2001년 한국정보처리학회 춘계 학술발표논문집 제8권 제1호

M-Commerce 상에서의 Off-Line 지불 비즈니스 모델의 설계에 관한 연구

강병모*, 홍인식*
*순천향대학교 정보기술공학부
e-mail:asman@cse.sch.ac.kr

A Study on Design of Off-Line Payment Business Model in M-Commerce

Byung-Mo Kang*, In-Sik Hong*
*Division of Information Technology Engineering,
SoonChunHyang University

요약

인터넷의 발달과 더불어서 M-Commerce 상에서의 Off-Line 지불에 관한 관심이 높아지고 있다. 이것을 가능하게 해는 핵심 요인중에 하나는 차세대 이동통신인 IMT 2000과 Bluetooth 기술이다. 본 논문에서는 IMT 2000과 Bluetooth에 관한 관련 기술과 M-Commerce 상에서의 Off-Line 지불 비즈니스 모델의 설계를 제안하였다.

1. 서론

뉴 밀레니엄의 키워드는 'M'. 지금 전 세계를 뒤덮고 있는 '이커머스(e-Commerce)'의 물결이 앞으로는 'M-커머스(M-Commerce)'로 바뀔 전망이다. 앞으로는 이동전화나 개인휴대정보단말기(PDA)를 이용해 인터넷에 접속, 각종 온라인 서비스를 이용하고, 사이버쇼핑을 하는 시대가 오고 있고, M-Commerce 상에서의 Off-Line 지불에 관한 관심이 높아지고 있다. 이것을 가능하게 하는 핵심 요인중에 하나는 차세대 이동통신인 IMT 2000과 Bluetooth 기술이다. 본 논문에서는 IMT 2000과 Bluetooth에 관한 관련 기술과 M-Commerce 상에서의 Off-Line 지불 비즈니스 모델의 설계를 제안하였다. 제안된 비지니스 모델들은 크게 구매/지불 분야, 개인인증을 통한 응용분야, 그리고 블루투스를 이용한 오프라인 응용분야 등으로 구분되며 특히 가장 근간이 구매/지불분야는 오프라인지불에 관한 연구를 진행하였다.

2 관련 기술

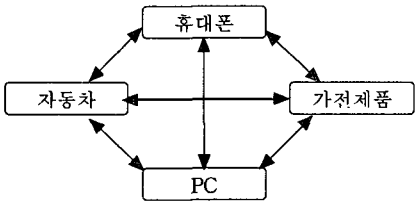
2.1 IMT-2000

IMT-2000은 'Any Time, Any Where'라는 꿈을 실현하기 위하여, 진화하고 있는 이동전화 네트워크의 다음 세대 발전단계로서 음성 위주의 1세대 아날로그 이동전화, 음성과 저속데이터 전송이 가능한 2세대 디지털 이동전화를 거쳐 고속 무선 멀티미디어 서비스의 구현이 3세대이다. IMT-2000은 공통 주파수 사용과 단일 기술표준으로 이용자가 세계 어느 곳으로 이동하더라도 하나의 단말기로 이동전화 서비스를 이용할 수 있도록 한다는 목표로 연구 및 추진되어 온 서비스이다. IMT-2000은 단말기를 바꾸지 않고 언제 어디서나 이동통신 서비스를 이용한다는 꿈을 실현하자는 것을 목표로 하였지만 통신업체간, 국가간 및 대륙간 이해문제가 부딪힘으로 인해 이 목표는 다소 불확실해지고 있는 현실이다. 그러나 스마트카드 등을 이용하여 상이한 기술방식간의 호환성을 확보할 수는 있지만 사용자에게는 불편이 따르게 될 수 있다.

이에 따라 각국은 pre IMT-2000이라 할 수 있는 IS-2000, GPRS 등 144Kbps급의 데이터 전송이 가능한 서비스를 준비하면서, 현재 운용중인 이동전화망을 진화·발전시키는 방향으로 사업화를 진행시키고 있다.

2.2 Bluetooth

블루투스란 일정거리(10m or 100m)내에서 소출력(100mW)를 이용하여 휴대폰이나 휴대용PC 등과 같은 휴대장치들, 네트워크 액세스 포인트들, 기타 주변장치들간의 무선연결을 위한 기술적인 국제규격을 말한다. 즉, 휴대용 PC로 주변의 유선통신망및 무선통신망 등과 연결시 케이블을 사용하지 않고 무선을 이용할 수 있음을 의미한다.



<그림 1> 블루투스 개념도

블루투스는 주파수 대역이 2.4GHz대의 ISM Industrial, Scientific, Medical)으로, 이 때문에 라이센스 없이 무료로 사용할 수 있다. 또한 데이터 전송속도가 1Mbps(실제 속도는 721Kbps)로 최대 10m 내의 거리에서 각종 단말기들을 무선으로 접속해 사용할 수 있다. 블루투스는 이외에도 동기화(자동 업데이트), 프리젠테이션, 명함교환, 홈 네트워킹, 선 없는 PC, 자동차(자동 제어와 네비게이션) 등과 같은 분야에 활용 가능하다.

3. On-Off Line 통합 결재 시스템

3.1 무선 PKI

PKI (Public Key Infrastructure)란 공개키 암호 시스템이나 서명 시스템을 이용하는 정보 시스템에서 사용자 공개키의 무결성(integrity)과 신뢰성을 보장하는 수단을 제공한다. 따라서 액세스 제어가 가능하여 다단계 인증에서도 사용 가능하다. 인터넷 전자상거래에서 필수적인 사용자 인증 기능을 제공하며 서명 알고리듬으로 RSA, KCDSA 등과 해쉬 알고리듬으로 MD-, SHA 등과 함께 사용된다. 무선용 PKI구축은 무선 인터넷의 강력한 보안을 제공할 수 있는 좋은 방법이며 다음과 같은 요구조건이 있게된다.

1) 유선 PKI와 동일한 서비스를 제공하여야 한다.
2) 단말기의 제한된 리소스를 고려한 사용자 인터페이스를 제공하여야 한다.
3) 리소스를 고려하여 단말기의 작업부하를 최소
4) 무선환경의 제한된 대역폭 등의 제한조건을 면밀히 고려하여 설계, 구현되어야 한다.
5) 기존 시스템들과의 상호연동을 위해 표준을 고려
6) 키생성 등은 자체연산이 가능한 IMT200의 UIM 카드를 사용하여 사용자가 생성한다.

3.2 인증서 발급신청 및 등록과정

가입자는 인증서를 발급 받기 위해 등록기관(RA)에서 직접대면을 통한 신원확인을 하며 신원이 확인된 가입자는 등록기관으로부터 인증서 요청시 사용할 참조코드(ID/Password)를 부여받는다. 가입자는 자신이 서명에 사용하는 전자서명 생성키(Private Key)와 자신의 서명을 검증에 사용하는 전자서명 검증키(Public Key)를 생성후, 전자서명 검증키와 개인정보를 담은 인증서 요청형식을 작성하여 등록기관으로 발급요청을 한다. 인증기관은 자신의 전자서명 생성키로 가입자의 전자서명 검증키에 대하여 서명함으로써 가입자 인증서를 생성하여 가입자에게 인증서를 발급하게 된다.

(1) 인증서 등록절차
- 등록기관이 직접대면을 통해 사용자 신원을 확인
- 확인후 ID와 Password를 생성후 사용자에게 전달
- 등록기관은 자신의 DB에 가입자를 등록하며 인증기관에 가입자 등록정보를 전송한다.

(2) 인증서 발급절차
- 가입자는 인증서 발급에 필요한 전자 서명키 쌍, 인증서 요청정보를 생성한다.
- 가입자는 자신의 전자서명 생성키로 인증서 요청정보 및 전자서명 검증키를 등록 한 후 등록기관에 전송한다.
- 실제로 전자서명 검증키에 대응하는 전자서명 생성키의 소유여부를 확인 POP (Proof Of Possession)한 후 인증서 요청정보를 인증기관에 전송한다.
- 인증기관은 무선용 X.509V3 인증서를 생성하여 자신의 디렉토리에 등록하고, 이를 사용자에게 전송

(3) 인증서 확인절차

인증기관으로부터 인증서를 받은 가입자는 자신이 받은 인증서의 이상유무를 확인한다.

3.3 인증서 검증과정

(1) 가입자가 전송받은 인증서의 검증
- 서버는 인증서(무선용 X.509V3)를 가입자에게 전송
- 가입자는 서버로부터 받은 인증서를 검증한다.

(2) 서버가 전송받은 인증서의 검증
- 가입자는 자신의 인증서, URL을 서버에게 전송
- 서버는 가입자로부터 받은 인증서를 검증한다.

3.4 관련 기준

(1) 인증서 발급요청

가입자의 경우 인증서 발급요청을 PKCS#10, CMP (Certificate Management Protocol) 혹은 등록기관이 대신 생성 전송하는 방법중 하나를 이용할 수 있다.

(2) 인증서 전송방법

인증서를 전송하는 방법은 인증서 자체를 전송하는 것과 인증서에 대한 URL만을 전송하는 것 두 가지로 나눌 수 있다.

(3) 인증서 규격

가입자, 서버 모두 인증서 규격은 무선용 X.509V3인증서 규격을 준용한다.

(4) 인증서 프로파일

인증서 프로파일은 인증기관 및 응용프로그램이 인증서를 생성하고 처리하는데 필요한 요구사항들을 명시하고 있다.

(5) 인증서 효력정지 및 폐지목록 규격

사용자는 인증기관에 의해 전자서명 검증키의 무결성을 보장받을 수 있다. 그러나 인증서에 포함된 전자서명 검증키에 대응되는 사용자의 전자서명 생성키가 노출되거나, 도난, 분실된 경우에는 큰 문제가 발생할 수 있다. 이러한 경우 인증서를 신뢰하여 상대방의 전자서명을 검증하는 신뢰당사자(Relying Party)가 선의의 피해를 입을 수 있다. 따라서 전자서명 생성키의 누출과 같은 키의 손상(compromise)이 발생한 경우 다른 사용자가 해당 전자서명 검증키에 대한 인증서를 신뢰하고 사용하지 못하도록 함으로써, 전자서명 생성키의 누출에 따른 피해를 예방하여야 한다. 인증기관은 손상된 전자서명 생성키에 대응하는 전자서명 검증키의 인증서를 즉시 폐지하여, 인증서 효력정지 및 폐지목록은 인증서의 효력정지 및 폐지여부를 인증서 사용자에게 알리기 위한 수단으로 개발되었다.

(6) 인증서 인코딩

인증서 인코딩 방법에는 DER (Distinguished Encoding Rules), PEM (Privacy Encoding Mail) 등이 있는데 DER로 인코딩된 파일 확장명은 .der로 끝나며, 파일 내용은 바이너리 형태이다. PEM은 안전하지 못한 방법으로 전송되는 E-Mail을 보호하기 위하여 전자서명 및 암호화 통신이 가능한 메일 프로토콜로 규정되어 있다.

(7) 고유이름(DN)

DN (Distinguished Name)은 인증서 및 인증서 폐지목록을 전자서명 인증관리체계 내에서 고유하게 식별하기 위한 표준화된 이름이다.

(8) 인증서 유효기간

인증서 유효기간은 인증기관이 인증서 상태에 대한 정보를 유지하겠다고 보증하는 시간 간격을 의미한다. 각 날짜는 인증서 유효기간이 시작하는 날짜(notBefore)와 인증서 유효기간이 종료하는 날짜(notAfter)이다. 무선에서의 가입자 또는 서버의 유효기간은 전자서명 인증관리 체계에서 정의하고 있는 유효기간과 동일하다.

(9) 인증서 및 인증서 폐지목록 저장방식

인증서 및 인증서 폐지목록은 WIM (Wireless Application Protocol Identity Module Specification) 카드를 사용할 때와 사용하지 않을 때의 두 가지 경우로 나뉜다. 가입자, 서버 모두 인증서 및 인증서 폐지목록 저장방식은 WIM 카드를 사용할 때는 WIM카드 규격에 맞게 저장하고 그렇지 않을 때는 PEM이나 DER 방식으로 저장한다.

(10) 전자서명 생성키 저장방식

가입자의 경우 전자서명 생성키 저장방식은 WIM카드를 사용할 경우 WIM카드 규격을 따르고 소프트웨어를 사용할 경우 PKCS#5 (Password-Based Encryption Standard)로 암호화하여 PKCS#8 (Private-Key Information Syntax Standard)을 이용해 저장한다. 서버의 경우 생성키 저장방식은 PKCS#5로 암호화하여 PKCS#8을 이용해 저장한다.

(11) 전자서명키 및 인증서, 인증서 폐지목록 전달방식

가입자의 전자서명키 및 인증서, 인증서 폐지목록 전달방식은 WIM카드의 경우 WIM카드 규격을 따르고 소프트웨어를 사용할 경우 PKCS#12 (Personal Application Protocol Identity Module Specification)를 사용하여 전달한다.

3.5 알고리듬

(1) 키생성

키생성은 가입자는 단말기에서, 서버는 서버에서 자체 생성한다.

(2) 전자서명 알고리듬

전자서명 알고리듬은 인증기관이 인증서와 인증서 효력정지 및 폐지목록을 생성하는 경우와 전자문서에 사용자가 전자서명을 하는 경우에 사용된다.

(3) 해쉬 알고리듬

해쉬 알고리듬은 기본적으로 메시지 인증에 사용되며 전자서명 알고리듬과 함께 전자서명 생성 및 검증에 사용된다. 지원되는 해쉬 알고리듬은 HAS

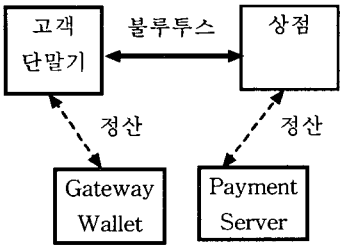
-160, SHA-1를 사용한다.

4. 시뮬레이션

본 장에서는 앞장에서 설계한 Off line 비즈니스 모델의 유효성을 검증하기 위하여 지불 시스템의 각 부분들을 시뮬레이션 하였다.

4.1 오프라인 지불 시스템의 전체적인 구조

오프라인 지불은 통상적으로 Wallet Server에 연결할 수 없는 곳이나 아니면 오프라인 지불이 가능한 곳, 자판기와 같은 마이크로 지불(Micro Payment)이 필요한 곳에서 이루어진다. 오프라인 지불은 지불 서버나 Wallet 서버 등이 개입하지 않은 상태에서 블루투스와 같은 지역적인 통신 방법을 통하여 카드 소유자와 상점간에 모든 지불 절차가 수행된다. 거래 내역은 카드 소유자의 USIM 카드와 상점의 컴퓨터 안에 저장되며 온라인으로 연결할 수 있는 상태가 되면 저장된 모든 거래 내역이 Wallet 서버로 전송되어 데이터의 동기화를 하게 된다.



<그림 2> 오프라인 지불 시스템의 구조도

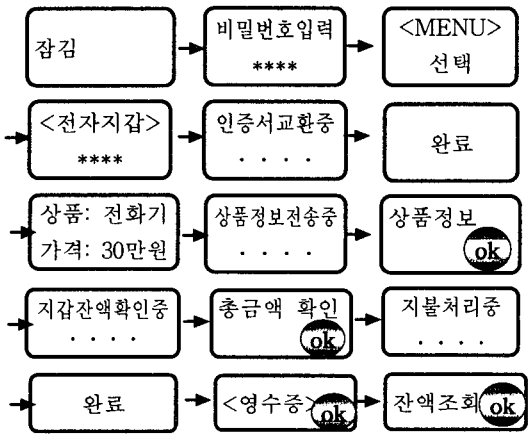
현재 오프라인 지불에서 참조할 수 있는 지불 프로토콜은 스마트 카드를 위한 EMV 지불 모델이다. 본 연구에서는 EMV의 규격을 참고하여 여러 가지 데이터 형식을 정하되, 지나치게 지엽적이고 일반성이 없는 데이터는 제외하고 중심적인 데이터와 프로토콜만을 포함시켰다. 오프라인 지불은 다음과 같은 단계를 거쳐서 진행된다.

- Step 1: 물품 구매 요청
- Step 2: 상호 인증
- Step 3: 물품 견적서 전송
- Step 4: 전자 화폐 전송
- Step 5: 확인 정보 전송

4.2 Off-line 지불 시뮬레이션 시나리오

상점의 컴퓨터는 전화번호나 BLUETOOTH를 이용하여 단말기에 결제를 요청한다. 단말기는 결제에 필요한 초기화를 시작한다. 상점의 컴퓨터와 서로 인증서를 교환한다. 인증서의 공개키를 이용하여 암호화된 Session Key를 발생시킬 수 있는 Master Key 데이터를 서로 교환한다. Session Key에 대하여 일치가 되면 이 Session 키를 이용하여 DES 암호화 방법을 사용하여 모든 데이터를 암호화한다.

4.3 Off-line 지불 시뮬레이션 흐름도



<그림 3> 오프라인 지불 시나리오

5. 결론

본 연구에서는 M-Commerce상에서 Off-Line 지불 비즈니스 모델의 개발에 대한 연구로 본 연구에서는 M-Commerce에서의 지불/인증시스템의 최근 동향과 표준화 노력을 고찰하고 IMT-2000이나 Bluetooth를 이용한 새로운 비지니스 모델을 발굴하기 위한 연구를 진행하고자 한다. 비지니스 모델로 모바일 고객 관리 시스템을 연구하였다. 연구가 진행됨에 따라 새로운 분야의 비지니스 모델이 나타날 수도 있다. 비즈니스 모델을 살펴보면 아직 해결되지 않은 문제점들을 많이 발견할 수 있다. 이러한 문제점들은 국내의 문제가 아니라 국제적인 규격과 합리적인 장치 및 어플리캐이션의 개발이 뒷받침되어야 가능할 것으로 생각된다.

참고 문헌

[1] Nathan J. Muller "Bluetooth Demystified"

[2] H.Antwerpen, "Electronic Cash", Master's thesis Univ. Eindhoven'1990

[3] S.Brands,"Off-Line Cash Transfer by Smart Cards",CWI'1994

[4] S.Brands,"Untraceable Off-Line Cash in Wallets with Observers",Crypto'1993