情 報 保 護 學 會 誌
第19卷 第3號, 2009. 6

미국의 개인신원검증 기준 FIPS 201-1에 관한 분석

이 동 범*, 곽 진**

요 약

개인신원검증은 사용자가 자원 및 시스템에 접근할 수 있는 자격을 증명하고, 사용자가 요청한 업무를 수행하기 위해 필요한 권한을 부여 받는 과정이다. 즉 인증 과정이 성공적으로 수행된 후 인가 수준을 결정하는 중요 요소로서 활용된다. 이러한 개인신원검증은 신원 도용, 변조의 위험과 비인가 된 사용자의 접근을 허용할 수 있는 문제점을 가지고 있다. 이에 따라 국·내외적으로 개인신원검증에 대한 다양한 연구가 진행되고 있다. 따라서 본 고에서는 NIST의 FIPS 201-1에서 규정하는 개인신원검증에 대한 주요 인프라, 인증 메커니즘, 암호키에 대한 기술적인 세부 내용을 분석하고자 한다.

Ⅰ. 서 론

개인신원검증(PIV: Personal Identity Verification)은 물리적·논리적인 접근 통제 과정의 기본적인 구성요소이며, 넓은 범위의 신원 인증 메커니즘은 다양한 종류의 신원 증명서들을 활용한다.

물리적인 접근을 위한 개인 신원은 기존의 신분증, 운전면허증 등의 자동화되지 않은 증명서들을 이용하여 인증을 수행하고, 컴퓨터와 데이터의 접근 인가는 사용자가 선택한 비밀번호를 이용하여 인증을 수행한다.

최근의 암호 기법들과 생체인식 기술들은 물리적·논리적인 보안 애플리케이션을 대체하거나 기존의 신원 증명서들을 보완하여 활용되고 있으며, 인증의 강도는 신원 증명 유형, 발급 과정, 인증 메커니즘을 사용하는 유효성에 따라 변화되고 있다.

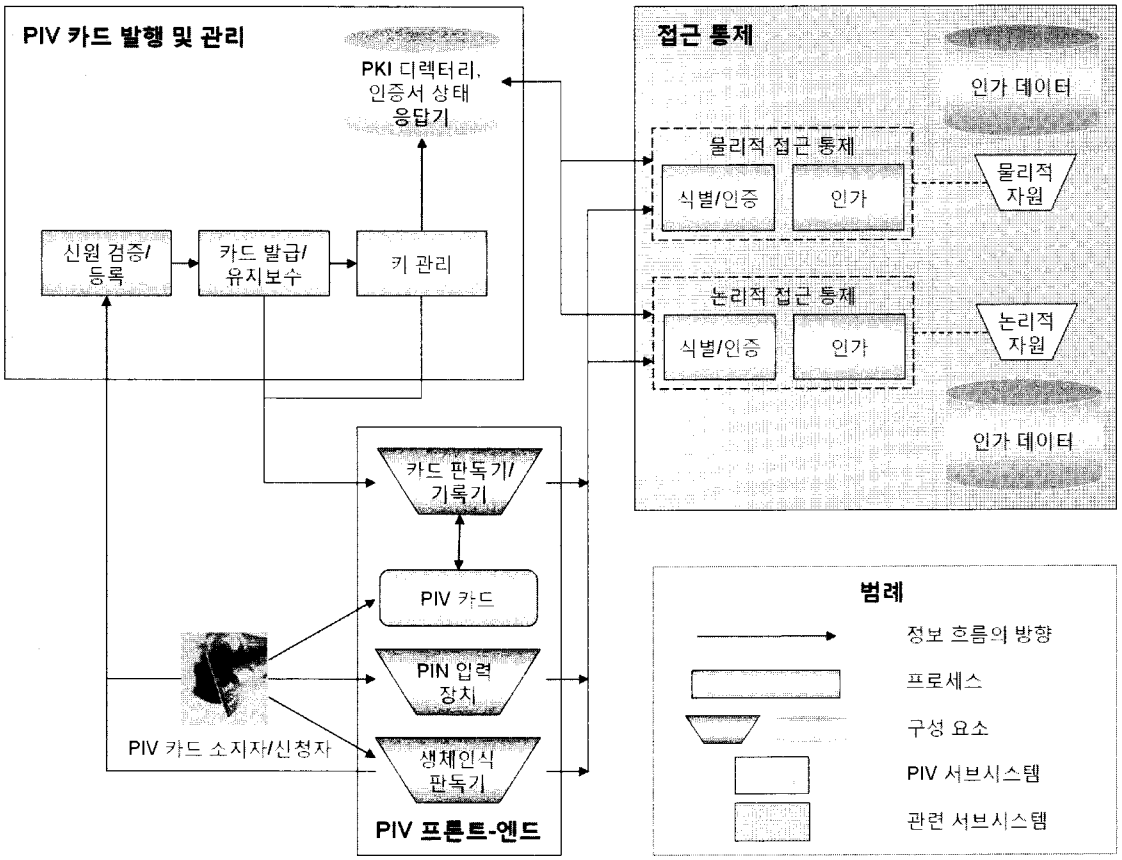
하지만 개인신원검증은 비인가 된 사용자로 인한 정보 시스템의 파괴와 신원 도용 및 변조 등의 사용자 프라이버시 침해에 대한 문제점이 발생할 수 있다. 이러한 문제를 해결하기 위해서 미국에서는 연방기관 직원 및 계약자들이 연방기관에 의해 관리되는 시설들의 물리적 접근과 통제되는 정보 시스템의 논리적인 접근 허용에 대한 개인신원검증 표준과 요구사항을 수립하기 위해서 NIST에서는 2004년 8월 27일 발효된 국토보안대통령 지침-12를 반영하여 개인신원검증을 위한 표준을 2005년 3월에 FIPS 201[Personal Identity Verification (PIV) of Federal Employees and Contractors]를 발표하였고, 2006년 3월에 FIPS 201-1로 개정하였다.

따라서 본 고에서는 미국의 개인신원검증에 대한 표준을 파악할 수 있도록 2장에서는 FIPS 201-1에 제시된 개인신원검증 시스템의 각 구성요소에 대해서 설명하고 3장에서는 개인신원검증 카드의 생명주기 활동에 대해서 기술한다. 4장에서는 개인신원검증의 인증 메커니즘에 대한 각각의 방식에 대해서 설명하고, 5장에서는 개인신원검증의 암호화 사양에 대해서 분석한 후 6장에서 결론을 맺는다.

Ⅱ. 개인신원검증 시스템

개인신원검증 시스템은 복합적인 타입들의 물리적·논리적인 환경들의 접근을 위한 구성 요소들과 연방기관 직원의 신원 검증을 위해 스마트카드 기반의 공통된 플랫폼을 지원한다. 개인신원검증 시스템의 구성요소들은 균일성과 상호 운용성을 촉진시키며, 개인신원검증 시스템 내에 수행되어야 하는 다양한 활동을 위해 최소한의 요구사항을 설정한다. 개인신원검증 카드는 FIPS 201-1의 표준에 따라 필요한 권한을 받을 때 연방기관들이 사용할 수 있는 신원 인증 메커니즘을 수행하여야 하며, 인증된 신원 정보는 연방기관의 물리적·논리적

* 순천향대학교 정보보호학과 정보보호응용및보증연구실 석사과정 (dblee@sch.ac.kr)
** (교신저자) 순천향대학교 정보보호학과 교수 (jkwak@sch.ac.kr)



〔그림 1〕 개인신원검증 시스템

인 접근 환경에서 접근 통제를 위한 기초 자료로 사용된다. 개인신원검증 시스템은 논리적인 개인신원검증 프론트-엔드 서브시스템, 개인신원검증 카드 발행 및 관리 서브시스템, 접근 통제 서브시스템으로 구분된다[1].

2.1 개인신원검증 프론트-엔드 서브시스템

개인신원검증 프론트-엔드 서브시스템(PIV Front-End Subsystem)은 카드 판독기 및 기록기, 개인신원검증 카드, 개인식별번호 입력 장치, 생체인식 판독기로 구성된다.

2.1.1 개인신원검증 카드

개인신원검증 카드는 사용자 인증 및 등록 과정을 완료하고, 신청자에게 배부된다. 개인신원검증 카드는 신용카드만한 크기를 가지며, 기억 용량과 계산 능력을 제공하는 임베디드 집적 회로칩(ICC : Integrated Circuit Chip)을 내장하고 있다. 개인신원검증 카드는 개인신원검증 시스템의 주요한 구성 요소이며, 카드 소지자는 여러 가지 물리적 · 논리적인 자원들의 인증을 위해 개인신원검증 카드를 이용한다. 개인신원검증 카드에는 개인신상정보, 인증서, 개인식별번호(PIN: Personal Identification Number), 생체인식 데이터를 포함하고 있다.

2.1.2 카드 판독기 및 기록기

카드 판독기는 카드 소지자가 개인신원검증 카드를 사용하여 자원을 이용하기 위한 논리적 · 물리적으로 접근하는 지점에 위치한다. 판독기는 접근 승인 또는 거부를 위한 접근 통제 서브시스템에 전송하기 위해서 정보를 검색하고, 개인신원검증 카드와 통신을 한다. 카드 기록기는 개인신원검증 카드에 저장된 정보를 저장하고, 초기화를 수행한다.

2.1.3 생체인식 판독기

생체인식 판독기는 카드 소지자가 접근을 원하는 안전한 장소에 위치한다. 카드 소지자의 실시간 생체인식 정보와 개인신원검증 카드에 저장된 카드 소지자의 생체인식 정보를 비교하여 카드 소지자의 추가적인 인증 요소를 제공한다.

2.1.4 개인식별번호 입력 장치

개인식별번호 입력 장치는 보다 강한 인증이 필요할 때 카드 판독기와 함께 사용된다. 카드 소지자가 개인신원검증 카드를 제시할 때 개인식별번호도 함께 개인식별번호 입력 장치에 입력한다. 물리적인 접근을 위한 개인식별번호는 개인식별번호 패드 장치를 사용하고, 논리적인 접근은 일반적으로 키보드를 사용한다. 개인식별번호의 입력은 카드에 저장된 정보에 대한 접근 통제의 추가적인 인증요소로 사용되며, 이것은 높은 등급의 인증을 보증한다.

2.2 개인신원검증 카드 발급 및 관리 서브시스템

개인신원검증 카드 발급 및 관리 서브시스템은 신원검증 및 등록, 카드 발급과 유지 보수, 키 관리, PKI 디렉터리와 인증서 상태 응답기로 구성되며 인증 기반 구조의 일부분으로서 필요하다.

2.2.1 신원 검증 및 등록

신원 검증과 등록에 필요한 정보의 수집, 저장, 유지관리에 카드 신청자의 신원 검증을 요구한다. 정보의 다양한 유형들은 카드 등록 시 신청자로부터 수집한다.

2.2.2 카드 발급 및 유지 보수

카드 발급과 유지 보수는 카드의 시각적인 표면인 물리적인 부분과 집적 회로 칩의 논리적인 부분으로 구성된다. 이것은 사진, 이름, 기타 정보를 인쇄하는 것뿐만 아니라 관련된 카드 애플리케이션, 생체인식 정보 등의 데이터를 포함한다.

2.2.3 키 관리 및 PKI 디렉터리와 인증서 상태 응답기

키 관리 구성 요소는 카드 소지자의 공개키를 포함하는 디지털 인증서의 키 쌍을 생성, 분배 및 인증서의 상태 정보를 관리하고 배포한다. 키 관리 구성 요소는 인증키와 PKI 인증서의 생성, 저장, 안전한 운영을 위한 키의 사용, 카드의 갱신 · 재발행 · 폐기까지의 개인신원검증 카드의 생명주기 동안 계속 사용된다. 또한 키 관리 구성 요소는 공개적으로 접근하기 쉬운 저장소의 공급과 PKI 인증서 상태에 대한 애플리케이션의 정보를 제공하는 PKI 디렉터리와 인증서 상태 응답기도 제공한다.

2.3 접근 통제 서브시스템

접근 통제 서브시스템은 보호 자원, 인가 데이터, 물리적 · 논리적인 접근 통제 시스템으로 구성된다.

2.3.1 보호 자원

접근 통제 서브시스템은 물리적 · 논리적인 자원에 특정한 개인신원검증 카드 소지자의 접근을 결정하기 위해서 신뢰할 수 있는 구성 요소를 포함한다.

- 물리적인 자원 : 카드 소지자가 접근을 원하는 안전한 시설을 나타낸다.
  ex) 주차장 출입구, 건물 출입문, 사무실 출입문 등

- 논리적인 자원 : 카드 소지자가 접근을 원하는 네트워크가 위치한 곳을 나타낸다.
  ex) 컴퓨터 워크스테이션, 폴더, 파일, 데이터베이스 레코드, 소프트웨어 프로그램

2.3.2 인가 데이터

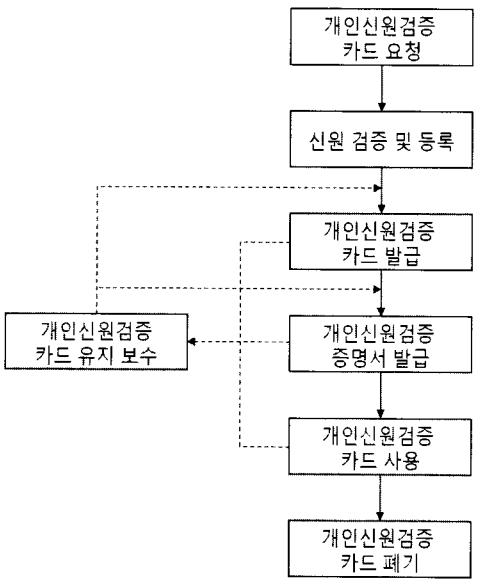
인가 데이터 구성 요소는 특정한 논리적 · 물리적 자원에 접근하기 위해서 엔티티(entity) 요구에 의해 소유되어 있는 특권(인가)을 정의하는 정보로 이루어진다. 컴퓨터 시스템의 파일과 관련된 접근 통제 목록(ACL : Access Control List)을 대표적인 예로 들 수 있다.

2.3.3 물리적 · 논리적 접근 통제 시스템

물리적 · 논리적 접근 통제 시스템은 특정 자원의 접근을 승인 또는 거부하는 인가 구성 요소뿐만 아니라 식별 및 인증(I&A : Identification and Authentication) 구성 요소를 포함한다. 인증 이후 인가 구성 요소는 카드 소지자가 제공한 정보와 카드에 저장되어 있는 정보를 비교하기 위해서 인가 데이터와 상호 작용을 수행한다. 접근 통제 구성 요소는 일반적으로 카드 판독기, 인가 데이터, 개인식별번호 입력 장치, 생체인식 판독기, 인증서 상태 서비스로 이루어진다.

Ⅲ. 개인신원검증 카드 생명주기 활동

개인신원검증 카드는 개인신상정보, 생체인식 정보 등의 중요한 개인 인증 정보를 안전하게 저장하기 위하여 다음과 같은 7단계의 생명주기에 따라 발급된다.



〔그림 2〕 개인신원검증 카드 생명 주기

○ 1단계 - 개인신원검증 카드 요청
: 개인신원검증 카드 신청자가 카드를 신청하는 단계

○ 2단계 - 신원 검증 및 등록
: 개인신원검증 카드 신청자의 신원을 검증하고, 제출한 신원 정보 증명서류를 검증하는 단계

○ 3단계 - 개인신원검증 카드 발급
: 물리적 · 논리적인 구성 요소를 갖춘 개인신원검증 카드를 생성하여 카드 신청자에게 발급하는 단계

○ 4단계 - 개인신원검증 증명서 발급
: PKI의 논리적인 증명서를 발급하고, 개인신원검증 카드에 저장하는 단계

○ 5단계 - 개인신원검증 카드 사용
: 개인신원검증 카드는 카드 소유자의 물리적 · 논리적 자원의 접근을 인증하는데 사용하며, 접근인가는 카드 소지자의 신원검증 및 인증의 성공적인 수행 이후 결정

○ 6단계 - 개인신원검증 카드 유지 보수
: 발급된 개인신원검증 카드 및 애플리케이션, 개인식별번호, PKI 증명서, 생체인식 정보를 갱신하거나 유지보수를 실시하는 단계

○ 7단계 - 개인신원검증 카드 폐기
: 영구적으로 개인신원검증의 인증을 위해 필요한 키와 데이터를 파괴하거나, 무효화 시키는 것으로 추후 개인신원검증에 카드가 사용되는 것을 막는 단계

Ⅳ. 개인신원검증 인증 메커니즘

개인신원검증 카드는 카드 판독기의 설치 유 · 무의 모든 환경에서 신원 인증을 위해 사용된다. 사용 환경의 파라미터들은 특정한 상황에 적용할 수 있는 개인신원검증의 신원 인증 메커니즘에 영향을 준다.

접근 통제 지점이 연방기관의 네트워크 기반 연결성을 가지고 있으면 각각의 인증 메커니즘은 백-엔드 인증서 상태 인증 구조의 사용을 통해서 더욱 더 강화되며, 개인신원검증에 대한 인증 인증서의 상태는 카드에 보관된 모든 인증 요소 상태에 따라 결정된다.

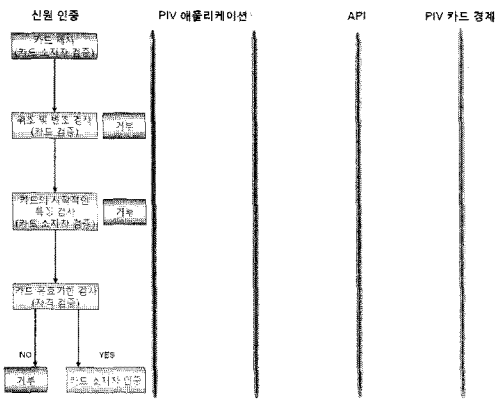
다음은 기본적인 형식의 개인신원검증 카드에 적용되는 인증 메커니즘을 설명한다[2][3][4][5].

4.1 시각적인 자격 증명을 이용한 인증

개인신원검증 카드 소지자의 시각적인 인증은 물리적인 기능 및 자원의 접근 통제를 하기 위해서만 이용된다. 개인신원검증 카드는 시각적인 식별과 인증을 지원하는 다음과 같은 기능들이 카드의 전면과 후면에 위치하고 있다.

- ○ 사진, 이름, 소속 직원의 고용 식별자
- ○ 유효기한, 카드 일련 번호
- ○ 발급인 ID, 기관명/부처
- ○ 기관 도장, 신청인 서명
- ○ 개인신원검증 카드 소지자의 물리적인 특성

카드 소지자가 연방 기관에 의해 통제되는 시설의 접근 통제 지점을 통과할 때 관리자는 카드 소지자의 시각적인 신원 검증을 수행하며, 통제 지점에서 개인 식별 여부를 확인하는 과정을 거친다. 시각적인 인증 과정은 다음과 같은 일련의 단계로 진행된다.

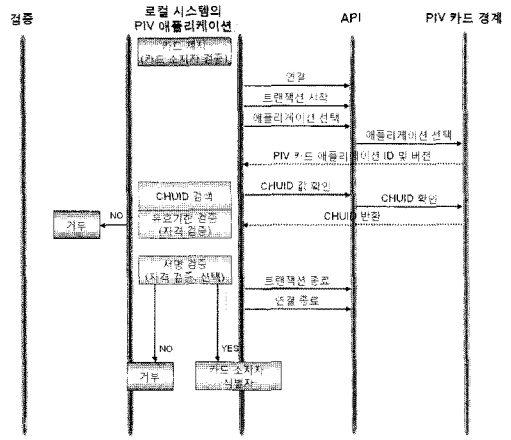


〔그림 3〕 시각적인 자격 증명을 이용한 인증

1. 카드 소지자는 접근 통제 지점에서 카드를 제시한다. (카드 소지자 검증 과정)
2. 관리자는 개인신원검증 카드의 위·변조를 확인한다. (카드 검증 과정)
3. 관리자는 카드 소지자의 신원을 검증하기 위해서 카드에 인쇄된 사진과 카드 소지자의 얼굴 특징을 비교한다. (카드 소지자 검증 과정)
4. 관리자는 카드의 유효기한을 검사한다. (자격 검증 과정)
5. 카드 소지자의 물리적인 특성들을 비교한다. (선택사항)
6. 카드 소지자의 서명과 카드에 저장된 서명을 비교한다. (선택사항)
7. 카드의 다른 데이터 요소(이름, 발급인 ID, 카드 일련번호, 기관명/부처 등)들은 카드 소지자의 접근 권한을 결정하기 위해서 이용된다.

4.2 카드 소지자의 고유 식별자를 이용한 인증

개인신원검증 카드는 필수적인 논리적 자격 증명 요소로 카드 소지자의 고유 식별자(CHUID : Cardholder Unique Identifier)인 데이터 객체를 제공한다. 카드 소지자의 고유 식별자는 각 카드의 유일한 요소인 연방기관의 자격 증명 번호(FASC-N : Federal Agency Smart Credential Number)를 포함한다.



〔그림 4〕 카드 소지자의 고유 식별자를 이용한 인증

카드 소지자의 고유 식별자를 이용한 인증은 다음과 같은 과정으로 진행된다.

1. 카드 소지자는 접근 통제 지점에서 카드를 제시한다. (카드 소지자 검증 과정)
2. 판독기는 개인신원검증 카드로 연결한 후 트랜잭션을 시작한다. 그 후 애플리케이션을 선택한다.
3. 개인신원검증 카드에서는 개인신원검증 카드의 애플리케이션 ID와 버전 정보를 판독기로 전송한다.

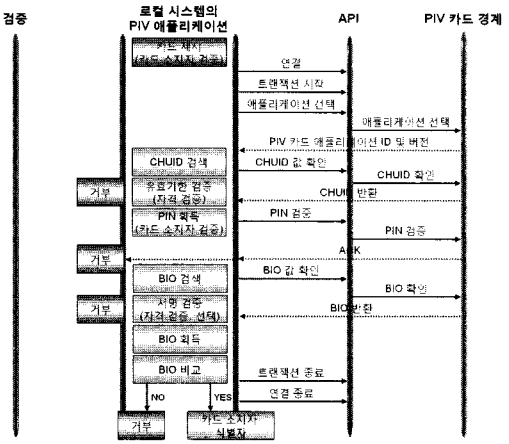
4. 판독기는 카드 소지자의 고유 식별자를 검색하고, 관련 정보를 개인신원검증 카드로 전송한다.
5. 개인신원검증 카드는 카드 소지자의 고유 식별자를 판독기로 전송한다.
6. 판독기는 개인신원검증 카드의 유효기한을 검증하고, 카드 소지자의 고유 식별자에 대한 전자서명이 신뢰받은 기관에 의해 서명을 받고, 카드에 저장된 데이터가 변경되지 않았다는 것을 보장하기 위해서 서명을 검사한다. (자격 검증 과정, 선택사항)
7. 카드 소지자의 고유 식별자에 대한 데이터 요소(연방기관의 자격 증명 번호, 기관 코드 등)들은 카드 소지자의 접근 통제를 결정하기 위해서 사용된다.

4.3 생체인식을 이용한 인증

개인신원검증 카드 호스트가 서명한 생체인식 정보는 카드 소지자가 입력한 개인식별번호를 이용해서 카드 소지자와 카드간 인증을 통하여 카드로부터 읽는다. 개인신원검증 생체인식 정보는 match-off-card 스키마를 통하여 카드 소지자와 외부 시스템 인증 메커니즘을 지원한다. 개인신원검증의 생체인식을 이용한 인증은 다음과 같이 2개의 방식이 있다.

4.3.1 개인신원검증의 생체인식 정보를 이용한 무인 인증

개인신원검증의 생체인식 정보를 이용한 무인 인증은 다음과 같은 과정으로 진행된다.



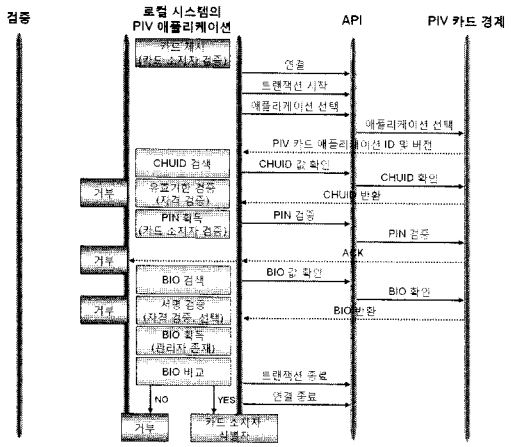
〔그림 5〕 개인신원검증의 생체 인식 정보를 이용한 무인 인증

1. 카드 소지자는 접근 통제 지점에서 카드를 제시한다. (카드 소지자 검증 과정)
2. 판독기는 개인신원검증 카드로 연결한 후 트랜잭션을 시작한다. 그 후 애플리케이션을 선택한다.
3. 개인신원검증 카드에서는 개인신원검증 카드의 애플리케이션 ID와 버전 정보를 판독기로 전송한다.
4. 판독기는 카드 소지자의 고유 식별자를 검색하고, 관련 정보를 개인신원검증 카드로 전송한다.
5. 개인신원검증 카드는 카드 소지자의 고유 식별자를 판독기로 전송한다.
6. 판독기는 개인신원검증 카드의 사용기한이 끝나지 않은 것을 보장하기 위해서 유효기한을 검증한다. (자격 검증 과정)
7. 판독기는 카드 소지자로부터 개인식별번호를 획득한 후, 개인신원검증 카드로 검증을 요청한다. (카드 소지자 검증 과정)
8. 판독기는 카드 소지자의 개인식별번호의 정당성을 확인하고, 개인신원검증 카드를 활성화 시킨 후, 개인신원검증 생체인식 정보를 개인신원검증 카드로부터 읽는다.
9. 카드 소지자의 생체인식에 대한 전자서명이 신뢰받은 기관에 의해 서명을 받고, 카드에 저장된 생체인식 정보가 변경되지 않았다는 것을 보장하기 위해서 서명을 검사한다. (자격 검증 과정, 선택사항)
10. 판독기는 카드 소지자의 실시간 생체인식 정보를 획득한다. 획득한 생체인식 정보와 카드에 저장되어 있는 생체인식 정보를 비교한 후 동일하다면 카드 소지자의 인증을 수행한다.
11. 카드 소지자의 고유 식별자에 대한 연방기관의 자격 증명 번호는 생체인식에 대한 외부 디지털 서명의 서명 속성 필드(연방기관의 자격 증명 번호)와 비교한다.
12. 카드 소지자의 고유 식별자에 대한 데이터 요소(연방기관의 자격 증명 번호, 기관 코드)들은 카드 소지자의 접근 통제를 결정하기 위해서 사용된다.

4.3.2 개인신원검증의 생체인식 정보를 이용한 유인 인증

개인신원검증의 생체인식 정보를 이용한 유인 인증 메커니즘은 무인 인증 메커니즘의 생체인식 자격 증명

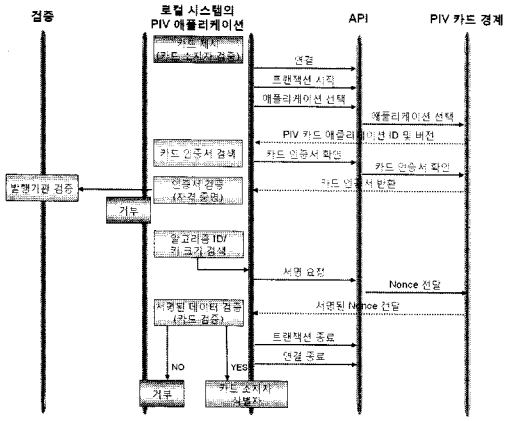
검사와 유사하다. 유일한 차이는 개인신원검증 카드의 사용과 개인식별번호의 입력, 생체인식 정보에 대한 사용이 관리자에 의해 관리·감독되는 부분이다. 개인신원검증의 생체인식 정보를 이용한 유인 인증은 다음과 같은 과정으로 진행된다.



〔그림 6〕 개인신원검증의 생체인식 정보를 이용한 유인 인증

4.4 비대칭 암호를 이용한 인증

개인신원검증 카드는 필수적인 비대칭키 인증 비밀키와 인증서를 저장하고 있다. 다음은 개인신원검증의 비대칭 인증키를 이용해서 인증을 실행하는 과정이다.



〔그림 7〕 비대칭 암호를 이용한 인증

1. 카드 소지자는 접근 통제 지점에서 카드를 제시한다. (카드 소지자 검증 과정)
2. 판독기는 개인신원검증 카드로 연결한 후 트랜잭션을 시작한다. 그 후 애플리케이션을 선택한다.
3. 개인신원검증 카드에서는 개인신원검증 카드의 애플리케이션 ID와 버전 정보를 판독기로 전송한다.
4. 판독기는 카드에 저장된 인증서를 검색하고, 관련 정보를 개인신원검증 카드로 전송한다.
5. 개인신원검증 카드는 카드 인증서를 전송한다.
6. 판독기는 개인신원검증 카드로부터 전송받은 인증서가 신뢰 받고 있는 기관으로부터 온 것을 보장하기 위하여 검증한다. (자격 증명 과정)
7. 판독기는 개인신원검증 카드의 알고리즘 ID 및 키 크기를 검색한 후 개인신원검증 카드로 서명을 요청하기 위해서 Nonce를 도전값(Challenge)으로 전달한다.
8. 개인신원검증 카드는 개인신원검증 인증 비밀키를 사용하여 인증서에 서명함으로써 판독기의 도전값에 대해서 응답(Response)을 수행한다.
9. 판독기는 개인신원검증 카드의 응답 서명을 확인하고, PKI 경로에 대한 유효성 검사를 수행한다. 인증서 폐지 상태는 현재의 유효성을 보장하기 위하여 검사한다.
10. 판독기는 개인신원검증 카드로부터 전송받은 서명된 데이터가 정당한 도전값인지 유효성을 검증한다. (카드 검증 과정)
11. 인증을 실행하기 위한 인증서에서 고유 이름(DN: Distinguished Name)과 연방기관의 자격 증명 번호는 인가 기능으로서 이용된다.

V. 개인신원검증의 암호화 사양

FIPS 201-1은 카드 소지자의 인증, 개인신원검증 카드의 정보 보안, 지원하는 인프라 보안을 위해 암호 메커니즘을 사용한다. 개인신원검증 시스템에 사용하는 암호 알고리즘 및 키 크기를 나타내는 FIPS 201-1의 보조적인 지침인 SP 800-78-1에서 분류하는 PIV 암호키의 종류는 다음과 같다[6][7].

- ○ 비대칭 PIV 인증키
- ○ 대칭·비대칭 카드 인증키
- ○ 비대칭 디지털 서명키
- ○ 비대칭 키 관리키

〔표 1〕 개인신원검증 키 유형별 알고리즘 및 키 크기

개인신원검증 키 유형	유효기간	알고리즘 및 키 크기
개인신원검증 인증키	2013/12/31 이전	- RSA(1024, 2048 비트) - ECDSA(Curve P-256)
	2013/12/31 이후	- RSA(2048 비트) - ECDSA(Curve P-256)
카드 인증키	2010/12/31 이전	- 2DEA - 3DEA - AES-128, AES, 192, AES-256 - RSA(1024, 2048 비트) - ECDSA(Curve P-256)
	2011/01/01 부터 2013/12/13 까지	- 3TDEA - AES-128, AES-192, AES-256 - RSA(1024, 2048 비트) - ECDSA(Curve P-256)
	2013/12/31 이후	- 3TDEA - AES-128, AES-192, AES-256 - RSA(2048 비트) - ECDSA(Curve P-256)
디지털 서명키	2008/12/31 이전	- RSA(1024, 2048 비트) - ECDSA(Curves P-256, P-384)
	2008/12/31 이후	- RSA(2048 비트) - ECDSA(Curves P-256, P-384)
키 관리키	2008/12/31 이전	- RSA 키 전송(1024, 2048 비트) - ECDH, ECC MQV(Curves P-256, P-384)
	2008/12/31 이후	- RSA 키 전송(2048 비트) - ECDH, ECC MQV(Curves P-256, P-384)

FIPS 201-1은 인증 메커니즘 또는 다른 보안 프로토콜에서 사용하기 위해서 개인신원검증 카드에 저장된 대상을 식별하였다. 이러한 대상은 3개의 분류로 나눌 수 있다.

○ 암호키
○ 디지털 서명 인증 정보
○ 정보의 메시지 다이제스트

5.1 개인신원검증 암호키

FIPS 201-1은 개인신원검증 카드 소지자의 자격증명으로 사용되는 4가지의 암호키를 분류한다. [표 1]은 암호화 알고리즘을 위한 구체적인 조건과 각각의 키 유형을 위한 키 크기를 설정한다. 또한 각각의 키 유형이 수용할 수 있는 알고리즘의 유효기간을 나타낸다.

5.1.1 개인신원검증 인증키

개인신원검증 인증키(PIV Authentication Key)는 개인신원검증 카드에서 생성되어 외부로 노출되지 않으며, 개인신원검증 카드의 접촉식 인터페이스를 통해서만 이용할 수 있다. 개인신원검증 카드는 인증키의 검증을 위한 X.509 인증서를 저장하고 있으며, X.509 인증서는 Subject alternative name 확장필드에 연방기관의 자격 증명 번호를 포함해야 한다. 인증서의 폐기 날짜는 개인신원검증 카드의 유효 기간 내에 있어야 한다. 개인신원검증 인증키는 인증을 지원하는 비대칭 개인키이며, 개인신원검증 카드를 사용하기 위한 필수 요구사항이다.

5.1.2 카드 인증키

카드 인증키(Card Authentication Key)는 개인신원

〔표 2〕 개인신원검증 정보에 대한 서명 알고리즘 및 키 크기 요구사항

서명 생성 날짜	공개키 알고리즘 및 키 크기	해쉬 알고리즘	패딩 스킴
2009/12/31 이전	RSA(2048, 3072, 4096 비트)	SHA-1	PKCS #1 v1.5
	RSA(2048, 3072, 4096 비트)	SHA-256	PKCS #1 v1.5
	ECDSA(Curve P-256)	SHA-256	없음
	ECDSA(Curve P-384)	SHA-384	없음
2010/01/01 부터 2010/12/31 까지	RSA(2048, 3072, 4096 비트)	SHA-1	PKCS #1 v1.5
		SHA-256	PKCS #1 v1.5, PSS
	ECDSA(Curve P-256)	SHA-256	없음
	ECDSA(Curve P-384)	SHA-384	없음
2010/12/31 이후	RSA(2048, 3072, 4096 비트)	SHA-256	PKCS #1 v1.5, PSS
	ECDSA(Curve P-256)	SHA-256	없음
	ECDSA(Curve P-384)	SHA-384	없음

검증 카드에서 생성되어 외부로 노출되지 않으며, 물리적인 접근을 위해 대칭(비밀)키 또는 비대칭 개인키를 사용한다.

개인/비밀키의 키 운영은 개인식별번호와 같이 명시적인 사용자의 동작 없이 키를 사용해서 실행할 수 있다. 또한 카드 인증키는 키 관리 프로토콜 또는 인프라에 대한 요구사항을 지정하지 않으며, 개인신원검증 카드를 사용하기 위한 선택 사항이다.

5.1.3 디지털 서명키

디지털 서명키(Digital Signature Key)는 개인신원검증 카드에서 생성되어 외부로 노출되지 않으며, 비대칭 개인키를 사용한다.

디지털 서명키를 사용하고 있는 암호 연산은 개인신원검증 카드의 접촉식 인터페이스를 사용하여 실행해야 하며, 개인키 연산은 반드시 사용자가 참여해야 한다. 또한 디지털 서명키의 검증을 위해 개인신원검증 카드는 X.509 인증서를 저장한다.

디지털 서명키는 개인신원검증 카드를 사용하기 위한 선택 사항이다.

5.1.4 키 관리키

키 관리키(Key Management Key)는 키 생성과 분배를 지원하는 비대칭 개인키이며, 개인신원검증 카드에서 생성되거나 외부에서 생성 후 개인신원검증 카드의 접촉식 인터페이스를 통해서만 이용할 수 있다. 개인키의 운영은 명시적인 사용자의 동작 없이 키를 사용해서 실행 할 수 있다.

키 관리키는 암호키로 불리기도 하며, 개인신원검증 카드를 사용하기 위한 선택 사항이다.

5.2 개인신원검증 카드에 저장된 인증 정보

개인신원검증 카드에 저장된 정보의 무결성과 신뢰성을 보호하기 위해서 FIPS 201-1, SP 800-73-2(개인신원검증을 위한 인터페이스), SP 800-76-1(개인신원검증을 위한 생체인식 데이터 사양)은 다음과 같은 대상에 디지털 서명을 사용하도록 요구하고 있다. [표 2]는 개인신원검증 카드에 저장된 정보에 대한 구체적인 요구사항을 나타낸다[8].

- ○ X.509 비대칭키 인증서
- ○ 카드 소지자의 고유 식별자
- ○ 생체인식 정보
- ○ SP 800-73 보안 객체

5.3 개인신원검증 카드 관리키

개인신원검증 카드 관리키(Management Key)는 개인신원검증 카드를 갱신하거나 개별 서비스를 받기 위해서 사용한다.

개인신원검증 카드는 카드 관리 시스템을 인증하기 위해 대칭 암호키를 사용해서 도전-응답(Challenge-Response) 프로토콜을 수행한다. 인증을 수행한 후, 카

드 관리 시스템은 개인신원검증 카드에 수정된 정보를 저장한다. [표 3]은 카드의 유효기한에 따라 암호 알고리즘을 위한 구체적인 요구사항 및 개인신원검증 카드 관리키를 위한 키 크기를 나타낸다.

〔표 3〕 알고리즘 및 키 크기 요구사항

카드 유효기한	알고리즘
2010/12/31 이전	- 2TDEA - 3TDEA - AES-128, AES-192, AES-256
2010/12/31 이후	- 3TDEA - AES-128, AES-192, AES-256

Ⅵ. 결 론

본 고에서는 미국의 개인신원검증 기준 FIPS-201-1에서 제시된 개인신원검증 시스템, 개인신원검증 카드 생명주기 활동, 개인신원검증 인증 메커니즘, 개인신원검증 암호화 사양에 필요한 기술적인 세부사항을 분석하였다.

개인신원검증에서는 비인가 된 사용자로 인한 정보 시스템의 파괴와 신원 도용 및 변조 등 기관의 안전성에 심각한 문제를 초래할 수 있다. 이를 해결하기 위해서 기존의 스마트카드를 이용한 신원검증 메커니즘에 추가적으로 개인식별번호, 생체인식 정보, 비대칭 암호를 이용한 개인신원검증이 필요로 한다.

개인신원검증에서의 접근 통제는 기관의 인위적 위협 환경을 고려하여 해커, 산업 스파이, 내부자에 의한 비인가 된 건물 및 정보 시스템의 접근을 식별하는데 효과적으로 대처할 수 있다. 따라서 기관의 자산과 데이터를 보호하기 위해서 추가적인 정보보호 인증요소들을 적용하는 물리적 · 논리적인 개인신원검증에 대한 연구가 진행되어야 할 것이다.

참고문헌

[1] NIST, "FIPS Publication 201-1 : Personal Identity Verification (PIV) of Federal Employees and Contractors", March 2006.

[2] NIST, "Special Publication 800-73-2 : Interfaces for Personal Identity Verification -Part 1 : End-Point PIV Card Application, Namespace, Data Model and Representation", September 2008.

[3] NIST, "Special Publication 800-73-2 : Interfaces for Personal Identity Verification -Part 2 : End-Point PIV Card Application Card Command Interface", September 2008.

[4] NIST, "Special Publication 800-73-2 : Interfaces for Personal Identity Verification -Part 3 : End-Point PIV Client Application Programming Interface", September 2008.

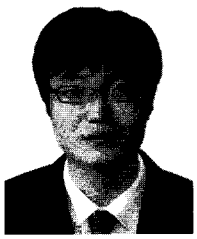
[5] NIST, "Special Publication 800-73-2 : Interfaces for Personal Identity Verification -Part 4 : The PIV Transitional Interface and Data Model Specification", September 2008.

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

[7] NIST, "FIPS Publication 186-1 : Digital Signature Standard(DSS)", November 2008.

[8] NIST, "Special Publication 800-76-1 : Biometric Data Specification for Personal Identity Verification", January 2007.

〈著者紹介〉



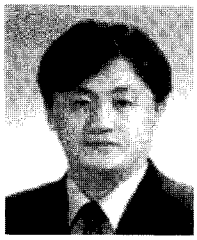
이 동 범 (DongBum Lee)

학생회원

2008년 2월: 순천향대학교 정보보호학과 학사

2008년 3월~현재: 순천향대학교 정보보호학과 석사과정

<관심분야> 정보보호, 정보보호제품 평가



곽 진 (Jin Kwak)
종신회원

성균관대학교 학사, 석사, 박사
2006년 4월~2006년 11월: 일본 큐슈대학교 시스템정보공학부 방문연구원
2006년 8월~2006년 11월: 일본 큐슈시스템정보기술연구소 특별연구원
2006년~2007년 2월: 정보통신부 정보보호기획단 개인정보보호팀 통신사무관
2007년 2월~현재: 순천향대학교 정보보호학과 교수
<관심분야> 암호프로토콜, RFID 시스템 응용 보안, 개인정보보호, 정보보호제품 평가, u-City 정보보호 기술 등