通信情報保護學會誌
第 10 券 第 4 號, 2000. 12

전자서명 키관리시스템에 대한 고찰

김 영 백*, 이 석 래*, 이 재 일*, 고 승 철*

A Study on the Private Key Management System

Young-Baek Kim*, Seok-Lae Lee*, Jae-Il Lee*, Seung-Cheol Goh*

요 약

공개키기반구조에서 전자서명생성키를 안전하게 관리하기 위한 방법 중 하나로 스마트카드를 사용한다. 연산기능이 없는 대부분의 스마트카드는 자체적으로 전자서명 기능을 수행할 수 없기 때문에 전자서명생성키를 시스템으로 읽어들인 후 전자서명을 수행하여야한다. 이 경우 전자서명생성키가 일시적으로 시스템에 존재하기 때문에 해킹 등에 의해서 키가 외부에 노출될 위험이 있다. 본 고에서는 전자서명 키관리시스템의 안정성을 강화시키기 위하여, 자체 전자서명이 가능하며 FIPS PUB 140-1 레벨 3을 만족하는 암호장치(PCMCIA 암호모듈)을 이용한 전자서명 키관리시스템에 대해서 설명하고 이를 인증서시스템에 적용하여 인증기관의 전자서명키를 안전하게 관리하는 방법에 대하여 설명하고자 한다.

Ⅰ. 서 론

글로벌 전자상거래 시장규모가 증가하면서 전자거래의 안정성 및 거래 당사자의 신원을 확인하는 방법으로 PKI(Public Key Infrastructure)에 대한 인식이 점차 확산되고 있다. 이러한 시대적 흐름에 따라서 세계 각국은 전자서명인증서비스를 제공할 수 있도록 정부 및 민간차원에서 PKI 구축을 서두르고 있는 실정이다. PKI 구축에서 간과해서는 안될 중요한 요소중의 하나가 전자서명생성키를 안전하게 관리하는 방법이다.

전자서명생성키의 관리를 위하여 전자서명기능이 없는 스마트카드를 사용할 경우 스마트카드로부터 전자서명생성키를 시스템으로 읽어와 전자서명을 수행하여야 한다. 이 경우 전자서명생성키는 일시적으로 시스템에 존재하기 때문에 해킹 등에 의해서 전자서명생성키가 외부로 노출될 위험이 있다. 외국의 경우는 키저장 뿐만 아니라 전자서명이 가능한 스마트카드가 널리 사용되고 있다. 또한 고비도 키저장을 위하여서는 FIPS PUB(Federal Information Processing Standard Publication) 140-1 레벨 3를 만족하는 저장장치(암호토큰)을 사용하고 있다.

본 고에서는 스마트카드 및 하드웨어 암호토큰을 이용한 전자서명키 관리 방법에 대해서 다음과 같은 내용으로 설명하고자 한다. 2장에서 암호장치에 대한 보안규정인 FIPS PUB 140-1 과 RSA사의 암호장치 인터페이스인 PKCS #11에 대하여 알아보고 3장에서는 스마트카드를 이용한 키관리 방법과 PCMCIA 암호모듈을 사용한 키관리 방법을 설명한다. 4장에서는 안전성이 강화된 키관리 시스템으로 스마트카드를 이용한 방법과 암호모듈을 이용한 방법을 소개하고 5장에서 결론을 맺는다.

Ⅱ. 암호장치에 대한 보안규정 및 인터페이스

1. 암호장치에 대한 보안규정(FIPS PUB 140-1)

FIPS PUB 140-1[1]은 미국의 국가표준기술연

* 한국정보보호센터, Korea Information Security Agency

표 1 FIPS PUB 140-1

	보안 레벨1	보안 레벨2	보안 레벨3	보안 레벨4
암호장치	암호장치와 암호 경계 명세. 모든 하드웨어, 소프트웨어 및 펌웨어 요소를 포함하는 암호장치에 대한 설명. 모듈 보안 정책에 대한 설명			
모듈 인터페이스	필수 및 선택적 인터페이스. 모든 인터페이스와 모든 내부 데이터 경로 명세		중요한 보안 매개변수용 데이터 포트를 다른 데이터 포트와 물리적으로 분리	
역할 및 서비스	필수 및 선택적 역할과 서비스를 논리적으로 분리	역할 기반 조작자 인증	ID 기반 조작자 인증	
유한 상태 머신	유한 상태 머신 모델 명세. 필수 상태와 선택적 상태, 상태 전이 도표와 상태 전이 명세			
물리적 보안	제품 등급 장비	잠금 또는 무허가 침투 방지	덮개와 도어에 대한 무허가 침투 발견과 응답	무허가 침투 발견과 응답 봉투
EFP/ EFT	규정 없음			온도와 전압
소프트웨어 보안	소프트웨어 설계 명세. 무한 상태 머신 모델에 대한 소프트웨어와 관련됨		고급 언어 구현	공식 모델, 사전 상태 및 사후 상태
운영체제 보안	실행 코드, 인증됨, 단일 사용자, 단일 프로세스	접근 통제 보호(C2 또는 그와 동등한 등급)	라벨을 이용한 보호(B1 또는 그와 동등한 등급), 안전한 통신 경로	구조화된 보호(B2 또는 그와 동등한 등급)
키 관리	FIPS가 승인한 생성/분배 기법		암호화된 형태로 키를 들어감/나감, 또는 split knowledge 절차로 직접 들어감/나감	
암호 알고리즘	분류되지 않은 정보를 보호하기 위해 FIPS가 승인한 암호 알고리즘			
EMI/ EMC	FCC 파트 15, 하위 파트 J, 클래스 A(업무용), 적용 가능한 FCC 규정(음성용)		FCC 파트 15, 하위 파트 J, 클래스 B(가정용)	
자체테스트	전원 공급 테스트 및 상태 테스트			

구소(NIST : National Institute of Standards and Technology)에서 발간하는 미연방 정보처리 표준 문서 시리즈 중 하나로 암호장치에 대한 보안 규정이다. 이 규정은 네 개의 점증적인 보안 단계인, 레벨1, 레벨2, 레벨3 및 레벨4로 구성되어 있으며 암호장치의 안전한 설계와 문서, 모듈 인터페이스, 인가된 역할 및 서비스, 물리적 보안, 키관리 등이 있다.

보안 레벨1은 가장 낮은 단계의 보안으로 암호장치에 대한 기본적인 보안규정을 지정하며 레벨2는 침투 방지 장치 또는 밀봉을 통하여 레벨1 암호장치의 물리적 보안을 개선시켰다. 또한 레벨 2는 조작자에게 특정 역할을 부여하는 역할기반 인증을 제공한다.

레벨 3에서는 ID를 기반으로 하는 인증을 제공하며 이는 레벨 2에서 사용된 역할 기반 인증보다 더욱 강력하다. 모듈은 조작자의 ID를 인증해야 하며 식별된 조작자가 특정 역할을 담당하고 있고 해당 서비스를 수행할 수 있도록 권한이 부여되었는지를 검증해야 한다.

레벨 3에서는 중요한 보안 매개변수를 입출력하는 데 있어서 보다 강력한 규정이 적용된다. 중요한 보안 매개 변수에 사용된 데이터 포트는 다른 데이터 포트들과 물리적으로 분리되어 있어야 한다. 또한 매개변수는 암호화된 형태로 모듈과의 입출력을 다루거나 split knowledge 절차를 사용하여 모듈과의 입출력을 직접 처리해야 한다.

안전한 운영체계에서 레벨 3를 이용하면 시분할 시스템에서 소프트웨어 암호화 기법이 가능해지기 때문에 시스템에서 실행될 수 있는 여타의 신뢰할 수 없는 소프트웨어로부터 암호 소프트웨어 및 중요한 보안 매개변수를 보호할 수 있다. 그러한 시스템은 일반 텍스트가 암호화된 텍스트와 혼용되는 것을 방지하여 일반 텍스트 키가 실수로 유출되는 것을 막아준다.

레벨 4는 가장 높은 단계의 보안을 제공한다. 레벨 4의 물리적 보안은 암호장치 주변에 일종의 보호장치를 제공한다. 레벨 4의 보호장치는 모든 방향으로부터 장치에 침투하는 것을 예방하도록 만들어진다. 또한 모듈이 온도와 전압이 정상 운영 범위를 벗어날 경우에 대비하여 환경 장애 보호(Environmental Failure Protection) 기능을 채택하거나 환경 장애 테스트(Environmental Failure Test)를 수행해야 한다.

2. FIPS PUB 140-2

FIPS 140-1 Validation 이 FIPS 140-2 로 대체 된다. FIPS 는 U.S Department of Commerce의 표준으로서 FIPS PUB ###-#의 형태로 나타내어진다. FIPS 140-2에서 바뀐점은 향상된 알고리즘과 난수/의사난수 생성 알고리즘 등이다. FIPS 140-2 Validation의 과정은 다음 그림 1과 같다.

FIPS 140-1과 CC의 기본적인 환경이 FIPS 140-2에 들어가 있다. 따라서 CC와 FIPS 140-2의 매핑이 가능하며, 이때 필요한 사항에 대하여 설명하였다. NIST는 CC에 기반한 NIAP(National Information Assurance Program)를 개발하여 사용중이다.

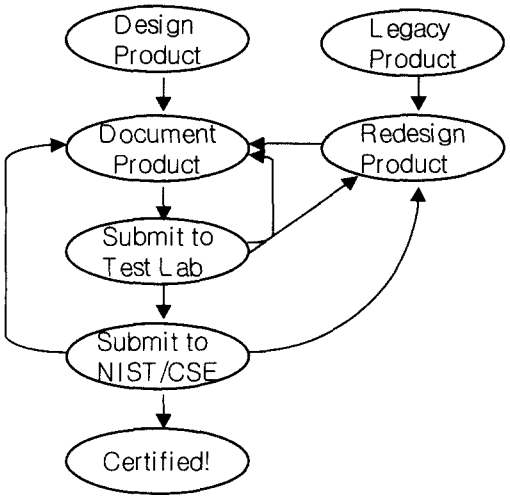


그림 1 FIPS 140-2 Validation 과정

3. CryptoKi(PKCS #11) API

CryptoKi[2]는 RSA사의 공개키 암호 표준 시리즈 중에서 PKCS #11 Cryptographic Token Interface Standard이며 암호토큰(스마트카드, PCMCIA 암호모듈)과 응용들 사이의 인터페이스를 지원한다. 1995년 4월에 버전 1.0 이 나온뒤로 현재 버전 2.10 까지 발표되었다.

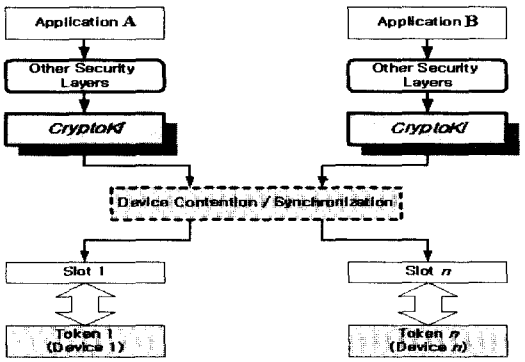


그림 2 CryptoKi 보안 서비스 구조

CryptoKi는 Cryptographic Token이라는 암호장치의 공통적 모델을 표현하는 것으로 암호토큰에 대한 최하위 프로그래밍 인터페이스를 제공한다. CryptoKi의 부가적인 목표는 휴대성, 확장성, 일반성, 자원공유지원 그리고 알고리즘 독립성이며 CryptoKi의 보안 서비스 구조는 그림 2와 같다.

CryptoKi는 여러개의 슬롯(Slot)을 통하여 시스템상에 활성화된 하나 또는 그 이상의 암호장치들에 대하여 인터페이스를 제공하며 물리적인 리더기 또는 다른 장치 인터페이스에 대응하는 것이다. 함수들은 PCMCIA 암호모듈 서비스나 소켓 서비스 같은 표준장치 드라이버를 통하여 전달된다.

CryptoKi의 세션은 응용프로그램과 암호토큰 사이에 논리적인 연결을 제공하며 응용프로그램이 암호토큰의 객체와 함수들에 대한 접근을 얻기 위하여 하나의 암호토큰과 하나 또는 그 이상의 세션을 열것을 요구한다. 응용프로그램은 세션 객체에 대하여 생성, 읽기, 쓰기 및 파괴를 하고 암호토큰으로부터 데이터들을 읽는다.

III. 키관리 방법 동향

1. 스마트카드를 이용한 키관리 방법

1.1 스마트카드

스마트카드는 신용카드 크기의 플라스틱 카드로서 데이터를 가공·처리 할 수 있는 칩을 내장하고 있다. 스마트카드는 20 Kbytes 정도의 저장용량을 가지고 있으며 특히 비인가된 접근 및 훼손공격으로부터 스마트카드에 저장된 데이터를 보호 할 수 있는 기능을 가지고 있다. 또한 스마트카드에 마이크로프로세서와 더불어 co-processor를 추가하여 복잡한 산술 연산을 빠른 시간 내에 할 수 있도록 한다면 암호연산을 스마트카드 내에서 처리할 수 있다. 그러나 현재 국내의 인증서비스 등에서는 co-processor가 추가된 스마트카드는 널리 사용되고 있지 않다.[5]

스마트카드에 대한 접근은 스마트카드 운영체제 및 보안논리 회로를 통해서만 가능하도록 접근통제 메커니즘이 구현되어 있다. 접근통제는 외부 실체가 스마트카드의 파일 및 데이터에 대한 접근을 시도할 경우 접근통제 메커니즘에서 정의한 접근규칙에 따라서 접근을 허가 또는 금지하는 보안기능이다. 즉 스마트카드의 파일 및 데이터에 대한 접근을 통제하여 스마트카드의 정보를 보호하는 수단을 제공한다.

스마트카드의 보안구조는 보안속성, 보안상태 및 보안 메카니즘으로 구성되며 보안상태와 보안속성 정보를 기초로 하여 접근통제 메커니즘을 구현할 수 있다.

1.2 스마트카드의 활용[7]

스마트카드는 현재 유/무선통신서비스, 인터넷전자상거래, 금융, 교통 분야에서 활발히 사용되고 있다. 유/무선통신서비스에서의 스마트카드는 통신 서비스 액세스 및 보안수단 그리고 서비스에 대한 지불수단으로 활용되고 있다. 무선통신 분야에서의 스마트카드는 이용자에게 다양한 서비스를 제공함은 물론이고, 보다 안전하고 신뢰성 있는 서비스를 제공하기 위해서 제공된다. 예를 들어 현재 유럽을 중심으로 널리 이용되고 있는 GSM(Global System for Mobile Telecommunications)에서 스마트카드는 서비스 가입자에 대한 인증, 정보의 안전한 저장, 암호알고리즘 등을 수행한다. 유선분야의 스마트카드 사용으로는 공중전화서비스가 있다. 이동통신의 발전에 따른 공중전화 시장은 단순 음성 서비스 제공과 함께 데이터 서비스, 멀티미디어 서비스 제공을 위한 기반구조를 형성하고 있다. 이를 위해서 기존의 공중전화 단말의 멀티미디어 단말화, 지불매체의 고도화 등에 대한 연구가 진행 중에 있다. 지불 매체의 고도화는 기존의 MS(magnetic stripe)카드나 메모리형 IC카드에서 벗어나 다양한 응용서비스를 제공하는 스마트카드 기반의 지불매체 형태로 변화하고 있다.

인터넷 전자상거래분야의 활성화를 위해서 가장 중요한 것은 안전하고 신뢰성 있는 지불수단과 보안을 확보하는 것이라 할 수 있다. 현재 대다수의 전자상거래 참여자는 이러한 지불과 보안의 최적의 수단으로 스마트카드를 손꼽고 있다. 스마트카드를 활용하여 정보를 안전하게 저장 및 처리하며, 이를 이용한 상거래 대금 지급이 활성화될 전망다. 현재 스마트카드 기반의 전자상거래 지불 솔루션은 시험단계에 있다.

금융분야의 경우 금융업무의 전산화가 세계 각국의 커다란 이슈로 등장하면서 지급결제수단의 전산화, 지불매체의 전자화가 급속하게 진행되고 있다. 금융분야의 전산/전자화의 가장 중요한 문제는 사용자의 편의 제공 및 보안문제이며, 이를 해결하기 위한 해결방안으로 스마트카드 기술이 채택되고 있다. 금융분야에서 스마트카드의 도입은 현금이나 MS 카드가 가져왔던 보안성, 데이터 저장능력 등의 문제점을 크게 개선하고, 전자금융(electronic banking) 서비스에 있어 중요한 지불 및 보안을 용이하게 한것이다.

교통분야의 경우 최근 세계 여러국가들은 첨단화되고 지능화된 교통, 운송 체제 구축을 준비중에 있으며, 이를 위해 미래형 ITS(Intelligent Transportation System)중 하나인 자동요금징수시스템(ETC:Electronic Toll Collection)을 구축 중에 있다. 차량 자동인식기술(Auto-mate Vehicle Identification)을 이용한 ETC는 지불수단 및 개인정보보호 수단으로써 스마트카드를 택함으로써 보다 안전하고 편리한 서비스를 사용자에게 제공하며, 대중 교통 수단인 버스, 지하철, 택시 등에 비접촉식 스마트카드의 도입은 사용자에게 동전의 소지나 환전 등의 불편함을 덜어주게 될것이다. 또한 서비스 제공자에게 유연성 있는 요금정책과 지불 시스템의

유지관리 비용 절감, 보안의 향상과 같은 효과를 제공한다.

2. PCMCIA 암호모듈을 이용한 키관리 방법

2.1 PCMCIA 암호모듈

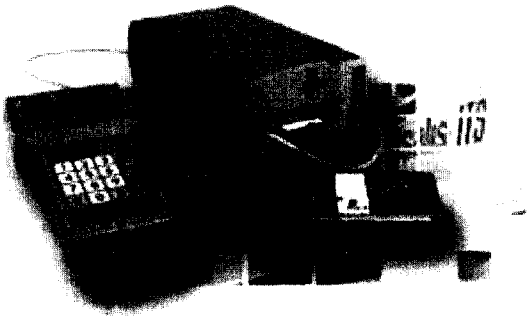


그림 3 PCMCIA 장비들

미국의 연방 BCA(Bridge CA)와 캐나다의 경우, 전자서명용 암호장치는 FIPS 140-1 레벨 3를 만족하여야 한다. PCMCIA 암호모듈은 PKCS#11을 지원하며 RSA 2048Bit 서명기능을 제공한다.

PCMCIA 암호모듈은 실제로 전자서명 생성키가 저장될 암호토큰과 이에 접근하기 위한 PED(Pin Entry Device)로 구성되며, PED에 접근하기 위한 PIN KEY가 있다. 사용자는 PIN KEY를 가지고 PED를 통하여 암호토큰에 로그인 한 후 암호토큰을 사용하여 키생성 및 전자서명 생성등을 수행하게 된다. 또한 비밀 분산 기능도 가지고 있어서 3인 이상이 모여야만 장비에 접근 할 수 있다.

2.2 PCMCIA 암호모듈의 활용

키생성시에는 PCMCIA 암호모듈이 내부적으로 생성하여 사용하거나, 외부에서 생성한 전자서명생성키를 저장한다. 키생성을 PCMCIA 암호모듈 내부에서 생성 할 경우는 키가 외부로 노출되는 일이 전혀 없으므로 안정성이 증가한다. 또한 기존에 사용하고 있던 전자서명생성키를 계속사용 하면서 전자서명생성키의 보관 장소만을 PCMCIA 암호모듈로 변경할 수도 있다.

인증서 생성시에는 PCMCIA 암호모듈 접근용 PED를 이용하여 2인이상의 사람이 자신의 PIN을 입력하여 카드에 로그인 한다. 인증서 생성시에는 전자서명 생성키는 카드외부로 누출되지 않으며, 인증서 생성 시스템이 서명할 값의 해쉬값을 PCMCIA 암호모듈로 넘겨주고 전자서명값을 받게 된다 (그림 4).

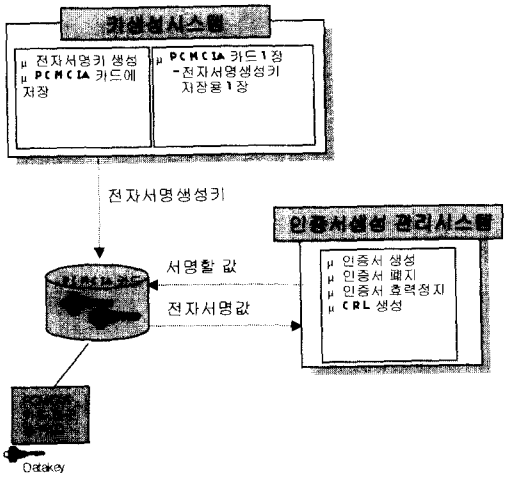


그림 4 PCMCIA 암호모듈을 이용한 키관리방법

따라서 한번 생성되거나 Import된 전자서명 생성키는 PCMCIA 암호 모듈 외부로 누출되지 않으며 전자서명시에는 FIPS PUB 140-1 레벨 3 기준에 의거한 방법을 사용하여 암호장치에 접근하게 된다.

IV. 안정성이 강화된 키관리 시스템 소개

1. KCDSA용 스마트카드 기반 키관리시스템[8]

현재 한국의 PKI에서 사용되는 전자서명 알고리즘은 RSA와 KCDSA(Korea Certificate-based Digital Signature Algorithm)가 있다. RSA기반의 키관리시스템에 대하여서는 이미 많은 연구 및 개발이 되어 있지만, KCDSA기반의 키관리시스템에 대한 연구 개발은 미비한 실정이다. 이에 KCDSA기반의 전자서명생성키를 안전하게 보관, 관리할 수 있는 키관리시스템을 소개하고자 한다.

KCDSA기반의 키관리시스템에서 사용되는 스마트카드 내에는 전자서명생성키를 외부에서 입력 또

는 자체 생성하는 기능을 포함하여 서명생성/검증 기능들이 구현되어있다(표 2). 실제 구현결과 카드의 서명생성 및 검증 추정시간은 1024Bit의 경우 서명생성에 120ms, 서명검증에 790ms이다(표 3).

표 2. KCDSA 스마트카드 명령어

명령어	내용
Put Key for KCDSA	P,Q,G 또는 X,Y 외부입력
Generate Key for KCDSA	X,Y 내부 생성
Read Public Key	공개키(Y) 읽기
Initialize Sign Generation	서명생성 초기화
Generate Sign	서명생성
Initialize Sign Verification	서명검증 초기화
Verify Sign	서명검증

KCDSA용으로 구현된 카드에서의 1024Bit 서명 생성 및 검증에 걸리는 추정시간은 실제 응용에 적용하는데 무리가 없는 것으로 나타났다. 그러나 2048Bit의 경우는 서명 생성 초기화 및 서명검증에 소요되는 추정시간이 실제 응용에 적용하기에는 약간 부담스러운 것으로 나타났다. 사용자의 경우에는 1024Bit 키길이를 갖는 스마트카드를 이용하면 전자상거래등 응용분야에서의 안전한 활용이 가능할 것으로 판단된다. 그러나 인증기관등에서 2048Bit 서명키를 사용하기 위해서는 궁극적으로 32Bit CPU를 채택한 스마트카드개발이 요구된다.

표 3. 실제카드의 서명/검증 추정시간

	1024 bits	2048 bits
서명생성초기화	390ms	7sec
서명생성	120ms	130ms
서명검증초기화	4ms	6ms
서명검증	790ms	12sec

2. 암호모듈 기반 키관리시스템

2.1 암호모듈 API

CryptoKi에서 정의하고 있는 대부분의 API를 지원한다. 함수의 구분은 일반적인 목적의 함수, 슬롯(Slot)과 암호토큰을 관리하는 함수, 세션관리 함수, 객체관리 함수, 암/복호화 함수, 서명/검증 함수, 키관리 함수 등이 있다. 암호모듈을 인증서버에 연동하기 위해서 필요로 하는 함수에는 키관리 함수중 키를 생성하거나 외부에서 생성된 키를 Import 하는 함수와 서명/검증 함수중 전자서명을 생성하는 함수등이 있다(표 4).

C_GenerateKey 는 PCMCIA 암호모듈 자체에서 키를 생성하고자 할 때 사용되며 C_UnwrapKey 는 외부의 키생성시스템에서 생성된 키를 암호장치에 저장하고자 할 때 사용된다. 서명 과정은 일반적인 다른 API들과 동일한 과정을 거치며 파일형태의 서명할 값을 입력하면 이를 서명하여 파일 형태로 전자서명값을 넘겨준다.

표 4. CryptoKi 호출함수(일부)

범주	함수
Key Management Functions	C_GenerateKey
	C_GenerateKeyPair
	C_WrapKey
	C_UnwrapKey
	C_DeriveKey
Signing and MACing Functions	C_SignInit
	C_Sign
	C_SignUpdate
	C_SignFinal
General Purpose Functions	C_Initialize
	C_Finalize
	C_GetInfo
	C_GetFunctionList
Slot and Token management Functions	C_GetSlotList
	C_GetSlotInfo
	C_GetTokenInfo
	C_InitToken
	C_InitPIN
	C_SetPIN
Session Management Functions	C_OpenSession
	C_CloseSession
	C_Login
	C_Logout
Object Management Functions	C_CreateObject
	C_DestroyObject
	C_CopyObject
	C_GetObjectSize

전자서명 생성시나 키생성 시에는 암호토큰의 초기화때 정해진 사용자에 의한 로그인이 수행되므로

PIN을 이용한 인증은 필수적이다.

그 밖에도 암호 장치를 초기화하고, PIN을 이용하여 로그인하며 세션을 관리하는 함수들이 존재하며 생성된 암호토큰을 백업하는 함수들도 제공되어 진다.

2.2 PCMCIA 암호모듈을 이용한 PKI 구현 예

신뢰할 수 있는 인증기관의 필수 조건중 하나는 그림 5와 같이 전자서명키에 대한 신뢰경로를 갖추는 것이다. 전자서명생성키의 생성 및 백업은 안전한 방법으로 이루어져야하며, 인증기관의 전자서명 생성시에 안전하게 참조되어야 한다. 따라서 전자서명생성키의 안전한 보관은 신뢰할수 있는 암호학적 실행경로 상에서 이루어져야만 한다. 예를 들어 전자서명생성키를 암호화하여 저장하는 경우 실제 사용할 때 복호화하여 평문 형태로 사용게 되므로 키가 누출될 수 있다. 이때 키를 Capture 하는 등의 공격이 발생할 수 있다. 따라서 키는 사용 중 평문 형태로 노출되는 일이 없어야만 하며, 그림 5와 같이 사용자인증, 키생성, 키분배 및 저장 등에 신뢰할 수 있는 경로(Trusted Path)를 구축해야 한다.

먼저 사용자 인증 과정에서는 초기화 작업후 Security Officer(SO)와 사용자의 PIN을 설정하게되고 이를 이용하여 초기 로그인을 수행한다. 암호토큰에 로그인 하기 위해서는 데이터 키를 사용하여 SO 혹은 사용자로 로그인한 상태여야 하며 비밀분산(M/N)을 아용하여 여러사람이 데이터키를 소유할 수 있다.[4]

로그인이 끝나면 키생성과정으로 전자서명생성키를 암호토큰에서 생성하거나 기존의 키생성시스템에서 생성된 전자서명생성키를 Import 하게 된다. 이 모든 과정은 PCMCIA 장비에 연결된 별도의 PED를 통하여 이루어지게 된다.

키분배 및 저장과정에서는 PCMCIA 암호모듈을 이용하여 키를 백업하고 만일 비밀분산(M/N)이 사용되었을 경우 이때 사용된 데이터키도 백업한다.

PCMCIA 암호모듈에서 전자서명생성키를 이용하여 인증서를 생성시에는 인증서버에서 암호모듈로

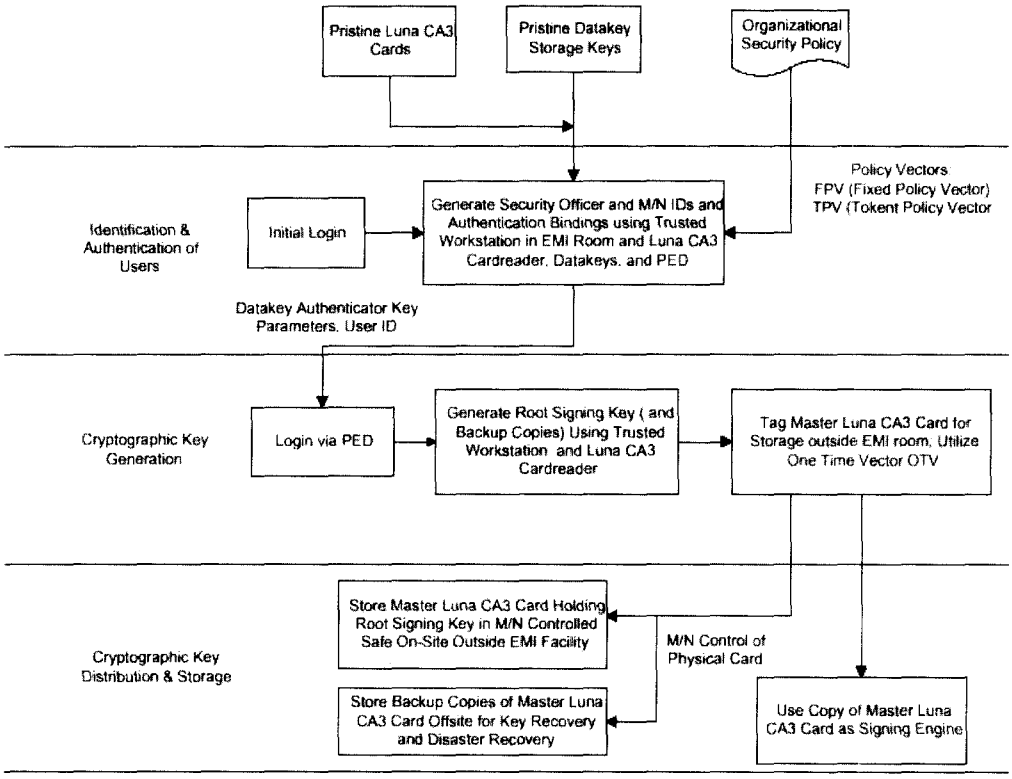


그림 5 CA Root Key Trusted Path

넘어온 값에 서명한 후 서명값을 돌려준다. 이때 미리 정해 두었던 SO 혹은 사용자가 암호토큰으로 데이터 키를 이용하여 로그인을 수행하여야 하며 비밀분산(M/N)을 설정해 두었다면 해당하는 숫자만큼의 데이터 키가 필요하게 된다.

V. 결 론

본 고에서는 PKI 구축의 안전신뢰성을 보장하기 위한 방법으로 스마트카드기반의 안전한 전자서명생성키 관리시스템과 FIPS PUB 140-1 레벨 3를 만족하는 보안장치에 대하여 언급하였다. 스마트카드는 사용 및 휴대가 간편하기 때문에 사용자에게 적합한 키관리시스템을 제공할 것이다. 그리고 FIPS PUB 140-1 레벨 3를 만족하는 보안장치는 더 안정성을 요하는 키관리시스템에 적합하다.

향후 전자상거래의 발전과 전자서명의 필요성이 증가할 것으로 예상되며 더불어 전자서명생성키의 안전한 관리에 대한 필요성도 더욱 증가할 것이다. 따라서 국내 전자서명 알고리즘 뿐만 아니라 국제적으로 널리 사용되고 있는 알고리즘을 수용할 수 있는 스마트카드 및 보안장치기반의 키관리방식에 대한 연구가 필요할 것이다.

참 고 문 헌

[1] NIST, "FIPS PUB 140-1: Secutity Requirements For Cryptographic Modules", NIST, January 11, 1994

[2] RSA Laboratories, "PKCS #11: Cryptographic Token Interface Standard", RSA, December 22, 1997

[3] IETF RFC 2459(1999), Internet X.509 Public Key Infrastructure Certi ficate and CRL Profile

[4] Deloitte & Touche, Certificate Authority Root Key Protection: Recommended Practices, White Paper, July, 1999

[5] 권현조, 원동호, "스마트카드 데이터 보호를 위한 접근통제 모델 분석", *통신정보보호학회학회지*, Sept, 2000.

[6] 김점구, 김석우, 강창구, 이재광, "효율적인 정보보호를 위한 상용 암호 서비스 기술(CryptoAPI 중심)", *통신정보보호학회학회지*, Dec, 1998.

[7] 한국정보보호센터, "스마트카드 제품 평가기준 해설서", 최종연구보고서, Nov, 2000.

[8] JaeIl Lee, SoungJin Kim, JooSeok Song, "Designing and Implementing Smart Card-Based Key Management Systems for the KCDSA", WISA2000, Nov, 2000.

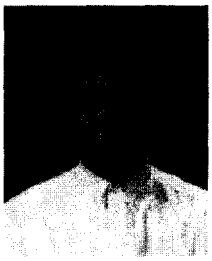
[9] Chrysalis-ITS, http://www.chrysalisits.com/

[10] Chrysalis-ITS,http://www.chrysalis its.com/

〈著者紹介〉

김 영 백 (Young-Baek Kim)
1995년 2월 : 순천향대학교 정보통신공학과 졸업
1997년 2월 : 순천향대학교 정보통신공학과 석사
1996년 12월~2000년 3월 : 한전정보네트웍
2000년 4월~현재 : 한국정보보호센터
관심분야 : 정보보호

이 석 래 (Seok-lae Lee)
1992년 2월 : 한양대학교 전자통신공학과 졸업
1994년 2월 : 한양대학교 전자통신공학과 석사
1994년 2월~1999년 6월: LG 전자
1999년 7월~현재: 한국정보보호센터 연구원
관심분야 : 데이터 보안, 통신공학



이 재 일(Jae-il Lee)
1986년 2월 : 서울대학교 계산통계학과 졸업
1988년 2월 : 서울대학교 계산통계학과 석사
1991년 1월~1996년 6월 : 한국 IBM
1996년 7월~현재 : 한국정보보호센터 선임연구원/팀장
관심분야 : 유·무선 PKI, 전자상거래 보안

고 승 철(Seung-Cheol Goh)
1981년 2월 : 연세대학교 졸업
1983년 2월 : 연세대학교 이학석사
1992년 8월 : 포항공대 이학박사
1984년 3월~1996년 5월:
한국전자통신연구소 책임연구원
1996년 6월~현재: 한국정보보호센터 책임연구원/부장
1999년 3월~현재: 광운대학교 전산과학과 겸직교수
관심분야 : 침입탐지시스템, 전자서명기술