PDA환경에 적합한 ECC기반 신용카드 결제 프로토콜 설계

조성지[0], 유성진, 김성열*, 정일용
조선대학교 전자계산학과, 울산과학대학 컴퓨터정보학부
csjart@hanmail.net[0], tiger@stmail.chosun.ac.kr, *green@mogent.net, iyc@mina.chosun.ac.kr

A Design of Protocol for Credit Card Transaction on PDA Using ECC

Seong-Ji Cho[0] Seong-Jin You Seong-Yeol Kim* Il-Yong Chung
Dept. of computer science, Chosun University, *School of Computer Information, Ulsan College

요 약

M-Commerce에서 안전한 서비스를 제공하기 위해서는 보안 기능을 갖춘 결제 솔루션이 필수적이다. M-Commerce를 이용하기 위한 사용자의 이동 단말기는 핸드폰, PDA, 스마트폰 등으로 다양화 되어가고 있으며, 이 중에서도 PDA의 인터페이스와 이동 접속은 기존 핸드폰의 유선 인터넷의 정보 의존도가 높은 단점을 극복할 수 있다. 본 논문에서는 타원곡선 암호를 이용하여 PDA 기반의 신용카드 결제 시스템을 설계하였다. 제안된 시스템의 SECURE CARD모듈은 PDA 단말기 자체에 개인정보, 배송정보, 카드정보를 암호화하여 안전하게 저장함으로써 단말기의 정보입력시에 필요한 불편함을 제거하였다. 또한 프로토콜은 M-Commerce에서 인증, 기밀성, 무결성, 부인봉쇄 서비스 등의 보안기능을 제공하도록 설계되었다.

1. 서 론

최근 이동통신망의 급속한 발전과 더불어 PDA 등 소형정보 단말기의 보급 확대 및 고속데이터전송을 근간으로 하는 IMT-2000의 상용화가 국내뿐 아니라 세계적으로 확대되고 있다. 이러한 흐름에 따라 기존 개인용 컴퓨터 등의 고정 단말기를 기반으로 한 E-Commerce 형태를 벗어나 이제는 이동성(mobility), 휴대성(portability)를 제공하는 새로운 형태의 M-Commerce가 보편화되고 있다[1]. 이러한 M-Commerce에서 안전한 서비스를 위해서는 서비스의 특성에 알맞은 무선 결제서비스(Mobile Payment Service)의 연구가 활발하게 진행되고 있다[2][3]. 현재 무선결제 서비스는 이동통신사를 중심으로 소액결제 서비스가 주로 이루어지고 있으며, 현재 핸드폰 중심의 상거래는 무선 서비스 독자적인 경우보다는 사용자가 유선 상에서 자료를 보고 구매를 결정하는 유선 의존도가 높은 결제방식이다[4]. 이에 반하여 신용카드 기반의 결제구조는 고액결제가 가능하다는 강점을 가지고 있다. 그러나 신용카드 기반 결제구조는 무선인터넷 인프라가 부족하여 무선결제시스템에 취약하다는 문제점을 내포하고 있다. 따라서 무선기반 정보제공능력, 고액결제 서비스가 가능한 시스템이 요구된다.

<표 1>은 무선 결제 서비스의 제공능력을 나타내고 있는데 이에 따르면 이동통신사는 무선결제 플랫폼, 과금시스템, 소액결제능력 등에 대해서는 우수하게 나타나고 있으나, 고액결제능력, 신용위험관리, 타 금융서비스와의 연계 등의 부분에서는 다소 미흡한 결과를 보여주고 있다[5].

<표 1> 무선결제 서비스 제공능력

[illegible]	[illegible]	[illegible]	[illegible]
무선결제플랫폼	●	○	○
과금(빌링)시스템	●	◑	●
소액결제 능력	●	◑	◑
고액결제 능력	○	●	●
신용위험관리	○	●	●
소비자 확보	●	◑	◑
가맹점 확보	○	◑	●
계정관리	○	●	●
타금융서비스와 연계	○	●	◑
자금결제 신뢰감	◑	●	●

● : 우수 ◑ : 보통 ○ : 부족

현재 보안측면에서 RSA와 같은 공개키 암호 시스템은 유선상에서 우수한 보안도구로 여겨지고 있으나, 키 사이즈가 너무 크고 처리속도가 느리다는 단점이 있다. 따라서 무선 환경의 낮은 CPU, 적은 메모리의 무선단말기에 적합하지 않은 것으로 판단되고 있다. 이를 보완하기 위해서 무선단말기에 적합한 무선 공개키 기반구조(WPKI)[6]의 방향으로 연구가 진행되고 있고 적은 비트수와 빠른 계산 속도를 지원하는 ECC 공개키 암호 시스템에 대한 관심이 증가되고 있다[7].

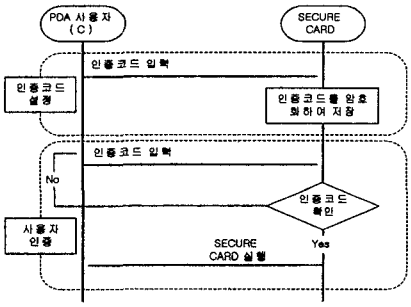
2. Secure Card 설계

2.1 Secure Card 모듈

PDA는 이동성이 강한 정보기기로 기존 유선상의 정보

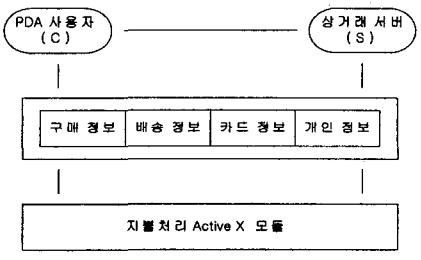
기기에 비하여 정보 입력 작업이 원활하지 않은 입력 구조를 가진다. 따라서 PDA기반의 결제 솔루션을 제공하는데 거론될 수 있는 문제가 사용자와의 인터페이스이다. 이동기기의 정보입력 불편의성의 문제를 해결하고 안전한 결제 솔루션을 제공하기 위하여 'SECURE CARD'를 설계하였다. SECURE CARD는 사용자가 한번의 정보 입력으로 모든 상거래 서버와 거래를 할 수 있도록 구성 하였다.

본 연구에서 제안하는 SECURE CARD는 설치 모듈, 인증 모듈, 거래정보 관리 모듈, 암복호화 모듈로 구성된다.



[그림 1] SECURE CARD 인증모듈

Secure Card 설치는 사용자가 처음으로 M-Commerce를 이용할 때 안전한 거래를 위하여 전자 상거래 서버로부터 Secure Card 프로그램을 다운받아 설치한다. 인증모듈은 어플리케이션을 실행할 권한이 있는지를 결정하며 사용자는 설치후 인증코드를 설정하고 암·복호화 모듈에 의해 암호되 되어 저장된다. 거래정보 관리는 온라인 상에서 회원가입 또는 상거래 거래시 필요한 정보의 활용을 위해서 개인정보, 배송정보, 카드정보의 필수 항목을 관리한다. 개인정보에는 ID, 인증코드, 이름, 주민등록번호, E-mail 주소, 전화번호를 필수 항목으로 하여 사전에 입력 받는다.



[그림 2] 지불처리 Active X 모듈

배송정보와 카드정보는 다수의 데이터를 입력 받을 수 있어야 한다. 사용자들은 보통 최소 집, 회사 2개의 배송지를 사용하고 카드도 1개 이상을 사용하는 것이 일반적이다. 그리고 자신이 소유한 카드정보도 PDA에 설치한 Secure Card에 미리 암호화되어 저장한다.

사용자가 상품을 구매 요청하는 경우 서비스 제공자로부터 구매금액에 대한 정보를 전달받고 사용자는 자신의 배송정보, 카드정보를 선택할 수 있다. 구매금액은 Active X 컨트롤을 통해서 온라인 결제시 Secure Card로 전달되며 암·복호화 모듈에 의해서 배송정보와 카드정보가 암호화 된다. 최종적으로 전달되는 데이터는 구매금액, 배송정보, 카드정보이다.

2.2 Secure Card를 이용한 프로토콜 표기

무선인터넷 환경에서 PDA에 기반한 신용카드 결제시스템을 제안한다. 제안하는 프로토콜의 표기법은 [표2]와 같다.

<표 2> 제안된 프로토콜 표기법

C	PDA 사용자 고객
S	상서래 서버
PG	지불 게이트웨이
Item	상품
PList	구매 목록
PR	지불 요청
PRA	지불 요청 승인
CI	신용카드 정보(카드번호, 유효기간)
PI	개인 정보(이름, 주민등록번호, 전화번호)
DI	배송 정보(주소, 우편번호)
CAI	신용카드 승인 정보
CR	신용카드 영수증
ID_i	i의 식별자
PK_i	i의 공개키
SK_i	i의 개인키
K_{cs}	C와 S의 공유된 세션키
S_{cs}	C와 S의 공유된 비밀키
A || B	A와 B 데이터의 연접
$E_k[m]$	k를 이용하여 m을 암호화
h{m}	m을 해쉬함수로 수행
$Time_i$	타임스탬프

제안된 프로토콜 수행절차는 [그림 3]과 같고, 사용자는 신용카드를 발급 받을 때 비밀번호를 함께 등록한다. 비밀번호는 M-Commerce를 이용할 때 지불서버와 사용자의 비밀키로 사용되어진다. 사각형 점선 부분은 처음 거래하는 상거래 서버에서만 발생하게 된다.

[각 단계별 Transaction 표기]

[단계 1] C → S : Item

[단계 2] C → S : $E_{SKauth}[Time_1, ID_c, KU_c]$

[단계 3] S → C : $E_{SKauth}[Time_2, ID_s, KU_s]$

[단계 4] S ↔ C : 세션키 공유

[단계 5] C → S : $E_{Kcs}[PInfo]$

[단계 6] S → C : $E_{Kcs}[PList \,||\, PR]$

[단계 7] C → S : $E_{Kcs}[PRA]$

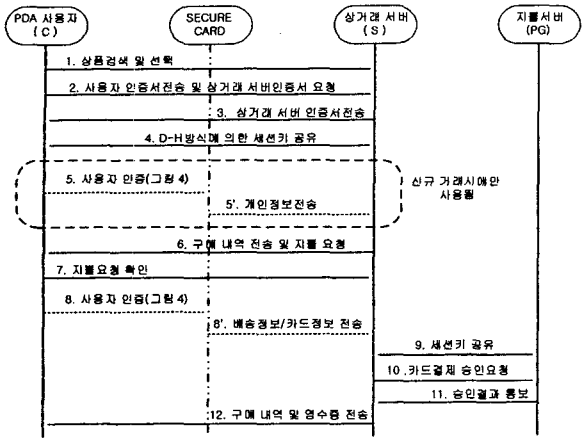
[단계 8] C → S : $E_{Kcs}[DI \,||\, E_{Scvc}[CI] \,||\, Time_3 \,||\, E_{SKc}[h\{DI \,||\, E_{Scvc}[CI] \,||\, Time_3\}]]$

[단계 9] S ↔ PG : 세션키 공유

[단계 10] S → PG : $E_{Kcs}[E_{Kscvc}[CI] \,||\, Time_4 \,||\, E_{SKc}[h\{E_{Kscvc}[CI] \,||\, Time_4\}]]$

[단계 11] PG → S : E_{Kcs}[CAI || E_{Ksvc}[CR] || $Time_5$ || E_{SKc}[h{E_{Ksvc}[CR] || $Time_5$}]]

[단계 12] S → C : E_{Kcs}[PList || E_{Ksvc}[CR] || $Time_6$ || E_{SKs}[h{PList || E_{Ksvc}[CR] || $Time_6$}]]



[그림 3] Secure Card를 이용한 프로토콜

3. 제안된 프로토콜 보안 서비스 분석

제안한 프로토콜을 이용하여 전자 상거래를 한다면 종단간 보안, 기밀성, 인증, 무결성, 부인봉쇄 서비스 등을 제공받을 수 있다. 또한 사용자와 지불서버와의 종단간 보안이 가능하고, 무선 환경에 적합하게 정보 입력의 불편함을 해소하기 위하여 거래 정보를 PDA에 암호화하여 저장하였다.

종단간 보안은 [단계 8]과 [단계 10]에서 볼수 있듯이 사용자와 지불서버만이 공유하는 비밀키로 암호화 하여 상거래 서버에 전달되기 때문에 상거래 서버에서는 볼 수가 없고 사용자와 지불서버만이 신용카드 정보를 알 수가 있다.

기밀성은 안전한 세션키 교환이 필수적인데 세션키 교환은 [단계 4]와 같이 Diffie-Hellman의 변형된 타원곡선을 이용하여 세션키를 안전하게 교환한다. 이렇게 교환된 세션키를 이용하여 [단계 5]부터 전송되는 모든 데이터를 안전하게 암호화하여 다른 사용자의 도청으로 보호한다.

인증은 1차적으로 무선 단말기의 분실에 대비하여 [그림 1] 과 같이 PDA 자체에서 일방향 함수를 이용하여 인증코드를 암호화하여 저장하고, 인증코드가 정확히 입력되었을 때 개인 정보를 볼 수가 있게 된다. 2차적으로 전자상거래시 거래정보를 전송하기 전에 인증코드 확인 절차를 거쳐 상거래 서버로 거래 정보를 전송하게 된다. 그리고 사용자와 상거래 서버간의 인증은 [단계 2]와 [단계 3]에서와 같이 신뢰된 인증기관으로부터 발부 받은 인증서를 서로 교환하여 서로 인증이 가능하다.

무결성은 거래 정보가 변경 되었을때 확인 할 수 있는 방법이다. 제안된 프로토콜에서는 중요 정보에 대하여만 해쉬 함수를 수행하여 불필요한 오버헤드를 줄였다. 즉, 신용카드 정보와 결제에 대한 데이터인 [단계 8], [단계 10], [단계 11], [단계 12]에서 해쉬 함수를 사용하였다.

부인봉쇄는 거래 정보를 개인키로 서명함으로써 이루어지는데 기존의 유선에서 사용하는 공개키 암호 시스템을 M-Commerce에서 사용하면 연산 속도가 오래 걸리는 단점이 있다. 제안된 프로토콜에서는 타원곡선 암호 시스템을 이용하여 M-Commerce에 적합한 서명을 하여 부인봉쇄 서비스를 제공한다. 또한 모든 거래 정보에 서명을 하지 않고 [단계 8], [단계 10], [단계 11], [단계 12]과 같은 중요한 데이터에만 서명을 함으로써 불필요한 오버헤드를 줄였다.

4. 결론

M-Commerce 환경에서 데이터 서비스를 원활하게 제공하면서 정보보호 기술을 만족하기 위해서는 안전한 전자상거래 시스템 설계가 중요하다. 일반 공개키 암호 시스템은 M-Commerce에 적합하지 안았지만, 적은 비트수와 빠른 계산 속도를 보장하는 타원곡선 공개키 암호 시스템으로 인하여 M-Commerce에서 공개키 암호시스템이 사용 가능하게 되었다. 제안된 프로토콜에서는 M-Commerce에 적합한 타원곡선 암호 시스템을 이용하여 PDA 기반의 신용카드 결제 시스템을 설계하였다. 세션키 교환에서는 Diffie-Hellman의 키 교환 기법을 이용하였고, 타원곡선과 안전한 블록암호 알고리즘을 이용하여 거래 정보의 기밀성, 무결성, 인증, 부인봉쇄 서비스 등을 갖춘 안전한 M-Commerce 프로토콜을 설계하였다. 제안된 프로토콜의 장점은 PDA를 이용하여 거래를 할 때 정보 입력의 불편의성을 극복할 수 있게 설계 하였다. 또한 중요한 정보만을 선택적으로 전자 서명 및 해쉬 함수를 수행함으로써 불필요한 오버헤드를 줄였고 타임스탬프를 이용하여 재전송 공격으로부터 안전하다.

따라서 본 논문에서 제안된 프로토콜에 의해 PDA의 정보입력 인터페이스의 단점을 극복하고 이를 통해 신용카드 결제 서비스의 무선 전자상거래 활성화에 기여할 수 있을 것으로 기대된다.

5. 참고문헌

[1] 이재규 외 3인, "전자상거래원론" 법영사, 2000.
[2] 무선인터넷백서 편찬위원회, "무선인터넷 백서", 소프트뱅크미디어, 2000.9.
[3] 김선형 외 2인, "이동 통신 시스템에서의 효율적인 소액 지불 기법", 한국정보과학회 춘계 학술 발표, pp. 181~183, 2002.
[4] 임수철 외 3인, "M-Commerce를 위한 고액 지불 시스템", 춘계 학술발표 논문집, 한국정보처리학회, pp. 1455~1458, 2002
[5] Forrester Research, "Mobile Payment's Slow Start", May 2001.
[6] Gunter Horn, Bart Preneel, "Authentication and Payment in Future Mobile Systems", ESORICS, LNCS 1485, pp. 277-293, 1998.
[7] 최용락 외 3인 공역, "컴퓨터 통신 보안" 도서출판 그린, 20001.2.