디지털콘텐츠 유통을 위한 스마트카드기반의 다중인증처리방법설계 및 구현

(Design and implementation of smart card-based multi-authentication mechanism for digital contents delivery)

김 용*·이 태영**

초 록

폭발적인 디지털콘텐츠의 성장과 함께, 지식과 정보를 중계하고 유통시키는 조직으로서 도서관과 정보센터는 지식소유자와 이용자사이에서의 새로운 역할을 수행하여야 한다. 정보화사회에서 무형의 정보와 지식에 경제적인 가치가 더하게 되므로서 전자지불시스템은 이러한 중계서비스를 수행하기 위하여 필수적으로 요구되고 있다. 그러나 네트웍상에서 디지털콘텐츠를 전자적으로 사고 팔기 위해서는 데이터와 사용자의 정보에 대한 보안이 필수적으로 요구된다. 지식중계시스템(전자도서관)은 이용자가 안전하고 편리하게 인터넷을 통하여 자신이 필요로 하는 디지털콘텐츠를 입수 및 구매할 수 있어야 한다. 그러나 정보의 공유와 개방을 목표로 개발된 인터넷이 갖고 있는 기본적인 취약성 때문에 거래내용, 신용카드정보, 은행계좌정보, 혹은 관련 비밀번호, 사용자 정보 등의 중요정보들이 쉽게 노출될 수 있다. 이러한 인터넷과 같은 개방망에서의 전자거래의 보안성을 높이기 위한 방법으로서 본 연구에서는 기존의 인증시스템과 관련된 암호관련 기술을 살펴보고 보다 보안성을 높일 수 있는 방법으로서 고려되고 있는 스마트카드가 가지고 있는 장점을 온라인상의 전자거래에 적용하는데 있어서의 사용자와 스마트카드에 대한 인증방법을 제안하고 있으며 특히 개방형 네트워크상에서의 스마트카드를 기반으로 하는 전자중계시스템에서의 사용자 및 스마트카드에 대한 동시적 다중인증 및 암호통신에 대한 프로토콜을 설계하고 이를 구현하였다.

ABSTRACT

With explosively increasing digital contents, library and information center should have a new role between knowledge providers and knowledge users as information brokering organization. Electronic transaction system should be required for performing this brokering service since economic value is added to information and knowledge in information society. The developments and changes around library are keeping up with increasing building digital library and digitalizing printed sources. With the rapidly changing circumstances, the Internet is currently witnessing an explosive growth. By serving as a virtual information resource, the Internet

* KT 멀티미디어연구소 e-Portal 연구팀(yongkim@kt.co.kr)

** 전북대학교 문헌정보학과

can dramatically change the way business is conducted and information is provided. However because of features of the Internet like openness and information sharing, it has fundamental vulnerabilities in security issues. For instance, disclosure of private information and line eavesdropping such as password, banking account, transaction data on network and so on are primary obstruction factors to activation of digital contents delivery on network. For high network security and authentication, this paper looks at smart card technologies and proposes multi-authentication protocol based on smart card on open network, implements and analyzes it.

키워드: 인증, 스마트카드, 디지털콘텐츠, 보안, 암호화 authentication, smart card, digital contents, 3-DES, cryptography

1. 서 론

현대사회에 있어서 과학기술의 발전은 사회 전분야에 있어서 커다란 변화를 가져오고 있다. 특히 폭발적인 정보의 생산은 이를 효율적으로 처리하고 유통하기 위한 새로운 방법들을 요구하게 되었다. 따라서 이러한 정보를 효율적으로 관리하기 위하여 새로운 정보기술을 적용하고 있으며 이러한 정보기술을 활용하므로서 정보를 처리하고 이를 유통하는데 있어서 중계자로서 이용자에게 제공하는 역할을 수행하기 위하여 많은 도서관 특히, 전문도서관, 대학도서관 및 일부 공공도서관은 전자도서관을 구축하고 자료를 디지털화하므로서 이를 네트워크를 통하여 이용자에게 제공하고 있으며 이러한 흐름은 지속될 것으로 예상되고 있다. 이러한 일련의 흐름과 함께, 전통적으로 인쇄정보가 주형식이었던 정보저장소로서 도서관이 아닌 새로운 형식의 정보저장 및 중계시스템으로서 전자도서관의 출현은 극히 자연스러운 일이라 할 수 있을 것이며 이를 통한 정보처리의 새로운 방향성을 제시되고 있다. 한편 이러한 일련의 정보의 처리, 저장 및 관리와 관련된 정보기술의 발전, 전자도서관의 구축 및 사회적인 새로운 요구들은 실질적으로 지식의 저장, 관리 및 유통에 대한 전반적인 체계화를 이루고 있는 도서관을 포함하여 지식을 생산하고 있는 개별적인 기관이나 실질적인 지식이나 정보의 생산자 및 수요자로서 개인이 인터넷에 접속된 컴퓨터를 통해 유형 및 무형의 지식을 네트워크를 통하여 실제의 상거래와 같이 구매, 거래, 지식의 검색 및 교환 등의 상거래행위를 수행하는 도서관분야의 새로운 역할로서뿐만이 아니라 인터넷 비즈니스 영역의 새로운 분야로서 대두되고 있다. 전통적으로 경제적인 가치를 단지 유형의 상품에 두었던 것과는 달리 무형의 지식은 오히려 또 다른 측면에서 유형의 상품보다 큰 가치를 지니게 되었다. 이러한

지식에 대한 경제적인 가치 부여와 함께, 지식을 판매, 구매, 중계하는 지식에 대한 상거래 개념은 그 정보와 지식에 대한 유통을 담당하고 있는 도서관이나 지식과 정보를 유통하고 있는 조직에 있어서는 네트워크를 통한 안전한 정보 및 지식의 전달을 위한 보안적인 측면에 있어서 많은 딜레마를 안겨 주고 있다. 이러한 딜레마의 근본적인 이유는 먼저 디지털 콘텐츠의 특성상 불법적 생산과 복제가 가능하여 판매자가 소비자에게 유료화된 상품으로 유통하기 위해서는 특별한 디지털 컨텐츠의 관리(DRM: Digital Rights Management) 및 보호(Access Control, Usage Control, Content Control)가 필요하며, 또한 정보의 공유와 개방을 목표로 개발된 인터넷이 갖고 있는 기본적인 취약성 때문에 전자도서관을 통한 자료의 이용 또는 중계과정에서의 부정한 사용자의 시스템에 대한 불법적인 접근, 거래내용, 금융정보, 혹은 관련 비밀번호, 사용자정보 등의 중요정보들이 쉽게 노출될 수 있기 때문이다(Schneider 1996).

네트워크를 통한 전자거래의 활성화를 저해하는 위협요소들은 시스템과 네트워크에서의 위협 요인들과 밀접한 관계가 있다. 특히, 전자도서관시스템은 기존의 다른 응용시스템과는 보안요구사항의 핵심이 현저히 다르다고 할 수 있다. 즉 전자도서관시스템은 해당 기관의 중요정보자원을 저장 및 관리하고 있으며 또한 네트워크를 통하여 자료가 제공되기 때문에 자료와 시스템자원에 대한 사용자의 접근통제 및 시스템이용에 대한 자료의 관리를 근간으로 하며 또한 사용자 실체에 대한 증명과 전자도서관을 통한 거래 내용에 대한 사후검증이 필요함으로써 이에 대한 보안의 강도가 훨씬 높다고 할 수 있다. 이러한 보안요구사항에 있어서 가장 우선시 되는 요구사항으로서 전자도서관 또는 지식중계시스템과 이용자의 정당성을 검증하는 인증절차는 가장 중요하며 반드시 필요한 부분이라고 할 수 있다.

1.1 연구목적

정보와 지식이 경제적인 가치를 지니게 되므로서 이를 관리하고 유통하는 기관으로서 도서관은 정보와 지식의 유통을 위한 전통적인 관점에 있어서 많은 부분에서 수정되어야 하며, 또한 수정되고 있다. 예를 들어 정보기술분야에서 대표적인 학술단체인 IEEE, ACM과 같은 기관에서는 자체적으로 전자도서관시스템을 구축하여 웹을 통하여 이를 필요로 하는 이용자에게 유료로 제공하고 있으며 도서관분야의 대표적인 단체인 미국전문도서관협회(SLA) 또는 미국도서관협회(ALA)는 홈페이지를 통하여 제공되는 특정서비스의 경우에는 사용자에 대한 인증 후에 자료를 이용할 수 있도록 하고 있다. 또한 대부분의 전문도서관, 기업도서관, 대학도서관 및 일부 공공도서관에서는 전자도서관 시스템을 구축하여 자관자

료를 디지털화하여 이를 정당성이 검증된 사용자에게 네트웍을 통하여 제공하고 있다. 그러나 전통적인 인쇄자료와는 달리 디지털화된 정보나 지식의 유통에 있어서 이에 대한 적절한 통제와 관리는 사회적으로 중요한 과제가 되고 있다. 특히, 정보와 지식을 직접적으로 저장, 관리, 유통 업무를 수행하는 도서관에 있어서는 이러한 디지털콘텐츠에 대한 통제와 보안은 매우 중요한 분야가 되고 있다.

과거와 같이 도서관에서 사서가 직접 개입하여 이용자 및 이용자료에 대한 통제를 할 수 있던 것과는 달리 전자도서관 또는 지식중계시스템을 통한 자료를 제공하거나 중계하는 경우에 있어서 전통적인 통제방법으로서는 불가능하며, 특히 디지털콘텐츠의 유통이 물리적인 방법을 통하여 제공되는 것이 아닌 인터넷과 같은 개방형 네트워크를 통하여 제공되기 때문에 이러한 어려움은 더욱더 크다고 할 수 있다. 따라서, 대부분의 전문도서관 또는 기업체의 도서관의 경우에 있어서 자료에 대한 접근권한을 두어 자료의 중요도에 따라서 네트워크를 통한 사용자의 접근에 대하여 통제하고 있다. 그러나 현재 대부분의 전자도서관에서 접근통제의 수단으로서 사용되고 있는 방법으로서 단순한 사용자인증번호와 비밀번호의 입력을 통하여 이루어지고 있다. 그러나 이와 같은 단순한 접근통제방법으로는 부정한 이용자의 해킹이나 크래킹을 효과적으로 예방할 수 없으며 또한 네트워크를 통한 자료의 전송시 제3자(the third party)에 의한 도청(eavesdropping)이나 자료의 기밀성(confidentiality)을 유지 할 수 없다. 특히, 기존의 구축된 전자도서관시스템이 지식중계소로서 지식을 판매하거나 중계하는 것과 같은 경우에 있어서 위에서 언급된 방법으로서는 예상되는 문제점을 효과적으로 처리할 수 없다. 따라서 인터넷상에서의 디지털콘텐츠의 안전한 유통 및 지불과 함께, 전자도서관이 단순히 디지털자료를 저장하고 관리하는 것이 아닌 디지털콘텐츠의 유통을 위한 중계소로서의 기능을 수행하기 위해서는 인터넷뱅킹시스템(internet banking system)이나 전자지불시스템(electronic payment system) 등의 전자금융시스템에서 요구하는 것과 같은 매우 높은 보안성을 요구된다. 따라서 본 논문에서는 전자도서관에서 네트워크를 통하여 이용자에게 자료를 제공하기 위하여 요구되는 보안요구사항 및 도서관의 새로운 기능으로서 고려될 수 있는 지식중계소로서 역할을 보다 안전하게 수행하기 위하여 요구되는 보안요구사항을 알아보고, 보다 보안성을 높일 수 있는 방법으로서 고려되고 있는 스마트카드를 전자도서관 또는 지식중계시스템에 적용하기 위한 인증메커니즘을 제안하고 이에 대한 평가를 목적으로 하고 있다.

1.2 정보보호의 방법

현재 다양한 멀티미디어 정보를 포함

하고 있는 전자문헌들을 포함한 멀티미디어 자원을 인터넷상에서 우리는 자주 접할 수 있다. 이러한 디지털콘텐츠의 폭발적인 증가와 함께, 이에 대한 정보보호라는 측면이 주요한 관심사로 떠오르고 있다. 특히, 정보와 지식이 중요한 경제적가치로서 평가되고 있는 시점에서 이러한 지식과 정보의 저장소로서 전자 도서관의 중요한 기능을 보다 효율적으로 수행하고 발전시키면서, 또한 정보의 유통 및 공유라는 인터넷의 기본 목적을 충족하기 위한 중요한 요소 중의 하나로서 디지털컨텐츠에 대한 효과적인 보호장치를 갖추어야 한다는 것이다. 만일 이러한 보호장치를 갖추지 못한다면 정보와 지식소유자들은 인터넷을 통한 디지털콘텐츠의 공급과 새로운 미디어를 이용한 콘텐츠의 생산을 꺼리게 될 것이다. 한편, 세계적으로 많은 국가들은 국가기반 정보화사업의 일환으로 각종 정보원들의 디지털화 및 서비스를 적극 추진 중이며 추가 지원하려는 계획을 세우고 있다. 현재 국내에서 진행중인 국회·중앙 도서관의 소장 자료 디지털화가 대표적인 사례라 할 것이다. 디지털콘텐츠의 보호를 위해 적용할 수 있는 방법은 크게 다음 세 가지로 분류할 수 있다.

첫째, 기존의 대칭키 또는 공개키 암호화 알고리즘을 이용하여 주어진 데이터를 암호화하는 방법으로, 정보와 지식을 원래의 데이터로 복구하기 위해서는 관련 키를 알고 있어야 한다. 이 방법은 수학적으로는 안전하나 사람이 개인키로 암호화 된 정보를 배포하는 것을 막을 수 없다는 단점을 가지고 있다. 그리고 단순한 대칭키나 공개키 암호화만으로는 정보보호를 위한 보안 요구사항을 완벽하게 만족하게 할 수는 없다. 이러한 암호키기반의 정보보호 방법은 현재 많은 전자상거래시스템 및 금융시스템에서 구현, 적용되고 있다.

둘째, 디지털콘텐츠 자체에 대한 기밀성(Confidentiality) 또는 불법적인 내용 조작을 막고, 정보나 지식의 소유권을 보장할 수 있는 방법으로 디지털 워터마크(digital watermark)가 있다. 디지털 워터마크는 공개키 알고리즘이나 방화벽 등으로 해독된 영상에 대하여 부가적인 보호를 제공한다. 저작권 정보, 배포자 정보 그리고 사용자 정보를 콘텐츠 자체에 삽입함으로써 법적인 문제가 발생하였을 때 해결책을 제시할 수 있다. 그러나 이러한 워터마킹 방법은 정보보호를 위한 부가적인 방법이며 근본적인 해결방법이 될 수 없으며 또한 여기에는 여전히 많은 연구가 필요한 실정이다.

셋째, 보호대상이 되는 정보나 지식에 대하여 접근제어용 방화벽(firewall) 등을 구축하는 방법으로서, 인터넷과 같은 개방형 네트워크를 통하여 전자도서관과 같은 정보원에 접근하는데 있어서 웹에서 제공되는 서비스중에서 특정한 서비스만을 제공하는 것으로서 파일전송서비스(FTP)와 같은 서비스를 제한하는 것과 함께, 사전에 허가된 사용자에 대한 인증절차를 거쳐 정보와 지식에 대한 사용

을 제한하는 방법이다. 이러한 사용자 접근에 대한 통제방법은 전자도서관에 저장되어 있는 정보원에 대한 불법적인 접근과 데이터의 불법적인 사용을 방지하기 위한 가장 효율적인 방법이라고 할 수 있다.

본 연구에서는 전자도서관에서 자관에 디지털형태로 저장된 데이터의 불법적인 사용과 부정한 사용자에 대한 접근을 통제하거나 또는 인터넷상에서의 디지털콘텐츠의 유통을 보다 안전하게 하기 위하여 사용자 및 매체 인증방식에 대하여 알아보고자 하며 이를 위하여 보안도구로서 고려되고 있는 스마트카드를 접근통제의 매체로서 적용하여 온라인상에서 동시에 다중의 인증요청을 처리하기 위한 다중인증메커니즘을 구현하고 실험하였다.

1.3 연구범위

현재 암호화알고리즘 기반의 전자거래 프로토콜을 이용한 전자거래가 이루어지기 위해서는 통상 고객시스템 즉 고객의 컴퓨터에 설치되는 사용자측 단말프로그램(전자지갑)이 요구된다. 이러한 사용자측 단말프로그램은 다양한 전자거래 프로토콜을 지원함으로써, 사용자의 거래요청을 처리하는데 있어서 효율성을 가능하게 하여준다. 그러나 이러한 보안방법은 모든 보안과 관련된 비밀키와 사용자정보가 고객의 단말기에 저장되므로서 제3자로부터의 해킹이나 크래킹의 약점 및 사용자가 거래를 위하여 반드시 해당 단말을 이용해야 한다는 불편함이 있다. 따라서 이러한 보안상의 취약점 및 사용자 편의성을 을 해결하고 보다 안전한 수단으로서 고려되고 있는 것이 IC카드 즉, 스마트카드가 고려되고 있다. 스마트카드에는 사용자정보, 비밀키, 정보의 안전한 전송을 위한 암호화알고리즘 등이 저장되며 이를 이용하여 네트워크를 통한 온라인거래시 보다 안전한 거래처리가 가능하며 또한 사용자가 휴대할 수 있기 때문에 사용자 편의성이 높다고 할 수 있다. 따라서 본 연구에서는 인터넷과 같은 개방망에서 스마트카드를 기반으로 하는 전자도서관 또는 지식중계소와 같은 디지털콘텐츠 유통시스템에서의 스마트카드와 사용자에 대한 인증을 수행하기 위한 방법으로서 동시에 다중인증을 처리할 수 있는 메커니즘을 제안한다. 이를 위하여 보다 구체적으로 알아보고자 하는 분야는 아래와 같다.

① 스마트카드 및 사용자에 대한 인증 메커니즘
② 다중처리요청에 따른 다중인증처리방법

이러한 목적과 함께, 본 논문은 아래와 같이 구성되어져 있다. 먼저 2장에서는 스마트카드에 대한 개괄과 함께 스마트카드기반의 온라인 거래시스템에서의 인증방법 및 보안요구사항에 대하여 알아보고 3장에서는 제안된 온라인상에서의 스마트카드인증메커니즘의 설계와 구현을 하였으며 4장에서는 구현된 시스템에 대한 실험 및 평가를 하였으며 마지막으로 5장에서는

결론 및 향후 연구과제에 대하여 알아보았다.

2. 스마트카드기반 인증서비스

2.1 스마트카드의 종류

스마트카드를 분류하는데 있어서 일반적으로 마이크로프로세서의 유무 및 외부단말과의 인터페이스 방법에 따라 다음과 같이 구분할 수 있다(ISO 1987, 1988, 1992, 1995).

2.2 스마트카드 기반 인증메커니즘

(1) 보안요구사항

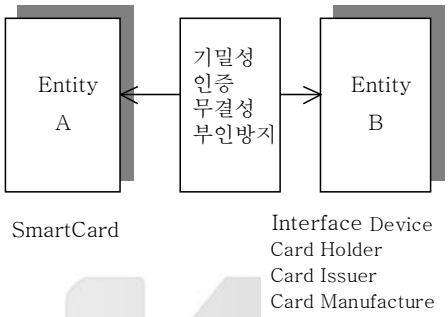
전자지갑서비스를 제공하는 스마트카드는 안전하고 신뢰성 있는 거래를 위하여 아래의 4가지의 보안특성을 만족하여야 하며 이를 위한 보안알고리즘과 보안메커니즘을 수행할 수 있는 능력을 갖추어야 한다(Turban 1998).

스마트카드[엔티티 A]와 외부환경(카드소지자, 외부장치, 스마트카드발급자, 스마트카드제조자, 등)[엔티티 B]와의 통신에 있어 엔티티 A와 엔티티 B사이에는 서로를 인증할 수 있어야 하며 서로간에 전송된 데이터가 타인에게 노출되지 않도록

〈표 1〉 스마트카드의 종류

구 분	종 류	기 능
마이크로프로세서 유무	메모리카드	CPU가 없음 내장기능이 단순하고 가격 저렴하며, 단일응용에 사용
	마이크로프로세서카드	CPU를 가지고 있으며, 읽기/쓰기 기능과 강화된 보안 기능을 제공 상당한 융통성을 가지고 있어서 액세스 제어, 전자화폐, 항공사 좌석표 발매, 신용카드, ID 카드 등 다양한 어플리케이션에 사용
인터페이스방식	접촉식 카드	칩의 동작을 위하여 판독기와의 물리적인 접촉이 필요 .보안을 요구하는 전자화폐 등에 사용
	비접촉식카드	안테나를 통해 판독기와 통신을 하며 내장 배터리로부터 전원을 공급받음
	하이브리드카드	접촉식 및 비접촉식 인터페이스를 둘 다 갖으며 접촉식은 마이크로프로세서 칩 모듈에 의해 사용되며, 비접촉식 인터페이스는 메모리 칩 모듈에 의해 사용. 칩 사이에는 메모리공유가 불가능
	콤비카드	콤비카드는 접촉식 및 비접촉식 표면을 가지고 있지만, 하이브리드카드와는 달리 두 인터페이스가 상호연결됨

암호화되어야 하며 이 암호화된 데이터가 아무런 변조없이 안전하게 상대방에게 전송되어지며 전송된 데이터에 대하여 자신이 전송한 데이터임을 부인할 수 없어야 한다. 이들을 보다 자세히 살펴보면 다음과 같다.



〈그림 1〉 엔티티간의 보안요구사항

1) 기밀성(Confidentiality)

기밀성은 데이터를 소지한 자가 자신의 데이터를 노출시키기를 원하는 사람외에 그 어느 누구도 그 데이터를 알지 못하도록 하는 것을 말한다. 스마트카드에서 외부단말(IFD:Interface Device)사이의 통신에서 상대방에 전송하는 데이터를 평문이 아닌 암호화된 문장을 전송을 하여야 한다. 이때 암호화를 위하여 사용되는 알고리즘은 대칭/비대칭키 알고리즘을 이용하여 행할 수 있다. 여기서, 대칭알고리즘은 수행속도가 빠른 반면에 보안의 정도가 낮으며 비대칭알고리즘은 보안정도는 높으나 수행속도가 스마트카드에서 행하기는 다소 느린 장·단점을 가지고 있다.

2) 인증(Authentication)

인증이란 상대자의 정당성을 확인하고 상대방에게 자신이 정당한 통신상대자임을 인식시킬수 있도록 정당성을 확보하는 것으로서 사용자, 단말, 상점 등의 거래에 관계되는 엔티티에 대한 모든 인증을 포함하고 있다.

□ 사용자 인증

스마트카드 소지자가 정당한 소유자인지를 알기 위하여 개인인증식별번호 (PIN: Personal Identification Number)과 같은 비밀번호를 입력함으로써 스마트카드소지자가 정당한 소유자임을 확인 받을 수 있는 기능이 스마트카드에서 제공되어야 한다.

□ 스마트카드와 외부단말 (Interface device)의 상호인증

외부단말이 자신이 수용하는 스마트카드가 정당한 카드인지를 인증하는 것으로서 카드의 인증을 위하여 스마트카드에게 필요한 정보를 요구하는 형식으로 이루어진다. 이들 상호간의 인증을 위해서 공개키 인증서(예:ITU-T의 X.509)가 분배되며 이때 비대칭키 암호화알고리즘과 해쉬 알고리즘 그리고 전자서명(digital signature)과 같은 보안메커니즘을 통하여 이루어진다. 전자지갑의 경우 동적인증방식을 지원하여야 하며 이를 위하여 다양한 암호화 알고리즘(예:RSA, DES, SHA1등) 및 보안메카니즘(전자서명(Digital Signature), 이중서명(Dual Signature), 전자봉투(Digital

Envelope), 서명값(MAC) 등을 스마트카드에서 지원할 수 있어야 하며 이에 필요한 스마트카드 명령어들이 존재하여야 한다(신진원, 권태경, 송주석 1995). 또한 스마트카드는 자신을 수용하는 외부단말이 과연 적법한지를 인증할 수 있어야 한다. 실제로 스마트카드가 외부단말을 인증하는 경우가 대부분이지만 간혹 불법의 위조된 외부단말이 존재하는 사례도 있다. 위에서 기술된 카드소지자의 인증 그리고 카드와 단말간의 인증 외에도 전자지갑의 용도와 사용목적에 따라 스마트카드발급자, 상점, 인증서발급자 등과의 인증도 이루어져야 한다.

3) 무결성(Integrity)

무결성은 데이터의 내용에 대한 수정이나 변경이 되지 못함을 보장하는 것을 말한다. 만약 스마트 카드로부터 전송된 데이터가 어떤 방해물(전기물리적인 요소나 외부침입자등 외부요인)로 인하여 정보가 변경되었다면 데이터의 무결성이 보장되지 않는 것이다. 이와 같이 송수신된 데이터의 무결성을 보장하기 위해서는 여러 가지의 보안 메커니즘이 있다. 이들은 전자서명, 서명값(MAC)등이 있으며 이런 메커니즘을 위하여 DES, RSA, SHA등의 알고리즘등이 필요하다(Menezes 1997).

4) 부인봉쇄(Non-Repudiation)

부인봉쇄는 전지지갑을 이용하여 구매행위을 할 경우 가장 중요한 보안요구사항이다. 예를 구매자가 상품을 구매하고 전자지갑을 이용하여 지불을 한 뒤 자신의 거래를 부인할 경우, 즉 자신의 스마트카드에서 전송된 거래내역이나 서명 등을 부인할 경우가 있을 수가 있다. 이처럼 부인봉쇄란 송신측이 자신의 정보를 정확하게 상대방에게 전송하였다고 할지라도 수신측이 이를 부인하거나, 수신측이 정확한 정보를 받았음에도 불구하고 송신측이 자신이 보낸 정보를 부인하는 것을 방지하는 것을 말한다. 전자지갑서비스를 제공하여주는 스마트카드는 전자서명과 같은 보안메카니즘을 통하여 부인봉쇄의 기능을 제공할 수 있어야 한다(Rhee 1994).

3. 온라인환경하에서의 제안된 다중인증메커니즘 설계 및 구현

3.1 새로운 인증프로토콜 요구사항

인터넷사용자의 폭발적인 성장과 정보기술의 발전은 전자문서교환(EDI), 인터넷뱅킹(internet banking), 전자상거래(electronic commerce) 등과 같은 새로운 분야의 성장을 가능케 하였다. 이러한 서비스의 활성화를 위한 보안방법으로서 스마트카드에 대한 관심이 더욱 커지고 있는 상황이다. 이러한 관심과 전자서비스 규모의 급격한 증가는 스마트카드를 활용한 새로운 서비스영역을 제공하고 있다(Lee 1998). 그러나 스마트카드를 기반으로 하는

대부분의 서비스들이 현재까지는 오프라인 환경하에서 이루어 지고 있다. 이러한 스마트카드를 기반으로 오프라인환경에서 제공되고 있는 서비스들을 온라인환경으로 적용하기 위해서는 해결해야 할 여러 가지 문제점이 상존하고 있다.

• 네트워크 보안

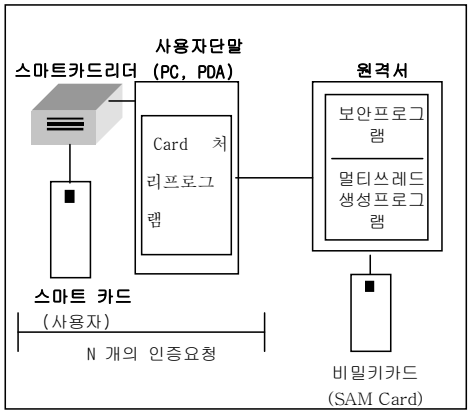
오프라인의 경우, 스마트카드와 외부단말(POS: Point of Sales)과는 직접적인 통신을 통한 인증작업이 이루어지고 있기 때문에 네트워크상에서 발생할 수 있는 보안적인 위협요소가 적다고 할 수 있으나 온라인환경에서는 네트워크상의 보안적인 측면을 고려하여야 하며 (최용락 외 1996) 특히 거래를 위한 사용자 및 스마트카드자체에 대한 인증방법에 있어서 스마트카드소지자에 대한 사용자인증과 함께 스마트카드 자체의 정당성을 검증하기 위한 방법이 제공되어야 한다.

• 동시다중인증처리

오프라인 환경하에서 스마트카드를 이용한 서비스를 위하여 사용자 및 스마트카드에 대한 인증처리를 하는 경우 각각의 인증처리가 순차적(sequential)으로 수행이 된다. 즉 인증요청이 있는 경우 스마트카드에 대한 인증처리를 하기 위해서는 비밀키카드(SAM card)로부터 비밀키를 읽어와서 이를 통하여 스마트카드에 대한 인증을 하여야 하는데 외부단말기(예: EFT-POS)는 단지 하나의 비밀키카드만을 수용하기 때문에 다음의 인증작업을 처리 하기 위해서는 해당 인증작업이 완료되어야 다음의 인증요청을 처리할 수 있다. 그러나 온라인의 경우 전자도서관이나 디지털콘텐츠 판매사이트에 동시에 접속한 사용자가 스마트카드를 가지고 디지털콘텐츠에 대한 지불처리를 원하는 경우, 원격서버에서는 동시에 다중인증(multi-authentication)이 이루어져야 한다.

3.2 구현환경

〈그림 2〉는 스마트 카드의 인증 및 암호화 통신을 구현하기 위한 전체 구성도로서, 전체 시스템의 구성은 다음과 같다. 먼저, 원격 서버에서의 스마트 카드 인증 및 상호간의 암호화 통신을 위하여 인증관련 키와 암호화 알고리즘을 가지는 스마트 카드, 스마트 카드리더, 사용자측 단말로서 PC, 휴대전화, PDA는 서비스를 위한 각종 응용프로그램, 스마트카드리더



〈그림 2〉 스마트카드기반 인증체계구성

를 제어프로그램, 스마트카드처리프로그램(e-purse)을 포함 하고 있으며, 스마트카드 기반의 서비스를 제공하기 위해 서비스 제공자가 운영하는 원격서버에는 스마트카드의 인증 및 데이터의 암호화를 수행하는 보안프로그램과 다중인증처리를 동시에 수행할 수 있도록 쓰레드를 생성하는 멀티쓰레드 생성프로그램이 포함되어 있으며 마스터키를 저장하고 있는 비밀키카드로 구성된다.

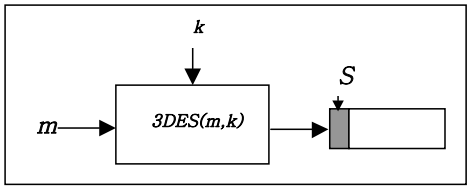
(1) 암호화 알고리즘

시스템의 효율성, 구현의 용이성 및 보안성을 위하여 대칭키알고리즘을 적용하였으며 이를 위하여 DES 알고리즘을 개선한 3-DES알고리즘을 채택하였으며 키 적용에 있어서 *K1≠K2, K1=K3* 방식을 적용하였다(ANSI 1999).

(2) 서명생성 및 검증방법

- 서명(Signature)값의 생성

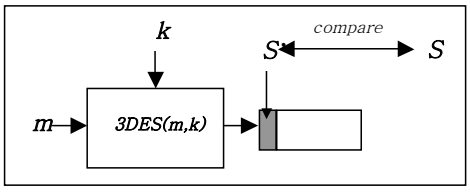
① 3DES함수를 수행한다.
② 생성된 암호문중 상위 4바이트(32bits)를 서명(S) 값으로 취한다.
③ 서명(S) = Sign(m,k) = 3DES(m,k)



〈그림 3〉 서명 생성(Sign Generation)

- 서명(Signature)값의 검증

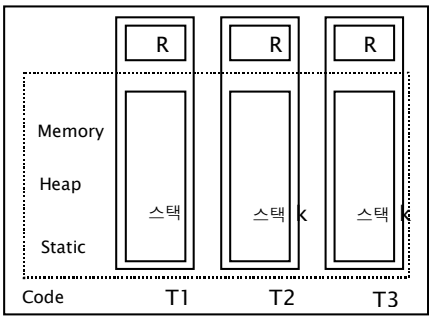
① 서명(S') = 3DES(m, k)(S'값을 생성)
② 검증 (S') = Compare(S, S')(생성된 S'과 S를 비교하여 검증한다)



〈그림 4〉 서명 검증(Sign Verification)

3) 다중인증처리 방법

인터넷과 같은 개방망에서 동시에 요청되는 다중의 인증작업과 같은 동시작업이 필수적인 시스템에서 하나의 프로세스에 대해 다중의 쓰레드를 생성하여 개별 작업들을 처리하는 것은 매우 효과적이라고 할 수 있다. 이를 통하여 시스템의 효율성과 속도면에서 상당히 많은 장점을 가져올 수 있다. 본 연구에서는 동시에 다중의 인증작업을 수행하기 위하여 멀티쓰레드를 이용한 다중인증메커니즘을 적용하여 구현하였다. 멀티쓰레드를 이용한 다중인증처리방법은 먼저 시스템의 성능(처리량, 계산속도, 응답속도)을 향상시킬 수 있으며 동시에 여러 쓰레드가 작업을 수행할 수 있기에 멀티프로세서 시스템에서 최대한의 효과을 얻을 수 있으며 싱글프로세서 시스템에서의 느린 작업(Disk I/O, 계산 수행)을 겹쳐 수행할 수 있어 다른 프로세스을 생성시키는 것보다 뛰어난 성능을 보여줄 수 있다(Prasad 1997).



〈그림 5〉 멀티쓰레드의 구조

다음의 〈그림 5〉는 멀티쓰레드의 구조를 보여주고 있다.

3.3 온라인환경하에서의 스마트 카드 기반의 다중인증프로토콜

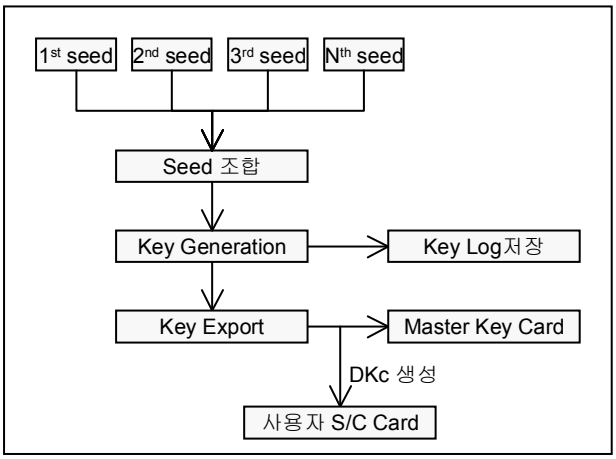
온라인환경하에서의 스마트카드기반의 서비스를 제공을 위한 동시 다중인증처리를 수행하기 위하여 스마트카드 소지자가 스마트카드를 스마트카드 리더에 삽입하여 사용자의 개인인증번호를 입력하여 사용자를 확인하는 제 1단계와, 온라인상에서의 스마트 카드와 원격서버가 직접 통신하여 상호인증하는 2단계로 구분할 수 있으며 두번째 단계에서는 데이터의 서명값(MAC)을 생성하기 위한 각 세션별 세션키를 생성하는 과정을 포함 한다. 〈표 2〉는 스마트카드와 원격서버에 저장되는 각각의 비밀키와 본 연구에서 사용되는 요소들에 대한 표기들을 보여주고 있다.

〈표 2〉 사용된 표기

기 호	설 명
PIN	사용자 비밀번호
DKc	카드 파생키(16byte)
RNG( )	난수 생성 알고리즘
E( )	대칭키 암호화 알고리즘
D( )	대칭키 복호화 알고리즘
Sek	세션키(16byte)
MAC	서명값(4byte)
MKs	원격서버 마스터키(16byte)
Pthread( )	멀티쓰레드 생성 알고리즘
RNs	생성난수(원격서버: 8byte)
RNc	생성난수(: 8byte)
Seed1	거래일련번호(8byte)
Seed2	카드발급자 ID (8byte)
Seed3	카드제조번호 (8byte)
Seed4	사용자 ID (8byte)

(1) 제안메커니즘의 인증개념

온라인환경에서의 스마트카드에 대한 인증에 있어서 네트워크상에서 서비스요청의 특성상 순차적인 지불처리가 아닌 동시에 다중의 인증처리를 수행하기 위해서는 원격서버측에서는 다중처리를 동시에 수행할 수 있는 다중인증프로그램이 요구되며 이를 통하여 요청된 인증을 처리할 수 있는 쓰레드 또는 하위프로세서가 생성되므로서 해당 요청을 처리하여야 한다. 본 논문에서 제안하는 스마트카드 기반의 동시다중인증시스템은 오프라인에서의 순차적인 인증방법 또는 온라인상에서의 하드웨어적으로 구현된 방식과는 달리 동시에 다중의 인증처리를 수행하기 위하여 네트워크상의 높은 보안성과 함께 멀티쓰레드(multi-thread)방식을 통하여 소프트웨어적으로 구현된 메커니즘을 제안하고 있다.



〈그림 6〉 비밀키생성 과정

(2) 제안된 인증메커니즘

제안된 인증개념을 통하여 스마트카드, 사용자측 단말프로그램과 원격서버사이의 인증처리 절차는 아래와 같다. 먼저 스마트카드사용자에 대한 정당성을 인증한 후 정당성이 인증된 경우 스마트카드자체에 대한 인증이 이루어진다. 이러한 인증과정에서 요구되는 각각의 비밀키의 생성과 분배는 중앙서버에서 수행되며 〈그림 6〉은 각 단계별로 사용되는 마스터키와 파생키의 생성과정을 보여주고 있다.

원격서버의 비밀키카드(SAM card: Secure Application Module Card)에 저장되는 마스터키의 생성은 보안성을 높이기 위하여 시스템에서 임의로 생성된 값이 아닌 3명의 사람이 직접 초기값(seed value)을 입력하는 방식을 적용하였으며 사용자의 스마트카드에 저장되는 파생키는 생성된 마스터키, 발급자 ID 및 카드자체의 제조번호를 암호화하여 생성한다.

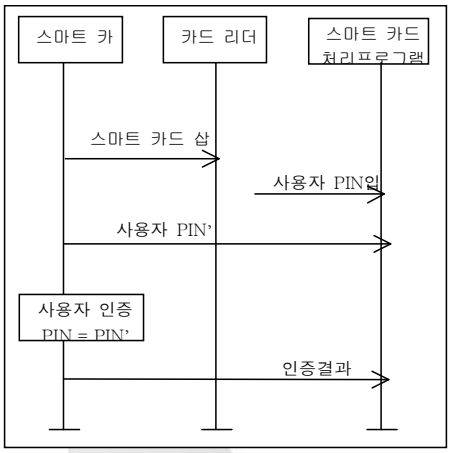
MKs = E(Seed 1||Seed2||seed3)
DKc = E(발급자 ID||카드제조번호, MKs)

각각의 초기입력값을 통하여 마스터키(MKs)와 파생키(DKc)를 생성하기위한 암호화알고리즘에는 3-DES를 적용되었으며 생성된 마스터키(MKs)는 원격서버측의 비밀키카드(SAM card)에 저장되어 관리되며 파생키(DKc)는 사용자 스마트카드에 저장되어 배포된다.

1) 스마트카드 사용자인증

스마트카드사용자에 대한 정당성을 인증하는 방법에는 다양한 방법들이 사용될 수 있다. 예를 들어 개인인증번호(PIN: Personal Identification Number)와 같은 식별번호로서 인증하는 방법과 눈동자의 홍채인식이나 지문인식과 같은 생체인식시스템(Biometrics)와 같은 방법들이 있다고 할 수 있다(박창섭 1999). 현재 가장 일반적

으로 사용되고 있는 방법은 개인인증번호를 이용하는 것으로서 본 연구에서 제안하고 있는 방법의 구현의 용이성과 보안성을 동시에 만족할 수 있는 개인인증번호방식을 적용하였다.



〈그림 7〉 스마트카드 사용자인증 처리도

〈그림 7〉에서 사용자는 스마트 카드를 스마트 카드리더에 삽입한 후 사용자의 개인인증번호를 입력하여 사용자에 대한 인증을 처리하는 과정을 보여주고 있으며 이를 구체적으로 알아보면 아래와 같다.

① 사용자가 스마트 카드를 스마트카드리더와 같은 외부단말에 삽입하여 스마트카드를 인식한다

② 사용자가 스마트 카드 처리프로그램에 입력장치를 통하여 사용자의 개인인증번호를 입력한다.

③ 입력된 사용자의 개인인증번호를 스마트 카드 처리프로그램이 스마트 카드로 전송한다.

④ 스마트카드는 전송받은 개인인증번호와 스마트 카드에 저장된 개인인증번호와 비교하여 일치여부를 확인한다. 일치하면 사용자가 정당함을 인증하고 그렇지 않으면 부정한 사용자임을 확인한다.

⑤ 비교한 결과를 스마트카드 처리프로그램으로 전송한다.

2) 스마트카드인증 프로토콜

스마트카드사용자에 대한 인증이 이루어진후 스마트카드에 대한 다중인증절차를 수행하기 위하여 본 논문에서는 시스템자원의 효과적인 분배와 활용을 위하여 멀티쓰레드기법을 이용하여 다중처리를 수행하였으며 시스템의 효율성과 키관리의 용이성을 위하여 대칭키(Symmetric) 기반의 암호화알고리즘을 적용하였다.

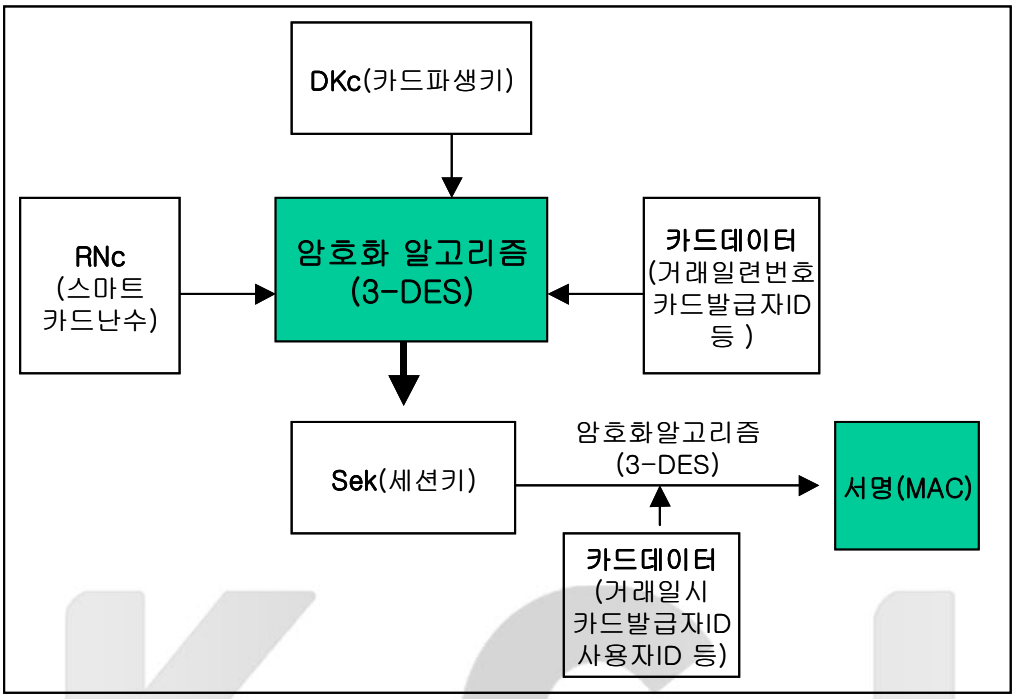
Step 1 - 멀티쓰레드 생성과정

① 동시 다중인증작업을 처리하기 위하여 특정 이벤트(인증요청)이 발생하면 원격서버측의 멀티쓰레드생성프로그램이 구동된다.

② 멀티쓰레드생성프로그램이 구동되면서 원격서버측의 비밀키카드(SAM card)로부터 마스터키(MKs)를 읽어서 이를 RAM에 상주시킨다.

③ 이러한 과정이 끝나면 요구되는 작업에 따라 pthread_create() 함수를 통하여 쓰레드가 생성된다.

④ 생성된 쓰레드는 개별 인증작업을 수



〈그림 8〉 스마트카드에서 서명생성과정

행한다.

위와 같은 과정을 통하여 다중요청을 처리하기 위한 쓰레드가 생성된 후, 각 인증요청에 대한 처리과정은 아래의 과정을 통하여 이루어진다.

Step 2 - 스마트카드는 원격서버와의 통신 채널을 생성하기 위하여 메시지 전송

Step 3 - 스마트카드에서의 1차 서명(MAC) 생성과정

① 스마트카드에서 난수생성알고리즘(RNG ( ))을 통하여 난수 RNc을 생성한다.

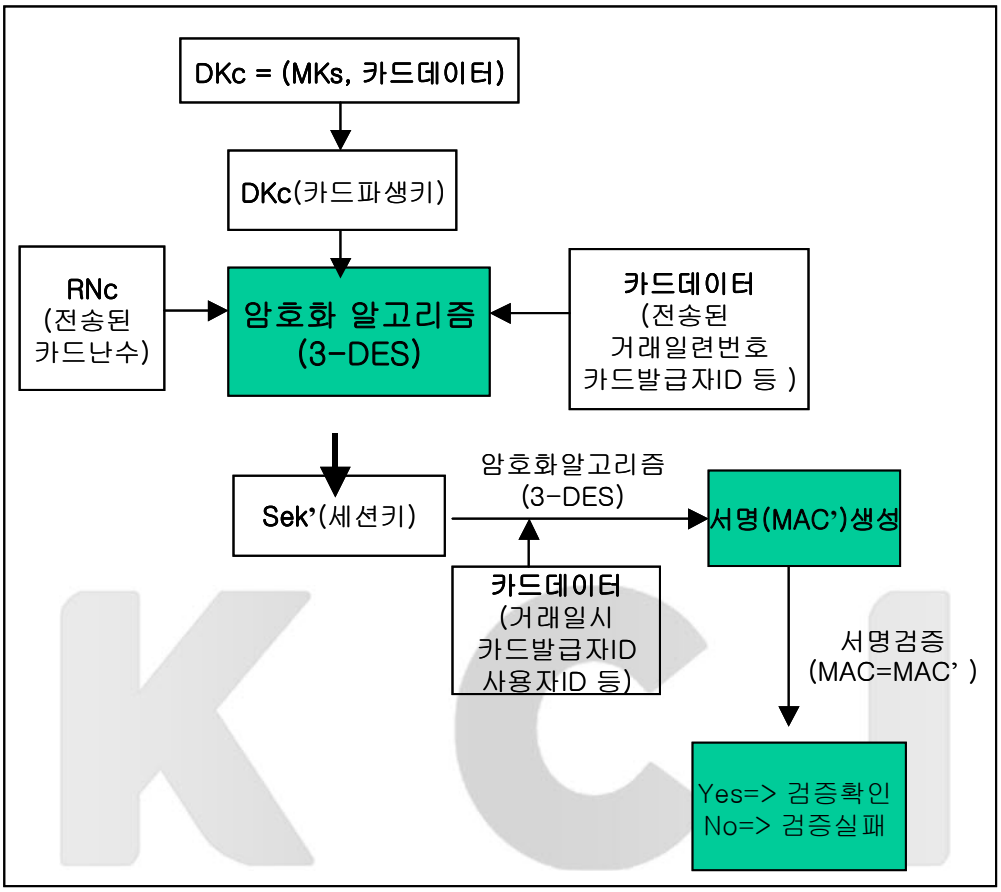
② 생성된 RNc을 통하여 세션키(Sek)를 생성한다.

$Sek = E(RNc \parallel seed1), DKc)$

③ 생성된 세션키(Sek)를 3-DES알고리즘을 통하여 생성된진 결과값에서 상위 4byte를 서명(MAC)으로 취한다.

$MAC = E(seed2 \parallel seed3 \parallel seed4, Sek)$

Step 4 - 생성된 서명(MAC), RNc, 그리고 원격서버에서의 인증요청된 각각의 스마트카드의 파생키(DKc)를 생성하기 위한 카드데이터가 동시에 원격서버로 전송된다.



〈그림 9〉 스마트카드서명 검증

Step 5 - 스마트카드 검증과정

① 전송된 카드데이터를 통하여 카드파생키인 DKc를 생성한다.

$DKc = E(seed1||seed2, MKs)$.

② 생성된 파생키(DKc)를 통하여 세션키(Sek')를 생성한다.

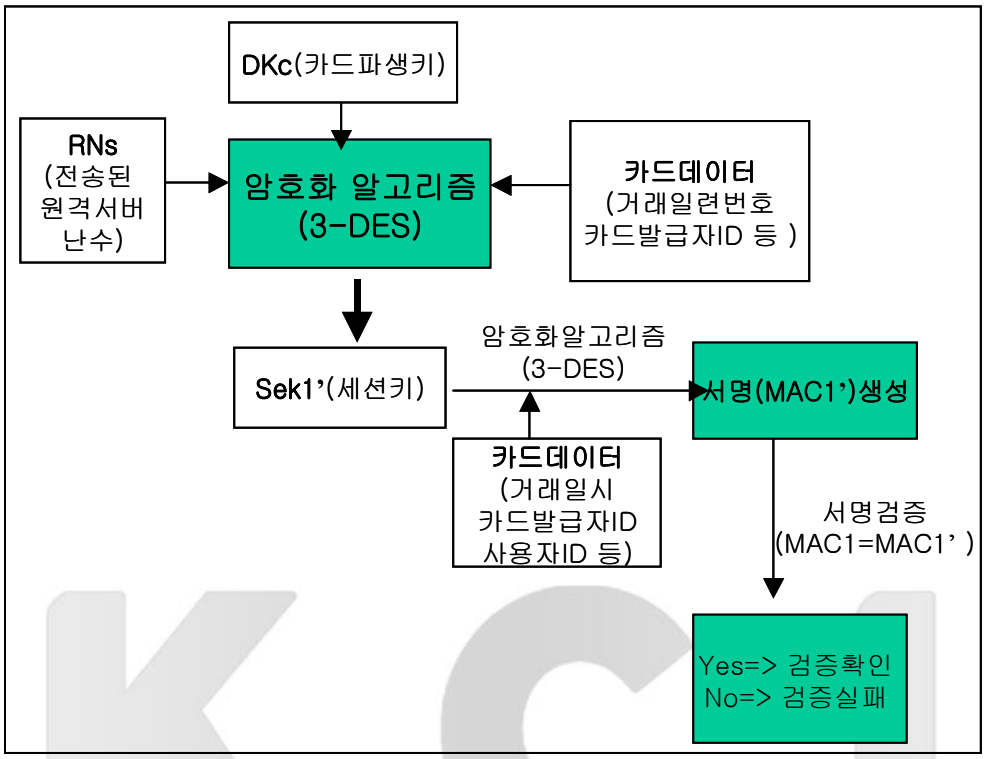
$Sek' = E(RNc||seed1, DKc)$

③ 생성된 세션키(Sek')를 3-DES알고리즘을 통하여 생성된 결과값에서 상위 4byte를 서명(MAC')으로 취한다. 이를 전송된 서명(MAC)과 비교하여 같은 경우 카드에 대한 인증이 이루어지며 일치하지 않는 경우 인증실패메세지를 전송한다.

$MAC' = E(seed2||seed3||seed4, Sek')$

$compare\ MAC = MAC'$

Step 6 - 원격서버에 대한 상호인증을



〈그림 10〉 원격서버서명 검증

위하여 2차 서명생성과정

① 원격서버에서 난수생성프로그램 (RNG())을 통하여 1차 생성된 난수(tempRNs)의 상위 8byte는 2차 난수(RNs)생성을 위한 seed로서 사용되며 하위 8byte는 키로서 사용한다.

② 생성된 RNs을 통하여 세션키(Sek 1)를 생성한다.

Sek 1 = E(RNs||seed1, DKc)

③ 생성된 세션키(Sek 1)를 통하여 서명 MAC 1를 생성한다.

MAC 1 = E(seed2||seed3||seed4, Sek 1)

Step 7 - 생성된 2차 서명(MAC 1), 서버난수(RNs), 카드데이터를 스마트카드로 전송한다.

Step 8 - 스마트카드에서의 원격서버 인증

① 전송된 RNs을 통하여 세션키 Sek 1'을 생성한다.

Sek 1' = E(RNs || seed1, DKc)

② 생성된 세션키 Sek 1'를 통하여 서명 MAC 1'을 생성한다.

MAC 1' = E(seed2||seed3||seed4, Sek1')

③ 카드에서 새로이 생성된 MAC 1' 과 원격서버로부터 전송된 MAC 1을 비교하여 같으면 인증이 완료되며 다른 경우 인증실패라는 메시지를 전송한다.

MAC 1 = MAC 1'

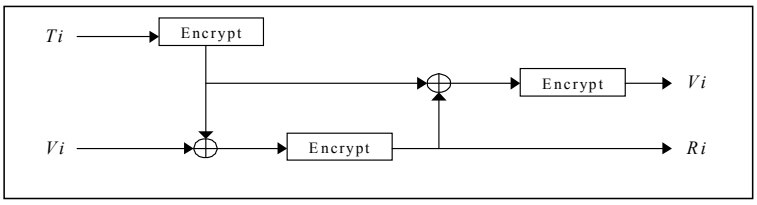
위의 단계가 완료된후 각각의 개별적인 거래가 이루어 지며 모든 거래의 전단계로서 스마트카드에 대한 인증작업이 선행된다.

4. 다중인증 프로토콜 실험 및 평가

4.1 난수생성알고리즘

사용데이터의 유일성을 확보하기 위한 방법으로서 일반적으로 난수(Random number)를 생성하여 이를 기본값으로 많은 응용서비스에서 사용되고 있다. 난수의 생성은 암호시스템(Cryptographic system)에 있어서는 중요한 요소이다. DES, RC2 그리고 RC5와 같은 대칭형 암호화알고리즘(Symmetric Encryption Algorithm)은 무작위로 생성된 난수(Random number)를 필요로 하며 RSA, Diffie-Hellman, 그리고 DSA와 같은 비대칭형 암호화 알고리즘(Asymmetric Encryption Algorithm)도 소수를 생성할 때 무작위로 생성된 값을 가지고 암호화를 수행한다. 뿐만 아니라 SSL이나 기타 암호화 프로토콜에서도 인증(Authentication)과정에서도 난수가 사용된이다. 따라서 난수는 전체적인 시스템의 보안성을 결정하는 중요한 부분이다. 따라서 난수를 생성하는데 있어서 일반적으로 요구되는 사항으로서 1)생성이 용이하여야 하며, 2)뛰어난 난수성(Randomness)을 가져야 하며, 3)구현이 간편해야 하고, 4)긴 주기를 지녀야 한다. 이러한 기준을 가지고 기존의 난수생성알고리즘을 분석하여 보았을 때 LFSR과 3-DES 난수발생알고리즘이 통계적 특성에서 뛰어나지만 LFSR로 생성된 난수열은 2n 개의 연속된 비트를 조사하여 LFSR의 주기인 2 비트 전체를 알 수 있으므로 난수 생성에 사용하기는 부적합하다. 따라서 3-DES 난수 발생알고리즘과 같은 암호알고리즘을 이용하여 주기성을 갖지 않고, 통계적 특성이 좋은 난수를 발생시키는 방법을 사용하는 것이 난수생성시 가장 적합하다(Matthews 1995). 따라서 본 논문에서는 이러한 난수에서 요구되는 요구사항들과 함께, 본 논문에서는 ANSI X9.17에서 정의하고 있는 난수발생방법을 적용하였으며 이 알고리즘은 암호화 모듈로서 3-DES를 사용하며 그 구성요소는 다음과 같다.

- 입력 : 두개의 초기값이 생성기를 구동한다. 하나는 현재의 날짜와 시간을 나타내는 8byte값으로 시스템으로부터 입력되며 난수 생성시 갱신된다. 다른 하나는 임의의 값으로 초기화되는데 본 논문에서는 카드에 저



〈그림 11〉 ANSI X9.17 난수생성알고리즘

장되는 사용자의 사용자 데이터를 초기값으로 설정한다.

- 키 : 암호화알고리즘으로서 3-DES 모듈을 사용하며 키크기는 128bit이다.
- 출력 : 출력은 64비트 난수와 64 비트의 seed 값으로 구성된다.

임의 키(Random Key) Ri의 생성과 Vi+1은 다음과 같다.

$Ri = E_K(E_K(T_i) \| V_i)$,----------Ⓐ
$V_{i+1} = E_K(E_K(T_i) \| R_i)$,---------Ⓑ
$E_K(X)$: *3DES Algorithm*,
V_0: *Secret 64-bit seed*
T_i: *TimeStamp*,
R_i: *Random Key*

4.2 서명검증실험

서명은 본 연구에서 스마트카드와 원격서버와의 상호인증을 위하여 적용되는 궁극적인 인증요소로서 먼저 스마트카드사용자에 대한 인증을 위하여 사용자가 직접 입력하는 개인식별번호를 통한 사용자 인증단계와 스마트카드와 원격서버와의 상호인증을 위한 서명 생성 단계에서의 각 단계별 실험을 수행하였다.

1) 원격서버의 인증데이터 요청을 통하여 스마트카드에서 사용되는 정보와 함께 이를 통하여 생성되는 세션키(Sek), 서명(MAC)는 다음과 같다.

초기값	*0, 0, 0, 0, 0, 0, 0, 0*
RNc	*00, 43, ff, 23, 79, 59, 43, aa*
DKc	*6a, 7b, 34, a1, 38, ae, 6b, 73, f4, 34, e4, a9, aa, cf, 89, c7*
Sek	*85, 84, 4D, 1D, BB, CC, 84, 4C, 8B, 7D, 57, ED, 33, 42, F5, 0F*
Seed1	*30, 30, 30, 30, 30, 34, 33, 32*
Seed2	*30, 34, 32, 31, 36, 32, 37, 33*
Seed3	*73, 6b, 33, 32, 31, 36, 32, 34*
Seed4	*6b, 79, 39, 30, 01, 34, 38, 33*
MAC	*89, 05, FD, A3*

2) 스마트카드에서 생성된 정보는 사용자측 단말프로그램(전자지갑)에서의 암호화 과정을 통하여 원격서버로 전송되며 이때 전송되는 정보는 RNc, MAC, seed 1,2,3,4 이다.
3) 스마트카드로부터 전송된 정보와 함께, 원격서버에서는 스마트카드에 대한 인증을 수행하기 위하여 자체서명(MAC)을 생성하며 생성되는 정보

는 다음과 같다.

MKs	*17, D7, 94, A2, 10, 60, E0, DE, 55, E1, 33, E8, 4E, 1D, 74, 90*
DKc'	*6a, 7b, 34, a1, 38, ae, 6b, 73, f4, 34, e4, a9, aa, cf, 89, c7*
Sek'	*85, 84, 4D, 1D, BB, CC, 84, 4C 8B, 7D, 57, ED, 33, 42, F5, 0F*
MAC'	*89, 05, FD, A3*

4) 스마트카드에 대한 인증후 원격서버에 대한 스마트카드의 상호인증을 위하여 원격서버에서는 자신의 서명(MAC1)을 생성하며 이때 사용되는 정보와 생성되는은 서명은 다음과 같다. 생성된 정보(RNs, MAC 1)는 인증을 위하여 스마트카드로 전송한다.

RNs	*c9, 4d, 3c, 5e, 30, 4a, a1, d4, c9 4d, 3c, 5e, 30, 4a, a1, d4*
Sek1	*9C, DC, 17, 85, C1, 99, 4C, A1 89, C9, 7F, B1, 42, 33, CA, FD*
MAC1'	*8D, 89, 1A, 17*

5) 원격서버로부터 전송된 정보와 함께, 스마트카드에서는 원격서버를 인증하기 위한 자체서명(MAC 1')을 생성하며 이때 사용되는 정보와 생성되는 서명(MAC 1')는 다음과 같다.

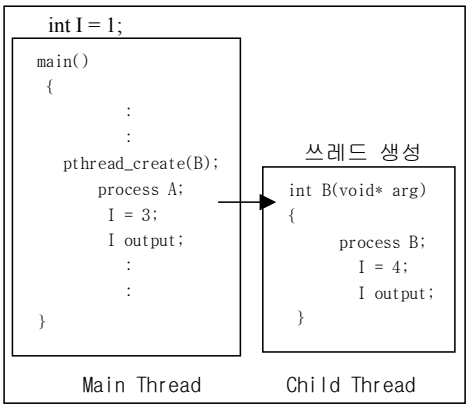
Sek1'	*9C, DC, 17, 85, C1, 99, 4C, A1, 89, C9, 7F, B1, 42, 33, CA, FD*
MAC 1'	*8D, 89, 1A, 17*

6) 원격서버로부터 전송된 서명(MAC 1)과 스마트카드에서 생성된 서명(MAC 1')를 비교하여 상호인증을 완료한다.

compare MAC 1 = MAC 1'

4.3 멀티쓰레드생성

오프라인상에서의 스마트카드에 대한 인증시 수행되는 순차적인(sequential) 방법이 아닌 동시 다중인증방식을 적용하는데 있어서 시스템의 효율성을 구현하기 위하여 멀티프로세스방식이 아닌 멀티쓰레드(multi-thread)방식을 적용하였으며 쓰레드 라이브러리로는 가장 널리 쓰이는 POSIX(Portable Operating System Interface)의 pthread()함수를 사용하여 인증요청이 들어오면 pthread_create()를 통하여 쓰레드를 생성시켜주는 방식을 사용하였다.



〈그림 12〉 하위쓰레드 생성

4.4 상호검증연산시간

T(time): t1 + t2 + t3 = 130ms + 1.9ms + 10.1ms = 142 ms

T1 : 스마트카드에서의 원격서버 인증시간(smart card authentication time)

Card : RNG() ×1, E(m) ×2, D(m) ×2

10ms + 30ms × 2 + 30ms × 2 = 130 ms(m=8 bytes)

t2 : 원격서버에서의 스마트카드 인증시간 (server authentication time)

Server : RNG() ×1, E(m) ×3 D(m) ×2

0.1ms + 0.36ms × 3 + 0.36 × 2 = 1.9 ms(m=8 bytes)

t3 : 난수생성 시간 (random number generation time)

User card: 10 ms

Server: 0.1 ms

〈표 3〉 3-DES Computation Time

	Smart	Server
H/W	5㎒	PⅢ 500㎒
Key Size	196 bits	196 bits
Date Size	64 bits	64 bits
Encryption time	30ms	0.36ms
Decryption time	30ms	0.36ms

4.5 평 가

본 연구에서 제안된 동시다중인증시스템을 평가하는데 있어서 가장 우선시 고려되어야 하는 것은 시스템의 효율성 및 보안성이다.

(1) 효율성

본 시스템은 오프라인 환경의 스마트카드방식 및 온라인상에서 부분적으로 사용되고 있는 다중비밀키카드(multi-SAM card)방식과의 비교를 통하여 시스템의 효율성 측면에 있어서 다음과 같은 장점을 가지고 있다고 할 수 있다.

- 멀티쓰레드 방식을 통한 인증처리를 수행하므로서 시스템에 대한 부하를 줄일 수 있다.
- 카드를 통하여 요청된 모든 서비스를 동시에 처리할 수 있다.
- 모든 서비스에 대한 거래내역을 DB에 저장이 가능하다. 따라서 구매취소 등의 서비스가 요청되는 경우 즉각적인 처리가 가능하다. 즉, 모든 거래에 대한 추적이 용이하다.
- 보안알고리즘을 변경하는 경우 해당 알고리즘에 대한 모듈만을 변경하기 때문에 새로운 카드를 생산할 필요성이 없다. 즉 시스템의 보안정책을 수립하는데 있어서 용이하다.
- 개방형네트웍 즉, 인터넷상에서의 구현이 용이하다.

(2) 보안성

스마트카드기반의 전자지불시스템에서 상품구매, 인터넷뱅킹, 사용자인증 등에서 사용되어질 수 있는 비밀키등이 스마트카드에 직접 저장하여 분배하고 관리되므로서 키관리 및 키분배에 있어서 보안단계를 높였다고 할 수 있으며 스마트

카드에 대한 인증과 함께 스마트카드를 수용하고 있는 원격서버에 대한 검증을 통하여 상호인증이 이루어진다. 즉 부정한 단말 또는 스마트 카드 처리 프로그램일 경우 서비스를 제공하는 서버 운용자는 스마트 카드의 정당성을 확인할 방법이 없으며, 스마트 카드와 스마트 카드 처리프로그램의 평문 통신으로 인하여 데이터의 기밀성을 확보할 수 없다. 본 연구에서는 부정한 단말 또는 스마트 카드 처리 프로그램이 부정한 스마트 카드를 수용할지라도 원격측의 서비스 운용자의 서버가 직접 카드와 온라인으로 직접 통신하여 단말 및 스마트 카드 처리 프로그램의 개입 없이 스마트 카드의 정당성을 인증하고 스마트 카드와 서버 사이의 데이터 기밀성을 해결할 수 있다. 또한 인증에 있어서 단말에 대한 단순한 인증체계가 아닌 스마트카드사용자에 대한 1차 검증을 수행한 후 인증이 이루어진 사용자가 사용하기를 원하는 스마트카드에 대한 인증이 2차적으로 수행되며 이때 스마트카드에 대한 인증과 함께 원격서버에 대한 인증이 동시에 수행되므로서 다단계 인증을 통하여 높은 보안성을 실현할 수 있다

5. 결 론

본 연구에서 제안하고 있는 온라인환경상에서의 스마트카드기반의 다중인증메커니즘은 현재 오프라인에서 주로 사용되고 있는 편의성과 보안성이 검증된 스마트카드를 온라인에 적용하는데 있어서 가장 중요한 요소로서 고려되고 있는 사용자 및 스마트카드에 대한 인증처리를 수행하기 위한 메커니즘으로서 이를 통하여 개방망에서의 보안문제를 해결하고 온라인상에서의 스마트카드를 이용한 사용자 인증서비스에 있어서의 동시다중인증을 위한 제한점과 함께, 기존의 온라인상에서의 다중인증을 처리하기 위하여 오프라인상의 문제점을 부분적으로 해결하고 있는 다중비밀키카드(multi-SAM card) 방식에서의 제한점을 해결하기 위하여 멀티쓰레딩기법을 활용하여 소프트웨어적으로 문제점을 해결하였다. 이를 위하여 스마트카드 사용자와 스마트카드 자체에 대한 인증을 위하여 인증메커니즘을 설계하고 이를 구현하였으며 각 인증 단계별로 사용되는 비밀키의 생성을 위하여 기존의 복잡하고 구현이 힘든 키생성메커니즘이 아닌 구현이 용이한 키생성 및 인증메커니즘을 제안하였다. 본 논문에서 제안한 동시다중인증메커니즘의 보안성을 강화하기 위하여 DES/ 3DES를 지원하는 저비용, 저 성능의 스마트카드 기반으로 전자지불시스템에서의 인증메커니즘을 구현하였으나, 향후에는 개방형 카드 플랫폼(Open Card Platform)인 자바카드(Java Card)(Java Card Technology 2001)를 채택한 인증시스템에 대한 연구가 요구된다

참고 문헌

박창섭. 『암호이론과 보안』. 서울:대영사. 1999.

신진원, 권태경, 송주석. 1995. 스마트카드 시스템의 보안기능 분석 및 설계에 관한 고찰, 『한국통신정보보호학회 종합학술발표회 논문집』. 5(1) : pp. 265~274.

최용락, 소우영, 이재광, 이임영. 1996. 『통신망정보보호(Network and internetwork security principles and practice)』. 서울:도서출판 그린.

ANSI. 1999. *Data Encryption Standard (DES/3DES)*. FIPS PUB 46-3. http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf

ISO. 1987, *Identification cards-Integrated circuit(s) cards with contacts - Part 1:Physical characteristics*, ISO. 7816-1.

ISO. 1987, *Identification cards-Integrated circuit(s) cards with contacts - Part 2:Dimension and location of contacts*, ISO 7816-3.

ISO. 1988. 7816-3, *Identification cards-Integrated circuit(s) cards with contacts - Part 3:Electronic signals and transmission protocol*, ISO 7816-3.

ISO. 1992, *Identification cards-Integrated circuit(s) cards with contacts - Part 3, Amendment 1: Protocol type T=1, Asynchronous half duplex block transmission protocol*, ISO 7816-3.

ISO. 1995, *Identification cards-Integrated circuit(s) cards with contacts - Part 4:Inter-industry commands for interchange*, ISO 7816-4.

"Java Card Technology". 2001. [cited 2001. 11. 23]. http://java.sun.com/products/javacard

Kimberley, M. 1997. "Comparison of two statistical tests for keystream sequences. "Electronic Letter, 23(8) : pp. 365~366.

Lee, Hyung-Woo and Tai-Yun Kim, 1998. "Smart card based off-line micropayment framework using mutual authentication scheme". *Proceedings of the Global Tele-communications Conference*, 4: p. 2514~2519.

Matthews, Tim, 1995. *Suggestions for random number generation in software*, An RSA data security engineering report,

Menezes, Alfred J., Paul C.Van Oorschot, and Scott A. Vanstone. 1997. *Handbook of applied cryptography.*

Boca Raton, FL:CRC Press.

Prasad, Shashi, 1997. *Multithreading programming techniques*. New York: McGraw-Hill.

Rhee, Man Young. 1994. *Cryptography and Secure Communications*, New York:McGraw-Hill.

Schneider, Bruce. 1996, *Applied Cryptography*, 2nd ed, London:John Wiley & Sons.

Turban, Efraim and Debbie McElroy. 1998. "Using smart cards in electronic commerce." *IEEE proceedings 31st Annual International Conference on System Science*, pp. 62~69.