무선 환경에서 XML 전자서명을 이용한 Java Card 기반 시스템

장 창 복[†] · 최 의 인[††]

요 약

무선 인터넷의 발전과 무선 단말기의 성능이 발달함에 따라 무선 인터넷 환경에서의 전자상거래(M-Commerce)가 활성화되고 있다. 이러한 전자상거래에서는 사용자 인증 기술과 데이터 보안이 중요한 기술로 인식되고 있으며, 무선 인터넷에서의 WPKI나 Hermes 시스템, 유선 인터넷 환경에서의 XML 전자서명 같은 인증 기술이 연구되고 있다. 하지만 WPKI는 인증 시스템들이 서로 이질적이라 구현하기 어렵고 유선 인터넷의 인증 시스템과 상호 연동가능하지 않으며, XML 전자서명을 지원하지 않는 단점을 지니고 있다. Hermes 시스템 역시 XML 전자서명 시스템과 상호 연동 가능하지 않는 문제점이 존재한다. 따라서 본 논문에서는 무선 인터넷 환경에서도 기존의 유선 인터넷 환경에서 사용되고 있는 XML 전자서명 기법을 이용하여 유, 무선 환경에서 전자서명할 수 있는 Mediator를 설계한 뒤, Java Card를 이용하여 시스템을 설계 및 구현하였다.

System based on Java Card Using XML Digital Signature on Wireless Internet

Chang-Bok Jang[†] · Eui-In Choi[††]

Abstract

As wireless network was developed and Capability of Wireless Phone was increased, M-Commerce was activates in Wireless network environment. User Authentication and Security in E-Commerce Environment is very important, so Authentication Technology, such as WPKI and Hermes System, XML Digital Signature in Wire Network is studying. But if authentication systems was implemented heterogeneous, WPKI is difficult to implement the system, it's not interoperate with authentication system on wire internet, not support XML digital Signature. Hermes system also not interoperate with XML digital signature system. So our paper designed System that can interoperate among digital signature systems and XML document to apply XML digital signature technology on wire network to wireless network, and then implemented system that can XML digital signature to use Java Card.

키워드 : 무선인터넷 인증(Wireless internet Authentication), WPKI, XML 전자서명(XML Digital Signature)

1. 서 론

이동성과 휴대성을 갖춘 무선 단말기의 성능이 향상되고 기존 유선 인터넷환경과 달리 물리적 네트워크와 연결되어 있지 않아도 되는 무선 인터넷 환경의 발달로 인하여 지난 4~5년간 세계 경제의 한 축을 담당했던 유선 인터넷 중심의 전자상거래인 E-Commerce(Electronic-Commerce)가 무선 인터넷 환경 중심의 전자상거래인 M-Commerce (Mobile-Commerce)로 옮겨가고 있다[2]. M-Commerce는 일반적으로 쇼핑몰에서 물품 혹은 디지털 콘텐츠를 구매할 때 휴대폰 같은 무선 단말기를 이용하여 지불결제가 이루어지는 전자상거래 형태이다[11, 12, 14, 15]. 또한 이러한 전자상거래에서는 금전적인 문제로 인하여 사용자 인증이나 데이터 보안 같은 기술이 아주 중요한 문제로 여겨지고 있기 때문에 인증기관(CA : Certification Authority)으로부터 인증서를 발급 받아 거래문서에 전자서명하여 사용자 신원을 확인하는 기술들이 연구되고 있다. 최근에는 유선 인터넷 환경에서 XML 문서를 이용한 전자상거래가 활성화되고 있어 사용자 인증분야에서 XML 전자서명 기법을 사용하기 위한 연구가 진행되고 있다[1, 4, 16, 21, 22]. 이처럼 무선 인터넷에서도 기존 유선인터넷 환경처럼 전자상거래시 사용자를 확인할 수 있는 전자서명 기술에

※ 본 연구는 과학기술부 지역협력연구사업(R12-2003-004-03002-0) 지원으로 수행되었음.
† 준 회 원 : 한남대학교 컴퓨터공학과
†† 종신회원 : 한남대학교 컴퓨터공학과 부교수
논문접수 : 2004년 5월 19일, 심사완료 : 2004년 10월 11일

관한 연구가 필요하다. 현재 무선인터넷 환경에서 연구되는 인증 기술로는 WAP 포럼의 WPKI와 독일의 Constance 대학교에서 제안한 Hermes 시스템이 있다[3, 10, 13]. 하지만 무선 인터넷 환경은 무선 단말기의 성능 면이나 네트워크 환경 면에서 기존 유선 인터넷에 비해 많은 제약사항을 가지고 있기 때문에 무선 단말기 상에 데이터의 암호화와 인증처리 같은 연산 기능을 수행하기에는 어려운 점이 많다. 따라서 무선 단말기에서 수행하게 될 암호화와 인증 처리 연산을 독립된 모듈에 두어 처리할 수 있는 Java Card 기술이 연구되었다[11, 18, 23]. 또한 WPKI는 인증기관과 이동통신 업체, 금융기관, 콘텐츠 제공자의 시스템들이 서로 이질적이기 때문에 WPKI 기반 인증시스템을 구축하기 어렵다는 단점을 가지고 있으며, Hermes 시스템은 XML 문서를 이용하여 전자상거래에서 사용하였지만 XML 전자서명 기법을 사용하지 않기 때문에 XML 전자서명 시스템과 상호 연동 가능하지 않다는 단점이 있다.

따라서 본 논문에서는 WPKI와 Hermes 시스템의 단점을 해결하기 위해서 전자서명의 핵심인 전자서명 값을 생성하는 부분은 무선 단말기에서 이루어지도록 하고, 그 외의 XML 전자서명 문서를 생성하는 부분은 Mediator를 두어 처리하는 Java Card 기반의 전자 서명 시스템을 설계 및 구현하였다.

본 논문에서 제안한 시스템은 서로 이질적인 시스템에서도 전자서명이 가능한 XML 전자서명 기법을 무선 인터넷 환경에 적용하여 전자상거래의 범위를 무선 인터넷 환경으로 확대시켰으며, 무선 인터넷 환경에서도 XML 전자 문서에 대하여 서명할 수 있기 때문에 업무처리에 효율성을 가져 올 수 있다. 또한 인증기관과 이동통신업체 그리고 금융기관 같은 서로 다른 시스템으로 구성되어 있는 전자서명 시스템에서도 전자서명 시스템을 쉽게 구현할 수 있고, 기존 유선 인터넷 환경에서 사용되고 있는 전자서명 시스템들과도 상호 연동이 가능하다.

2장은 관련연구로써 무선인터넷 환경과 WPKI, Hermes 시스템, XML 전자서명과 관련된 연구에 대하여 설명하고, 3장은 Java 기반의 Mediator를 본 논문에서 제안하는 시스템에 설계 및 구현한다. 4장에서는 본 논문에서 제안한 시스템과 WPKI, Hermes 시스템을 비교 분석하고, 5장에서 결론 및 향후 연구 과제를 제시한다.

2. 관련 연구

무선 인터넷 환경에서 데이터 보안 및 사용자 인증에 관한 연구로는 WPKI(Wireless Public Key Infrastructure)와 독일 Constance 대학교에서 제안한 Hermes 시스템이 있다. 유선 인터넷 환경에서는 PKI 기반의 사용자 인증 기술이 연구되었고, XML 문서를 이용한 전자 상거래 연구가 활발하게 진행됨에 따라 XML 문서에 전자서명 할 수 있는 XML 전자서명 기법이 연구되고 있다. 그리고 무선 인터넷 환경은 환경적 제한으로 사용되어지는 단말기의 성능이 유선 인터넷의 단말기보다 현저하게 떨어진다. 특히 이러한 낮은 단말기의 처리 성능으로는 보안 및 인증 알고리즘을 구현하기 어렵다. 따라서 이러한 단점을 보안하고자 현재 Java Card와 같은 Smart Card를 이용한 단말기 성능 향상의 연구가 이루어지고 있다[7, 8].

2.1 WPKI

WPKI는 무선 환경을 위해 기존의 유선 인터넷의 PKI 방식을 최적화하여 확장시킨 것으로, WAP 포럼의 WPKI 표준이 가장 일반적으로 사용된다. 무선 인터넷 환경에서 사용자가 서비스 제공자와 보안 통신을 하거나 트랜잭션에 전자서명을 하기 위해서는 인증기관에 등록한 뒤 인증서를 발급받아야 한다. 이렇게 발급 받은 인증서를 통하여 무선 단말기에 저장된 비밀키로 전자상거래 문서에 전자서명한다. 이러한 전자서명된 문서를 WAP 게이트웨이를 통해 웹 서버로 보내고 웹 서버에서는 다시 인증기관으로 서명된 문서를 보내어 문서를 검증하게 된다[3, 17, 19, 20].

2.2 Hermes 시스템

Hermes 시스템은 독일의 Constance 대학교에 무선 인터넷 환경에서 전자서명을 이용하여 사용자 인증을 처리하기 구현된 시스템으로 Hermes 시스템에서 전자서명하기 위한 절차는 다음과 같다[10].

① 사용자는 서비스 제공자에 서비스 요청을 보낸다.
② 서비스 제공자는 사용자의 서비스 요청을 수신하고 전자상거래 XML 문서를 전송한다.
③ 서비스 제공자로부터 XML 문서를 수신한 후 Request receiver가 XML 파서를 이용하여 XML 문서의 표준 형태를 검사한다. 그리고 난 뒤 frontendcommunicator가 Front-end에 displaying 하기 적당한 형태로 전자서명을 위한 메시지 생성하며 생성된 메시지를 무선 단말기에 전송한다. 생성된 메시지에는 처리할 서비스 내용, 트랜잭션 번호, 생성 날짜, 만료 날짜가 포함된다.
④ Mobile Phone으로 전송된 메시지는 Signature Front End 모듈에 의해 전자서명되며 서명된 메시지는 다시 전송된다.
⑤ 서명된 메시지를 수신한 후 verifier에서 서명된 메시지를 Trust Center를 통하여 검증하고 검증이 완료되면 서명된 메시지를 새로운 XML 문서를 작성하기 위

하여 Financial-institute communicator로 전달한다.

⑥ 서명된 메시지를 수신한 Financial-institute communicator에서는 컨텐츠 제공자의 초기 요청, 사용자의 요청, 트랜잭션, 계좌번호, 거래금액 같은 정보를 포함하는 XML 문서를 생성하고 이를 Financial-institute에 서명된 메시지와 같이 보낸다.

⑦ Financial-institute에서는 XML 문서와 전송된 전자서명 메시지를 검증하고 서비스를 처리한다.

⑧ 처리된 서비스는 다시 Verifier에 서명된 영수증 형태로 전송되고 이를 Verifier에서는 Trust Center를 통해 검증한다.

2.3 XML 전자서명

XML 전자서명은 W3C의 XML-Signature Working Group에서 제정하였으며 XML 문서에 전자서명 할 수 있는 규칙과 구문처리를 명시하고 있다[1, 4]. XML 전자서명 문서는 Signature 엘리먼트로 표현되는 다음과 같은 구성 요소를 갖는다.

① Signature : XML 전자서명 문서의 부모 엘리먼트

② SignatureValue : SignatureMethod에 정의된 알고리즘을 적용하여 생성한 전자서명의 실제적인 값을 가지고 있다.

③ SignedInfo : Canonicalization 알고리즘, Signature 알고리즘, 또는 Reference를 포함한다.

④ CanonicalizationMethod : XML 문서를 정규화하기 위해 필요한 알고리즘을 포함한다.

⑤ SinatureMethod : 실제적인 서명값을 생성하기 위해 사용되는 알고리즘 명시

⑥ Reference : 선택적으로 서명문서에 포함시킬 수 있으며 ID를 통해 다른 곳에서 참조 할 수 있다.

⑦ Transforms : 서명자가 메시지 다이제스트 객체를 어떻게 얻는지를 명시

⑧ DigestMethod : 다이제스트 값을 생성하기 위한 다이제스트 알고리즘 명시

⑨ DigestValue : DigestMethod를 통해 생성된 다이제스트 값 포함

⑩ KeyInfo : 키 발생기를 통해 생성되는 키에 대한 정보 포함

3. Java Card 기반의 Mediator 설계

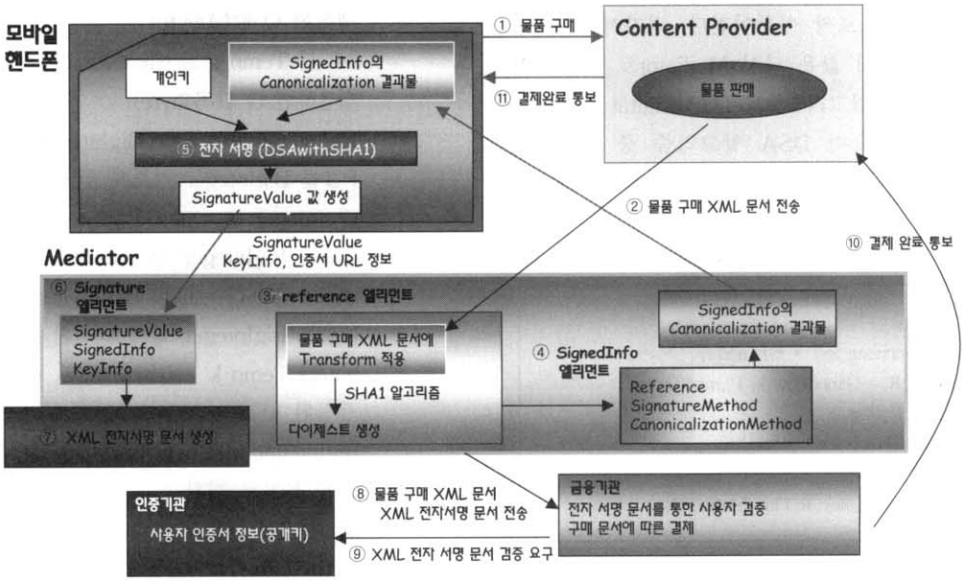
3.1 XML 전자서명을 위한 Java Card 기반의 Mediator

무선 인터넷 환경은 기존의 유선 인터넷 환경보다 좁은 대역폭, 덜 강력한 CPU, 적은 메모리 량, 데이터와 프로그램을 위한 적은 저장장치 크기, 작은 디스플레이와 같은 제한 요소를 가지고 있다. 이러한 제한 요소로 인하여 XML 전자서명을 무선단말기에서만 처리하기에는 사실상 불가능하다. 따라서 본 논문에서는 XML 전자서명 과정 중 전자서명 값을 계산하는 부분만 무선 단말기에서 수행하도록 Java Card를 이용하여 연산을 분산시켜 설계하였고, 본 논문에서 제안한 전자서명 시스템은 다음 (그림 1)과 같다.

본 논문에서 제안한 Java card 기반의 XML 전자서명 시스템은 다음과 같은 요소들로 구성되어져 있다.

① 모바일 핸드폰

사용자가 물품을 구매하거나 서비스를 제공받기 위해



(그림 1) Java card 기반의 XML 전자서명 시스템

사용되는 무선 단말기이며, 사용자 인증시 실제 전자서명이 이루어지기 위해 서명에 필요한 SignatureValue를 계산하는 부분이다.

② 컨텐츠 제공자(Content Provider)
유선 인터넷 환경에서 컨텐츠와 서비스 제공을 담당하며 사용자와 전자 상거래가 이루어진다.

③ Mediator
전자상거래시 XML 전자서명 문서에 필요한 각각의 엘리먼트를 생성하며 모바일 핸드폰에 SignInfo의 Canonicalization 결과물을 전송한다. 최종적으로는 SignatureValue와 다른 정보들을 모바일 핸드폰으로부터 전송받아 XML 전자서명 문서를 생성한다.

④ 인증기관
사용자에게 인증서를 발급하며 전자서명된 문서를 검증하기 위한 정보(공개키 및 인증서에 관한 정보)를 제공한다.

⑤ 금융기관
사용자와 컨텐츠 제공자 사이의 거래를 위한 금융 서비스를 제공하는 곳으로써 사용자에 의해 전자서명된 문서를 검증하고 지불 결제를 처리한 후 컨텐츠 제공자에게 지불 결제 완료를 통보한다.

3.2 전자서명 알고리즘

① 전자서명 애플리케이션

본 논문에서 제안한 시스템에서 전자서명은 Content Provider로부터 전송된 XML 문서로부터 Mediator에 의해 생성된 SignInfo의 정규화 결과물을 무선 단말기에 전송하고 SignInfo 정규화 결과물(다이제스트 값)과 인증기관으로부터 발급 받은 인증서를 통해 생성된 개인키를 통하여 서명 값 r, s를 생성함으로써 이루어진다. 전자서명 후 생성된 r, s 값과 사용된 키 값은 다시 Mediator로 전송한다. 본 논문에서는 전자서명 알고리즘으로 DSA(Digital Signature Algorithm)을 사용하였으며 DSA 알고리즘 중 전자서명은 다음과 같이 r과 s 값을 계산함으로써 이루어진다[5, 6, 9].

```
r = (g^k mod p) mod q
s = (k^-1(SHA^-1(M) + private_key * r)) mod q
BigInteger Sign_Result_R = G.modPow(k, P).mod(Q);
BigInteger Private_key_R_Plus_h =
    Sign_Result_R.multiply(private_key).add(h);
BigInteger Sign_Result_S =
    k_inverse.multiply(Private_key_R_Plus_h).mod(Q);
```

따라서 r, s 값을 무선 단말기 내에서 계산하기 위해 Java Card에서 제공하는 API를 이용하여 다음과 같이 구현하였다.

본 논문에서 구현한 전자서명 애플리케이션에 사용된 중요한 변수 및 함수는 <표 1>과 같다.

〈표 1〉 전자서명 애플리케이션 데이터

변수 및 함수	내 용
P, Q, G	전자서명에 필요한 키
private_key	전자서명시 사용되는 개인키
Sign_Result_R, Sign_Result_S	전자서명후 생성되는 r, s 값
h	Mediator로부터 전송되는 SignInfo 엘리먼트의 Canonicalization 결과물(다이제스트 값)
verify()	생성된 값과 키 정보를 Mediator에 전송하여 전자서명을 검증하기 위한 함수
install()	Java Card내 애플릿 설치
process()	Java Card내 전자서명 연산처리

Java Card내에서 전자서명 처리하기 위해 r, s 값을 계산하는 process 모듈은 다음과 같이 구현하였다.

```
public void process(APDU apdu)
    {
        ...
        byte[] Temp_p = {(byte)0x8d, ... ,(byte)0x91}; //
        생성된 P 값(64byte)
        byte[] Temp_q = {(byte)0xc7, ... ,(byte)0x5f}; //
        생성된 Q 값(20byte)
        byte[] Temp_g = {(byte)0x62, ... ,(byte)0x02};
        //생성된 G 값(64byte)
        BigInteger P = new BigInteger(1, Temp_p); //
        P값을 BigInteger 형으로 전환
        BigInteger Q = new BigInteger(1, Temp_q); //
        Q값을 BigInteger 형으로 전환
        BigInteger G = new BigInteger(1, Temp_g); //
        G값을 BigInteger 형으로 전환
        byte[] Temp_k = {(byte)0x35, ...,(byte)0xbf}; //
        생성된 k 값
        BigInteger k = new BigInteger(1, Temp_k); // k
        값을 숫자로 변환
        byte[] Temp_k_inverse = {(byte)0x0d,
        ...,(byte)0x17}; //k-1 값
        BigInteger k_inverse = new BigInteger(1,
```

```
        Temp_k_inverse);
        //k-1 값를 BigInteger 형으로 변환
        BigInteger h = new BigInteger(1, Temp_Digest);
        // SignInfo 엘리먼트 정규화 결과값을 숫자로 변환
        byte[] stored_private_key = {(byte)0x20, …,
        (byte)0x14};// 개인키 값
        BigInteger private_key = new BigInteger(1,
        stored_private_key);
        // 개인키를 숫자로 전환
        BigInteger Sign_Result_R = G.modPow(k,
        P).mod(Q);
        // R 값 계산
        BigInteger Private_key_R_Plus_h =
        Sign_Result_R.multiply(private_key).add(h);
        // 해시값 + (R*개인키값) 계산
        BigInteger Sign_Result_S =
        k_inverse.multiply(Private_key_R_Plus_h).mod(Q);
        // S 값 계산
         …
}
```

② 전자서명 검증 애플리케이션

전자서명된 문서를 검증하기 위해서는 서명시 생성된 값(r, s)과 사용된 키 정보, 공용키를 이용하여 복호화함으로써 이루어지며, 사용한 DSA의 검증 알고리즘은 다음과 같다.

$w = (s')^{-1} \bmod q$
$u1 = (SHA^{-1}(M') * w) \bmod q$
$u2 = (r' * w) \bmod q$
$v = ((g^{u1} * public\_key^{u2}) \bmod p) \bmod q$

본 논문에서는 전자서명에 대한 검증 애플리케이션 역시 Java Card에서 제공하는 API를 이용하여 검증시 필요한 값을 계산하는 연산을 다음과 같이 구현하였다.

```
BigInteger W = Sign_Result_SS.modInverse(QQ);
BigInteger u1 = Verify_hash.multiply(W).mod(QQ);
BigInteger u2 = Sign_Result_RR.multiply(W).mod(QQ);
BigInteger v1 = GG.modPow(u1, PP);
BigInteger v2 = public_key.modPow(u2, PP);
BigInteger v = v1.multiply(v2).mod(PP).mod(QQ);
```

또한 본 논문에서 구현한 전자서명 검증 애플리케이션에 사용된 중요 데이타는 <표 2>와 같다.

<표 2> 전자서명 검증 애플리케이션 데이터

변수 및 함수	내 용
PP, QQ, GG	전자서명에 사용되었던 키
public_key	전자서명을 검증할 때 사용되는 공용키
W, u1, u2, v1, v2, v	전자서명의 검증시 생성되는 값
Hash	SignInfo 엘리먼트의 Canonicalization 결과물 (다이제스트 값)

3.2 전자 서명 절차

본 논문에서 제안한 시스템에서 XML 전자서명 절차는 다음과 같다.

① 사용자가 상품을 구매
② XML 구매 문서를 Mediator에 전달
③ XML 서명 문서 작성
- Reference 엘리먼트, SignedInfo 엘리먼트 생성
  SignedInfo Canonicalization 결과물 단말기 전송
- 무선 단말기의 연산 처리
  - 개인키를 이용한 SignatureValue 계산
  - SignatureValue와 KeyInfo 등을 Mediator에 전달
- Signature 엘리먼트 생성

④ XML 서명 문서와 구매 문서를 금융 기관에 전송
⑤ 금융기관에서는 서명문서와 구매문서 검증
- 참조 검증
  - 구매 문서를 transform 한 뒤 다이제스트 값 계산
  - XML 서명 문서내의 다이제스트 값과 비교
- 서명 검증
  - SignedInfo Canonicalization 결과물 계산
  - 공개키와 SignatureValue를 가지고 복호화

⑥ 검증 완료 후 결제 완료
⑦ 사용자에게 결제 완료를 통보

3.4 XML 메시지 코드

다음 (그림 2)는 본 논문에서 사용한 XML 전자서명 문서의 예제를 보여주고 있다. 무선 단말기의 경우 단말기의 성능이 유선 환경의 단말기보다 현저하게 떨어지기 때문에 (그림 2)와 같은 XML 전자서명 문서를 직접 생성하기가 어렵다. 따라서 <SignatureValue> 엘리먼트에 들어갈 실제 서명 값을 계산하기 위해 XML 전자서명 문서 중 다이제스트 값(E6lwx3RvEPS0vKtMep4NbeVu8nk)만을 무선 단말기로 전송한다. 이러한 다이제스트 값을 본 논문에서는 자바 카드에서 제공하는 API를 이용하여 숫자 값

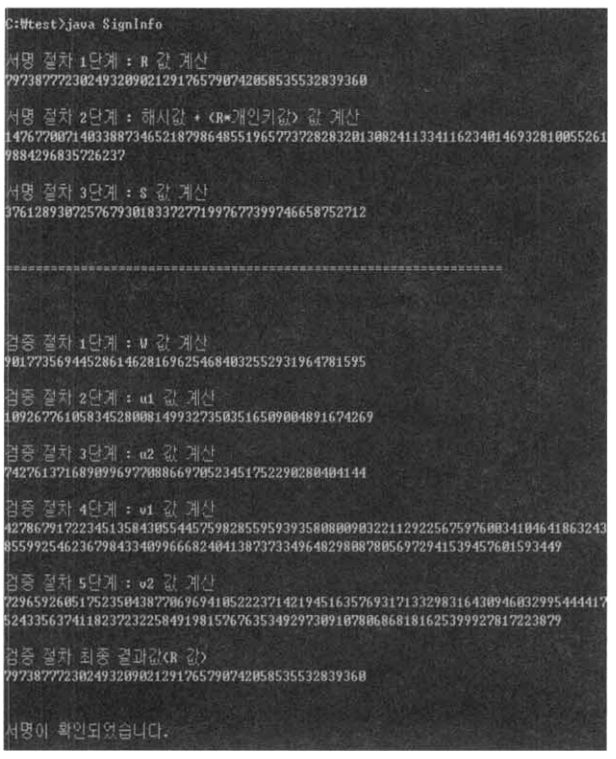
으로 전환한 후 서명 값(797387772300...)을 계산하도록 구현하였다.

```
<?xml version="1.0" encoding="UTF-8"?>
<Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
<SignedInfo Id="Example">
<CanonicalizationMethod
    Algorithm "http://www.w3.org/TR/2001/REC xml c14n-20010
    315"/>
<SignatureMethod
    Algorithm="http://www.w3.org/2000/09/xmldsig#dsa-sha1" />
<Reference URI="http://larkspur.hannam.ac.kr/example.htm">
<DigestMethod
    Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
<DigestValue>E6lwx3RvEPS0vKtMep4NbeVu8nk=</DigestValue>
</Reference>
</SignedInfo>
<SignatureValue>797387772300...</SignatureValue>
</Signature>
```

(그림 2) XML 전자서명 메시지 코드

3.3 실행결과

본 논문에서 구현한 애플리케이션의 실행 결과는 (그림 3)과 같다. 전자서명 애플리케이션과 검증 애플리케이션에 의해 R, S 값을 계산하여 전자서명이 이루어지고, 서명된 값과 공용키, 사용된 키 값에 따라 서명의 검증이 올바르게 수행되는 것을 볼 수 있다.



(그림 3) 전자서명 및 검증 결과

4. 비교 분석

본 논문에서 제안한 시스템과 WPKI, Hermes 시스템을 비교 분석한 결과는 <표 3>과 같다.

WPKI 환경의 인증 시스템을 구현하기 위해서는 인증기관, 서비스 제공업체, 금융기관, 무선 단말기 제공 업체, 통신 업체 시스템간의 유기적인 상호 연동이 필요하다. 하지만 아직까지 WPKI의 표준이 완벽하게 이루어지지 않고 있기 때문에 이질적인 환경에서 WPKI 기반의 인증 시스템을 구현하기는 매우 어렵다[3, 17]. 또한 Hermes 시스템의 경우는 XML 전자문서를 전자상거래에 사용하였지만, 실제적인 전자서명은 XML 전자서명 기법이 아닌 트랜잭션(메시지)에 전자서명하는 기법을 사용한 시스템이기 때문에 기존 XML 전자서명 시스템과 상호 연동이 어렵다[10]. 하지만 본 논문에서 제안한 시스템은 XML 전자서명을 이용하여 전자서명하기 때문에 기존 XML 전자서명 시스템을 그대로 사용할 수 있고, 새로운 컨텐츠 제공자와 통합함에 있어 XML을 이용하므로 쉽게 통합이 가능하다는 장점을 갖는다.

<표 3> WPKI와 Hermes 시스템과의 비교분석

	WPKI	Hermes 시스템	제안한 전자서명 시스템
서명 대상	컨텐츠, 트랜잭션	트랜잭션(메시지)	SignedInfo Canonicalization 결과물
다른 서비스 제공자와의 통합	시스템이 이질적인 경우 통합이 어려움	XML 문서를 이용하므로 통합 가능	XML 문서를 이용하므로 통합 가능
XML 전자서명 시스템과의 연동성	불가능	불가능	가능
구현 및 확장	이질적인 시스템에서 구현 및 확장이 어려움	확장시 컴포넌트 변경이 필요할 수 있음	기존의 XML 전자서명 시스템을 이용할 수 있음
안정성	좋음	좋음	-

5. 결 론

현재 유·무선 환경에서의 전자상거래가 활성화됨에 따라 WPKI, Hermes 시스템, PKI, XML 전자서명 기법과 같은 사용자 인증에 관한 연구와 무선 단말기 성능 향상을 위한 Smart Card 활용 연구가 활발하게 진행되고 있다. 하지만 WPKI 시스템은 인증 시스템이 서로 이질적이라 구현하기 어려운 단점을 가지고 있으며, Hermes 시스템 역시 XML 전자서명 시스템과 상호 연동가능하지 않은

문제점을 지니고 있다. 또한 아직까지 유·무선간의 인증 기술들이 상호 호환되지 않기 때문에 인증기관들은 유·무선에서 서로 다른 인증시스템을 구축해야 하는 문제점을 가지고 있다.

따라서 이러한 문제점을 해결하기 위해 본 논문에서는 무선 인터넷 환경에서 XML 전자서명 기법을 사용하여 유·무선 환경에서 전자서명 할 수 있는 전자서명 시스템을 설계 및 구현하였다. 또한 무선 단말기의 제한요소로 XML 전자서명을 단말기에서 모두 처리하기에는 사실상 불가능하므로, 전자서명 값의 계산을 Java Card에서 이루어질 수 있도록 구현하였다. 본 논문에서 제안한 전자서명 시스템은 무선 인터넷 환경에서의 XML 전자서명과 유·무선 전자서명 시스템간의 상호 연동이 가능하며, 기존 유선 인터넷에서 사용되는 XML 전자서명을 그대로 사용함에 따라 무선 인터넷 환경에서도 XML 전자서명을 사용할 수 있다.

향후 연구 과제로는 본 연구에서 제안하고 있는 시스템의 안정성과 데이터 보안에 관한 검증이 필요하고, 전자서명 알고리즘으로 무선 인터넷 환경을 위해 제안된 ECC(타원 곡선) 알고리즘을 제안한 시스템에 적용시키는 연구가 필요하다. 또한 무선 환경은 유선 환경보다 환경적으로 많은 제약점을 가지고 있기 때문에, XML 문서를 무선 환경에서 생성하거나 이용하기가 매우 어렵다. 따라서 본 논문에서는 XML 전자서명 값만을 무선 단말기에서 계산하도록 하였다. 하지만 이러한 전자서명 값을 무선으로 전송시킬 때 서명 값에 관한 보안이 필요하다. 서명 값에 대한 보안은 매우 중요한 사항이므로 이러한 보안 문제 해결을 위한 WTLS와 XML 보안에 관련된 연구가 필요하다.

참 고 문 헌

[1] XML-Signature Syntax and Processing, W3C, 12 February, 2002.

[2] Aphrodite Tsalgatidou, "Mobile Electronic Commerce : Emerging Issues," Procs of EC-WEB 2000, pp.477-486.

[3] WPKI(Wireless Public Key Infrastructure), Version 24 Apr., 2001.

[4] 장우영, 유승범, 장인걸, 차석일, 신동일, 신동규, "XML/ EDI와 XML 전자서명 통합 시스템의 설계", 한국정보처리학회 춘계 학술발표대회논문집, 제8권 제1호, 2001년, pp.407-410.

[5] Henna Pietiläinen, "Elliptic curve cryptography on smart cards," Helsinki University of Technology, 2000.

[6] Rivest, R. L., Shamir, A., Adleman, L., "A method for obtaining digital signatures and public key cryptosystems," ACM, 21(2), February, 1978.

[7] Patrice Peyret, 'Java CardTM Technology for Smart Cards : Architecture and Programmer's Guide,' Addison Wesley.

[8] Java CardTM 2.1.1 Development Kit User's Guide, Sun Microsystems.

[9] Digital Signature Standard(DSS), U.S. Department of Commerce/National Institute of Standard and Technology, January, 2000.

[10] Sebastian Fishmeister, "Hermes - A Lean M-Commerce Software Platform Utilizing Electronic Signatures," IEEE. Hawaii Internation Conference on system Sciences, 7th 10, January, 2002.

[11] Brokat. WWW Site. http://www.brokat.com

[12] Paybox. WWW Site. http://www.paybox.de

[13] 한국정보통신기술협회, http://www.tta.or.kr

[14] SK텔레콤, http://www.moneta.co.kr

[15] KTF, http://www.npaymagic.co.kr

[16] "XML Signature Syntax and Processing", 전자상거래 표준화 통합포럼, 2002.

[17] 구자동, "무선 인터넷 환경에서 WPKI 응용 발전 방안", KSIGN, 2003.

[18] Thomas Weigold, "Java-Based Wireless Identity Module", London Communications Symposium 2002.

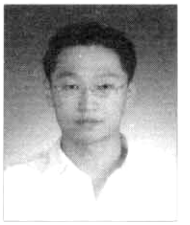
[19] 박근홍, 조성제, "무선 전자상거래를 위한 전자영수증 발급 및 검증 기법 구현", 정보처리학회논문지D, Vol.10, No.3, pp.0559-0566, 2003.

[20] 양대현, 이석준, "무선 인터넷을 위한 패스워드 기반의 인증 및 키 교환 프로토콜", 한국정보과학회논문지 I, Vol.29, No.03, pp.324-332, 2002.

[21] 강성민, 황기태, 김남윤, "M-Commerce를 위한 XML 전자계약서 저작 도구 설계 및 구현", 한국정보처리학회 춘계학술발표대회논문집, Vol.10, No.01, pp.2037-2040, 2003.

[22] 김세영, 원덕재, 송춘홍, 김현희, 신동규, 신동일, "XML 전자서명 시스템의 설계 및 구현", 한국정보처리학회 추계학술발표대회논문집, Vol.08, No.2, pp.891-894, 2001.

[23] 이주화, 설경수, 정민수, "자바카드 기반 무선 단말기용 사용자 인증 프로토콜의 설계 및 구현", 정보처리학회논문지 C, Vol.10, No.05, pp.585-594, 2003.



장 창 복

e-mail : chbjang@dblab.hannam.ac.kr

2000년 한남대학교 컴퓨터공학과(공학사)

2002년 한남대학교 컴퓨터공학과(공학석사)

2002년~현재 한남대학교 컴퓨터공학과 (박사과정)

관심분야 : 네트워크 보안, 액티브 네트워크, Middleware, 웹 DB, 실시간 데이터베이스

최 의 인

e-mail : cichoi@dblab.hannam.ac.kr

1982년 한남대학교 계산통계학과(학사)

1984년 홍익대학교 전자계산학과(이학석사)

1995년 홍익대학교 전자계산학과(이학박사)

1985년~1988년 공군 교육사 전산실장

1992년~1996년 명지전문대학 전자계산과 조교수

1996년~현재 한남대학교 컴퓨터공학과 부교수

관심분야 : 실시간 데이터베이스, 주기억 데이터베이스, 클라이언트/서버 데이터베이스