 널리 사용되고 있는 방법이지만, 전자신분증을 이용한 개인 신분확인과 인증이 안전하게 수행되기 위해서는 강건한 암호 알고리즘과 암호학적 키의 사용뿐만 아니라 시스템의 구성 및 운영에 대한 관리적 보안도 충분히 검토되어야 한다[1]. 또한 개인 신원정보에 대한 식별과 인증은 보안에 민감한 자원에 대한 물리적 접근통제뿐만 아니라 논리적 접근통제를 수행하기 위한 기본적인 수단이며, 올바른 인증 서비스를 제공하기 위해서는 개인의 신분증명(Credential) 수단에 대한 안전한 사용과 정확한 검증이 필요하다.

이미 유럽 일부 국가에서는 전자신분증이 발급되어 사용되고 있으며[2], 현재 국내에서도 전자주민증의 도입이 검토되고 있는 시점에서 전자신분증을 이용한 강건한 사용자 신분확인 및 효과적인 인증 시스템 구축에 대한 연구가 필요하다. 따라서 본 논문에서는 개인용 전자신분증에 대한 기술적 요구사항과 보안 요구사항이 잘 정립되어 있는 미국의 PIV (Personal Identity Verification)[3,4] 시스템 기술을 살펴보고, 이를 기반으로 전자신분증을 이용한 개인 신분확인 인증 프레임워크를 제안하고자 한다. 제안되는 인증 프레임워크는 전자신분증의 강화된 인증을 위해 온라인 인증서버를 이용한 신분증명 요소의 상태검증을 토대로 하며, 서로 다른 발급기관에 의해 발급된 전자신분증의 상호운영성(interoperability)을 위해 상호기관 연동 인증시스템 설계방안에 대해 고려한다.

본 논문의 구성은 다음과 같다. 2장에서는 PIV 시스템의 기본적인 구성과 PIV 카드의 신분증명 데이터 모델 및 인증 메커니즘들에 대해 간략하게 살펴본다. 3장에서는 PIV 신분증명 요소의 인증 보증등급을 강화하기 위한 온라인 신분증명 상태검증 기반의 인증 프레임워크를 제안한다. 4장에서는 전자신분증의 위협요인에 대한 대응방안과 시스템의 성공적인 도입과 운영에 필요한 고려사항들에 대해 모색하고, 마지막으로 5장에서 결론을 맺도록 한다.

2. 배경지식

2.1 PIV 시스템

PIV 시스템의 구성요소들을 기능에 따라 구분하면 그림 1과 같이 세 가지의 주요 하부시스템으로 구분될 수 있으며, 각각의 기능은 다음과 같다.

■ PIV 프런트-엔드(Front-end) 시스템

카드 판독기 및 기록기, PIV 카드, 개인식별번호(PIN) 입력장치 그리고 생체인식 판독기로 구성된

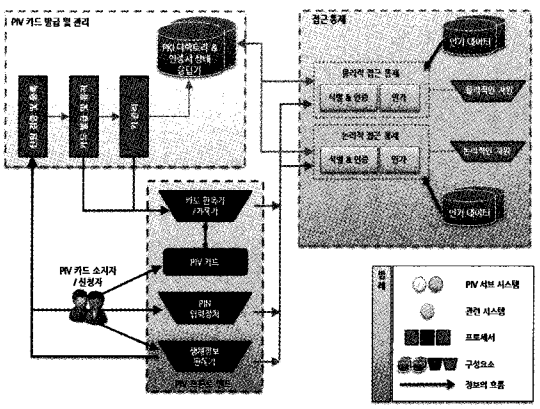

그림 1. PIV 시스템 구성 모델

다. 카드소유자는 물리적/논리적 접근권한을 획득하기 위해 이 시스템과 상호 동작한다.

■ PIV 카드 발급(Issuance)과 관리(Management) 시스템

신원 검증 및 등록, 카드 발급과 유지 보수, 키 관리를 담당하며, 공개키 인증서 디렉터리와 인증서 상태 검증 등의 PKI(Public Key Infrastructure) 구조를 지원한다.

■ 접근통제(Access Control) 시스템

보호 자원과 인가된 데이터에 대한 물리적 또는 논리적 접근을 통제하기 위한 정보들로 구성된다.

PIV 시스템에 대한 표준명세는 NIST FIPS PUB 201-1 문서에 정의되어 있으며[3], 이 문서는 PIV 시스템에 대한 기술적 요구사항들과 다양한 보안수준을 제공하기 위한 인증 메커니즘을 정의하고 있다. 그리고 SP 800-73[5]과 800-76[6], 800-78[7]은 PIV 카드 어플리케이션을 위한 데이터 모델과 인터페이스, 생체인식 데이터 명세, 암호 알고리즘과 키 길이 요구사항에 대해 각각 명시하고 있다. PIV 시스템에 구현된 모든 암호 모듈은 FIPS 140-2[8]를 기준으로 CMVP(Cryptographic Module Validation Program)에 따라 평가되며 보안등급(Security Level) 2 이상이 되어야 CMVP 인증을 획득할 수 있다[9].

2.2 PIV 신분증명 요소

PIV 카드는 카드소유자의 신분확인을 위한 물리적 신분증명 요소와 논리적 신분증명 요소들을 포함한다. 물리적 신분증명 요소는 시각적으로 카드소유자의 신원을 확인하기 위해 PIV 카드에 인쇄되는 신분확인 요소들이다. 표 1은 PIV 카드의 주요 인쇄요소들을 요약하여 나타내고 있다.

PIV 카드의 논리적 신분증명 요소는 전자적인 방법으로 개인의 신분을 확인하기 위한 수단으로, PIV 표준은 다음과 같은 네 가지 필수 신분증명 요소들을 정의하고 있다.

- 개인식별번호(Personal Identification Number, PIN)
- 카드소유자 식별자(Cardholder Unique Identifier, CHUID)
- PIV 인증키 인증서(PIV Authentication Key Certificate)
- 생체지문인식 정보(Biometric Fingerprints)

표 1. 시각적 신분증명을 위한 필수 및 선택 인쇄요소

필수 요소	- 카드소유자의 이름과 300dpi 이상 해상도 사진 - 소속기관(Organization)과 직위(Employee) 식별자 - 카드 유효기간 (YYYYMMMDD 형식) - 카드 일련번호 (Serial Number) - 발급기관 식별자 (Issuer Identifier)
선택 요소	- 기관명 또는 부서명 - 기관 또는 부서의 직인 - 카드소유자의 물리적 특징 - 카드소유자의 서명

CHUID는 접촉식과 비접촉식 칩 모두에 저장되며, 카드소유자를 유일하게 식별하기 위해 연방기관 자격증명 번호(Federal Agency Smart Credential Number, FASC-N)를 포함하여 구성되어 있다. PIV 표준은 또한 신분증명을 위한 네 가지의 암호학적 키 유형을 정의하고 있으며, 표 2는 이러한 암호학적 키의 분류를 요약하여 나타내고 있다.

2.3 PIV 인증 메커니즘

FIPS 201-1에서는 PIV 카드의 인증을 위해, 시각적 인증(Visual Authentication), CHUID 인증, PIV 인증서를 이용한 PKI 기반의 인증, 생체인식 인증 메커니즘과 선택적 구현사항으로 카드 인증키를 이용한 CAK 인증 메커니즘으로 정의하고 있다. SP 800-73에서는 이러한 인증 메커니즘을 카드 검증(Card Validation, CardV), 신분증명 검증(Credential Validation, CredV) 그리고 카드소유자 검증(Cardholder Validation, HolderV) 과정으로 구성하고 있고, 표 3은 각각의 PIV 인증 메커니즘에서 수행되는 검증 단계의 내용을 요약하여 보여주고 있다. 이때 BIO(A)는 보안 감독관이 카드소유자와 동반하여 생체인식 인증처리 과정을 감독하는 인증방법을 의미한다.

일반적으로 신분확인 요소는 "something you know", "something you have", "something you are"의 속성에 따라 분류될 수 있으며, 접근통제 시스템

표 2. PIV 신분증명을 위한 암호학적 키의 분류

PIV 키 유형		목 적
PIV 인증키 (PIV Authentication Key)	필수	- 상호운용성을 지원하는 환경에서 인증을 지원하기 위한 비대칭 개인키 - X.509 인증서 확장필드에 FASC-N을 포함
카드 인증키 (Card Authentication Key)	선택	- 물리적 접근 환경을 위한 대칭형 비밀키 또는 비대칭 개인키 - 상호운영성과 확장성을 위해 비대칭 개인키와 공개키 인증서의 사용을 권장
전자 서명키 (Digital Signature Key)	선택	- 문서의 서명을 지원하기 위한 비대칭 개인키 - 전자서명 키의 검증을 위한 X.509 인증서도 카드에 저장
키 관리키 (Key Management Key)	선택	- 키의 설정(establishment), 전송(transport) 및 암호화(encryption)에 사용하기 위한 비대칭 개인키

표 3. PIV 인증 메커니즘별 검증 내용

PIV 인증 메커니즘	CardV	CredV	HolderV
Visual	물리적 위조/변조/모조 등 진위 여부 검사	유효기간 검사	카드소유, 시각적 특징 비교
CHUID		유효기간 검사, CHUID 서명 검사	카드 소유
CAK	시도/응답(대칭키), 서명 검증(비대칭키)	카드 만료 검사, 인증서 검증	카드 소유
PIV 인증서 (PKI 기반)	서명 검증 수행	카드 만료 검사, PIV 인증서 검증	카드 소유, PIN 검증
BIO		카드 만료 검사, CHUID 서명 검증, BIO 데이터 서명 검증, CHUID의 FASC-N과 BIO의 FASC-N 비교	카드 소유, PIN 검증, 카드소유자의 실제 BIO와 PIV BIO 비교
BIO(A)		카드 만료 검사, CHUID 서명 검사, BIO 데이터 서명 검증, CHUID의 FASC-N과 BIO의 FASC-N 비교,	카드 소유, PIN 검증, 감독자의 동반

은 PIV 인증 메커니즘의 결합을 통해 다중요소(multi-factor) 인증 메커니즘을 구성할 수 있다. 물리적 접근통제시스템(Physical Access Control System, PACS)에 적용하기 위한 PIV 인증 메커니즘의 요구사항을 기술하고 있는 SP 800-116[10]에서는 다중요소 PIV 인증 메커니즘의 조합방법에 대해 표 4와 같이 분류하고 있다. 예를 들어, PKI와 BIO 인증은 각각 두 가지와 한 가지 요소를 만족하며, 이 둘을 결합하여 세 가지 요소를 만족하는 인증 메커니즘을 구성할 수 있다.

표 4. PIV 인증 메커니즘을 결합한 다중요소 인증 예

PIV Auth.	Have	Know	Are	Interface
PKI+BIO	○	○	○	접촉식
BIO-A	○		○	접촉식
PKI	○	○		접촉식
BIO			○	접촉식
CAK	○			접촉식/비접촉식
CHUID+Visual	○			접촉식/비접촉식

3. PIV 인증 프레임워크

본 장에서는 백-엔드 시스템(Back-End System)과 기관 상호연동 게이트웨이(Inter-Agency Gateway)를 통해 PIV 신분증명 요소에 대한 실시간 온라인 상태검증 트랜잭션을 수행할 수 있는 인증시스템 구현방안 대해 제시하도록 한다.

3.1 인증시스템 요구사항

SP 800-116에서는 PIV 카드에 대해 발생 가능한 위협요인들을 표 5와 같이 분석하였으며, 접근통제를 위한 인증시스템의 구축 시 이들 위협요인들에 대응할 수 있는 방안을 마련하도록 요구하고 있다.

일반적으로 접근통제를 위한 PIV 카드 인증은 로컬시스템에 의해 처리되고 카드 발급 시에 IC칩에 저장된 신분증명 요소들에 의존하게 되므로, 카드소유자에 대한 인증은 카드가 발급된 당시의 상태로 인증된 카드로 취급된다. 그러나 카드 발급 이후에 카드소유자에 대한 개인정보나 PIV 신분증명 요소들의 상태정보가 변경될 수 있으므로, 로컬시스템 제시된 PIV 카드만으로는 이러한 상태정보에 대한 유효성을 검증할 수 없다. 이에 대해 [10]에서는 온라인으로 PIV 신분증명 요소의 유효성을 검증함으로써 인증에 대한 보증을 강화하도록 권장하고 있다.

또한 PIV 카드는 여러 발급기관을 통해 발급될 수 있고 PIV 카드를 발급한 조직과 PIV 카드에 대한 인증을 수행하는 조직이 서로 다를 수도 있으므로, 개인용 전자신분증을 범용 환경에서 활용하기 위해서는 기관들의 상호연동을 통해 PIV 신분증명 상태를 검증할 수 있는 방안도 마련되어야 할 것이다. 이를 위해 미국의 Federal Smart Card Interagency Advisory Board의 백-엔드 인증 워킹그룹에서는 PIV 카드 발급기관들의 상호연동을 통한신분증명 상태검증을 위한 가이드라인을 제시하였다.

따라서 본 논문에서는 표 5의 위협요인들과 백-엔드 인증 워킹그룹의 가이드라인을 고려하여 백-엔드 시스템을 이용해 온라인으로 실시간적으로 PIV 신분증명 요소의 유효성을 검증할 수 있는 인증시스템 구현방안에 대해 제안하도록 한다. 본 논문에서는 개인용 전자신분증에 대한 인증시스템의 기술적 구성만을 목표로 하며, 전자신분증에 대한 개인정보보호 방안에 대해서는 논외로 한다.

표 5. PIV 카드에 발생 가능한 위협요인

위협요인	내 용
식별자 충돌	- 동일한 식별자를 사용하는 다수의 PIV 카드
종결된 카드 악용	- 도난/분실 또는 취소된 카드의 부당한 사용
인쇄요소 위조	- 카드의 물리적 신분증명 요소 복제
스키밍	- 카드 데이터에 대한 불법적 단말기의 접근
스니핑	- 카드와 단말기의 통신 도청
전자적 복제	- 논리적 신분증명 요소의 복제
전자적 모방	- 카드의 전자적 신분확인 동작 모방

3.2 상호기관 연동 인증시스템 모델

그림 2는 본 논문에서 고려하는 백-엔드 게이트웨이를 통한 상호기관 연동 PIV 인증시스템 모델의 기본적인 구성요소들을 도식화하여 나타내고 있으며, 각 구성요소의 기능은 다음과 같다.

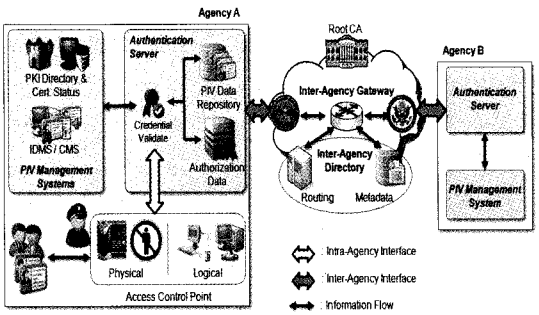

그림 2. 백-엔드 게이트웨이 연동 기관 상호 인증시스템 모델

3.2.1 인증서버

인증서버(Authentication Server)는 PIV 카드를 인증하기 위한 정보를 담고 있는 물리적 개체로서, 로컬 PIV 데이터 저장소나 OCSP 응답서버를 통해 PIV 신분증명의 인증과 유효성 검증을 수행한다. 또한 인증서버는 해당 기관내부에 접근통제 수행을 위해 설치된 접속 단말기에 대한 공개키 인증서의 발급과 관리도 담당한다. 표 6은 PIV 인증수행을 위한 인증서버 시스템의 주요 구성요소와 이들의 기능을 요약하여 나타내고 있다.

표 6. 기관 인증서버 및 백-엔드 시스템의 구성과 기능

구성요소	기 능
기관 내부 인터페이스 (Intra-Agency Interface)	- 접근통제지점이나 PIV 애플리케이션을 내부 신분증명 검증서비스와 연결
상호기관 인터페이스 (Inter-Agency Interface)	- 기관 상호 간의 PIV 신분증명 상태 질의 메시지와 이에 대한 응답 메시지를 교환 - 상태 질의 및 응답 메시지에 대한 보안 처리
신분증명 검증서비스 (Credential Validate)	- PIV 신분증명에 대한 검증을 처리하는 서비스 - PIV 인증/인가 데이터 저장소와 또는 PIV 관리 시스템과 연결
PIV 데이터 저장소 (PIV Data Repository)	- 기관내의 등록 관리와 카드 발급 시스템에서 생성된 인증정보의 로컬 저장소 - 개인 신원확인 정보 및 신분증명 상태정보 보관

3.2.2 PIV 관리시스템

PIV 관리시스템(PIV Management System)은 신원정보의 검증 및 등록을 위한 신원관리시스템(Identity Management System, IDMS)과 카드 발급과 유지를 위한 카드관리시스템(Card Management System, CMS) 그리고 PKI 기반의 공개키와 인증서 관리 및 인증서 상태정보 서비스를 위해 CRL (Certificate Revocation List)과 OCSP(On-line Certificate Status Protocol) 응답서버 등으로 구성된다. PKI 구성요소는 해당 기관에서 발급한 PIV 인증서와 접속 단말기들에 대한 인증서의 상태정보를 관리한다.

3.2.3 상호기관 연동 게이트웨이

상호기관 연동 게이트웨이(Inter-Agency Gateway)는 외부 PIV 발급 및 관리 기관들 사이의 안전한 메시지 전달을 담당한다. 게이트웨이는 인터넷을 통해 상호기관 디렉터리에 대한 연결과 백-엔드 인증을 위한 외부 기관들 사이의 안전한 네트워크 연결을 제공하며 VPN(Virtual Private Network) 기능을 이용하여 별도의 네트워크 연결로 구성될 수도 있다.

3.2.4 상호기관 디렉터리

상호기관 디렉터리(Inter-Agency Directory)는 서로 다른 기관들 사이의 정보전달과 통신보안에 적용하기 위한 메타정보(metadata)와 라우팅 정보(routing data) 디렉터리들로 구성되어 중앙집중식으로 관리된다. 상호기관 디렉터리는 백-엔드 게이트웨이를 통한 신분증명의 인증을 위해 다음과 같은 기능들을 제공한다. 표 7은 상호기관 디렉터리의 주요 구성요소와 각각의 기능에 대해 요약하여 설명하고 있다.

3.3 PIV 인증 및 신분증명 상태검증 절차

PIV 인증 절차는 카드소유자가 제시한 PIV 카드가 기관 내부에서 발급된 경우와 외부 기관에서 발급된 경우에 따라 기관내부 인증과 외부기관에 대한 상호기관 인증 절차로 처리된다. 본 논문에서 제안하는 인증 프레임워크에서의 인증절차를 설명함에 있어 다음 사항들을 가정한다.

- 각 기관의 인증서버는 최상위 인증기관(Root CA)이 발급한 공개키 인증서를 보유
- 카드소유자에 대해 인증서버는 신뢰되는 개체이고, 기관과 기관 사이에는 상호인증에 대한 신뢰관계가 형성되어 있음
- PIV 카드는 최상위 인증기관의 인증서를 포함하여 자신의 카드 발급기관의 공개키 인증서 체인을 포함

표 7. Inter-Agency Directory 주요구성 및 기능

구성요소	기 능
메타정보 디렉터리 (Metadata Directory)	- PIV 카드 발급기관의 조직 분류(Organization Category)와 식별자(Identifier) - 메시지 라우팅을 위한 상호기관 게이트웨이 식별자(Inter-Agency Gateway Identifier) - 메시지 암호화와 서명검증을 위한 기관들의 공개키
라우팅 디렉터리 (Routing Directory)	- 상호기관 게이트웨이 식별자에 대한 IP주소나 URL

- 접근통제지점의 접속 단말기는 해당 기관의 인증서버에서 발급한 공개키 인증서를 보유
- 사전 등록과정을 통해 PIV 카드 및 카드소유자에 대한 접근권한 정보가 로컬 데이터베이스에 저장

3.3.1 기관내부 인증

그림 3은 PIV 카드가 발급된 기관내부의 인증서버에 의한 PIV 인증과정을 도식화하여 나타내고 있으며, 세부적인 절차는 다음과 같다.

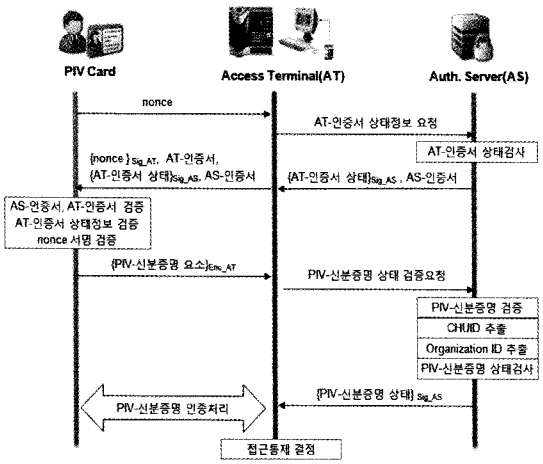

그림 3. 기관 내부 PIV 인증 절차

1) 카드소유자가 접속 단말기에 PIV 카드를 제시하면 단말기 인증을 위해 임의의 nonce를 생성하여 접속 단말기(AT)로 전달한다.
2) AT는 내부 인증서버(AS)에게 자신의 AT-인증서에 대한 상태정보를 요청한다.
3) AS는 AT-인증서 상태검사를 처리한 결과와 함께 AS-인증서를 넘겨준다. 이때 AT-인증서에 대한 상태정보는 AS의 전자서명 {AT-인증서상태}$_{Sig_AS}$를 포함한다.
4) AT는 nonce에 대한 서명 {nonce}$_{Sig_AT}$를 생성하여 AT-인증서와 AS로부터 넘겨받은 인증서 상태정보 {AT-인증서상태}$_{Sig\_AS}$ 및 AS-인증서를 PIV 카드로 전달한다.
5) PIV 카드는 먼저 AS-인증서를 검증하고 AS가 제공한 AT-인증서 상태정보 메시지를 검사한다. 만약 AT-인증서의 상태가 유효하다면 PIV 카드는 AT-인증서와 {nonce}$_{Sig_AT}$을 검증함으로써 AT에 대한 인증을 처리하게 된다.
6) AT에 대한 인증이 성공하면 PIV 인증을 위한 신분증명 요소를 AT를 통해 AS에게 전달한다. 이때 접속 단말기는 접근통제지점의 카드 리더기나 클라이언트 시스템이 될 수 있으며 기관내부 인터페이스를 통해 PIV 카드에 저장된 CHUID나 PIV 인증서 등의 신분증명 요소가 AS에게 전달된다. 그리고 필요한 경우 신분증명 요소는 AT의 공개키로 암호화되어 전송될 수도 있다.
7) AS는 CHUID를 파싱하여 조직 식별자(Organization ID)를 추출하고, 조직 식별자가 내부 기관임을 발견하고 PIV 신분증명의 상태를 검사하기 위해 기관내부의 신분증명 검증서비스를 호출한다.
8) 신분증명 검증서비스는 PIV 데이터 저장소나 CRL 분배서버 또는 OCSP 응답서버를 사용하여 주어진 PIV 신분증명 요소의 상태를 검사하고, 상태검사 결과를 AT에게 반환한다. 이때 상태검사 결과는 AS의 전자서명 {PIV-신분증명 상태}$_{Sig_AS}$를 포함한다.
9) AT는 PIV 신분증명 상태검사 결과 메시지에 포함된 AS의 서명을 먼저 검증하고, PIV 신분증명이 유효한 상태이면 2.3절에서 소개한 해당 신분증명 요소를 이용한 인증 메커니즘에 따라 PIV 카드에 대한 인증을 처리한다.
10) PIV 카드에 대한 인증이 정상적으로 완료되면 접근통제 결정이 접근통제지점의 제어 패널에 디스플레이 되거나 PIV 애플리케이션으로 전달된다.

3.3.2 상호기관 인증

그림 4는 PIV 카드가 외부기관에서 사용되는 경우 상호기관 연동에 의한 PIV 인증과 신분증명 상태검사를 도식화하여 나타내고 있다.

PIV 카드와 접속 단말기 사이의 처리과정은 기관내부 인증과 차이가 없으나 PIV 신분증명 요소의 상태를 검사하기 위해 상호기관 인터페이스를 통해 PIV 카드 발급기관의 인증서버와 상태 질의 메시지와 상태 응답 메시지를 교환하는 절차에 차이가 있다. 세부적인 절차는 다음과 같다.

1)~6) 접속 단말기에 대한 인증 과정으로, 기관내부

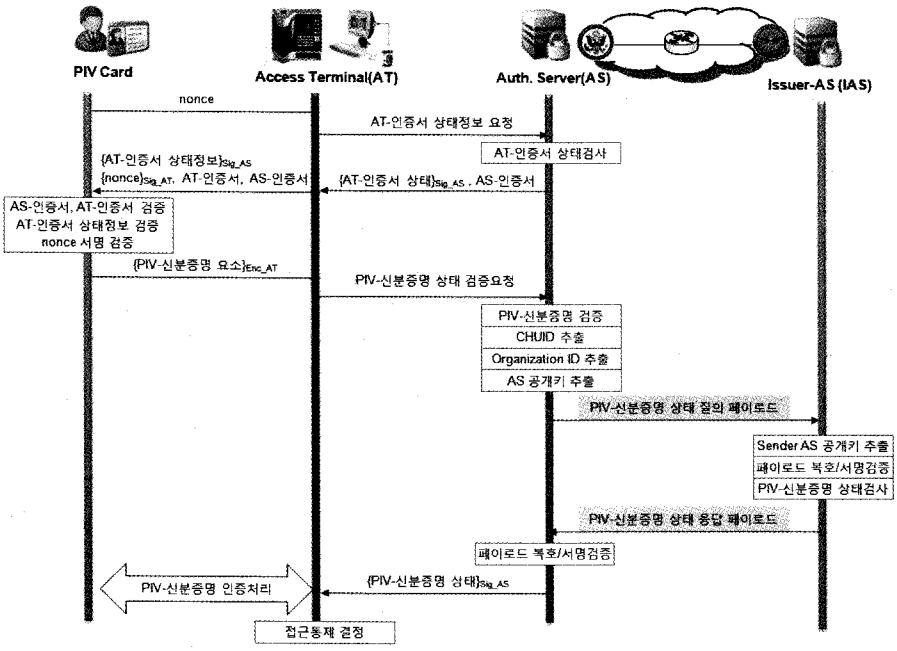

그림 4. 상호기관 PIV 인증 절차

인증 절차의 1)부터 6)까지 처리와 동일하다.

7) AS는 CHUID를 파싱하여 조직 식별자(Organization ID)를 추출하고, 조직 식별자가 외부 기관임을 발견하고 상호기관 인터페이스를 호출한다.

8) 상호기관 인터페이스는 메타정보와 라우팅 디렉터리를 검색하여 조직 식별자에 대한 Gateway ID를 찾아, 다음과 같이 PIV 신분증명 상태 질의 메시지를 생성하여 상호기관 게이트웨이를 통해 전달한다.
   - 송신측과 수신측의 Gateway ID가 모두 포함된 메시지 헤더
   - 신분증명 요소에 대한 상태 질의 정보로 구성된 페이로드로, 이때 페이로드는 X.509 인증서 또는 수집된 지문인식 이미지 등을 포함할 수도 있음
   - 페이로드에 대한 암호학적 해시 결과를 송신측(상태 질의 기관)의 개인키로 서명
   - 메타정보 디렉터리를 통해 검색된 수신측(상태 응답 기관)의 공개키로 페이로드를 암호화

9) 응답 기관의 상호기관 인터페이스는 수신된 상태 질의를 다음과 같이 처리한다.
   - 수신한 응답 기관의 개인키로 메시지 페이로드를 복호화
   - 헤더에 포함된 송신측 Gateway ID와 메타정보 디렉터리를 이용하여 송신측 기관의 공개키를 획득하고 서명을 검증
   - 메시지를 파싱하여 PIV 신분증명 요소를 내부의 신분증명 검증 서비스로 전달

10) 신분증명 검증서비스는 PIV 데이터 저장소와 CRL 분배서버 또는 OCSP 응답서버를 사용하여 주어진 PIV 신분증명 요소의 상태를 검사한다. 상태검사 결과 응답 메시지를 다음과 같이 생성하고, 수신측 기관의 Gateway ID를 이용하여 라우팅 디렉터리에서 주소를 검색하고 응답 메시지를 전달한다.
   - 질의 메시지의 헤더에 포함되어 있는 송신측 Gateway ID와 응답 기관의 Gateway ID를 포함하는 헤더를 생성
   - 반환되는 신분증명 상태 응답 정보들로 페이로드를 구성
   - 페이로드의 암호학적 해시 결과에 대한 전자서명 추가
   - 페이로드를 수신측 기관의 공개키로 암호화

11) 수신된 응답 메시지는 인증서버에 의해 다음과 같이 처리된다.
   - 메시지 페이로드를 개인키로 복호화

- 메타정보 디렉터리에서 응답 기관의 공개키를 획득하고 전자서명을 검증
- 응답 메시지를 파싱하고 기관내부 인터페이스를 통해 AT에게 PIV 신분증명 상태검사 결과를 반환

12) AT는 PIV 신분증명이 유효한 상태이면 해당 신분증명 요소를 이용한 인증 메커니즘에 따라 PIV 카드에 대한 인증을 처리한다.
13) PIV 카드에 대한 인증이 정상적으로 완료되면 접근통제 결정이 접근통제지점의 제어 패널에 디스플레이 되거나 PIV 애플리케이션으로 전달된다.

4. 시스템 운영에 대한 고려사항

PIV 시스템 표준은 신분증명의 보안성과 신뢰성 강화를 목표로 하고 있지만, 실제 구축 시스템이 올바로 운영되지 못한다면 완전한 보안성을 제공하지 못할 수도 있으며, PIV 인증 메커니즘의 수행에 대한 신뢰성이 보장되기 위해서는 올바른 PIV 시스템의 구현 및 운영이 수반 되어야 한다. 따라서 본 장에서는 PIV 카드 위협요인에 대한 PIV 시스템의 대응방안과, 범용 환경에서 개인용 전자신분증 기반의 접근통제를 위한 신분증명 기술의 상호운영성을 위해 고려되어야 기술적, 제도적 사항들에 논의하도록 한다.

4.1 인증 및 신분증명 검증 방안

PIV 신분확인은 제시된 PIV 카드의 신분증명 값이 유효한지를 결정하는 프로세스이다. 본 논문에서 논의한 온라인 신분증명 검증서비스를 적용함으로써 최신의 신분증명 상태정보를 제공받을 수 있을 것이며, 실시간 상태검사를 통해 분실이나 도난 등으로 인해 폐기된 PIV 카드의 부정적인 사용도 방지할 수 있다. 비록 3.3절에서는 PIV 인증서를 이용한 인증 메커니즘을 중심으로 설명하였지만, 신분증명 상태검증은 모든 PIV 인증 메커니즘에 대해 구현될 수 있어야 한다.

PIV 인증서의 상태는 카드에 포함된 모든 다른 신분증명 요소들의 상태와 직결되므로 PIV 신분증명에 대한 검증은 PIV 인증서상의 경로검증(Path Validation)을 필요로 한다. 이는 접속 단말기를 통해 PIV 카드로부터 읽어 들인 데이터 객체들은 모든 전자서명이 검증될 때까지는 인증되고 변조되지 않은 데이터라고 완전하게 신뢰될 수는 없으며, PIV 인증 메커니즘에서 완전한 신뢰를 위해서는 인증에 사용된 모든 PIV 데이터 객체의 전자서명에 대한 경로검증을 수행하는 것이 필요하다. PIV 표준인 FIPS 201에서는 BIO, CAK, CHUID 인증에 대해서는 경로검증을 요구하고 있지 않다. 그러나 이들 인증 메커니즘도 완전히 신뢰되기 위해서는 경로검증이 수행되어야 할 것이다.

또한 여러 발급기관을 통해 PIV 카드가 발급되는 경우, PIV 카드를 발급한 기관과 PIV 카드의 접근통제 결정이 발생하는 기관이 서로 다른 경우도 발생할 수 있으며, 본 논문에서는 이를 위해 백-엔드 게이트웨이를 통해 서로 연결된 기관들 사이의 기관 상호인증 인프라를 통해 신분증명 상태 질의 메시지와 응답 메시지를 교환함으로써 해결하고자 하였다.

4.2 PIV 카드 위협요인에 대한 대응방안

본 절에서는 NIST의 SP 800-116에 제시된 PIV 카드에 대한 위협요인들에 대응하기 위한 권고사항들과 PIV 인증시스템의 운영방안에 대해 논의하도록 한다. 표 8은 PIV 카드에 발생 가능한 위협요인과

표 8. PIV 카드 위협요인에 대한 대응방안

위협요인	대 응 방 안
식별자 해결	- 체계화된 개인식별번호 체계의 도입이 필요
종결된 카드 악용	- 모든 신분증명 요소에 대한 온라인 상태검사
인쇄요소 위조	- 전자신분증 신분증명 요소에 대한 부가적인 검증 필요
스키밍	- 접속 단말기에 대한 인증 수행 - 접근규칙에 의한 IC칩에 저장된 주요 정보의 접근제한 - 차폐기법을 이용한 전자적 데이터 노출 보호
스니핑	- 통신보안 기법을 적용한 암호화 통신 - VPN 등을 이용한 안전한 기관 상호연동
전자적 복제	- 인증서 검증 - 전자서명과 시도/응답을 이용한 강력한 인증 절차 수행
전자적 모방	- 신분증명 데이터 요소에 대한 전자서명 및 경로검증 수행 - 물리적 접근시도 횟수 제한

이들에 대한 인증시스템의 대응방안을 요약하여 나타내고 있다.

4.2.1 식별자 해결

식별자는 PIV 카드 발급 단계에서 PIV 카드 발급자에 의해 개인을 식별할 수 있는 유일한 식별자가 생성되어 부여되며, 이 식별자는 접근통제시스템이나 인증시스템에 의해 PIV 카드를 유일하게 확인하는데 사용된다. 미국의 PIV 시스템은 유일한 FASC-N 식별자를 정의하여 개인의 신분확인과 접근통제 결정에 이용하고 있다. 이는 SSN(Social Security Number)의 직접적인 노출로 인한 개인정보 도용을 방지하기 위함이며, 우리나라의 경우 I-PIN이 이 역할을 대신할 수 있을 것이다. 그러나 I-PIN을 단순한 개인식별번호가 아니라 온라인상에서 자동화된 신분확인과 접근통제에 활용하기 위해서는 체계화된 식별번호체계를 마련할 필요가 있다[11].

4.2.2 종결된 PIV 카드의 악용

분실이나 도난 등의 이유로 PIV 카드의 사용이 종결되더라도 이러한 상태정보가 로컬시스템에 제공되지 않는다면 사용 정지된 PIV 카드가 계속 사용될 수도 있다. PIV 인증서를 이용한 인증 메커니즘의 경우, PKI 기반의 OCSP나 CRL을 이용한 인증서 상태검증을 통해 해당 PIV 카드의 상태 유효성 유무를 확인할 수 있다. 그러나 PIV 표준의 CHUID 인증 메커니즘은 단지 PIV 카드로부터 읽혀진 CHUID 데이터 객체만을 검증하고, 접속 단말기에서의 접근통제 결정은 카드에 저장된 CHUID 데이터 요소만을 근간으로 하므로 PIV 인증 인증서에 대한 상태는 검사하지 않는다. 따라서 온라인 신분증명 검증 모델은 PIV 인증서뿐만 아니라 다른 PIV 신분증명 요소에 대해서도 적용함으로써 부적절한 PIV 카드의 사용에 대한 위험을 완화시킬 수 있다.

4.2.3 인쇄요소 위조

시각적 인쇄요소의 위조는 실제 PIV 카드의 전자적인 부분이 아닌 카드의 인쇄내용을 모방하는 것이다. 최근 고화질의 컬러 프린터나 스캐너, 카드 복제기 등이 판매되고 있으므로 시각적인 위조가 점차 용이해지고 있는 실정이다. 따라서 물리적 접근통제 시스템에서도 감독자의 시각적인 신분확인에 추가적으로 온라인을 통한 전자적인 검증도 수행할 것을 권장한다.

4.2.4 스키밍

PIV 카드는 비접촉식 인터페이스도 제공하고 있으므로 스키밍(skimming) 공격에 노출될 수 있다. 따라서 PIV 카드는 IC 칩에 저장된 중요 데이터를 보호하기 위한 물리적 보호기술을 이용하여 제작되어야 할 것이다[12]. 또한 접근규칙에 의해 생체인식 정보나 중요 정보들이 비접촉식 인터페이스를 통해 부당하게 읽혀지는 것을 방지하고, 카드에서 별다른 거부 없이 쉽게 읽혀질 수 있는 free-read 데이터 객체의 내용을 최소화할 필요가 있다. 그리고 물리적 보호수단으로 PIV 카드가 사용되지 않을 경우 전파차단 주머니와 같은 차폐기법(shielding technique)을 이용하여 카드에 저장된 데이터의 유출을 방지하는 것이 필요하다.

PIV 표준은 시스템 구축환경을 연방정부 관할의 건물이나 컴퓨팅 자원에 대한 물리적, 논리적 접근통제시스템을 가정하여 인증을 위해 PIV 카드 정보를 읽어 들이는 카드 리더기나 단말기에 대한 인증은 고려하지 않고 있다. 그러나 최근 전자여권 시스템에서의 보안문제[13]로 고려된 바와 같이, 전자신분증이 범용 환경에서 사용되는 경우 불법적인 단말기에 의한 정보의 노출을 방지하기 위해 접속 단말기에 대한 인증이 필요하며, 본 논문에서는 접속 단말기에 대한 인증절차를 고려하였다.

4.2.5 스니핑

PIV 카드는 생체인식 정보나 그 외 다른 정보들을 접촉식 인터페이스를 통해 읽을 수 있게 하여 스니핑에 대한 위험을 완화하고 있다. 그러나 CHUID는 비접촉식 인터페이스를 통해 무선으로 전송될 수 있으므로 스니핑될 수 있다[13], 따라서 스니핑을 방어하기 위해서는 PIV 카드와 비접촉식 단말기 사이의 통신보안 기법이 요구되나 현재 PIV 표준에서는 이에 대해 다루지 않고 있다. 이를 위해 [13]에서는 CHUID 노출을 방지하기 위해 PIV 카드와 단말기 사이의 상호인증과 보안 채널을 구성하기 위한 키 교환 프로토콜을 제안하였으며, [14]의 기법이 본 논문에서 제시한 접속 단말기 인증절차를 위한 기법으로 적용될 수도 있을 것이다.

4.2.6 전자적 복제

만약 공격자가 스키밍이나 스니핑, 사회공학 공격 등을 성공적으로 수행하였다면 PIV 카드의 데이터 객체에 대한 정보를 소유하게 될 것이고, 이러한 정보를 이용하여 전자적인 데이터 요소의 복제(electronic cloning)를 수행할 수 있을 것이다. 그러나 개인키나 비밀키는 IC칩 메모리의 보호영역에 저장되므로 이러한 공격으로도 암호학적 인증을 수행하는데 필요한 개인키나 비밀키는 획득할 수 없다. 따라서 공격자는 CHUID 기반의 인증을 수행할 수 있는 부분적으로 복제된 PIV 카드는 생성할 수 있을지라도, PKI나 CAK 인증 메커니즘을 위한 PIV 카드는 복제하지 못 한다. 따라서 CHUID 인증 메커니즘을 단독으로 사용하는 대신 PIV 인증서나 비대칭 CAK를 이용한 인증 메커니즘을 사용할 것을 강력히 권장한다.

4.2.7 전자적 모방

이 공격유형은 패스워드 크래킹을 위한 시도와 유사한 방식으로, 공격자가 선택한 CHUID의 FASC-N을 리더기에 제시함으로써 올바른 CHUID를 추측하는 방법이다. 공격자는 CHUID 인증 메커니즘을 모방하여 PIV 카드를 에뮬레이트(emulate) 하는 장비를 구성하고, 접속 단말기에 대해 CHUID를 테스트하고 FASC-N 신분증명 식별자를 변경하는 프로그램을 제작 가능하다. 만약 접속 단말기나 인증 서버가 CHUID의 전자서명을 검증하지 않는 경우 이러한 공격은 유효하게 된다.

PIV 카드는 CHUID의 전자서명 필드를 저장함으로써 이러한 공격을 방지토록 하고 있다. 비록 FIPS 201 표준에서는 전자서명의 검증을 요구하고 있지는 않지만, CHUID의 전자서명이 검증된다면 전자적 모방(electronic counterfeiting)은 상당히 어려워 질 수 있다. 또한 공격자가 유효한 CHUID를 도출(probe)하기 위한 시도를 할 수 있으므로 접근통제시스템은 성공하지 못한 CHUID 시도를 감지하고 차단할 수 있는 방안을 마련하는 것도 필요할 것이다.

5. 결 론

전자신분증은 일반적으로 IC칩이 내장된 스마트카드 형태로 제작되어 다양한 형태로 사용될 수 있으며, 현재 국내에서도 전자여권뿐만 아니라 전자주민증의 도입도 검토되고 있다. 따라서 전자신분증을 도입하기 위해서는 강건한 암호 알고리즘과 암호키의 사용뿐만 아니라 전자신분증의 올바른 활용을 위한 시스템의 구성에 대해서도 고려되어야 한다.

본 논문에서는 개인용 전자신분증에 대한 기술이 잘 정립되어 있는 미국의 PIV 시스템 기술을 토대로 하여 전자신분증 기반의 효과적인 개인 신분확인을 위한 인증 프레임워크를 제안하였다. 제안된 프레임워크는 온라인 신분증명 상태검증 모델을 적용함으로써 보다 높은 수준의 인증 보증등급을 제공하고자 하였으며, 또한 백-엔드 게이트웨이를 통한 상호기관 연동을 통해 상호운영성을 높이고자 하였다.

향후 전자신분증이 일상화 되어 다양한 분야에 활용될 것임은 분명하다. 그러나 전자신분증이 성공적으로 도입되고 활용되기 위해서는 전자신분증에 저장된 개인정보의 보호와 전자신분증의 도용으로부터 유형 및 무형의 자산을 보호할 수 있는 개인 신분확인과 접근통제 기술뿐만 아니라 법적, 제도적 장치도 반드시 마련되어야 할 것이다. 이에 본 논문의 인증 프레임워크 구성방안이 향후 전자신분증을 활용한 강건한 개인 신분확인 및 인증 시스템의 구축에 활용될 수 있기를 기대한다.

참 고 문 헌

[1] 김은, 이윤석, 정민수, "스마트카드를 이용한 위조방지 인증 시스템 설계 및 구현," 한국멀티미디어학회논문지, Vol.14, No.2, pp. 249-257, 2011.

[2] D. De Cock, K. Wouters, and B. Prenel, "Introduction to the Belgian EID Card BELPIC," *Proceedings of the 1st European PKI Workshop*, LNCS 3093, pp. 1-13, 2004.

[3] "Personal Identify Verification of Federal Employees and Contractors," NIST FIPS PUB 201-1, 2006.

[4] 이동진, 곽진, "미국의 개인신원검증 기준 FIPS 201-1에 관한 분석," 한국정보보호학회지, 제19권, 제3호, pp. 35-45, 2009.

[5] "Interfaces for Personal Identity Verification," NIST Special Publication 800-73-3, 2010.

[6] "Biometric Data Specification for Personal

Identity Verification," NIST Special Publication 800-76, 2007.

[7] "Cryptographic Algorithms and Key Sizes for Personal Identity Verification," NIST Special Publication 800-78-2, 2010.

[8] "Security Requirements for Cryptographic Modules," NIST FIPS PUB 140-2, 2001.

[9] 변진욱, "개인식별 시스템에 적용되는 보안 알고리즘 요구사항 분석," 정보통신산업진흥원 주간기술동향 1450호, 2010.

[10] "A Recommendation for the Use of PIV Credentials in Physical Access Control Systems (PACS)," NIST Special Publication 800-116, 2008.

[11] 이형호, 박희만, 조상래, 진승헌, "프라이버시 보호기능을 제공하는 온-오프라인 환경의 새로운 국민식별번호체계 제안," 한국정보보호학회지, 제20권, 제1호, pp. 74-87, 2010.

[12] O Kömmerling and M. G. Kuhn, "Design Principles for Tamper-Resistant Smartcard Processors," *Proceedings of the USENIX Workshop on Smartcard Technology*, pp. 9-20, 1999.

[13] V. Pasupathinathan, J. Pieprzyk, and H. Wang, "An On-Line Secure E-Passport Protocol," *Proceedings of The Information Security Practice and Experience*, LNCS 4991, pp. 14-28, 2008.

[14] P. A. Karger, "Privacy and security threat analysis of the federal employee personal identity verification (PIV) program," *Proceedings of the 2nd Symposium on Usable Privacy and Security*, pp. 114-121, 2006.

박 영 호

2000년 부경대학교 전자계산학과 학사
2002년 부경대학교 전자계산학과 석사
2006년 부경대학교 정보보호학과 박사

2010년~현재 부경대학교 박사후연구원
관심분야 : 암호 프로토콜, 암호기술 응용, 애드 혹 네트워크 보안

공 병 운

1986년 공업대학교 전자공학과 학사
2001년 부경대학교 전산정보학과 석사
2005년~현재 부경대학교 정보시스템협동 박사과정

관심분야 : 네트워크 보안, 개인정보 보호, 클라우드 컴퓨팅

이 경 현

1982년 경북대학교 수학교육과 학사
1985년 한국과학기술원 응용수학과 석사
1992년 한국과학기술원 수학과 박사

1993년~현재 부경대학교 IT융합응용공학과 교수
관심분야 : 정보보호론, 공개키 암호, 신원기반 암호, 멀티미디어 정보보호, 그룹 키 관리