네트워크형 전자화폐 표준(안)에 관한 고찰

장석철, 이임영
순천향대학교 정보기술공학부

A Study on Standard Draft of Network type Electronic Cash

Seok-Cheol Jang, Im-Yeong Lee
Division of Information Technology Eng. Soonchunhyang University

요 약

최근 정보통신기술의 발전과 인터넷의 폭발적인 사용자 증가로 인해 전자상거래가 활성화되고 있다. 또한 다양한 전자지불 시스템의 등장으로 이와 관련된 시장이 급성장하고 있다. 하지만 이러한 급성장에 비해 전자지불 시스템에 대한 표준화 작업이 더디게 진행되고 있다. 이에 본 논문에서는 표준화에 필요한 요구조건, 참여개체 역할 및 기능을 설명하고 전자지불 시스템의 한 부분인 네트워크형 전자화폐 표준(안)을 제시한다.

1. 서론

최근 정보통신기술의 발전과 인터넷의 폭발적인 사용자 증가에 다양한 응용프로그램들이 나오고 있다. 이중 기존 상거래 개념을 오픈네트워크인 인터넷 세계로 옮긴 것이 전자상거래라 할 수 있다.

이러한 전자상거래와 관련된 표준을 분류하는 방법은 여러 형태가 있으며 주요 부분으로서, CALS 절차, 전자지불, 데이터 형식 및 변환, 코드 및 검색, 통합 데이터베이스, 동시공학, 분산처리, 암호화, 보안·인증 그리고 통신 프로토콜 등이 있다.

대부분의 표준화는 국가 주도의 표준화 추진보다는 관련 기업들의 주도로 이루어지고 있다. 즉 국가 차원이 아닌 민간 차원에서 이루어지고 있다.

현재 우리 나라도 표준화에 대한 필요성을 인식하고 있어 정보통신부와 산업자원부가 이에 대한 제반 사항을 지원하도록 하고 있다. 특히 전자상거래 환경을 지원하기 위해 1999년도에 전자서명법과 전자거래 기본법을 제정하였고 이들 법에는 표준화의 부문이 포함되어 있다. 이와 관련하여 주요 관심 대상인 전자상거래 표준으로는 전자카탈로그 표준과 전자 지불 시스템의 전자화폐 등과 관련된 표준이다.

특히, 전자지불은 지급형태에 따라 민간 차원에서의 다양한 표준안이 제시되고 있다. IC카드형 전자화폐 경우는 Mondex라는 전자화폐가 사실상 국제적인 표준안이 되었고, 국내는 12개 은행과 1개 카드사 및 3개 VAN사가 참여하는 금융공동 전자화폐인 K-CASH가 사실상 표준안으로 제시되고 있다. 또한 산업자원부가 1999년부터 국제 표준과 호환이 되는 개방형 전자화폐 개발 사업을 진행하고 있고, 많은 벤처기업과 연구소들이 차세대 전자화폐 기술에 대해 연구를 진행하고 있다.

하지만 네트워크형 전자화폐에 대한 표준은 아직까지 미비하다. 따라서 본 논문에서는 우리 나라의 IC카드형 전자화폐의 표준(안)이라 할 수 있는 K-CASH를 기초로 하여 인터넷상에서 사용할 수 있는 네트워크형 전자화폐 표준(안)을 제시하려 한다.

2. 용어 정의

이 논문에서 사용할 용어에 대해서 다음과 같이 정의한다.

- 전자지갑 : 전자화폐를 저장할 수 있는 소프트웨어로서 전자화폐 발행은행이 이를 구현하여 사용자에게 제공
- 실계좌 : 전자화폐 발행은행에 사용자가 Off-line으로 등록하여 실생활에서 실제로 현금을 입·출금할 수 있는 계좌
- 인터넷계좌 : 전자화폐 발행은행이 인터넷상에서 사용

본 연구는 정보통신부의 ITRC(Information Technology Research Center)사업에 의해 수행된 것 임.

할 수 있도록 사용자에게 발급해주는 계좌로서 실제 전자화폐에 대한 거래 내용을 관리해 주는 계좌
- 인증서 : 신뢰할 수 있는 공인인증기관에 의해 발행되는 것으로 인증기관이 사용자를 인증하는 전자증명서 역할을 수행

3. 요구사항

금융감독원에서 제시한 전자금융 안전대책 기준에서의 전자지불 시스템에 대한 안전기준은 다음과 같다[1].
- 모든 거래 정보는 암호화 통신
- 거래 당사자 확인을 위한 전자 인증서 사용
- 전자지불 중계기관(gateway)에서의 금융거래정보 해독 및 기록 금지
- 금융기관과 전자지불 중계기관과의 접속은 전용회선 사용

4. 참여개체 역할 및 기능

본 논문에서 제시한 표준(안)에 실질적으로 참여하는 개체들에 대한 역할 및 기능을 설명한 것이다.

[전자화폐 발행은행]
- 사용자와 쇼핑몰의 실계좌를 가지고 있는 기관으로 우리 나라 모든 금융기관이 이에 해당한다.
- 기능
  - 전자화폐 발행 및 관리
  - 사용자와 쇼핑몰의 실계좌와 인터넷계좌 관리
  - 인터넷계좌와 실계좌 사이의 거래내역 관리
  - 메시지에 대한 암·복호화 기능

[쇼핑몰]
- 전자화폐를 통해 상품을 사용자가 구입할 수 있는 인터넷 상점이다.
- 기능
  - 전자화폐 발행은행에 실계좌와 인터넷계좌를 보유
  - 사용자가 구매한 구매내역을 사용자 전자지갑을 통해 전자화폐 발행은행에 전송
  - 사용자에게 영수증을 발행해 줄 의무

[사용자]
- 전자화폐 발행은행으로부터 전자화폐를 발급 받는 자이다.
- 기능
  - 전자화폐 발행은행에 실계좌와 인터넷계좌를 보유
  - 전자화폐를 사용 또는 관리

[사용자 전자지갑]
- 사용자, 쇼핑몰 및 전자화폐 발행은행과의 연결을 도와주는 소프트웨어이다.
- 사용자는 전자화폐 발행은행으로부터 다운로드 받아 설치할 수 있다.
- 기능
  - 전자화폐 구입
  - 전자화폐 잔액 표시
  - 메시지에 대한 암·복호화 기능

5. 프로토콜

본 장에서는 표준(안)으로 제안한 네트워크형 전자화폐 프로토콜이다.

우선 요구사항에 맞게 모든 거래는 공인 인증서를 통해 이루어지고 거래 내용은 모두 암호화를 통해 이루어진다라고 가정한다. 또한 실계좌 번호는 이미 사용자 또는 쇼핑몰이 오프라인 상으로 등록 후 발급 받은 상태라고 가정한다.

그림 1은 네트워크형 전자화폐에 대한 표준(안)을 제시하고 각 단계별 기능과 절차를 설명한다.

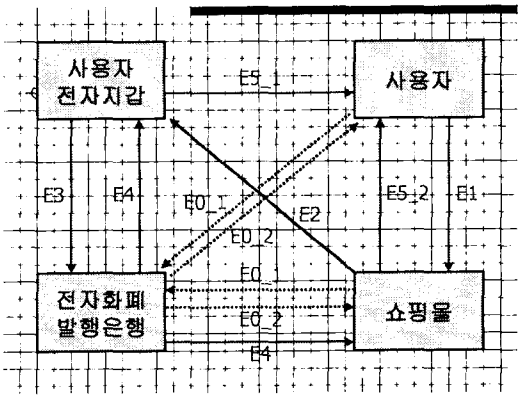

그림 1. 네트워크형 전자화폐 프로토콜 표준(안)

[E0_1 (사용자, 쇼핑몰 → 전자화폐 발행은행)]

사용자 또는 쇼핑몰이 최초 등록 시 전자화폐 발행은행에 자신의 인터넷계좌를 발급 받기 위해 개인 정보를 입력하는 단계이다.

[E0_2 (전자화폐 발행은행 → 사용자, 쇼핑몰)]

전자화폐 발행은행이 사용자 또는 쇼핑몰에게 인터넷계좌를 발급 해 주고 사용자 또는 쇼핑몰이 원하는 전자화폐를 발행해 주고 사용자 또는 쇼핑몰은 전자지갑을 다운로드 받아 설치하는 단계이다.

[E1 (사용자 → 쇼핑몰)]

사용자가 쇼핑몰에게 상품을 주문하고 결제를 요청하는 단계이다.

[E2 (쇼핑몰 → 사용자 전자지갑)]

사용자가 주문한 상품에 결제를 위해 쇼핑몰이 전자지갑에 결제 정보를 전송하는 부분이다.

[E3 (사용자 전자지갑 → 전자화폐 발행은행)]

사용자가 전자지갑을 통해 결제를 승인하면 실행되는 단계로 전자화폐 발행은행에 결제 금액이 가능한지를 확인하는 단계이다.

[E4 (전자화폐 발행은행 → 사용자 전자지갑, 쇼핑몰)]

결제가 올바르게 이루어지면 사용자 전자지갑 또는 쇼핑몰에 결제 처리 결과를 전송하는 단계이다.

[E5_1 (사용자 전자지갑 → 사용자)]

사용자 전자지갑이 전자화폐 발행은행으로부터 전송받은 처리 결과 값을 사용자에게 보여주는 단계이다.

[E5_2 (쇼핑몰 → 사용자)]

쇼핑몰이 사용자에게 상품구입에 대한 영수증을 발행하는 단계이다.

6. 데이터 형식

6.1 전체적인 데이터 형식

전체적인 데이터 형식은 그림 2와 같은 형태로 맞추어 보내진다.

데이터 형식에서 항목들에 대한 설명은 다음과 같다.

- Transaction Code : 각 단계별 코드를 나타낸다.
- Parameter Total Length : 뒤에 나오는 파라메터들의 길이
- Transaction Parameter : 파라메터들은 각 단계별 종류에 따라 다름.

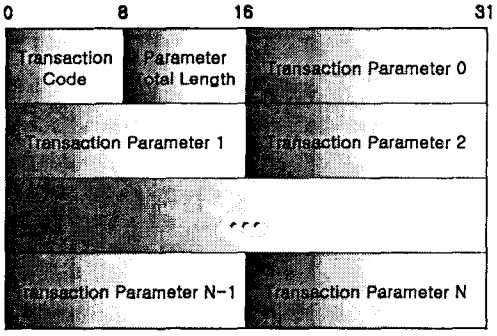

그림 2. 데이터 형식

6.2 각 단계별 데이터 형식

본 절에서는 네트워크형 전자화폐 시스템에서 각 단계별 데이터들이 어떻게 구성되어 있는지를 알아본다. 기본적인 데이터 구조는 그림 2와 같다.

[E0_1 (사용자, 쇼핑몰 → 전자화폐 발행은행)]

- Transaction Code : 0x01
- Transaction Parameter

이 메시지는 사용자 또는 쇼핑몰이 전자화폐 발행은행에 전송해야할 변수들이다. 데이터 형식은 표 1과 같다.

표 1. E0_1 단계에서 Transaction Parameter

Transaction Parameter	내 용
$ID_{(User,\ Shop)}$	사용자 또는 쇼핑몰 ID
$PW_{(User,\ Shop)}$	사용자 또는 쇼핑몰 패스워드
$RealAcct_{(User,\ Shop)}$	실계좌의 계좌번호
BankID	전자화폐 발행은행의 ID
$IABalance_{(User,\ Shop)}$	인터넷계좌의 잔액 (전자화폐 잔액)
EC	사용자 또는 쇼핑몰이 인출하려는 전자화폐 금액

만약 최초 거래 시에는 인터넷계좌의 잔액이 '0'으로 입력되어 처리된다.

[E0_2 (전자화폐 발행은행 → 사용자, 쇼핑몰)]

- Transaction Code : 0x02
- Transaction Parameter

이 메시지는 전자화폐 발행자가 사용자 또는 쇼핑몰에 전송해야할 변수들이다. 데이터 형식은 표 2와 같다.

표 2. E0_2 단계에서 Transaction Parameter

Transaction Parameter	내 용
$ID_{(User,\ Shop)}$	사용자 또는 쇼핑몰 ID
BankID	전자화폐 발행은행의 ID
$RealAcct_{(User,\ Shop)}$	실계좌의 계좌번호
$RABalance_{(User,\ Shop)}$	실계좌의 잔액
$InternetAcct_{(User,\ Shop)}$	인터넷계좌의 계좌번호
$IABalance_{(User,\ Shop)}$	인터넷계좌의 잔액 (전자화폐 잔액)
PNo	전자화폐 발행 거래번호

[E1 (사용자 → 쇼핑몰)]

- Transaction Code : 0x03
- Transaction Parameter

이 메시지는 사용자가 쇼핑몰에 전송해야할 변수들이다. 데이터 형식은 표 3와 같다.

표 3. E1 단계에서 Transaction Parameter

Transaction Parameter	내 용
$ID_{(User,\ Shop)}$	사용자 ID
ID_{Bank}	전자화폐 발행은행의 ID
$InternetAcct_{User}$	사용자의 인터넷계좌의 계좌번호
PaymentOk	결제승인
PaymentCancel	결제취소

여기서 결제에 대한 승인여부에 대한 파라미터는 PaymentOk 또는 PaymentCancel 중 하나만 선택되어야 한다.

[E2 (쇼핑몰 → 사용자 전자지갑)]
- Transaction Code : 0x04
- Transaction Parameter

이 메시지는 쇼핑몰이 사용자 전자지갑에 전송해야 할 변수들이다. 데이터 형식은 표 4와 같다.

표 4. E2 단계에서 Transaction Parameter

Transaction Parameter	내 용
ID_{User}	사용자 ID
ID_{Shop}	쇼핑몰의 ID
$InternetAcct_{Shop}$	쇼핑몰의 인터넷계좌의 계좌번호
OrderNo	주문번호
PaymentEC	결제금액

[E3 (사용자 전자지갑 → 전자화폐 발행은행)]
- Transaction Code : 0x05
- Transaction Parameter

이 메시지는 사용자 전자지갑이 전자화폐 발행은행에 전송해야할 변수들이다. 데이터 형식은 표 5와 같다.

표 5. E3 단계에서 Transaction Parameter

Transaction Parameter	내 용
ID_{User}	사용자 ID
ID_{Shop}	쇼핑몰의 ID
$InetnetAcct_{User}$	사용자의 인터넷계좌의 계좌번호
$InternetAcct_{Shop}$	쇼핑몰의 인터넷계좌의 계좌번호
OrderNo	주문번호
PaymentEC	결제금액

[E4 (전자화폐 발행은행 → 사용자 전자지갑, 쇼핑몰)]
- Transaction Code : 0x06
- Transaction Parameter

이 메시지는 전자화폐발행은행이 사용자 전자지갑 또는 쇼핑몰에 전송해야할 변수들이다. 데이터 형식은 표 6와 같다.

표 6. E4 단계에서 Transaction Parameter

Transaction Parameter	내 용
$ID_{\{UserShop\}}$	사용자 또는 쇼핑몰 ID
PNo	결제번호
OrderNo	주문번호
PaymentEC	결제금액
PaymentOK	결제 승인
PaymentCancel	결제 취소

여기서 결제에 대한 승인여부에 대한 파라미터는 PaymentOk 또는 PaymentCancel 중 하나만 선택되어야 한다. 만약 PaymentOK이면 표 6에서 PaymentCancel을 제외한 나머지 데이터를 전송하고 PaymentCancel일 경우는 거래를 끝낸다.

[E5_1 (사용자 전자지갑 → 사용자)]

이 단계는 사용자 전자지갑이 사용자에게 결제 처리에 대한 정보를 보여주기 위한 부분으로 사용자 전자지갑이 시각적으로 보여주는 역할만 함으로 데이터에 대한 이동은 없다.

[E5_2 (쇼핑몰 → 사용자)]
- Transaction Code : 0x07
- Transaction Parameter

이 메시지는 쇼핑몰이 사용자에게 전송해야할 변수들이다. 데이터 형식은 표 7와 같다.

표 7. E5_2 단계에서 Transaction Parameter

Transaction Parameter	내 용
$ID_{\{User, Shop\}}$	사용자 ID
$ID_{\{Shop\}}$	쇼핑몰 ID
Rec	영수증 정보

7. 결론

정보통신과 인터넷의 발전으로 많은 변화가 있었다. 이러한 변화들 속에 가장 많은 발전을 한 부분이 전자상거래 관련부분이다. 또한 표준화 작업도 가장 활발하게 진행되고 있다. 하지만 이러한 환경 속에서도 아직까지 미비한 부분이 지불관련 표준화이다. 국가나 민간이나 모두 민감한 부분이기 때문에 표준화 과정이 늦어지고 있다. 특히 IC카드형 전자화폐에 대한 민간차원에서의 표준(안)으로 국제적으로 Mondex가 있고 국내적으로는 K-CASH가 있다 하지만 네트워크형 전자화폐에 대한 표준으로 제시된 것은 없다. 이에 본 논문은 네트워크형 전자화폐의 표준(안)을 제시하였다. 본 논문에서 제시한 표준(안)이 향후 네트워크형 전자화폐 표준화 작업에 많은 기여를 할 수 있기를 바란다.

[참고문헌]

[1] 금융감독원 정보기술검사국, "전자금융 안전대책기준", http://www.fss.or.kr/data/brd/043/전자금융안전대책기준.hwp

[2]금융결제원, "금융 IC카드 표준", http://www.kftc.or.kr/board_data/ED/950_금융IC~1.HWP