情報保護學會論文誌
第17卷 第1號, 2007. 2

전자 상거래에서 거래 인증 모델 연구

이 창 열[1†]
[1]동의대학교

A study of the transaction certification model in the e-commerce

ChangYeol Lee[1†]
[1]Dongeui University

요 약

온라인 거래에서, 투명성은 전자상거래에 대한 과세나 고객의 권리를 위한 주요 요소이다. 오프라인에서 거래에 대한 신뢰성은 금전등록기 개념을 사용해서 이루어지고 있는 것처럼, 우리는 거래의 투명성을 위한 온라인 개념의 거래 등록기 모델을 연구하였다. 비록 온라인 거래 등록기가 전자상거래법과 관련되어서 사용될 수 있지만, 여기서는 등록기의 메카니즘에 대한 연구만을 고려하였다. 거래 등록기는 디지털 영수증을 발행하며, 영수증은 본 논문에서 개발한 모델로 진위가 판별될 수 있다.

ABSTRACT

In on-line transaction, the transparency is the key factor for the taxation and customer's rights. Using the cash register concept of the off-line transaction, we studied on-line transaction register model for the e-commerce transparency. Although on-line transaction register may be used under the related e-commerce laws, in this paper, we only considered the mechanism of the register. The register issues the digital receipt, and then the receipt can be verified the validation by the models developed in this paper.

Keywords : *transaction certificate, e-commerce, transaction register model, digital receipt*

I. 서 론

OECD(Organisation for Economic Co-operation and Development)는 온라인 거래에 세금을 부과하기로 결정하였고, 이에 대한 이행을 연기하고 있는 상태이다[1][2][3][4]. 우리나라도 OECD 국가와 마찬가지로 온라인 거래에 세금을 부여하고, 이에 대한 이행을 연기한 상태이다. 그러나 과세의 기반이 되는 온라인 거래의 투명성을 증명하기가 기술적으로 쉬운 문제는 아니다. 과세를 위하여 세무 기관은 온라인 판매업체(이하 ISP (Internet Service Provider)라는 용어를 사용할 예정임)의 거래 정보를 알아야 하지만 쉬운 일은 아니다.

전자상거래에서 또 다른 이슈는 구매한 디지털 콘텐츠의 반품이나, 구매한 콘텐츠가 부주의하게 삭제되었을 경우 콘텐츠의 재 다운로드와 같은 소비자의 권리에 관한 사항이 있다. 이런 종류의 권리는 디지털 영수증과 관련된 온라인디지털콘텐츠산업발전법 11조를 이용하여 행사될 수 있다[5].

실 세계에서 이런 문제는 매장의 금전 등록기를 사용하여 해결하고 있다. 구매에 대한 증거로 금전등록기에서 발행하는 영수증을 고객에게 제공하고 있으며, 금전

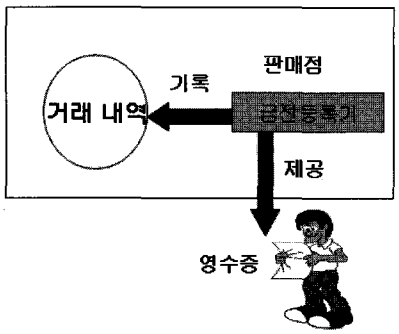
접수일 : 2006년 11월 23일; 채택일 : 2006년 12월 11일
† 주저자, lcy@deu.ac.kr

등록기는 내부적으로 또 다른 영수증을 발행하여 추후 세무 당국이 확인할 수 있게 함으로써 과세에 대한 투명성을 제공하고, 소비자에게 제공된 영수증은 추후 반품 등에 대한 소비자 권리를 이행할 때 사용될 수 있을 것이다[6][7]. 그러므로 금전 등록기는 상거래에서 고객의 권리를 보호하는 수단으로 작용할 수가 있다. 세무 당국에서 영수증은 부가가치세(VAT; Value Added Tax) 부과의 기본 정보가 되는 것이다.

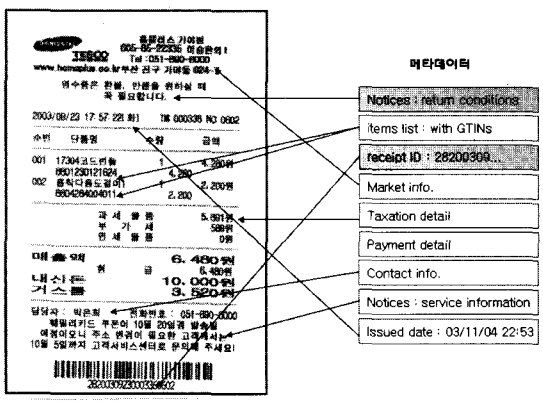
본 논문에서는 실 세계의 금전 등록기를 모방한 개념을 통하여 온라인 거래 등록기(Transaction Register) 모델을 제시하려고 한다. 온라인 거래 등록기를 사용하여 디지털 영수증을 발행하고, 고객은 디지털 영수증을 이용하여 고객의 권리 행사를 하고, 세무 당국은 이를 과세의 기반으로 사용할 수 있을 것이다.

Ⅱ. 금전등록기 모델

금전등록기 서비스 구조가 [그림 1]에 기술되었다.



[그림 1] 금전등록기 모델



[그림 2] 샘플 영수증

고객이 상품을 구매할 때 금전등록기는 구매 상품 내역을 포함하는 영수증을 발행한다. 예를 들어 그림 2는 금전 등록기에서 발행한 샘플 영수증이다. 샘플 영수증에는 구매 내역과 반품이나 소비자 권리 행사를 위하여 필요한 정보가 기술되어 있다. 그러나 영수증에는 고객 정보를 포함하지 않는다. 그것은 매장은 누가 해당 상품을 샀는지 알지 못한다는 것이다. 그러나 고객은 그가 구매한 상품을 판매한 매장을 알 수 있다. 즉 영수증은 양방향 정보가 아니라서 소비자의 사생활 보호 역할을 제공하고 있다.

또한 금전 등록기 내부에는 발행한 영수증의 복사본이 기록되어서 추후 과세 자료로 사용될 수 있을 것이다.

Ⅲ. 유통 모델 연구

3.1 해외 디지털 콘텐츠 권리 모델

1995년 디지털 콘텐츠 유통에 관한 연구로 IMPRIMATUR(Intellectual Multimedia Project Rights Model and Terminology for Universal Reference) 프로젝트가 3년간 진행되었다[8]. 프로젝트 결과로 나온 IMPRIMATUR Business Model은 디지털 콘텐츠 유통에서 통제 기관(Monitoring Service Provider)의 중요성을 보여주고 있다. MPEG-21[9] 프로젝트의 출발 모델 또한 IMPRIMATUR Business Model에서 시작되었다. MPEG-21은 Event Reporting 구조를 사용한 거래 개념을 보여주고 있다. IMPRIMATUR 프로젝트의 통제 기관이나 MPEG-21의 Event Reporting 구조는 온라인 디지털 콘텐츠 거래에서 투명한 거래 메카니즘을 표현하는 것을 가장 중요한 요소로 제시하고 있다. 즉 거래 정보가 제3기관으로 보고가 되는 메카니즘이 필요한 것이다.

3.2 국내 디지털 콘텐츠 유통 모델

우리나라의 거래 인증에 대한 연구는 온디콘법(온라인디지털콘텐츠산업발전법)에 따라 2002년부터 소프트웨어진흥원을 중심으로 연구된 다양한 연구와 관련된 논문에서 제시되고 있다[10][11][12]. 온디콘법에 의하면 디지털 콘텐츠에 대한 표시제도를 도입하고, 식별 표준 체계를 개발하며, 거래 및 품질인증을 시행하는 것으로 되어 있다.

표시제도는 디지털 콘텐츠 판매업체가 판매되는 디

지털 콘텐츠에 대한 정보를 소비자에게 제공함과 동시에, 소비자 권리 관리를 위한 관련 제도를 표시하는 것으로 [그림 3]과 같이 표시될 수 있을 것이다[13].

Ⅳ. 온라인 거래 인증 모델

4.1 개념 모델

온라인 거래 등록 모델은 [그림 4]처럼 거래인증기관, ISP, 그리고 소비자로 구성된 모델이다. 소비자가 온라인 거래를 하면 ISP는 디지털 영수증을 발행하고 해당 사항을 거래인증기관에 통보하는 형태로 구성되어 있다. 이때 발생할 수 있는 것이 소비자에게 제공하는 위조된 디지털 영수증이나 거래인증기관에 통보하는 위조된 거래 내역서 일 수 있다.

거래 내역서는 소비자에게 판매한 내역을 거래인증기관에 통보하는 것으로 헤더, 암호화된 영수증 리스트, 그리고 전자서명으로 구성된다.

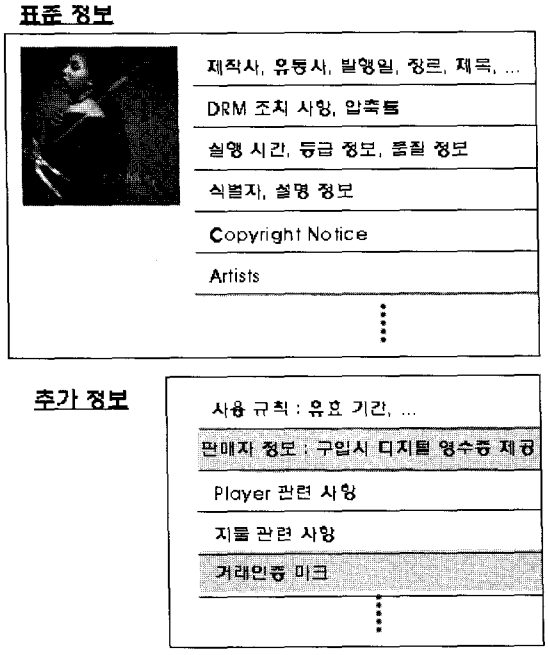
[그림 5]에 기술된 거래인증기관의 거래 내역서 관리기는 ISP와 소비자 사이 연계 역할을 한다. ISP로부터 거래 내역서를 받고, 디지털 영수증과 관련하여 소비자가 거래 확인 요청이 오면 응답을 하는 것이다. 이때 소비자가 제시한 디지털 영수증의 위조 여부를 거래 내역서 관리기는 판별할 수 있어야 한다.

4.2 거래 등록기 관리기

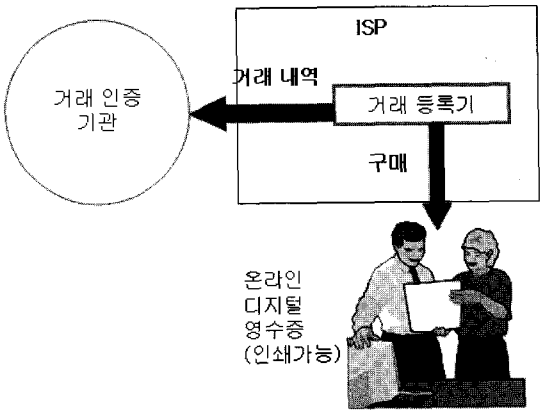
거래 등록기 관리기는 ISP에게 제공하는 거래 등록기를 생성하는 모듈이다. ISP가 거래 등록기를 요청시 ISP 정보를 이용하여 프로파일 정보를 만든다. 프로파일 정보는 모든 ISP 마다 다른 정보로 구성된다. 즉 거래 등록기 관리기로부터 만들어진 거래 등록기는 본 프로파일 정보를 내장하여 ISP에게 제공된다.

거래 등록기를 만드는 상세 단계를 살펴보면 다음과 같다 :

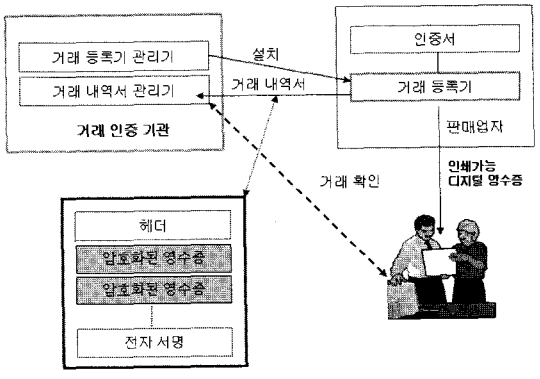
- ISP는 거래 인증 기관에 거래 등록기를 신청한다.
- 거래 인증 기관은 ISP의 회사 ID(사업자등록번호)



[그림 3] 샘플 표시 정보

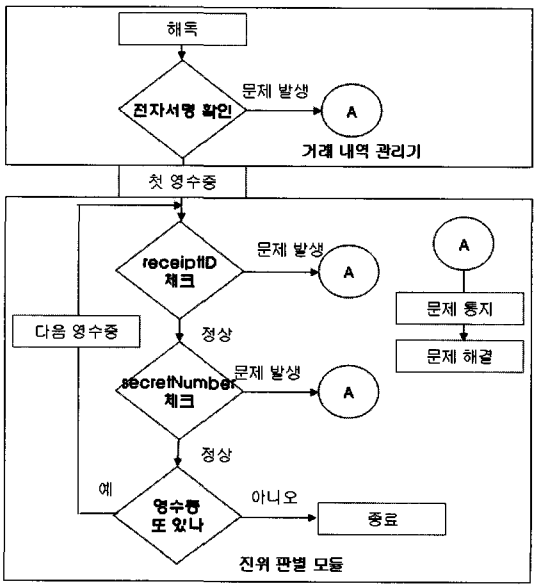


[그림 4] 거래 인증 개념 구조

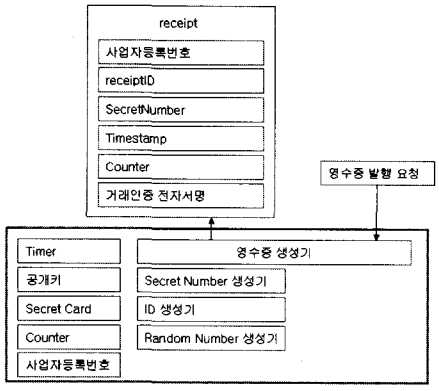


[그림 5] 거래 인증 모델

를 포함한 회사 정보를 받는다.
- 거래 등록기 관리기는 비 대칭키를 생성한다.
- 비밀키(private key)는 거래 등록기 관리기 내부에 저장하며, 추후 거래 등록기로부터 제공받는 거래 내역에 대한 암호를 해독할 때 사용한다.
- ISP를 위한 비밀 카드를 생성한다. 비밀 카드 개념은 현재 인터넷 뱅킹에서 사용하는 비밀 카드 개념과 비슷하다고 생각하면 될 것이다.
- 비밀 카드와 공개키 정보를 포함한 ISP를 위한 프로파일을 생성한다.
- 비밀 카드 내역을 복제하여 거래 등록기 관리기에 보관한다. 이것은 추후 소비자가 요청한 디지털 영수증에 대한 진위 파악과 거래 내역서의 진위 파악에 사용된다.
- 거래 등록기 관리기는 개별화된 프로파일을 포함하는 요청 기관의 거래 등록기를 생성한다. 거래 등록기 내부에 프로파일을 운영하는 규칙 정보가 포함되어 있다.
- 거래 등록기 관리기는 ISP에게 거래 등록기를 제공(다운로드)한다([그림 5]에 기술).



[그림 6] 진위 판별 모듈 처리 절차



[그림 7] 거래 등록기와 발행 영수증 구조

거래등록기가 사용하는 키 관리는 다음과 같다 :
- 프로파일에 있는 공개키는 거래 내역 암호화 용
- 자체 인증서의 비밀키는 전자서명 용
- 비밀 카드와 내부 규칙(뒤에 설명)은 *secretNumber* 생성용으로 사용

4.3 거래 내역서 관리기

4.3.1 거래 내역서 관리 모듈

ISP로부터 거래 내역서가 도착하면, 거래 내역서 관리기는 거래 내역의 전자 서명을 확인한 후 암호를 해독한다. 해독된 거래 내역은 개별 영수증의 변조가 없음을 확인하는 진위 판별 모듈로 보내진다. 만약 문제가 없으면 개별 영수증 정보는 거래 내역서 관리기에 저장된다.

4.3.2 진위 판별 모듈

진위 판별 모듈은 개별 영수증의 진위를 파악한다. [그림 6]에서 처럼 *receiptID*와 *secretNumber*를 사용하여 진위 파악을 한다. 이 모듈은 ISP의 거래 등록기의 *secretNumber* 생성과정의 순서를 진위판별 모듈에서 재현하여 진행하는 것이다. 자세한 *secretNumber* 생성 과정은 거래 등록기 모듈에서 설명할 것이다. 특정 ISP의 비밀 카드 내용은 해당 판매업자도 확인할 수 없으며, 오직 판매업자에게 제공된 거래 등록기 내부에서 관리되기 때문에 정보 유출 염려가 없고, 내부 알고리즘으로 생성된 *secretNumber*는 비밀 카드를 복제하여 가지고 있는 거래 인증 기관만 *secretNumber* 생성 과정을 수행하여 확인할 수 있는 것이다.

4.4 거래 등록기

4.4.1 내부 구조

〔그림 7〕처럼 거래 등록기는 고객의 요청에 따라 영수증을 발행한다. 영수증을 발행하기 위하여, 내부적으로 다양한 정보를 간직하고 있다. 영수증은 *receiptID, secretNumber*, Timstamp, Counter, 전자서명 등의 정보로 구성된다. 고객은 *receiptID*를 사용하여 진위 판별을 거래인증기관에 요청할 수 있으며, 거래인증기관은 *secretNumber*를 이용하여 거래 내역에 대한 진위 판별을 할 수 있게 시스템을 구성하였다.

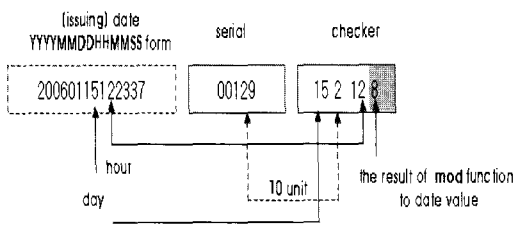
4.4.2 고객용 영수증 ID(receiptID) 생성

(1) 개념 구조

고객이 상품을 구매할 때, 거래 등록기는 저장 가능하고 인쇄 가능한 디지털 영수증을 발행하며, 해당 내역을 자동으로 즉시(아니면 주기적으로) 거래 인증 기관에 제공한다. 제공 시간은 시스템에 따라 다를 수 있지만, 영수증 내역은 거래 등록기 내부에 기록된다. 거래 내역은 거래 등록기의 프로파일에 있는 공개키를 사용하여 암호화되고, 전자서명을 한 후 거래 인증 기관에 제공된다. 거래 내역의 암호화는 거래 내역의 기밀성을 위하여 사용된다.

거래 등록기가 만드는 2개의 결과물(소비자를 위한 디지털 영수증과 거래 인증 기관을 위한 거래 내역)은 별도의 진위 판별 과정을 거친다.

2개의 결과물 중에 고객에게 제공되는 영수증에는 *receiptID*가 있다. *receiptID*의 구조는 그림 8처럼 순차번호(serial)와 검사기(checker)로 이루어진다. 순차번호는 "01"로 부터 시작하는 거래 등록기에서 발생하는 내부 영수증 발행 순서 번호이다. 검사기는 발행날짜와 순차번호로 부터 발생한다.



〔그림 8〕 샘플 receiptID 생성 규칙

〔그림 8〕의 검사기는 6개 숫자로 구성되었다. 첫 2수는 발행 날짜 정보에서 날짜 2자리이며, 2번째 1개 번호는 순차번호의 10 단위 자리에서 왔으며, 세 번째 숫자는 발행시간의 두 번째 자리에서 추출하였다. 마지막은 에러 체크 문자로 다음과 같은 방법으로 생성될 수 있다 :

```
char * checkDigit_generator(char * issuing_date)
{
    int i, result, sum = 0;
    char * last;
    for (i = 0; i < strlen(issuing_date); i++)
        sum = sum + atoi(issuing_date[i]);
    result = mod(sum, 11);
    if (result == 10) strcpy(last, "X");
      else
      { last[0] = number_to_string(result);
        last[1] = '\0'; }
return last;
}
```

(2) 진위판별 알고리즘

고객은 거래 인증 기관의 소프트웨어를 사용하여 디지털 영수증의 *receiptID*를 이용하여 영수증의 진위 여부를 확인할 수 있다. 진위 여부는 **validate** 메소드를 수행하여 판별한다.

validate 메소드는 *receiptID* 생성 방법과 동일한 방법으로 거래 내역서 관리기에서 ID를 생성하여 ID 위조를 확인한 후, ID 위조가 없으면, *receiptID*를 사용하여 구매한 내역을 제공한다. **validate** 메소드의 결과가 **Boolean** 형태가 아닌 것은 만약에 과거에 유효했던 남에게 제공한 *receiptID*를 ISP가 타인에게 부여시 ID 자체는 유효하지만 구매 내역이 다를 수 있기 때문에, 해당 사항을 고객이 판단하게 하는 것이다.

```
Char * validate(char * receiptID, char * issuing_date) {
char * comparingID, serial, first, second, third;
    strcpy(serial, substr(receiptID, 13, 5));
    strcpy(first, substr(issuing_date, 6, 2));
    strcpy(second, substr(serial, 3,1)
```

```
    strcpy(third, substr(issuing_date, 9, 1));
    strcpy(comparingID,
        strcat(serial, first, second, third,
            checkDigit_generator(issuing_date)));
  if(strcmp(receiptID, comparingID) !=0)
    return "receiptID is counterfeited"; /* 번호 위조 */
    return receipt_list(receiptID); /* 구매 내역 */
}
```

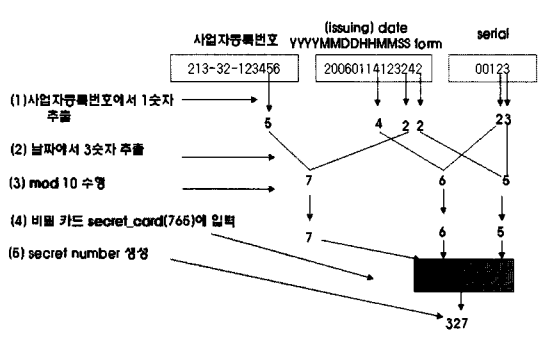
(3) 핵심사항

본 알고리즘의 핵심은 *issuing_date*에 의한 ID 생성에 있다. 거래 등록기는 발행날짜와 순차번호를 기반으로 *receiptID*를 생성한다. 비록 ISP가 영수증을 위조할 수 있지만, 발행날짜를 위조하는 것은 쉽지 않다. 왜냐하면 고객이 금방 알아차리기 때문이다. 〔그림 7〕의 *receiptID* 생성 과정은 샘플일 뿐이며, 중요한 것은 소비자에게 발행날짜를 일반적으로 속일 수 없으며, 또한 *receiptID* 생성 규칙을 모르기 때문에 본 ID 검증 체계는 안전하다는 것이다.

4.4.3 거래 내역서 비밀 번호(secretNumber) 생성

(1) 개념 구조

비밀 번호(secretNumber)는 거래인증기관이 ISP로부터 받은 모든 거래내역서의 진위판별을 하는 수단으로 사용한다. 비밀 번호 생성은 〔그림 9〕처럼 생성될 수 있다. 예를 들어, 〔그림 9〕의 샘플처럼 프로파일에 있는 정보와 상태 정보를 기반으로 생성된 코드(〔그림 9〕에서 1, 2, 3, 4단계)는 비밀 카드의 입력으로 사용하고 이를 통하여 나온 최종 결과(〔그림 9〕의 5단계)인 *secret-Number*를 사용한다.



〔그림 9〕 비밀 키 생성 사례

비밀 카드 모델은 인터넷 뱅킹[5]의 비밀 카드 개념을 사용한 것이다. 그러나 그림 9.의 단계 중 (3) 단계에서 생성되는 값(여기서는 "765")에 대한 유일성은 제공하지 않는다. 유일하지는 않지만 안전성은 보장되기 때문이다. 예를 들어 거래 내역을 제공하는데 있어서 만들어지는 최종 비밀키를 임의로 넣어서 우연히 맞힐 수는 있을 것이나, 연속성은 가지지 않는다. 또한 처음 위조 시도가 판정이 나면 해당 ISP는 감시 대상이 될 것이다.

(2) 알고리즘

〔그림 9〕의 (4) 단계는 다음과 같은 secret_card 함수를 사용하여 처리한다.

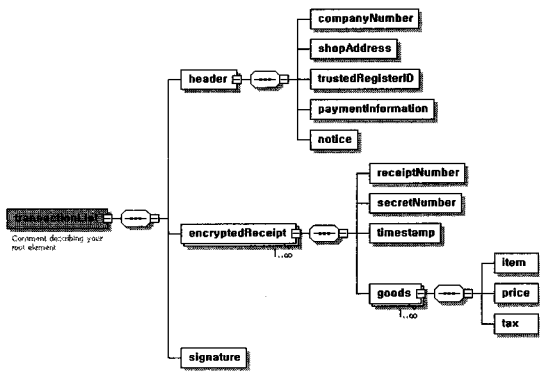
```
int card[1000]
 _init(){
  card[0] = 23; card[1] = 349; card[2] = 492; … ;
card[999]= 304;}

int secret_card(code){
return card[code];}
```

(3) 거래 내역서

거래 내역서는 판매업자가 거래 인증 기관에 보내는 메시지이다. 그것은 헤더, 암호화된 여러 개의 영수증, 그리고 전자서명으로 이루어진다. 암호화된 영수증은 핵심 요소인 *receiptID* 과 *secretNumber*을 포함한다. 거래 내역서 샘플 구조가 〔그림 10〕에 기술되었다.

4.4.4 위조 사례

(1) 고객 속이기



〔그림 10〕 샘플 거래 내역서 구조

• 임의로 receiptID 사용시
  – **validate** 함수로 판별됨
• 거래 등록기 사용하지 않고 디지털 영수증 발행
  – 유효한 과거 사용 receiptID 사용하고 날짜만 현재 것으로 변경
    • 거래인증기관의 **validate** 함수로는 진위 파악이 가능하다. 왜냐하면 *receiptID*는 날짜 기반 ID임.
  – 유효한 과거 발행 receiptID와 날짜 그대로 사용
    • 기본적으로 고객이 날짜 위조를 확인 가능
    • 만약에 고객이 확인 안하면, validate 함수에서 제공하는 구매 내역을 확인하여 수동적으로 가능함. 즉 해당 receiptID와 함께 구매한 내역이 자신이 구매한 내역과 동일한지 확인하면 가능하다([그림 10]의 goods 정보).

(2) 거래인증 기관 속이기
• *secretNumber* 위조/ *receiptID* 위조
  – *secretNumber*나 *receiptID*를 우연히 맞출 수도 있을 것이다. 그러나 확률적으로 매우 적으며, 첫 위조 시도가 적발되면 이후는 감시 대상이 되기 때문에 어려울 것이다.
• 보고 안하기
  – 판매 내역을 보고를 하지 않는 것은 디지털영수증을 발행하지 않을 때만 가능하다. 고객이 구매시 디지털 영수증을 발행하지 않으면, 거래 내역을 확인할 수 없다.

V. 결 론

온라인 거래에서 OECD는 과세 원칙을 결정하였지만, 100% 거래의 투명성을 밝히는 것은 쉽지 않을 것이다. 그러나 다양한 기술을 조합하고, 디지털 영수증 발행을 전제(법적으로)한다면, 생성되는 정보를 이용하여 최소한 발행되는 영수증과 거래 내역을 통하여 투명한 거래를 제공할 수 있을 것이다.

본 연구 모델의 하나는 고객의 권리인 디지털 영수증에 관한 것이며, 또 다른 하나는 거래 인증 기관의 권리에 관한 것이다. 비록 기본 모델이 금전등록기에서 왔지만, 온라인 모델은 자기 검증 가능하고 누구나 알 수 없는 거래 등록기의 비밀 카드와 숫자 조합 규칙에 기반을 가지고 있다. 온라인 마켓에서 모든 거래 등록기는 개별화된 프로파일이 있기 때문에 동일한 상태에서 동일한 ID를 발행하지 않는다. 비밀 카드와 프로파일이 안전하다면 *receiptID*와 *secretNumber* 또한 안전할 것이다.

참고문헌

[1] ESPRIT Project 27028, Electronic Commerce Legal Issues Platform, Draft Brochure : Legal Issues of Electronic Commerce - A Practical Guide for SMEs, 7 March 2002

[2] 윤광운 외, 전자상거래법, 삼영사 2002

[3] OECD Report, Electronic Commerce : Taxation Framework Conditions, October 1998

[4] OECD, Electronic Commerce : Implementing the Ottawa Taxation Framework Conditions, June 2000

[5] KIPA, 디지털콘텐츠 거래인증 활성화 방안 연구, KIPA 정책연구03-04, 2003, pp. 56-96

[6] 김정호, Digital Contents 소비자보호 정책 동행 및 전망, 디지털콘텐츠 표시 활성화 공청회, KIPA 2003년 12월 16일, pp. 53-73

[7] 김은기, 유료콘텐츠와 소비자 보호, 월간소비자, 2001년 12월호

[8] IMPRIMATUR, WP4 : The IMPRIMATUR Business Model Version 2.1, Esprit 20676, 1999

[9] MPEG-21 Requirements for a Rights Data Dictionary and a Rights Expression Language, W4336, Final v1.0, July 2001

[10] 신재호, 온라인디지털콘텐츠산업발전법에 관한 검토, 산업재산권 11호, 2002.

[11] 이창열, Digital Contents 메타데이터 표준화 동향 및 표시와 연계 방향, 디지털콘텐츠 표시 활성화 공청회, 2003년 12월 16일, KIPA, pp. 99-130

[12] KIPA, 디지털콘텐츠 표시 활성화 정책방향, 디지털콘텐츠 표시 활성화 공청회, 2003년 12월 16일, KIPA, pp. 1-18

[13] 이상정, 표시를 통한 지재권 등 보호, 디지털콘텐츠 표시 활성화 공청회, 2003년 12월 16일, KIPA, pp. 75-98

〈著者紹介〉

이 창 열 (ChangYeol Lee) 정회원
1985년 2월: 고려대학교 수학과 졸업
1991년 2월: 고려대학교 전산과학과 석사
1997년 6월 : University Paris VII 전산학 박사
2000년 3월~현재: 동의대학교 컴퓨터공학과 교수
<관심분야> DRM, RFID, ID