제1회 한국사이버테러정보전학회 춘계학술발표대회 (2004.5)

Java Card를 이용한 XML 전자서명 시스템 설계 및 구현

장창복*, 김동혁*, 최의인*
* 한남대학교 컴퓨터공학과

요 약

무선 인터넷과 무선 단말기의 성능이 발달함에 따라 기존 유선 환경에서의 전자상거래가 무선 인터넷 환경으로 이동하고 있다. 이러한 무선 인터넷 환경의 전자상거래를 M-Commerce라고 하며, 기존 유선 인터넷 전자상거래 환경처럼 사용자 인증 기술과 데이터 보안이 중요한 기술로 인식되고 있다. 이에 따라 WPKI, Hermes 시스템, XML 전자서명 같은 인증 기술이 연구되고 있다. 하지만 WPKI는 인증 시스템이 서로 이질적이라면 구현하기 어렵다는 점과 Hermes 시스템은 XML 전자서명 기법과 상호 연동되지 않는 단점을 가지고 있다. 따라서 본 논문에서는 무선 인터넷 환경에서도 기존의 유선 인터넷 환경에서 사용되고 있는 XML 전자서명 기법을 적용하여 XML 문서 및 전자서명 시스템들간에 상호 연동 가능할 수 있는 자바 카드 기반의 XML 전자서명 시스템을 구현하였다. 본 논문에서 제안한 시스템을 통해 무선 인터넷 환경에서도 XML 전자서명을 제공할 수 있고, XML 전자서명 시스템간에 상호 연동이 가능하다.

The Design and Implementation of XML Digital Signature System Using Java Card

Chang Bok Jang*, Dong Hyuk Kim*, Eui In Choi*

ABSTRACT

As developed wireless internet and performance of wireless terminal, E-commerce of wire internet move to wireless internet. This E-commerce in wireless internet environment called M-Commerce, recognized user authentication and data security as very important technology such as E-commerce in environment of wire internet. So authentication technology such as WPKI and Hermes system and XML digital signature was studied. But WPKI is difficulty to implement system, if authentication system that consisted in WPKI environment was heterogeneous. And Hermes system is not interoperate to XML digital signature system. So, our paper suggested XML digital signature system baed java card to interoperate among the digital signature system, to apply XML digital signature used in wire internet. Our system offer XML digital signature in wireless internet, can interoperate among the XML digital signature systems.

본 연구는 과학기술부 지역협력연구사업(R12-2003-004 -03002-0) 지원으로 수행되었음

1. 서 론

무선 인터넷의 발달과 무선 단말기 성능의 발달로 무선 인터넷을 이용한 전자상거래가 많이 활성화 되고 있다. 이러한 무선 단말기를 이용한 전자 상거래를 M-Commerce 라고 한다[2]. 기존의 유선 인터넷 사용자들은 전자상거래시 자신이 실제 거래자임을 확인시키기 위해 인증기관으로부터 인증서를 발급 받고 이 인증서를 통해 거래문서에 전자 서명하는 방법을 사용하고 있다. 또한 XML 기술이 발달함에 따라 상거래시 XML 문서를 사용하기 위한 연구와 XML 전자서명 기술 역시 연구되고 있다[1, 4]. 따라서 무선 인터넷 환경에서도 기존 유선 인터넷 환경에서처럼 사용자 인증을 통해 거래 당사자를 확인하는 기술이 필요하며, 이에 관한 연구로 WPKI나 Hermes 시스템들이 있다[3, 10]. 하지만 아직까지 WPKI 시스템은 인증 시스템들이 서로 이질적이면 구현하기가 어렵고, Hermes 시스템은 XML 전자서명 시스템과 상호 연동하지 않은 단점을 지니고 있다.

따라서 본 논문에서는 기존의 유선 인터넷 환경에서 사용되고 있는 XML 전자서명 기법을 무선 인터넷 환경에 적용하여 유선 인터넷 환경의 XML 문서와 상호 연동 가능하기 위해 Java Card를 이용하여 전자서명 시스템을 구현하였다.

2. 관련 연구

무선 인터넷 환경에서 데이터 보안 및 사용자 인증에 관한 연구로는 WPKI(Wireless Public Key Infrastructure)[6]와 독일의 Hermes 시스템이 연구되고 있고, 유선 인터넷 환경에서는 XML 문서를 이용한 전자 상거래 연구가 활발하게 진행됨에 따라, XML 문서에 전자서명 할 수 있는 XML 전자서명 기법이 연구되고 있다. 또한 무선 인터넷 환경에서 사용되는 단말기는 환경적인 요인으로 인하여 그 성능이 유선 인터넷의 단말기 보다 현저하게 떨어진다. 특히 단말기의 처리 성능이 매우 낮기 때문에 보안 및 인증 알고리즘의 구현이 어렵다. 따라서 이러한 단점을 보완하고자 Java Card와 같은 스마트 카드를 이용한 단말기 성능 향상 연구가 이루어지고 있다.

2.1 Java Card

Java card는 smart card에 Java system software를 구축하기 위해 Java 언어의 특징을 부분적으로 지원하고 이를 실행시킬 수 있는 가상 머신(Virtual Machine)을 구현한 것을 말한다[7, 8]. Java Card의 가상 머신은 크게 두 부분으로 나누어지며, 하나는 off-card에서 동작하고 나머지는 on-card에서 동작한다. 즉, 실행시점에 처리되는 부분 중에서 클래스 로딩(class loading), 바이트 코드 검증(byte code verification), 클래스 linking과 resolution 부분은 자원에 제약을 받지 않는 off-card에서 처리되고, 그 외의 암호화 알고리즘과 같은 부분은 on-card에서 처리한다.

2.2 WPKI

WPKI는 무선 환경을 위해 기존의 유선 인터넷의 PKI 방식을 최적화하여 확장시킨 것으로, WAP 포럼에서 제안하였다[3]. WPKI 환경에서 사용자가 서비스 제공자와 보안 통신을 하거나 트랜잭션에 전자서명을 하기위해서는 인증기관에 등록한 뒤 인증서를 발급받아야 한다. 사용자는 발급 받은 인증서를 통하여 무선 단말기에 저장된 비밀키로 문서에 전자서명하고 전자 서명된 문서를 WAP 게이트웨이를 통해 웹 서버로 보낸다. 웹 서버에서는 다시 인증기관으로 서명된 문서를 보내어 문서를 검증한다.

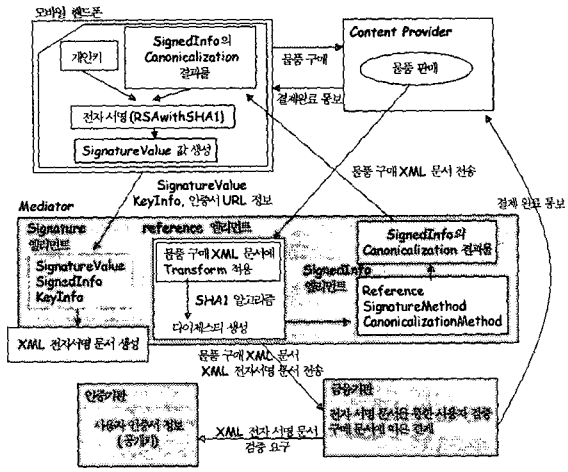
2.3 Hermes 시스템

Hermes 시스템은 독일의 Constance 대학교에서 제안한 것으로, 무선 인터넷 환경에서 전자서명을 이용하여 사용자 인증을 처리한 시스템이다[10]. Hermes 시스템에서 전자 서명하는 절차로는 먼저 Mediator가 서비스 제공자로부터 XML 문서를 수신한다. XML 문서가 수신되면 Request receiver가 XML 파서를 이용하여 XML 문서의 표준 형태를 검사하고, frontendcommunicator가 Front-end에 displaying하기 적당한 형태의 전자서명을 위한 메시지를 생성하며, 생성된 메시지를 무선 단말기에 전송한다. Mobile Phone으로 전송된 메시지는 Signature Front End 모듈에 의해 전자서명 되며, 서명된 메시지는 다시 Mediator에게 전송된다. 서명된 메시지를 수신한 Mediator는 verifier에서 서명된 메시지를 Trust Center를 통하여 검증하고 검증이 완료되면 서명된 메시지를 새로운 XML 문서를 작성하기 위하여 Financial-institute communicator로 전달한다. 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. Financial-institute에서는 XML 문서와 전송된 전자서명 메시지를 검증하고 서비스를 처리한다. 처리된 서비스는 다시 Mediator의 Verifier에 서명된 영수증 형태로 전송되고 이를 Verifier에서는 Trust Center를 통해 검증한다.

3. Java 카드 기반의 전자서명 시스템 설계 및 구현

3.1 XML 전자서명 시스템

무선인터넷 환경은 무선 단말기 성능 제한과와 작은 대역폭 같은 제한 요소로 인하여 XML 전자서명을 무선단말기에서 처리하기에는 사실상 불가능하다. 따라서 본 논문에서는 XML 전자서명 과정 중 전자서명 값을 계산하는 부분만 무선 단말기에서 수행하도록 연산을 분산시켜 설계하였다. (그림 1)은 본 논문에서 제안하는 XML 전자서명 시스템 구조이다.



(그림 1) XML 전자서명 시스템

본 논문에서 제안한 시스템을 구성하고 있는 요소로는 다음과 같다.

① 모바일 핸드폰

사용자가 물품을 구매하고 전자서명하기 위해 사용되는 수단이며, 실제 서명에 필요한 Signature Value를 계산하는 부분이다.

② 컨텐츠 제공자(Content Provider)

유선 인터넷 환경에서 컨텐츠 제공을 담당하며 사용자와 전자 상거래가 이루어진다.

③ Mediator

전자상거래시 XML 전자서명 문서에 필요한 각각의 엘리먼트를 생성하며 무선 단말기에 SignInfo의 Canonicalization 결과물을 전송한다.

최종적으로는 SignatureValue와 다른 정보들을 무선 단말기로부터 전송받아 XML 전자서명 문서를 생성한다.

④ 금융기관

전자상거래시 실제 지불 결제가 이루어지는 기관으로 XML 전자서명 문서를 검증하여 상거래를 처리한다.

⑤ 인증기관

사용자의 인증서를 발급하고 금융기관으로부터의 사용자의 인증을 처리하는 기관이다.

3.2 전자서명 알고리즘

① 전자서명 애플리케이션

본 논문에서 제안한 시스템에서 전자서명은 Mediator로부터 생성된 SignInfo의 정규화 결과물을 무선 단말기에 전송하고 SignInfo 정규화 결과물과 저장된 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, 전자서명에 필요한 데이터와 함수를 <표 1>과 같이 설계하였다.

<표 1> 전자서명 애플리케이션 데이터 및 함수

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

무선 단말기에서의 전자서명 처리를 위한 R과 S 값의 계산은 다음과 같이 구현하였다.

```
public void process(APDU apdu)
 {
 …
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

서명시 생성된 값을 사용하여 금융기관이나 서명을 확인할 필요가 있는 부분에서 서명값과 사용된 키 정보 그리고 공용키를 이용하여 검증한다. 본 논문에서 제안한 전자서명 검증 시 필요한 데이터는 <표 2>와 같다.

<표 2> 전자서명 검증 애플리케이션 데이터

변수 및 함수	내용
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 Canonicaliza-tion 결과물

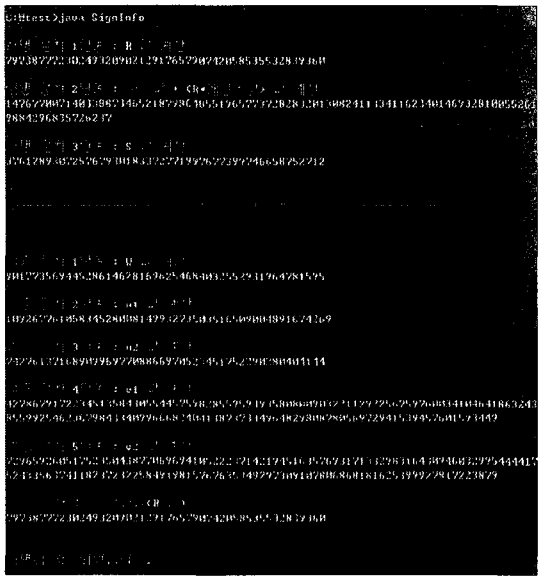
검증 함수 verify()의 소스는 다음과 같다.

```
public static void verify (byte[]
Temp_Sign_Result_RR, byte[]
```

```
Temp_Sign_Result_SS,
 byte[] Temp_pp, byte[] Temp_qq, byte[] Temp_gg)
{
...
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);
...
}
```

3.3 실행결과

본 논문에서 구현한 전자서명 애플리케이션의 실행 결과는 다음 (그림 2)와 같다. 전자서명과 검증이 올바르게 수행되는 것을 볼 수 있다.



(그림 2) 전자서명 및 검증 결과

4. 결론 및 향후 연구 과제

현재 유·무선 환경에서의 전자상거래가 활성화됨에 따라 사용자 인증에 관한 연구들이 이루어지고 있다. 이러한 기술로는 WPKI, Hermes 시스템, XML 전자서명 기법들이 있지만, 아직까지 이질 인증 시스템 환경에서의 WPKI의 구현 문제나 Hermes 시스템의 XML 전자서명 시스템과의 상호 연동 불가능 같은 문제점을 가지고 있다.

따라서 본 논문에서는 이러한 문제점을 해결하기 위해 무선 인터넷 환경에서 XML 전자서명 기법을 사용할 수 있도록 자바 카드 기반의 전자서명 시스템을 설계 및 구현하였다. 자바 카드를 이용한 XML 전자서명은 무선 인터넷 환경에서도 XML 전자서명이 가능하고, XML 문서와의 상호 연동 가능성이나 유·무선 전자서명 시스템간의 상호 연동성을 높일 수 있다.

향후 연구 과제로는 본 연구에서 제안하고 있는 시스템을 실제 무선 환경에 적용할 필요가 있으며, 보안 및 안정성 검증에 관한 연구가 필요하다.

참고문헌

[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/ EDI 와 XML 전자서명 통합 시스템의 설계, 한국정보처리 학회 춘계 학

술발표 제 8권 제 1호, 2001년, pp.407-410
[5] Henna Pietiläinen, Elliptic curve cryptography on smart cards, Helsinki University of Technology, 2000
[6] R.L. Rivest, A.Shamir, L.Adleman, 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, 2000 January 27
[10] Hermes - A Lean M-Commerce Software Platform Utilizing Electronic Signatures, Sebastian Fishmeister, IEEE. Hawaii International Conference on system Sciences, January 7th 10, 2002

장 창 복

2000년 한남대학교 컴퓨터공학과(공학사)
2002년 한남대학교 컴퓨터공학과(공학석사)
2002년 ~ 현재 한남대학교 컴퓨터공학과 박사과정

김 동 혁

1991년 한밭대학교 산업공학과(공학사)
2001년 한남대학교 컴퓨터공학과(공학석사)
2001년 ~ 현재 한남대학교 컴퓨터공학과 박사수료

최 의 인

1982년 숭전대학교 계산통계학과(학사)
1984년 홍익대학교 전자계산학과(이학석사)
1995년 홍익대학교 전자계산학과(이학박사)
1996년 ~ 현재 한남대학교 컴퓨터공학과 부교 수