CDKey를 이용한 KMI 구축과 사용자 인증

김철환*, 장현석**

KMI & User Authentication by CDKey

Chul-Whan Kim*, Hyeon-Seog Jang**

요약(Abstract)

은행간 계좌이체, 증권거래에서부터 출발한 공인인증시스템이 일반 전자상거래까지 확산되고 있는 가운데 인증키의 안전한 보관 및 이동사용의 중요성이 대두되고 있다. 본 연구에서는 KMI(Key Management Infrastructure)와 복제방지 기술이 적용된 CDKey 가 연동되는 시스템을 구성하고 이를 이용하여 이러한 시스템이 안전한 본인 인증, 안전한 인증키 보관, 편리한 인증서 이동에 활용될 수 있도록 하는 방안을 제시 한다.

Key Word : PKI, KMI, 인증

* 국방대학교 무기체계학과 교수
** 시디캐시 개발이사

1. 서론

1999 년 7 월 전자서명법이 시행된 이래 인터넷뱅킹과 인터넷 증권거래에 공인인증서가 의무화 되고 2004 년부터는 일정 금액 이상의 전자상거래에 있어서도 공인인증서 사용이 의무화 될 예정이다.[1]

공인인증서 확산 추세는 2001 년 2 백만 건 을 넘어선 이래 불과 2 년도 안되어 2003 년 3 월 8 백만 건에 이르고 있다.[2,3]

그러나 공인인증서의 보급 확대는 기관간의 상호 연동, 유료화, 중복발급, 시스템 정지 등 많은 문제점들을 노출하고 있다. 공인인증서 역시 여러가지 해킹 수단들에 노출되어 있음에도 불구하고 일반인들은 공인인증서를 사용하는 것 만으로 모든 보안문제가 해결된다고 생각 하거나 역으로 막연한 불안감을 느끼고 있다.[4] 조사에 따르면 공인인증서 사용시 불만족한 부분에 대한 답으로 안전성 문제가 63.2%, 이용시의 불편함과 복잡함이 47.4% 에 이르고있다.[5] 또한 사용자들의 인식부족과 인증서 이동매체 보급지연으로 인터넷 뱅킹과 증권거래에 있어 거래를 할 때마다 매번 인증서를 재발급 받는 사용자도 있는 실정이다.[6]

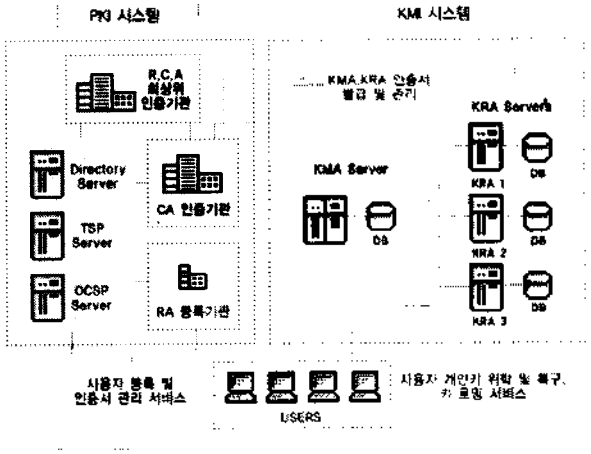
정부주도로 이루어진 인증서 정책은 확산의 측면에서 성공적이지만 공인인증서 발급 천만 건 시대에 걸맞게 사용자의 인식 제고와 PKI 의 정체성을 손상하지 않는 측면에서 사용편의를 제고해야 한다.

이러한 관점에서 본 연구는 인증서의 불필요한 재발급을 방지하고 인증서에 이동성을 부여할 수 있는 KMI 와 위탁자 신분확인 수단으로서 CDKey 를 접목, KMI 와 소지기반의 사용자 인증시스템을 연동시킴으로써 공인인증서의 안전한 보관과 편리한 이동 사용을 만족시킬 수 있는 시스템을 구성하고자 한다.

2. Key Management Infrastructure

2.1 KMI 의 개요

KMI 는 "암호키관리 기반구조"로 정의된다. 암호키 관리는 암호문의 소유자(일반적인 암호시스템에서 키를 소유한 사람-PKI 에서는 개인키를 보관한 사람)가 아닐지라도 사전에 약속된 어떤 특정한 조건하에서 허가된 사람에게 복호가 가능한 능력을 제공하는 시스템(관리체계)을 의미한다.[7] 여기서 약속된 조건이란 암호가 나쁜 목적으로 사용되었을 경우의 법 집행권한 확보를 위한 허가일 수도 있고, 암호용키를 분실했을 경우가 될 수도 있다. 암호키관리 기반구조는 이러한 상황에 대비해서 제 3 자가 키를 안전하게 보관하고, 일정한 조건이 갖추어 졌을 때 키를 복원해 주는 시스템이라고 할 수 있다.



< 그림 1 >국내 KMI 상용제품 구성[8,9]

현재까지 제안된 암호키관리 방식은 크게 위탁(*escrow*) 방식과 캡슐화(*encapsulation*)방식, TTP(*Trusted Third Party*) 방식으로 나눌 수 있다. 국내에서 개발된 상용제품은 위탁방식으로 <그림 1>과 같이 구성되어 있으며 KMA 서버는 키위탁 과정을 관리하고 KRA 서버는 위탁된 키를 안전하게 분산 저장한다. [10]

위탁방식은 사용자의 비밀키의 전부 또는 일부를 신뢰 받는 제 3 자에게 위탁하는 방식으로 유사시에 키를 확실하게 얻을 수 있다는 장점이 있다. 이 방식은 키를 제 3 의 개체에게 위탁함으로써 유사시에 키를 확실하게 얻을 수 있다는 장점이 있는 반면에, 키를 위탁하는 제 3 자의 신뢰도에 많은 영향을 받는다. 또한 이러한 키위탁방식에서 위탁되는 키는 대부분 한시적으로 사용되는 세션키(*session key*)가 아니라 사용자의 비밀키(*private key*)와 같은 긴 주기동안 사용되는 키(*long-term key*)가 되므로 신뢰도가 낮은 보안기관을 사용하는 경우에는 여러가지 문제점이 발생할 수 있다.

이 방식에서는 키위탁 기관의 신뢰도를 높이고 키 정보가 집중되어 공격 목표가 되는 것을 막기 위해서 비밀 분산 방식(*secret sharing scheme*)을 사용하여 위탁된 키를 여러 기관에 분산시키는 방식이 사용되고 있다. 또한 이외에도 위탁방식을 사용할 경우 제 3 자의 신뢰도 뿐만 아니라 사용자들이 위탁한 키의 안전한 보관과 관리문제, 키가 법률 기관에 의해 합법적인 도청 목적으로 공개되었을 경우에 키의 사용기간의 제한 등이 문제점으로 등장한다.

2.2 KMI 의 필요성

KMI 는 암호기술의 역기능으로부터 출발하였다. 암호기술의 역기능이라 함은, 개인적 관점에서 암호화된 문서에 대해 암호키 분실에 따른 복호화 불가능 상황의 초래이며 사회적 관점에서 범죄집단에서 은닉을 은폐하기 위하여 사용되는 경우이다.

구체적인 암호화 역기능 사례로써 암호용 키의 분실 및 손상으로 인한 주요 정보의 데이터 복구 불능, 문서를 암호화 하여 보관해 놓은 직원의 갑작스러운 퇴사나 휴가 등의 이유로 문서에 접근 할 수 없는 경우 등을 들을 수 있다.[11] 특히 공인인증서의 경우에 있어서 개인키를 보관해 놓은 PC 가 사용자의 실수, 바이러스, 해킹 등으로 인하여 파괴되는 경우, 불필요한 재발급으로 인한 경제적 손실이 대표적인 예이다.

해킹 등으로 PC 에 보관된 공인 인증서가 유출되어 발생하는 사고의 위험성에 대해서는 특별한 주의가 요구되고 있다. 최근들어 해킹의 유형은 기관 및 학교의 서버보다는 개인 PC 를 대상으로 하는 경우가 늘고 있으며 [12] 트로이(Trojan)류의 바이러스, 스파이웨어의 이용, 백오리피스(Back Orifice), 딥보 (Deep Bo), 키로그(Keylog) 등 해킹툴을 이용한 다양한 방법으로 개인 PC 자원의 유출 가능성이 열려있다. 따라서 공인인증서의 파손, 유출로 인한 손실을 방지하기 위하여 KMI 가 절실히 요구되고 있다.

2.3 KMI 를 통한 키로밍 서비스 구현

키로밍(Key-Roaming) 서비스는 사용자의 개인키를 "중앙보관소"에 위탁 보관하고, 이용자는 어느 곳으로 이동하든지 인터넷을

통해 중앙의 보관소에 접속, 자동으로 설치되는 이용자 소프트웨어를 통해 안전하게 신원확인을 한 후, 암호화된 개인키를 돌려 받을 수 있게 하는 서비스다. [13]

KMI 가 구축되면 인증서의 위탁과정을 통해 인증서를 안전하게 보관하고 위탁자의 필요 시에 위탁자가 있는 위치에서 다운로드하여 사용 할 수 있다. 이는 KMI 를 구축함으로써 키의 안전한 보관 이라는 기능이외에 키로밍이 구현된다는 것을 의미한다. 위탁자가 언제든지 원하는 위치에서 인증서를 다운로드하여 사용할 수 있게 됨으로써 인증서의 안전한 보관과 함께 이동성을 구현할 수 있는 것이다.

지금까지 PKI 서비스 구조에서는 타지에서 이용자가 자신의 인증서를 이용하는 서비스는 이용 할 수 없었으며 인증서를 저장하는 스마트카드나 USB 와 같은 저장매체는 인증서 자체를 항상 지니고 다니는 부담이 있으므로 KMI 구축을 통해 인증서비스의 사용자 편리성을 제고할 수 있다.

3. CDKey

3.1 CDKey 의 개요

CDKey 는 CD(Compact Disk)라는 실물 매체와 내장된 인증정보를 네트워크 상에서 인증하는 것으로 신용카드 크기의 CD 에 인증정보 기록 후 이를 검증함으로써 소지기반 인증의 보안성을 확보하는 것이다.

CDKey 에 저장되는 정보는 암호화된 인증데이터와 CD 레코더에 의하여 복제되지 않는 OPM (Optical media Physical Marking system) Code 로 구성된다.

CDKey 의 두드러진 장점은 별도의 하드웨어나 소프트웨어 없이 CD 드라이브에 CDKey 를 넣고 비밀번호만을 입력함으로써 편리하게 사용할 수 있다는 점이다. CD 드라이브의 경우 이미 거의 모든 PC 에 장착되어 있기 때문에 CDKey 사용을 위한 별도의 하드웨어가 요구되지 않는다. CDKey 는 높은 보안성에도 불구하고 별도의 인프라 비용이 요구되지 않는 경제적인 인증수단이다.

3.2 CDKey 의 기술적 특성

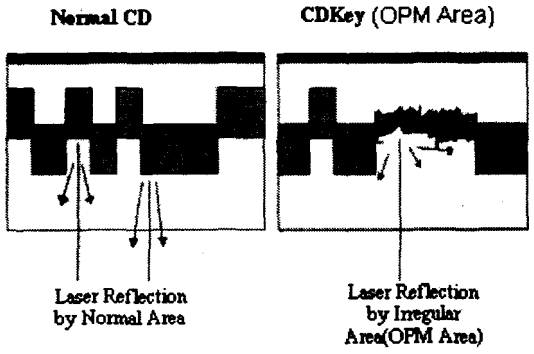
3.2.1 매체적 특성

CD 로 대표되는 광학매체(Optical Media)는(CD-ROM, CD-R, CD-RW, DVD-ROM, DVD-RAM, DVD-R, DVD-RW 등) 저장용량대 비용의 비가 여타의 다른 매체에 비하여 가장 경제적인 디지털데이터 저장 매체이다. CDKey 는 이들 광학매체중에서 CD-R 을 사용한다. 이는 발급되는 매 CDKey 마다 저장되는 인증 데이터와 OPM Code 가 다르기 때문이며 CD-ROM 드라이브, CD 레코더, CD-RW, DVD-ROM 드라이브, DVD 레코더, DVD-RW 의 모든 재생장치에서 사용이 가능하다.[14]

3.2.2 보안성

CD Key 와 타 Normal CD 와의 차이점은 <그림 2>에서와 같이 CD key 는 복사방지를 위한 OPM 영역이 형성되어 있다는 것이다. OPM 영역은 단순히 저장되는 데이터를 암호화한 것이 아니라 CD 기록부분을 물리적으로 변형시킨 것으로 CDKey 복사 시, 사본에는 OPM 영역이 형성되지 않는다. [15] 다시말해 CDKey 에 저장된 데이터

영역은 복사될 수 있으나 OPM 영역은 복사되지 않으므로 OPM 영역을 조사함으로써 복사본 여부를 판단 할 수 있다.



< 그림 2 > OPM 영역의 물리적 특성 개요

4. CD Key 기반 키로밍 서비스 사용자 인증

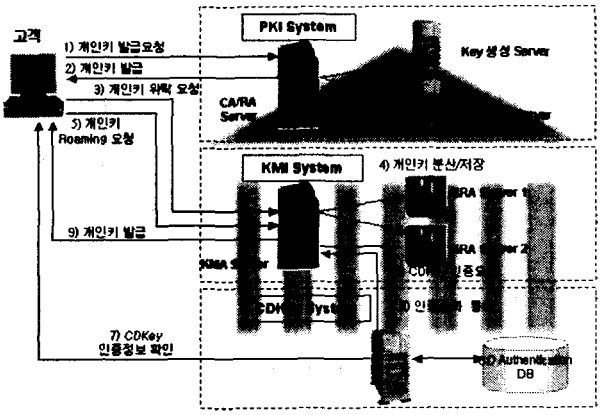
4.1 기존 키로밍 서비스의 사용자 인증

현재 개발되어 있는 키로밍 서비스의 상용화된 제품에서 사용자 인증은 단순한 ID, 패스워드 방식이다. 여기서 단순하다는 것은 각종 해킹툴에 의하여 ID 와 패스워드가 유출되었을 경우, 위탁자도 모르는 사이에 인증서가 타인에 의하여 사용될 수 있다는 것을 의미한다.

KMI 에 의하여 중앙의 암호는 분산되어 저장되어 있으며 사용자가 지정한 패스워드로 암호화되어 있기 때문에 관리자라 하더라도 암호정보를 조합하여 완전한 정보로 가공하기가 실질적으로는 불가능하다. 그러나 사용자가 지정한 ID 와 패스워드가 유출된다면 안전하게 보관 한다는 의미 자체가 퇴색되어 버린다.[16]

KMI 시스템이 구축됨으로써 공인인증서를 안전하게 보관하고 키로밍 서비스가 가능해졌지만 얼굴을 대면하지 않는 네트워크상에서의 위탁자 신분 확인을 위해 보다 안전한 방법이 요구된다.

4.2 CDKey 를 이용한 키로밍 사용자 인증



< 그림 3 > CDKey 를 이용한 키로밍

<그림 3>은 CD key 를 이용한 키로밍 시스템을 나타낸것이며, 기존 키로밍 서비스의 사용자(위탁자) 인증시에 ID, 패스워드 방식의 취약점을 극복하기 위해 CDKey 를 적용한 것이다. 사용자 인증에 CDKey 를 사용함으로써 사전에 약속된 단순한 디지털 데이터를 검증하는 방식이 아닌 물리적인 실체에 대한 인증을 함으로써 소지기반 인증 수준의 보안성 유지가 가능하다. 또한 CDKey 가 여타 소지기반의 매체를 채택 하는 것보다 추가 인프라비용 발생, 매체 자체의 가격 등 경제적으로 우수하며 기존 KMI 나 키로밍 서비스 시스템과의 연동에 따른 시스템 변경이 최소화 됨으로써 적용이 용이한 장점을 가지고 있다.

사용 절차상에서도 기존 ID 대신에 CD 드라이브에 CDKey 를 넣는 것으로, 패스워드는 CDKey 와 연동되는 패스워드 입력

으로 대체되어 크게 달라지는 부분이 없어 사용자 측면에서도 적용하기에 별다른 어려움이 없다.

5. 결론

2002 년에 발생한 법인계좌를 통한 허수주문으로 인한 증권거래 사고사례 [17]와 같이 네트워크를 통한 금융거래의 안전성이 확보되지 않을 경우 사고로 인한 피해금액은 수백억을 초과하기 쉽다.

대면을 하지 않은 상황에서의 인터넷 뱅킹이나 사이버 증권거래와 같은 금융거래는 철저한 본인 신원확인 과정을 필요로 하게 된다.

본 연구에서 살펴본 바와 같이 KMI 를 구축함으로써 공인인증서 사용자에게는 인증서를 안전하게 보관하여 각종 사고에 대비할 수 있을 뿐만 아니라 키로밍 서비스의 이용이 가능해져 이동 시에도 필요한 장소에서 위탁 보관하여 놓은 인증서를 복원하여 사용할 수 있는 것이다. 또한 사용자(위탁자) 인증을 위하여 CDKey 를 사용함으로써 보다 안전성 높은 키로밍 서비스를 구현할 수 있으며 위탁자 본인 확인에 소지기반의 CDKey 를 채택함으로써 불법적인 인증서 유출시도를 방지할 수 있어 키로밍 서비스를 안전하게 도입할 수 있는 토대가 된다.

참 고 문 헌

[1]"인터넷 쇼핑몰 카드결제 내년부터 공인인증 도입", 디지털타임즈 2003.7.2

[2]"전자서명 이용자를 수 늘려라'...정통부 팔 걷어 부쳐", inews24, 2002.10.30

[3]"공인인증 8 백만 돌파", 디지털타임즈 2003.3.20

[4]"못 믿을 보안열쇠 전자인증서", 국민일보, 2001.7. 11

[5] "전자서명에 관한 인식 및 이용실태 조사", 한국정보보호진흥원, 2001. 10

[6] "증권사 공인인증 의무 도입의 향후 해결 과제" , 전자신문, 2003.4.1

[7] 김지연, "국내 암호용 인증서의 안전한 관리,발급을 위한 암호키관리 기술개발 추진현황",한국정보보호진흥원,2001.6,p5

[8] http://www.bcqre.co.kr/product

[9] http://www.ksign.co.kr/products1_7.shtml

[10] 권현조,"암호키 복구기술과 키로밍 서비스",한국정보보호진흥원,2001.8 ,p5-16

[11] 김지연, "국내 암호용 인증서의 안전한 관리,발급을 위한 암호키관리 기술개발 추진현황",한국정보보호진흥원,2001.6,p4

[12] "해킹바이러스 통계 및 분석월보", 한국정보보호진흥원

[13] 권현조,"암호키 복구기술과 키로밍 서비스",한국정보보호진흥원,2001.8 ,p3

[14] N. V. Philips, "Specification of 8mm CD-Single", Sony Corporation, p2-57

[15] "マルチメディア CD/CD-ROM 技術", トリケップス, 1994.10, p15-77

[16] "공인인증서 사용 7 계명을 아시나요", 디지털타임스, 2003.4.4

[17] "줄줄이 터지는 '금융사고' 3 년 6 개월새 8311 억 샜다", 한국경제, 2002.8.25