通信情報保護學會學會誌
第 9 券 第 4 號, 1999. 12

전자화폐 시스템 보안기능 연구

송유진*, 오형근**, 이임영**

요 약

본 논문은 전자화폐 시스템을 구현하기 위한 프로토콜들의 표준과 전자화폐 안전성을 위한 정보보호 기능 표준을 제시하여 향후 국제적인 전자상거래에 대비하여 상호호환성 있는 전자화폐 시스템 구현의 기반을 제공하고자 한다.

본 논문에서 제시하는 전자화폐 프로토콜들과 관련 보안기술들은 전자화폐 시스템 구현에 직·간접적으로 적용될 수 있다. 또한 국제결제은행에서 발행된 문서와 각국에서 실용화중인 시스템 가이드라인을 근거로 하여 국내 전자지불 시스템뿐만 아니라 국제 전자상거래에도 사용될 수 있도록 작성되었으므로 전자화폐 시스템의 관리와 운영을 용이하게 할 수 있는 안전한 시스템 구현의 기초가 될 것이다.

I. 서론

최근 정보통신기술의 발전과 인터넷 사용의 폭발적인 증가로 인해 인터넷상에서 다양한 사업을 수행하려는 전자상거래 움직임이 활발하다. 인터넷상의 거래는 기존의 물리적인 상거래 방식에 비해 디지털 정보와 정보통신망을 이용하기 때문에 많은 편리성과 유용성을 제공한다. 반면에 직접적인 대면을 통한 상거래 방식이 아니라 원격지에서 비대면 거래를 수행하기 때문에 거래 당사자들간의 신뢰 문제나 대금 지불 문제 등이 발생하게 된다. 따라서 전자상거래가 개인이나 기업으로부터 신뢰성을 얻고 안전한 지불 처리를 하기 위해서는 전자지불 메커니즘의 개발이 선행되어야 한다. 즉, 전자지불시 거래정보의 위조나 복사에 의한 가치의 부당한 취득 방지 등의 안전한 지불방법의 확립이 중요하다. 그래서 인터넷상의 전자상거래를 위한 새로운 전자지불 수단으로써 안전한 전자지불을 실현하기 위해 전자화폐가 등장하게 되었다.

이렇듯이 전자상거래를 실용화하기 위한 핵심은 전자지불시스템이다. 전자지불시스템은 신용카드로부터 시작하여 e-cash와 같은 네트워크형 전자화폐로 발전하고 있으며, 다시 IC 카드를 이용하는 IC 카드형 전자화폐로 발전하고 있다. 이러한 전자지불시스템의 핵심기술은 보안 기술이다. 즉, 전자화폐의 인출, 지불 등의 단계에서 개인의 프라이버시와 이중 사용 문제를 해결하기 위해서 공개키 암호화, 디지털서명 그리고 은닉 서명(Blind Signature) 등의 암호 기술이 사용되고 있다.

현재 실용화되고 있는 전자화폐 시스템에는 First Virtual[13], Cyber Cash[14] 그리고 E-cash[15] 등으로 대표되는 네트워크형 전자화폐와 Mondex[16]로 대표되는 IC 카드형 전자화폐가 있다. 또한, 이밖에 이론적으로도 여러 가지 방식이 연구되고 있는데 이 중 관심을 끌고 있는 Brands의 전자화폐 시스템[1] 등이 있다.

전자화폐 시스템은 크게 사용자가 은행에 구좌를 개설하여 전자화폐를 발급받는 인출단계와 상점에서 물건을 사고 전자화폐를 지불하는 지불단계, 그리고 상점이 은행에 전자화폐를 예금하고 자신의 구좌에 현금을 넣는 예치단계

* 동국대학교 정보산업학과 (song@mail.dongguk.ac.kr)
** 순천향대학교 컴퓨터학부 (hgoh@ai-cse.sch.ac.kr, imylee@asan.sch.ac.kr)

로 이루어진다.

이러한 전자화폐 시스템을 안전하게 구현하기 위해서는 보안기능의 표준화가 시급하다. 본 논문에서는 전자화폐 시스템을 구현하기 위한 프로토콜들의 표준과 안전성을 위한 정보보호 기능 표준을 제시하여 향후 국제적인 전자상거래에 대비하여 상호호환성 있는 전자화폐 시스템 구현의 기반을 제공하고자 한다.

본 논문은 세 가지 분야를 취급하고 있다. 먼저 전자화폐의 개요와 요구조건[2][3][4]에 대해 설명하고 전자화폐 도입시 문제점에 대해 언급한다. 그리고 이를 위해 전자화폐에 적용되는 정보보호기능에 대해 설명한다.

II. 전자화폐의 개요와 요구조건

본 장에서는 전자화폐의 개요와 요구조건에 대해 기술하고 지불 방식과 사용 방식에 따라 분류해 보겠다.

1. 전자화폐의 개요

전자화폐는 디지털 데이터를 기반으로 하는 디지털 사회에서 가상 공간에서 동전이나 지폐와 같은 실물 화폐 역할을 수행하기 위해 디지털 데이터로 구성된 화폐이다. 또한 액면 가치를 보증하기 위해 은행이 서명한 디지털 정보라고 정의할 수 있으며 어떠한 물리 매체에도 의존하지 않고 정보 그 자체로서 가치를 지닌다. 전자화폐는 기존의 화폐가 가져야 하는 법적인 효력과 안전성 등에 관한 기능을 그대로 가지면서 IC 카드와 같은 별도의 기기나 또는 컴퓨터 등에 소프트웨어 형태로 존재하는 전자지갑에 의해 관리된다. 실물화폐가 가지고 있는 기능뿐만 아니라 효율성과 사용자 편리성 그리고 디지털 데이터가 가지는 특징으로 발생하는 문제점 등을 해결하기 위해 여러 가지 다른 요구 조건 등을 만족시킬 수가 있는데 이러한 기능은 선택적으로 부가시킬 수가 있으며 각국 통화 당국의 정책에 의해 결정이 될 것이다.

한편, 전자화폐는 편리성이나 안전성 등 많은 이점을 주는 반면에 문제점도 가지고 있다. 예를 들면, 디지털 정보이기 때문에 데이터로서의 취급이 용이한 반면에 전자화폐는 실물 화폐보다 복사가 쉬워 암호기술에 의한 위조 대책이 필요하고, 사용자의 지불이력이 수집 관리되는 등의 사용자의 프라이버시 침해에 대한 문제점 등이 있다. 또한 안전한 전자화폐 시스템을 실현하기 위해서 부정 사용시 발행 한도액을 초과하여 지불한 사용자의 이름을 검출할 수 있는 방법이 필요하다. 즉, 한도액 초과라는 부정이 발생했을 경우에 익명성이 취소되는 익명성 취소 메카니즘[5][6]도 필요할 것이다.

이와 같이 전자상거래의 하부구조로서 필수요소인 전자화폐 시스템이 정보화 사회에서의 영향력이 증가함에 따라 전자화폐 시스템의 안전성을 보장하는 방법의 강구가 매우 중요하게 될 것이며 향후 전자상거래 시대를 대비하여 전자화폐 시스템 정보보호 모델 표준 개발이 시급한 과제일 것이다. 본 논문은 이러한 관점에서 안전한 전자화폐 시스템을 구축하기 위해 필요한 정보보호 기능에 관련된 표준을 제공하고자 한다.

2. 전자화폐의 요구조건

전자화폐란 액면가치를 보증하기 위해 은행이 서명한 디지털 신호로 표현된 가치정보이다. 전자화폐는 디지털데이터 형태로 전자지갑(워크스테이션, IC 카드, 개인휴대단말 등)에 저장되는 형태가 많다. 이와 같은 형태의 전자화폐는 통신회선을 통해 자유롭게 전송할 수 있고 유통성, 편리성이 높은 시스템을 실현할 수 있다. 또한 전자화폐는 암호기술에 의해 디지털 데이터 그 자체에 가치를 갖고 있어 당사자간에 그것을 교환하는 것으로 결제가 즉시 완료되는 간단함과 편리함이 있다.

이와 같이 실물 화폐를 디지털화 하는 이점은 화폐 그 자체가 갖는 익명성(고객의 구매에 관한 프라이버시가 상점이나 은행에 노출되지 않는 성질), 오프라인성(거래 및 지불 결제시 고객과 상점 이외 제삼자가 개재하지 않는 성질), 양도 가능성(네트워크 등을 경유해서 전자적으로 가치를 이동할 수 있는 성질), 분할이용 가능성(액면 금

액이 될 때까지 분할해서 이용할 수 있는 성질) 등을 전자화폐에 부여해서 소액의 현금에 대해서도 이동성을 갖게 할 수 있으므로 원격지로의 지불에 요하는 비용이 거의 필요로 하지 않는 것이다.

그러나 전자화폐의 디지털 형태는 정보 그 자체가 화폐가치를 갖기 위해 부정한 이용 방지가 중요한 과제가 된다. 디지털 정보는 쉽게 복사가 가능하고 또 아무런 흔적도 없이 변조·개조가 가능하다. 즉 디지털 정보를 전자화폐로 사용하는 경우 현실의 화폐와 비교해 쉽게 복사, 위조될 가능성이 생긴다.

전자화폐를 안전하게 실현하기 위한 여러 방법들 중 한가지 방법은 물리적인 수단에 의해 안전성을 보증하는 방법이다. 예를 들면, 전자화폐 정보를 암호화하고 디지털 서명키 데이터를 tamper resistance를 가진 IC 카드 내에 저장하여 쉽게 읽어낼 수 없도록 하는 것이다. 여기서, tamper resistance란 IC 카드 내부의 데이터를 읽어내기도 하고 부정하게 조작하지 못하도록 하는 것을 말한다.

전자화폐는 물리적 화폐와 유사한 기능을 갖도록 설계하는 것이 기본 원칙이다. 그러나 완벽하게 물리적 화폐와 같은 기능을 갖는 전자화폐 시스템을 구축하기는 상당히 어려운 일이다. 이는 물리적 화폐의 다양한 기능을 전자화폐에 부여하기 위해서 고도의 수학적 방식이 필요하기 때문에 어려움이 있다. 그럼에도 불구하고 전자화폐가 필요한 이유는 물리적 화폐가 다음과 같은 문제점들을 가지고 있기 때문이다.

- 물리적 화폐의 제작, 유통, 관리 및 폐기에 수많은 인력과 자금이 소요
- 컬러 복사기 및 프린터의 발달로 위조 화폐의 제작이 용이
- 급속한 컴퓨터 네트워크의 발달에 따른 전자상거래 시대에 가상 공간에서 전자 결제 수단으로서 사용하기 어려움 등

그리고 전자화폐는 디지털 데이터 자체에 금액가치를 포함하고 있기 때문에 제 3자에 의한 네트워크 상에서의 다양한 공격 가능성과 사용자/소유자에 의한 위·변조 가능성이 존재한다. 또한 실물화폐에서처럼 화폐 사용시 사용자의 익명성을 유지시켜 주어야 한다. 이러한 문제점이 완벽히 해결되지 않는다면 화폐로서의 가치를 상실하게 될 것이며 경제 생활에 많은 혼란을 초래하게 된다. 따라서 전자화폐 도입 후 지급불능사태가 발생하거나 도용 및 무단 복제에 따른 신용질서 파괴, 바이러스 침입에 따른 가치 상실, 시스템 오류 등에 따른 소비자 보호 등에 관해 사전에 철저한 대비가 필요하다. 이를 위해 다양한 공격을 방지하고 화폐로서의 가치를 유지하기 위해 여러 가지 암호학적인 기법들이 사용되고 있는데 다음에서는 이를 위해 전자화폐에 있어서 요구되는 사항들에 대해 알아보도록 한다.

- 안전성(Security)

  화폐 가치를 포함하고 있는 전자화폐는 디지털 데이터 형태로 구성이 되어 있기 때문에 가치 정보에 대한 조작이 가능하며 실물 화폐보다 손쉽게 대량으로 복사가 가능하다. 만약 범죄자가 전자화폐를 만들어낼 수 있다면 경제 질서에 많은 피해를 가져 올 것이다. 따라서 전자화폐의 복사, 위조 등으로 인한 부정 이용을 방지해야 하며 어느 한 쪽이 거래 사실을 부인할 경우 그 진위 여부를 판명할 수 있어야 한다. 그리고 현재 개발되고 있는 대부분의 전자화폐는 오프라인(off-line)으로 거래가 이루어지기 때문에 전자화폐를 훔치거나, 위조할 경우 그 추적이 어려울 것이다. 만약 이런 사태가 광범위하게 발생한다면 전자화폐는 신뢰성을 상실하게 될 것이다. 따라서 화폐 발행자들은 부정한 조작이 불가능한 위·변조 방지형 마이크로칩으로 안전장치를 내장하고 고성능 암호처리 프로토콜 설치 등 정교한 위·변조 방지장치를 개발하여야 할 것이며 전자화폐 발행 은행의 지속적인 모니터링, 전자화폐 거래 관련 기록 유지 등의 보완대책도 강구할 필요가 있다. 그러나 기본적으로 전자화폐에 대한 안전성은 다른 방법에 의존하지 않고 전자화폐 데이터에 대한 처리만으로도 완벽히 실현될 수 있어야 한다. 또한 어느 한쪽이 거래 사실을 부인할 경우 그 진위여부를 판명할 수 있어야 한다.

- 추적불가능성(Privacy)

  실물화폐를 사용하였을 경우 지불인은 추후 은행이나 기타 감독기관의 추적을 피할 수 있다. 즉, 사용자 익명성을 유지하고 있다. 마찬가지로 전자화폐를 인터넷상에서의 물품 구매

대금으로 지불하더라도 사용자 익명성은 유지되어야 한다. 그러나 전자화폐는 전자화폐 발행시 또는 계정 개설시에 화폐 발급은행에 사용자의 식별 정보를 제공하기 때문에 전자화폐와 사용자 식별 정보를 연계시킴으로서 추적할 수가 있다. 정당한 사용자의 전자화폐 사용 내역은 알려져서는 안된다. 이러한 요구조건이 만족될 때 사용자의 사생활은 보장받게 된다.

- 오프라인성(Off-line payment)

사용자가 지불한 전자화폐는 상점에서 지불처리시 은행의 개입 없이 처리할 수 있어야 한다. 즉, 사용자가 상점에 지불한 전자화폐의 유효성, 정당성 등을 은행에 접속하여 확인을 받는 것이 아니라 상점에서 여러 가지 암호 기법을 통하여 즉시 확인이 가능해야 한다.

- 양도성(Transferability)

전자화폐는 실물 화폐와 같이 제 3자에게 즉시 화폐 가치의 이전이 가능해야 한다. 즉, 중간에 은행을 거치지 않고 직접 전달이 가능함으로써 매번 은행에 전자화폐를 예치하고 다른 전자화폐를 발행 받아 전달해야 하는 통신 부하를 감소시킨다.

- 분할성(Divisability)

실물 화폐에는 없는 기능으로 전자화폐에 새롭게 추가된 기능이다. 일정한 가치를 가지고 있는 전자화폐는 그 가치 범위 내에서 보다 작은 금액 단위의 전자화폐로 분할하여 사용할 수 있어야 한다. 이때 분할된 화폐의 안전성 및 유효성, 정당성 등은 본래 화폐와 동일한 강도를 지녀야 한다. 분할 사용 기능을 통해 사용자는 작은 금액을 지불하기 위해 은행으로부터 작은 금액의 전자화폐를 발행 받지 않아도 되는 등 화폐 관리 면에서 효율적이다. 또한 상점 측에서도 거스름 발생에 대비하여 작은 금액의 전자화폐를 보관하던가 또는 새로운 거스름 전자화폐를 발행하지 않아도 된다.

- 디지털 정보화(Independence)

컴퓨터를 매개체로 인터넷과 같은 네트워크 상에서 사용할 수 있기 위해서 전자화폐는 다른 물리적인 형태에 의존하여서는 안되며 디지털 데이터 자체로서 완벽한 화폐 가치를 가져야 한다. 즉, 지폐는 종이 위에 복사 방지 기술을 이용한 인쇄 기술을 사용하여 화폐를 구성하고 있으나 이와 같이 별도의 물리적인 매개체를 사용하여 구성되거나 안전성을 보장받아서는 안된다. 화폐의 정당성을 인증받기 위한 은행의 서명, 복사 방지를 위한 기술 등과 같은 모든 조건이 디지털 데이터의 조작만으로 만족시켜야 한다. 이때에만 비로소 네트워크 상으로 전송될 수 있다.

이외에 전자화폐에 완전한 익명성을 제공하게 되면 돈 세탁 및 돈 약탈, 불법 구매 자금으로의 이용 가능 등 부정한 방법으로 그 기능이 전용될 수가 있다. 따라서 초기에 완전한 익명성[7][8]을 제공하던 것으로부터 현재는 불법 사용시 사용자의 익명성을 제거하기 위한 익명성 취소 기능을 부가하고 있으며 이에 대한 연구[5][6][9]가 중요한 이슈로 등장하고 있다.

- 익명성 취소(Anonymity revocation)

불법적인 거래에 있어서 돈 세탁을 위해 현금을 이용하게 된다. 그러나 현금은 그 금액이 일정한 범위로 제한이 되어 있어 많은 양의 자금을 세탁하는 일은 어려운 일이였다. 그러나 익명성이 제공되는 전자화폐에 있어서는 비록 그 금액이 작은 소액이더라도 디지털 데이터로 구성 되어 있기 때문에 실물 화폐와 같이 운반 및 보관에 어려움이 발생하지 않는다. 따라서 실물 화폐에서 발생하지 않았던 부작용이 보다 용이하게 발생할 수 있으며 이에 대한 사전 대비가 반드시 필요하다. 이를 위해 필요한 기능이 익명성 취소 기능으로서 정당한 사용자의 익명성은 완벽하게 보호되지만 부정 사용시에는 법원과 같은 공정한 기관의 명령에 의해 사용자의 식별 값이나 동전 번호를 노출시킬 수 있어야 한다.

3. 전자화폐의 분류

전자화폐는 크게 IC 카드형과 네트워크형의 두 가지로 구분해 볼 수가 있으며 지불 방식에 따라 다시 온라인(on-line)형과 오프라인(off-line)형, 신용카드형, 선불카드형으로 나누어 볼 수가 있다. 그리고 IC 카드형은 다시 가치 이전성을 기준으로 폐쇄형(closed)과 개방형(open)으로 나누어 볼 수가 있다.

3.1 IC 카드형 전자화폐

플라스틱 카드 위에 부착된 IC칩에 화폐가치를 저장하였다가 지급수단으로 사용하며, 전자화폐가 소진되면 비동기전송모드(ATM)등 가치저장장치나 은행창구에서 화폐를 다시 저장하여 반복 사용할 수 있다.

IC 카드형 전자화폐는 가치의 이전성을 기준으로 폐쇄형과 개방형으로 구분되어진다. 폐쇄형은 어떤 사람의 카드에서 다른 사람의 카드로 카드간 가치이전이 허용되지 않는 것이고 개방형은 카드간 자유로운 가치이전이 허용되는 것이다. 가치이전이 자유로운 개방형이 현금과 더 유사하다고 볼 수 있다.

대부분의 국가에서 안전성 등을 이유로 폐쇄형을 채택하고 있는데 개방형으로는 영국의 Mondex사가 발행한 몬덱스 카드가 현재까지 개발된 것 중 유일한 개방형으로 알려져 있으며 많은 나라에서 몬덱스 카드의 도입을 추진하거나 검토하고 있을 만큼 전자화폐 중에서 주목받고 있는 카드이다.

3.2 네트워크형 전자화폐

컴퓨터 통신망을 통해 거래은행 예금을 인출하여 인터넷 등 공중망상의 가상은행(virtual bank)계좌나 공중망과 연결된 이용자의 PC에 화폐가치를 저장하였다가 전자상거래 대금의 지급 등에 사용한다. 사용자는 관련 소프트웨어를 다운 받아서 설치한 후 계정을 신청하여 이용할 수 있다.

이와 같은 전자화폐는 Cyber Cash 또는 E-Cash 등이 있다.

III. 전자화폐의 문제점

전자화폐는 도입 후 지급불능사태가 발생하거나 도용 및 무단 복제에 따른 신용질서 파괴, 바이러스 침입, 시스템 오류 등에 따른 소비자 보호 등에 관한 사전적 대비가 필요하다. 이를 위해서는 암호화, 인증 네트워크 등 기술적 문제 이외에도 금융제도, 사회경제구조 등 법·제도적인 정비가 선행되어야 한다.

1. 위·변조 및 도용 가능성

전자화폐는 디지털 데이터 형태로 구성 되기 때문에 기존의 화폐보다 훨씬 수월하게 복사가 이루어질 수 있다. 이를 통해 같은 화폐를 중복사용(double-spending)할 수가 있게 되는데 이는 거래 금액이 소액이더라도 거래의 높은 발생 빈도 때문에 전체 통화 시스템에 큰 피해를 끼칠 수가 있다. 또한, 범죄자가 전자지갑을 만들어낼 수 있다면 전자화폐 발행자는 커다란 손실을 입을 것이다. 그리고 전자지갑은 오프라인으로 거래가 이루어지기 때문에 카드를 훔치거나, 위조한 경우 그 추적이 어려울 것이다. 만약 이런 사태가 광범위하게 발생한다면 전자화폐는 신뢰성을 상실하게 될 것이다.

따라서 카드발행자들은 카드형 전자화폐의 경우 부정한 조작이 불가능한 위·변조 방지형 마이크로칩으로 안전장치를 내장하고 카드형과 네트워크형 전자화폐 모두에 적용되는 안전장치로 높은 수준의 암호처리 시스템들을 장착하는 등 정교한 위·변조 방지장치를 개발하여야 할 것이며 운영자의 지속적인 모니터링, 전자화폐 거래 관련 기록 유지 및 부정 사용시 전자화폐 거래의 추적 기능 등의 보완대책도 강구할 필요가 있다.

2. 소비자 보호 문제

전자화폐는 전자지갑이라는 물리적인 매체에 저장되어 사용될 수가 있는데 이러한 전자지갑으로 여러 개의 카드를 통합한 스마트 카드가 보급될 경우 개인 정보가 집적됨으로서 카드 사용자에 대한 정보 노출로 인해 사생활 침해라는 큰 문제로 대두될 수 있다. 전자화폐 시스템에서 사생활을 보호한다고 할 때는 첫째, 사용자의 금융거래가 어디에서 이루어졌는가가 알려져서는 안되고, 둘째 사용자가 금융거래를 두 번 했을 때 그 두 거래가 같은 사람에 의한 것이라는 사실이 알려져서는 안 된다. 이러한 보장은 은행에 대해서 보장되어야 할 뿐만 아니라 은행과 거래처(상점)가 공모를 해도 보장되어야 한다.

따라서 개인의 사생활 보호를 위한 법제면의 충분한 대비가 필요하다. 하지만 아직 소비자 보호법을 운용하고 있는 국가는 아직 없으며 미국 등에서 주요 관심사가 되고 있다.

3. 돈 세탁 등 범죄문제

불법적인 거래에 있어서 세금 및 거래 사실에 관한 기록을 회피하기 위해 주로 현금이 선호되나 현금의 경우 많은 양의 돈에 대한 운반이나 안전한 보관 등 어려운 문제점이 많다. 그러나 전자화폐는 이러한 문제점이 없기 때문에 돈 세탁 등 불법적인 용도로 악용될 가능성이 있다.

현재 개발되고 있는 대부분의 전자화폐가 가치 이전에 대한 제한 및 거래 기록유지 등과 같은 특징을 포함하고 있기 때문에 불법적인 용도에 사용될 가능성은 당분간 희박하지만 장기적으로 화폐 거래 금액이 커지고 몬덱스형 전자화폐와 같이 자금이체가 은행시스템을 경유하지 않고 카드 사용자들간에 곧바로 일어날 경우 돈 세탁 등 불법적인 목적으로 악용될 가능성이 크므로 자금 세탁 방지법 등 관련 법체계의 정비가 필요할 것이다.

4. 전자화폐에 대한 신뢰성 문제

현재 정부나 중앙은행이 발행하는 법정화폐에 대해서는 모든 사용자들이 신뢰성을 가지고 있다. 그러나 개별은행이나 비은행기관에서 전자화폐를 발행했을 때 이에 대한 신뢰성 문제가 대두될 수 있다. 특히 비은행기관의 경우 예금자의 보호를 위해 은행에 적용해온 은행 법규, 금융감독 및 예금자 보험에의 가입 의무 등과 같은 것들이 없기 때문에 일반의 신뢰를 얻기 어려울 것이다. 만약 일반 사용자들이 전자화폐를 신뢰하지 않는다면 이 화폐는 널리 사용될 수 없을 것이다.

따라서 전자화폐 발행주체, 전자화폐 운영에 따른 권리, 의무 등 제반 법적 기준을 명확히 할 필요가 있다. 그러나 전자화폐 발행금액이 소규모인 경우 그러한 기준으로 인해 불필요한 비용을 발생시키고 전자화폐의 보급에 장애가 될 수도 있다는 점도 고려해야 할 것이다.

IV. 전자화폐 시스템 보안 기능

본 장에서는 전자화폐 시스템 보안 기능 모델을 구성하기 위해 필요한 구성 요소와 안전한 전자화폐 시스템을 구현하기 위해 필요한 보안 기능 표준들에 대하여 기술한다. 특히, 여기서는 휴대성이 좋고 스마트 카드 자체에서 높은 보안성을 제공하고 있는 IC 카드형 전자화폐 시스템[10][12]을 중심으로 그 구성요소별 기능 표준과 구성 요소간 프로토콜들에 대해 기술한다. 구성요소간 교환되는 디지털 정보는 상호간 고려해야 할 사항이며 기타 전송로 상에서의 정보보호 기능은 시스템을 운용, 관리하고 있는 부문에서 충족시켜야 할 것이다.

1. 전자화폐 시스템 구성요소 기능 모델

전자화폐 시스템을 구성하는 요소는 발행기관, 금융 기관, 이용자, 상점, 인증/등록기관, 수사기관, 제조업체 등으로 각 구성요소간 정보 흐름은 다음 [그림 1]과 같다. 그리고 각 구성요소의 정보보호 기능은 4절에서 기술된다.

2. 구성요소별 기능 표준

2.1 발행기관

발행기관은 전자화폐를 발행하고 통화량을 관리하며 금융 기관과 함께 화폐의 부정한 사용을 검출하는 등 전체 화폐 시스템을 관할하는 기관이다. 전자화폐는 각각의 금융 기관이 개별적으로 발행하는 것이 아니라 발행기관이 공통의 전자화폐를 생성하고 이를 각 금융 기관에 전송하면 금융 기관은 이 금액의 한도 내에서 전자화폐를 발행한다. 즉, 현재의 실물 화폐와 같이 한국은행이 한국은행권을 발행하고 이를 시중 은행에 제공하면 해당 은행이 각 사용자들에게 화폐를 지급하는 형태를 가진다.

발행기관은 전체 전자화폐 시스템에 있어서 매우 중요한 역할을 수행하기 때문에 위조나 고장에 대응하고 안전성을 높이기 위해 거래시 여러 가지의 대책을 행한다. 예를 들면, 유효기간, 거래회수, 기기의 잔고 등에 대하여 미리 설정한 제한을 초월하는가 및 잔고의 최대치가 불법적으로 개조되지는 않았는가 등에 대하여 검증을 행한다.

발행기관이나 시스템 운용기관에 의한 데이터

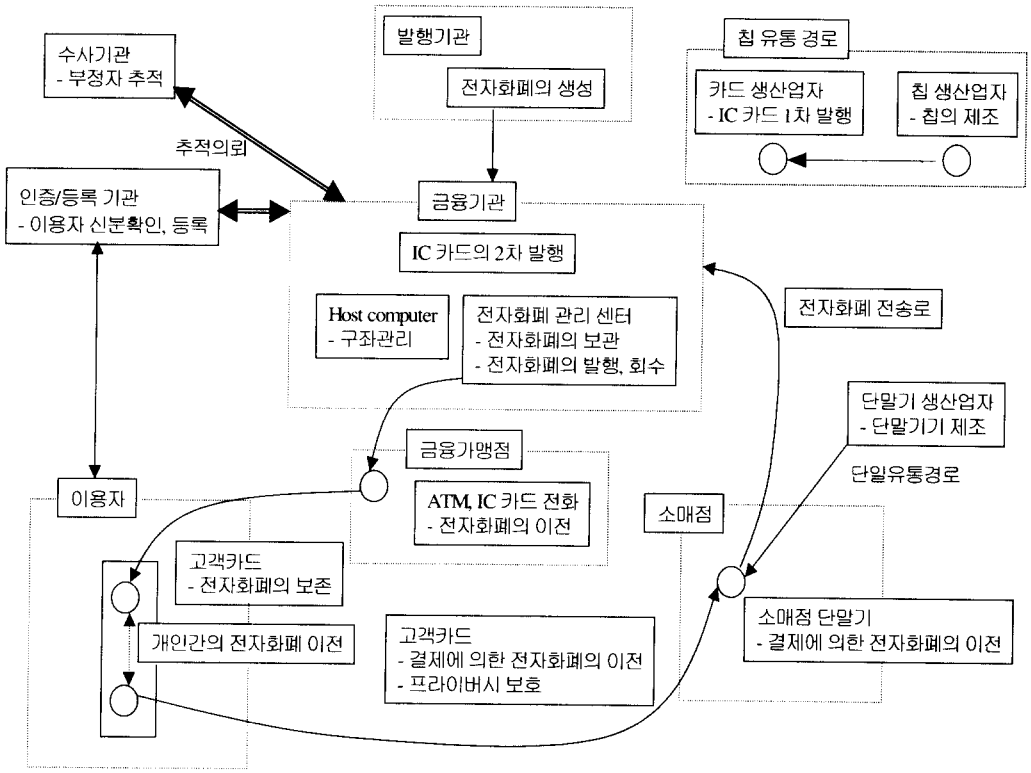

그림 1. 전자화폐시스템 구성요소 기능 모델

검증에는 메시지 인증자의 검증, 거래 일련번호의 검증, 과거의 결제나 충전정보의 검증 및 거래에 포함되거나 카드에 보존된 그 외의 정보의 검증이 있다.

다음에서는 발행기관에서 수행하는 정보보호 기능을 기술한다.

1) 비밀키 정보관리

IC 카드 발행시 그리고 화폐 발행시 사용되는 발행기관의 비밀키 유출 방지기능이 필요하다.

: 이를 위해서 비밀키 정보파일에의 부당한 접근방지 기능을 갖춘다. 또한 비밀키 생성의 권한관리를 철저히 하며, 데이터 전송시 제3자의 공격으로부터 계산적으로 충분히 견딜 수 있을 정도의 강도를 가지도록 설계한다.

2) IC 카드의 부정발행 방지

운영자의 실수나 의도적인 부정발행을 방지해야 한다.

: 이를 위해서 발행이력의 관리자료를 작성한다. 또한 발행작업장소에서의 입·퇴실 관리를 철저히 하고 비정기적인 감사를 실시한다.

3) 유효기간 제한 기능

전자화폐의 유효기간을 제한하여 비밀키 정보의 유출 위험성을 방지한다.

4) 상한 금액의 설정

분실, 도난 등에 대해 사용자 보호 차원과 돈 세탁, 약탈과 같은 부정한 용도로의 전용 등을 방지하기 위해 전자화폐 금액의 상한을 설정한다.

2.2 금융 기관

금융 기관은 전자화폐 발행기관으로부터 받은 금액 한도 내에서 전자화폐를 이용자에게 발행해 주고 그 금액에 해당하는 금액을 이용자의 계좌로부터 발행기관으로 이체한다.

다음에서는 금융 기관에서 수행하는 정보보호 기능을 기술한다.

1) 전자화폐의 부당한 인출 방지

전자화폐는 부정하게 발급된 카드를 범죄자

혹은 범죄 조직이 입수하여 부당한 인출을 시도하려는 것으로부터 보호되어야 한다.

: 이를 위해서 금융 기관에서는 인출시 사용자 본인 확인을 위한 인증 절차를 필요 요건으로 한다. 또한 IC 카드 자체에 대한 인증과 부정화폐나 부정거래에 대한 거래추적기능과 관리가 필요하다.

2) 전자화폐 전송시 가치의 무단절취 방지

전자화폐가 금융 기관에서 단말기로 네트워크 상에서 전송시 중간에 분기시켜 다른 단말기로 절취되는 것으로부터 보호되어야 한다.

: 이를 방지하기 위해서 상대 인증에 의한 고객카드와 단말기기의 위장을 방지하고, 금융 기관 시스템에 의한 본인확인과 단말기의 부당 접근 방지와 위·변조 검출 시스템을 설치한다.

3) 비밀 서명키 유출 방지

전자화폐에 적용되는 비밀 서명키의 유출 방지기능이 필요하다.

: 이를 위해서 비밀 서명키 정보에로의 부당한 접근방지 기능을 갖춘다. 또한 비밀키 생성의 권한 관리를 철저히 한다.

2.3 이용자

이용자는 금융 기관으로부터 발행 받은 전자화폐를 다른 이용자에게 양도하거나 상점에서 상품을 구입하는데 사용한다.

다음에서는 이용자와 관련하여 발생할 수 있는 문제점과 이를 해결하기 위한 기능을 기술한다. 이러한 정보보호 기능은 각 구성요소, 예를 들면 제조업체, 금융 기관, 발행기관, 상점 등과 밀접한 관련이 있다.

1) 전자화폐 인출의 부인 방지

이용자가 전자화폐를 인출 후 이를 부인할 가능성이 존재한다.

: 이를 위해서 디지털서명으로 인증하고 카드내의 거래 이력을 취득함으로써 이를 증명한다. 또한 사용자가 부인한 인출 전자화폐에 대해서는 해당 화폐의 유효성을 금융 기관과 발행기관에서 취소시켜 유통할 수 없도록 한다.

2) 이용자 프라이버시 침해 방지

금융 기관 시스템의 관리자에 의해서 또는 수사 기관에 의해 이용자의 개인 식별정보와 거래정보 또는 기타 사생활에 관련된 정보가 유출될 가능성이 존재한다.

: 이를 위해서 거래이력 취득시의 정보를 최소한으로 정하고, 정보의 보관 자격자를 특별히 선정한다. 또한 거래 이력을 금융 기관과 공유하는 비밀 정보로 암호화함으로써 권한 없는 제3자의 불법적인 정보의 접근을 방지한다.

3) 부정사용방지

전자화폐를 IC 카드 등의 기억장치에 저장해서 휴대하면 패스워드 등을 이용해서 도난 및 분실시에도 전자화폐의 부정사용을 방지할 수 있다.

2.4 상점/가맹점

상점에서는 이용자에게로부터 받은 전자화폐를 일정한 기간이나 또는 일정한 금액 이상이 되면 은행에 입금하며 필요시 실물화폐로 전환하여 사용한다.

다음에서는 상점/가맹점에서 수행하는 정보보호 기능을 기술한다.

1) 전자화폐의 부당한 인출방지

상점의 단말기에서는 매물대금 이상으로 이용자 IC 카드 등의 전자지갑으로부터 전자화폐를 인출할 수 있는 가능성이 존재한다.

: 이를 방지하기 위해서 단말기의 부당한 접근방지 기능을 부여하고 거래 이력을 취득하여 결제금액을 이용자가 눈으로 확인하도록 한다.

2) 상점 단말기내의 매상데이터의 조작 방지

상점은 자신이 이용자에게 매출한 금액보다 많은 금액을 매출한 것처럼 상점 단말기의 매상데이터를 조작할 우려가 있다.

: 이를 위해서 매상정보에 상점의 디지털서명을 하고, 이용자에게 영수증을 발급한다. 이용자는 상점으로부터의 매상정보 수신시 상점의 디지털서명을 검증한다.

2.5 등록/인증기관

전자화폐의 소유자 식별정보나 계정 정보 등을 등록해 놓는 것은 부정행위를 조사할 때 도움이

된다. 등록/인증기관은 이용자가 전자화폐를 사용하기 위해 미리 등록을 하기 위한 기관이고 이용자의 정당성을 보증한다.

이용자 등록처리는 전자화폐를 이용할 때에 필요한 등록서를 작성하는 부분이다. 등록서는 이용자 공개키, 등록/인증기관의 디지털 서명으로 구성된다.

발행기관이나 금융 기관에서 전자화폐의 이중사용이 검출이 되면 이를 등록/인증기관에 보내고 등록/인증기관은 다시 수사 기관과 협력하여 부정 사용자를 추적하게 된다. 여기서 익명성이 취소된다.

다음에서는 등록/인증기관에서 수행하는 정보보호 기능을 기술한다.

1) 부정한 등록 방지
등록과정에서 자신이 아닌 다른 사람의 명의로 등록을 할 수 있다.
: 이를 위해서 등록시 자신의 신분을 증명할 수 있는 자료제출을 요구한다.

2) 등록된 사용자의 개인정보 보호
등록/인증기관에 등록되어 있는 개인정보의 유출을 막기 위해서 각 데이터를 암호화하고, 이에 대한 암호키는 법원과 같은 공정한 기관과 등록/인증기관이 함께 관리한다. 수사 기관은 법원의 영장과 같은 공정한 기관의 명령 등에 의해서만 개인정보를 제공받아 사용자나 또는 전자화폐를 추적할 수 있다.

2.6 수사 기관

전자화폐는 기본적으로 익명성 기능을 제공하기 때문에 기존의 실물화폐의 돈 세탁 및 약탈 등과 같은 각종 범죄 행위가 더욱 용이하게 발생할 수 있으며 부정사용을 밝혀내기도 어렵다. 따라서, 이에 대한 해결 방법으로서 수사 기관은 발행기관과 금융 기관 그리고 등록/인증기관과 협력을 통해 추적기능을 수행한다. 이러한 수사 기관의 추적 기능은 전자화폐의 보급이 점차적으로 증가하고 그에 따라 문제점이 발생할 것으로 예상되기 때문에 그 중요성은 크게 증가하고 있다.

추적 프로토콜에서 수사 기관은 법원의 영장을 득한 후에 금융 기관에 추적을 의뢰하면 금융 기관은 예치 프로토콜 실행 중에 받은 정보를 등록/인증기관에게 제공한다. 그 후 등록/인증기관은 이 정보를 이용하여 금융 기관에게 사용자를 검출할 수 있도록 정보를 반송한다.

다음에서는 수사 기관에서 수행하는 정보보호 기능을 기술한다.

1) 수사에 사용되는 개인정보의 유출 방지
부정하거나 의심이 가는 거래에 대한 추적을 하기 위해 경우에 따라 개인정보가 수사 기관에 제공되는데, 이때 수사에 사용되는 개인정보가 유출될 수 있다. 또는 수사 기관의 수사권 남용으로 인해 정당한 사용자를 추적할 수도 있게 되는데 이는 심각한 프라이버시 침해를 가져오게 된다.
: 이를 위해서 수사에 필요한 개인정보는 수사 기관 자체에서 관리하지 않고 인증/등록기관에서 관리하고 수사 기관에서 필요한 자료만을 인증/등록기관과 연계함으로써 획득하도록 한다. 또한 수사 기관은 법원과 같은 공정성이 보장되는 기관에서 추적 허가를 받아 이를 인증/등록기관 및 금융 기관에 제시함으로써 추적을 할 수 있도록 한다.

2) 부정거래 추적기능
돈 세탁, 약탈시 또는 마약 거래와 같은 부정한 거래의 대금 결제로 사용되었을 경우 수사 기관은 해당 전자화폐나 또는 사용자를 추적할 수 있어야 한다. 이러한 수사 기관의 추적 기능은 크게 사용자 추적과 전자화폐 추적 기능으로 나누어 볼 수가 있다.

사용자 추적은 특정한 전자화폐를 소유한 사용자의 식별 정보를 드러내는 것으로서, 수사 기관 등이 의심스러운 전자화폐의 출처를 밝혀낼 수 있기 때문에 돈 세탁 등을 방지한다. 또한 당국은 불법 판매자가 식별된 후에 불법 구매를 하는 고객을 식별할 수 있도록 해 주기 때문에, 무기 구매나 마약 거래와 같이 불법적인 거래를 하는 고객을 식별할 수 있다.

전자화폐 추적은 인출된 전자화폐를 추적한다. 이 프로토콜에서 수사 기관이 금융 기관에 전자화폐의 추적을 의뢰하면 금융 기관은 등록/인증기관에 이용자가 전자화폐 발행시 제공한 계좌 정보 및 식

별 정보를 제공한다. 그 후, 등록/인증기관은 사용자가 전자화폐 발행 받기 위해 사용자 인증시 제공한 사용자 등록 정보와 전자화폐가 사용될 때 검출될 정보를 금융 기관에 회송하면 금융 기관은 전자화폐의 일련번호를 수사 기관에 제공함으로써 전자화폐 추적 기능을 수행한다.

2.7 제조업체

다음에서는 IC 카드 제조업체에서 수행하는 정보보호 기능을 기술한다.

1) 부정한 카드, 칩의 유출 방지

제조 공장 자체에서 종업원과 범죄자 등과의 공모를 통해 부정하게 카드나 칩을 유출할 가능성이 있다.

: 이를 위해서 엄밀한 수량관리가 필요하다. 또한 각 제조카드 등에 제조번호를 붙인다.

2) IC 카드, 칩의 도난 폐기된 IC 카드의 부정이용 방지

IC 카드의 접근방식을 비밀로 하고 IC 카드 폐기 처분시의 관리를 철저히 한다. 또한 기기의 유출이나 도난시에 물리적으로 기기를 보호할 수 있는 tamper resistance 기능을 갖춘다.

3) IC 카드 분실·도난 방지

이용자의 실수에 의한 IC 카드의 분실 가능성은 항상 존재한다. 이를 위해서 IC 카드 자체에 잠금 기능을 설치하고, 리로드시 패스워드 체크기능을 갖춘다. 또한 도난·분실시 사고설정 기능과 잔고 보증 기능을 가진 IC 카드를 사용한다.

또한 전자화폐 데이터의 전체 또는 일부의 백업으로 분실, 도난시에 소정기관에 신청하여 분실한 전자화폐를 무효로 할 수 있다.

전자화폐 시스템을 구성하는 요소별로 존재하는 위협에 대해 정리하면 〔표 1〕로 요약된다.

표 2. 구성요소별 위협의 존재

위협요소 \ 구성요소	이용자	상점	금융 기관	발행 기관	인증/등록기관	수사 기관	제조 업체
비밀키 유출			○	○			
IC 카드 부정 발행				○			
부당인출		○	○				
가치의 무단절취		○	○				
IC 카드 분실, 도난	○						
전자화폐 인출의 부인	○						
프라이버시 침해	○				○	○	
부정사용	○	○					
매상데이터조작		○					
부정등록	○				○		
개인정보유출			○	○	○	○	
부정거래	○	○					
부정한 카드,칩 유출							○
도난, 폐기된 카드의 부정사용							○

3. 전자화폐 시스템 프로토콜

전자화폐 시스템의 구성요소간 정보흐름은 프로토콜로서 표현된다. 전자화폐 시스템의 각 단계에서 필요한 프로토콜 및 기능은 다음과 같다.

3.1 이용자 등록 프로토콜

전자화폐 이용자는 자신의 신분을 확인시키고 정당한 전자화폐를 발행 받기 위해서 자신의 ID, 공개키를 인증/등록기관에 등록하고, 등록서를 수령한다.

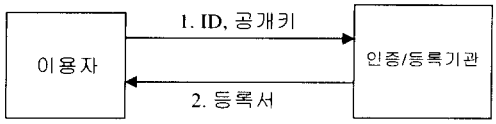

그림 2. 이용자 등록 프로토콜

3.2 전자화폐 인출 프로토콜

전자화폐의 인출은 이용자가 금융 기관으로부터 전자화폐를 취득하는 것이다. 전자화폐의 인출처리는 먼저 금융 기관이 전자화폐 발행기관으로부터 전자화폐 생성 요구를 하면 발행기관은 금융 기관에게 전자화폐를 생성하여 준다. 이용자는 등록/기관에서 이용자 인증과정을 위해 받은 등록서와 인출요구 정보를 금융 기관에 전송하여 금융 기관으로부터 전자화폐를 취득할 수 있다.

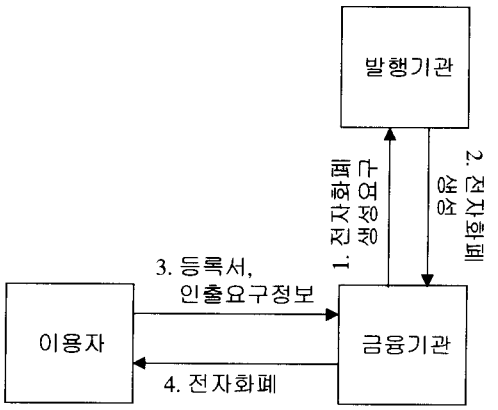

그림 3. 전자화폐 인출 프로토콜

3.3 전자화폐 지불 프로토콜

이용자는 상점/가맹점으로부터 challenge를 받고 이에 상응하는 응답(response)을 통해서 정당한 사용자라는 것을 확인시켜주고 전자화폐를 지불하고 서비스나 상품을 받는다.

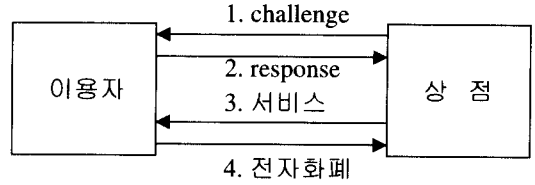

그림 4. 전자화폐 지불 프로토콜

3.4 전자화폐 예치(환류) 프로토콜

전자화폐가 일정량 축적된 시점에서 상점은 자신의 구좌에 파일전송의 형태로 해당 금융 기관에 입금한다.

금융 기관은 발행기관으로 전자화폐를 송부하고 이에 상응한 금액을 이체 받는다.

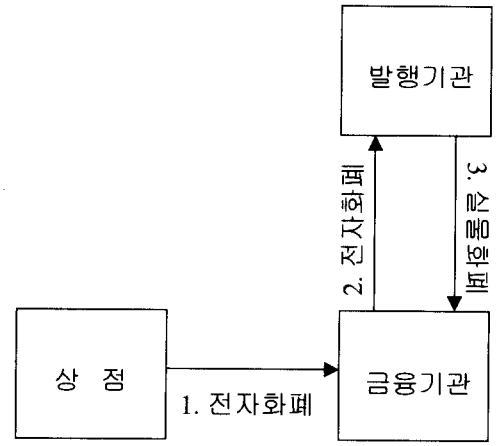

그림 5. 전자화폐 예치(환류) 프로토콜

3.5 이용자/전자화폐 추적 프로토콜

이용자가 전자화폐를 부정 사용시 수사 기관은 금융 기관과 인증/등록기관의 협조를 얻어 전자화폐/사용자를 추적한다.

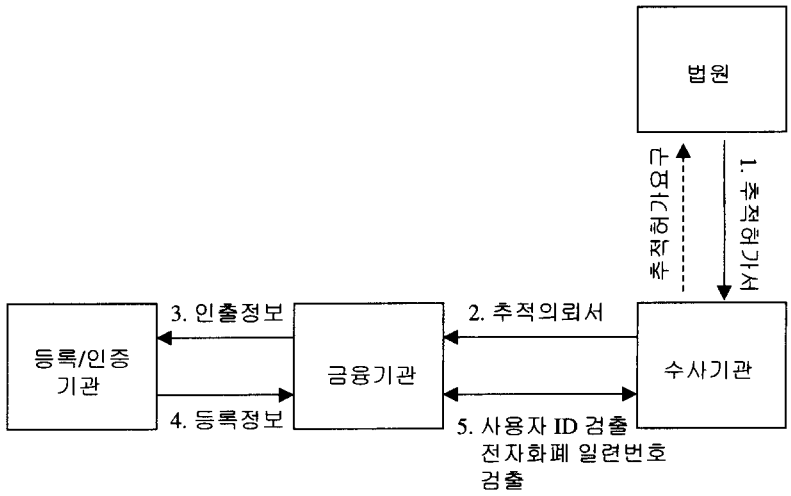

그림 6. 이용자/전자화폐 추적 프로토콜

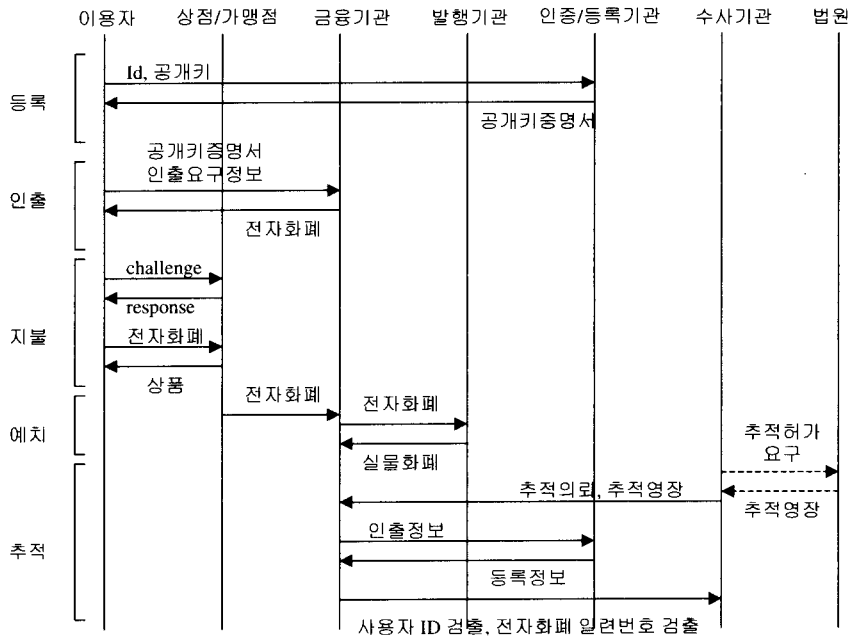

그림 7. 전체 프로토콜 구조

4. 정보보호 기능 표준

전자화폐의 보급에는 정보보호 기능의 확보가 가장 중요한 과제 중의 하나이며 전자화폐 시스템의 각 구성요소마다 존재하는 여러 가지의 위협에 대한 대책을 세울 필요가 있다. 특히 IC 카드의 위조, 또는 단말기 소프트웨어의 개조 등에 의해 부정으로 화폐가 발행된 경우 피해가 상당히 크다.

전자화폐 시스템의 정보보호 기능은 데이터 및 소프트웨어의 안전성, 정당성, 기밀성 확보 및 허위거래나 거래부인을 방지하도록 설계되어야 한다. 본 기능 표준은 전자화폐 시스템의 리스크

에 대응하기 위해 실현해야할 정보보호 기능에 대하여 기술한다.

전자화폐 시스템 정보보호 대책의 주요 기술은 암호이다. 전자화폐 시스템의 안전성을 보증하기 위해서 암호기술을 사용하는 주요 목적은 다음과 같다.

① 가치 이전 데이터의 기밀성 확보
② 단말기와 IC 카드의 인증 기능(위조 IC 카드 혹은 단말기 사용 방지 기능)
: IC 카드형 전자지갑은 상점 및 가맹점의 단말기로부터 인증을 받아야 한다.
③ 전자화폐 발행시 사용자 인증
④ 전자화폐 등의 가치이전 정보의 무결성 검증
⑤ 거래 부인 방지

다음에서는 전자화폐 시스템을 안전하게 구현하기 위해 필요한 정보보호 기능에 대하여 기술한다.

4.1 데이터나 소프트웨어의 개조, 변조 방지

○ 데이터나 소프트웨어는 개조할 수 없는 장치내에 보관.
○ 각 전자화폐 기기는 운용기관이 감시할 수 있도록 개조의 시도 또는 실제에 행해지는 증거를 보유.
○ 소매업자의 전자화폐 기기에서 의심스러운 정보가 검출되었을 경우 운용기관에 온라인 접속하고 해당거래에 대한 승인을 받음.
○ 운용기관은 각 전자화폐 기기를 시스템으로부터 제외 또는 사용불능으로 하는 것이 가능하게 함.
○ 전자화폐 기기에는 유효기한을 설정.
○ 전자화폐의 충전 및 회수처리 때는 전자화폐 기기 중의 보안 정보를 갱신.
○ 지불 거래 전자 문서에는 카드에 고유 암호키를 사용해서 전자적으로 서명.
○ 전자화폐 기기는 서로 정당한 기기라는 것을 확인. 즉, 상호인증.
○ 거래의 일련번호를 확인.
○ shadow balance (지금까지의 발행이력 및 회수이력으로부터 계산되는 각 카드잔고의 추정치)를 갖고, 인증시에 실제의 잔고와 큰 차이가 없는지를 확인.

4.2 거래 문서나 정보의 개조, 변조방지

○ 챌린지-응답법에 의해 자신의 정당성을 증명한 후 거래를 개시.
○ 거래시 전자문서의 교환은 거래 절차 및 세션키에 의해 통제.
○ 거래시 전자문서가 위·변조되지 않았는지를 (무결성을 만족하고 있는가) 해쉬 알고리즘이나 메시지 인증자(MAC)에 의해 확인.
○ 거래 전자문서의 정당성은 디지털 서명에 의해 보증.
○ 거래 일련번호의 정당성 확인.
○ 거래 전자문서중의 타임 스탬프에 대한 정당성 확인.
○ 거래할 때마다 변경되는 세션키를 사용.
○ 소비자가 전자화폐의 IC 카드에의 충전이나 은행구좌에의 예금을 할 경우에는 비밀번호를 입력.
○ 통계적 분석에 의해 의심스런 지불 패턴을 검출.

4.3 거래의 부인 방지

○ 발행기관은 거래 기록을 취득하여 보관.
○ 일정수의 거래는 IC 카드상에 기록되어 카드 보유자가 확인 가능하도록 함.
○ 각 거래는 거래번호에 의해 식별되고 또 타임 스탬프에 의해서도 식별.
○ 거래는 사용자와 상점에 의해 디지털 서명.
○ 등록/인증기관은 공개키의 데이터베이스를 관리.

4.4 암호키의 공격 방지

○ 암호키는 개조할 수 없는 기기에 보관
○ 단말기기는 해독된 키의 리스트 보유.
○ 비밀키와 암호알고리즘을 정기적으로 변경하거나 또는 긴급시 즉시 변경하도록 한다. 이때 키는 유효기간을 설정.
○ 엄격한 키 관리 실시.
○ 암호시스템은 제 3자의 평가를 받고 여러 가지 절차의 외부 감사를 받는다.

4.5 범죄 행위에의 사용 방지

○ 각 거래는 거래 식별자에 의해 고유식별이 가능.

○ 각 거래에 대한 전자문서를 디지틀 서명
○ 전자화폐 기기는 은행시스템과 접속하는 것을 의무화.
○ 통상의 패턴에서 벗어난 지불패턴을 검사.
○ 전자화폐 기기나 또는 각 거래마다 사용할 수 있는 전자화폐 한도액을 설정.
○ 가치를 보관하는 기기 (IC 카드)를 등록하고 은행구좌에 연결.
○ 기기의 보유자를 명확하게 한다.
○ 사용자와 상점/가맹점의 범죄 이력을 체크.
○ 전자화폐 시스템에 참가하는 금융 기관을 모니터링.

전자화폐 시스템을 각각 구성하는 요소별로 필요한 요구사항에 대해 정리하면 〔표 2〕로 요약된다.

또한, 전자화폐 시스템의 보안서비스별 정보보호기능에 대해 정리하면 〔표 3〕으로 요약된다.

표 2. 구성요소별 요구사항

구성요소 / 요구사항	이용자	상점	금융기관	발행기관	인증/등록기관	수사기관	제조업체
안전성(가치이전)	○	○	○	○			○
위조불가능성	○	○			○	○	○
프라이버시	○		○	○	○	○	
오프라인성		○	○	○			
양도성	○	○	○	○			
분할성	○	○	○	○			
익명성취소	○		○	○	○	○	

V. 결론

전자화폐는 암호기술 등의 고도 정보통신 기술 등에 의해 그 편리성과 안전성이 유지되고 있다. 급속한 정보기술 개발의 움직임 속에 전자화폐가 향후 기술적, 상업적으로 크게 발전할 것을 고려하면 민간부문이 기술개발이나 창의에 근거한 자유로운 설계·개발을 행하고, 다양하게 제공되는 서비스들 중에서 이용자가 그 요구에 따라 원하는 서비스를 선택하도록 함으로써 전자화폐의 건전한 발전을 도모하는 것이 필요하다.

본 논문은 이러한 전자화폐 시스템을 구현함에 있어서 기초가 될 수 있는 정보보호기능을 제시하였다. 전자화폐 시스템 구성요소 기능 모델은 국제결제은행의 단일 발행기관 모델[10]을 기초로 하였으며 구성요소별 정보보호기능은 각국의 실용화 모델[11]을 참고로 하였다. 특히, 몬덱스 및 NTT 전자화폐 시스템[12]의 정보보호기능을 참고로 하였다.

또한, 국제결제은행에서 발행된 문서와 각국에서 실용화중인 시스템 가이드라인[10]을 근거로 하여 국내 전자지불시스템뿐만 아니라 국내외 전자상거래에도 사용될 수 있도록 작성되었으므로 전자화폐 시스템의 관리와 운영을 용이하게 할 수 있는 안전한 시스템 구현의 기초가 될 것이다.

표 3. 보안서비스별 정보보호기능

보안서비스	위협	정보보호기능
기밀성 확보	데이터나 소프트웨어의 개조, 변조	○ 데이터나 소프트웨어는 개조할 수 없는 장치내에 보관. ○ 각 전자화폐 기기는 운용기관이 감시할 수 있도록 개조의 시도 또는 실제에 행해지는 증거를 보유. ○ 소매업자의 전자화폐 기기에서 의심스러운 정보가 검출되었을 경우 운용기관에 온라인 접속하고 해당거래에 대한 승인을 받음. ○ 운용기관은 각 전자화폐 기기를 시스템으로부터 제외 또는 사용불능으로 하는 것이 가능하게 함 ○ 전자화폐 기기에는 유효기한을 설정. ○ 전자화폐의 충전 및 회수처리 때는 전자화폐 기기 중의 보안 정보를 갱신. ○ 지불 거래 전자 문서에는 카드에 고유 암호키를 사용해서 전자적으로 서명. ○ 전자화폐 기기는 서로 정당한 기기이라는 것을 확인 즉 상호인증. ○ 거래의 일련번호를 확인. ○ shadow balance (지금까지의 발행이력 및 회수이력으로부터 계산되는 각 카드잔고의 추정치)를 갖고, 인증시에 실제의 잔고와 큰 차이가 없는지를 확인.
무결성 검증	거래문서, 정보의 개조, 변조	○ 챌린지 응답법에 의해 자신의 정당성을 증명한 후 거래를 개시. ○ 거래 전자문서의 교환은 거래 절차 및 세션키에 의해 통제. ○ 거래 전자문서를 위·변조가 되지 않은 본래의 문서(무결성을 만족하고 있는가)를 해쉬 알고리즘이나 메시지 인증자(MAC)에 의해 확인. ○ 거래 전자문서의 정당성은 디지털 서명에 의해 보증. ○ 거래 일련번호의 정당성 확인. ○ 거래 전자문서중의 타임 스탬프의 정당성 확인. ○ 거래할 때마다 변경되는 세션키를 사용. ○ 소비자가 전자화폐의 IC 카드에의 충전이나 은행구좌에의 예금을 할 경우에는 비밀번호를 입력. ○ 통계적 분석에 의해 의심스런 지불 패턴 검출
정당성 확인, 인증기능	거래의 부인	○ 발행기관은 거래 기록을 취득하여 보관. ○ 일정수의 거래는 IC 카드상에 기록되어 카드보유자가 확인 가능하도록 함. ○ 각 거래는 거래번호에 의해 식별되고 또 타임 스탬프에 의해서도 식별. ○ 거래는 사용자와 상점에 의해 디지털 서명. ○ 등록/인증기관은 공개키의 데이터베이스를 관리.
	범죄행위에의 사용	○ 각 거래는 거래 식별자에 의해 고유식별이 가능. ○ 각 거래 전자문서를 전자적으로 서명. ○ 전자화폐 기기는 은행시스템과 접속하는 것을 의무화. ○ 통상의 패턴에서 벗어난 지불패턴을 검사. ○ 전자화폐 기기마다 또는 거래마다 취급할 수 있는 한도액을 설정. ○ 가치를 보관하는 기기 (IC 카드)를 등록하고 은행구좌에 연결. ○ 기기의 보유자를 명확하게 한다. ○ 사용자와 상점/가맹점의 범죄 이력을 체크. ○ 전자화폐 시스템에 참가하는 금융 기관을 모니터링.
	암호키의 공격	○ 암호키는 개조할 수 없는 기기에 보관 ○ 단말기기는 해독된 키의 리스트 보유. ○ 비밀키와 암호알고리즘을 정기적으로 변경. 또, 긴급시 즉시 변경하도록 한다. 이때 키는 유효기간 설정. ○ 엄격한 키 관리 실시. ○ 암호시스템은 제 3자의 평가를 받고 여러 가지 절차의 외부 감사를 받는다.

참 고 문 헌

[1] S.Brands. "Untraceable off-line Cash in Wallets with Observers," *Pro-ceedings of Crypto '93*,pp. 302-318

[2] 전자지불 표준동향 분석에 관한 연구보고서, *한국전산원*, 1998.6

[3] 전자지불시스템 요구사항(한국전산원 번역), *St.Gallen 대학교 경영정보연구소*, 1996

[4] 오형근, 이임영, "전자화폐 시스템 개발 동향", 통신정보보호학회지 제9권 제1호, 한국통신정보보호학회, pp.13-32, 1999

[5] J.Camenisch. U. Maurer. M. Stadler. "Digital Payment Systems with Passive Anonymity-Revoking Trustees." *Cumputer Security - ESORICS 96*. pp. 33-43

[6] 오형근, 이임영, "익명성 제어와 화폐 분할 기능을 가지는 효율적인 전자화폐 프로토콜", 정보과학회 논문지(A) Vol 6, No 7, 한국정보과학회, pp.839-846, 1999

[7] D Chaum, "Blind Signatures for Untraceable Payments," *Advances in Cryptology - Proceedings of Crypto '82*, 1983. pp. 199-203

[8] D. Chaum, A. Fiat and M. Naor. "Untraceble Electronic Cash." *Advances in Cryptology - Proceedings of Crypto '88*. pp.319-327

[9] S. von Solms and D. Naccache. "On Blind Signatures and Perfect Crimes." *Computers and Security*. 11(1992) pp. 581-583

[10] Security of Electronic-money, *Bank for international Settlements*, 1996.

[11] 한국형 전자화폐를 활용한 유통시스템 모델 연구, *한국정보통신진흥협회*, 1997.12

[12] NTT 전자화폐 시스템 보고서, *NTT 정보통신연구소*, 1997

[13] First Virtual사, http://www.fv.com

[14] CyberCash사, http://www.cybercash.com

[15] DigiCash사, http://www.digicash.com

[16] 몬덱스사, http://www.mondex.com

著者紹介

송유진

1982년 2월 한국항공대학교 졸업
1987년 2월 경북대학교 석사
1995년 2월 일본동경공업대학교 박사
1986년~1988년 LG정보통신
1988년~1996년 한국전자통신연구원
1996년 ~ 현재 동국대학교 정보산업학과, 국제정보대학원 정보보호학과 교수
관심분야 암호이론, 인증 및 부호화이론, 전자상거래 응용, 전자화폐등

오형근

1998년 2월 순천향대학교 전산학과 졸업(학사)
1998년 3월 ~현재 순천향대학교 대학원 전산학과 석사과정 재학중

주관심분야 : 전자화폐, 전자상거래, 암호이론

이임영

1981년 홍익대학교 전자공학과 졸업(학사)
1986년 일본 오오사카대학 통신공학부(석사)
1989년 일본 오오사카대학 통신공학과(박사)
1992년 ~1994년 한국전자통신 연구원 선임 연구원
1994~ 현재 순천향대학교 컴퓨터학부 교수