무선 인터넷 환경에서 Java Card를 이용한 XML 전자서명 시스템 구현

장창복° 김동혁 조성훈, 최의인
한남대학교 컴퓨터 공학과
{chbjang°, dhkim, shcho, eichoi}@dblab.hannam.ac.kr

Implementation of XML Digital Signature System Using Java Card in Mobile Environment

Chang-Bok Jang° Dong-Hyuk Kim Sung-Hoon Cho Eui-In Choi
Dept. of Computer Engineering, Hannam University

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 유선 인터넷 환경에서의 XML 전자서명 같은 인증 기술이 연구되고 있다. XML 전자서명은 XML 문서를 이용하는 전자상거래분야에 사용되어 전자서명 시스템간의 상호 연동성을 높일 수 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 시스템을 설계하였고, 실제로 자바 카드를 이용하여 XML 전자서명이 가능한 시스템을 구현하였다. 본 논문을 통해 무선 인터넷 환경에서도 XML 전자서명을 제공할 수 있다.

1. 서 론

무선 인터넷의 이동성과 물리적으로 네트워크와 연결되어 있지 않아도 되는 장점으로 인해 무선 인터넷을 이용한 전자상거래가 많이 활성화 되고 있다. 이러한 무선 단말기를 이용한 전자 상거래를 Mobile Commerce 또는 M-Commerce 라고 한다[2]. 기존의 유선 인터넷 사용자들은 전자상거래시 자신이 실제 거래자임을 확인시키기 위해 인증기관으로부터 인증서를 발급 받고 이 인증서를 통해 거래문서에 전자서명하는 방법을 사용하고 있다. 또한 전자상거래시 XML 문서를 이용하기 위한 방법과 XML 문서에 전자서명 하기 위한 기법이 연구되고 있다[1, 4]. 따라서 M-Commerce에서도 기존 유선 인터넷 환경에서처럼 사용자 인증을 통한 거래 당사자 확인 과정이 필요하며, WPKI와 같은 연구들이 이루어지고 있다[3]. 하지만 아직까지 무선인터넷 환경과 유선 인터넷 환경에서의 인증 기술이 서로 상호 호환되지 않고 있어, 유·무선 인증시스템을 서로 다르게 구축해야 한다는 문제점이 존재한다.

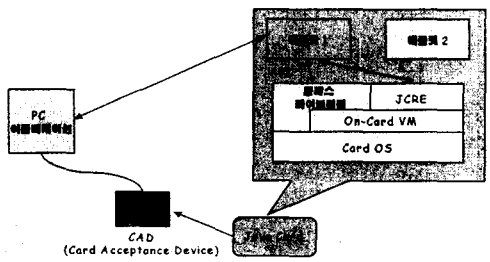
따라서 본 논문에서는 기존의 유선 인터넷 환경에서 사용되고 있는 XML 전자서명 기법을 무선 인터넷 환경에 적용하여 유선 인터넷 환경의 XML 문서와 상호 연동 가능하기 위해 J2ME 기반의 Java Card를 이용하여 전자서명 시스템을 구현하였다.

2. 관련 연구

무선 인터넷 환경에서 데이터 보안 및 사용자 인증에 관한 연구로는 WPKI(Wireless Public Key Infrastructure)[6]가 많이 연구되고 있으며, 유선 인터넷 환경에서는 PKI 기반의 사용자 인증 기술이 연구되었다. 또한 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 보안하고자 현재 Java Card와 같은 스마트 카드를 이용한 단말기 성능 향상의 연구가 이루어지고 있다.

2.1 Java Card 구조

Java Card는 Java로 쓰여진 프로그램이 smart card나 혹은 그 밖에 제한적인 자원을 가진 장치에서의 동작을 가능하도록 연구된 기술이다. 아래의 그림은 본 논문에서 구현하고자 하는 Java Card의 구조를 보여주고 있다[7, 8, 9].



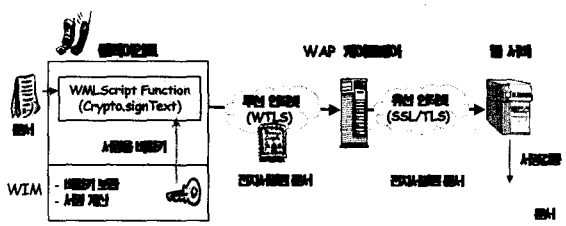
[그림 2] 자바 카드 구조

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

Java card는 smart card에 Java system software를 구축하기 위해 자바 언어의 특징을 부분적으로 지원하고 이를 실행시킬 수 있는 가상 머신(Virtual Machine)을 구현하였다. Java Card의 가상 머신은 두 부분으로 나누어지며, 하나는 off-card에서 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 포럼의 WPKI 표준이 가장 일반적으로 사용된다[3]. 사용자가 서비스 제공자와 보안 통신을 하거나 트랜잭션에 전자서명을 하기위해서는 인증기관에 등록한 뒤 인증서를 발급받아야 한다. 발급 받은 인증서를 통하여 무선 단말기에 저장된 비밀키와 서명함수를 이용하여 문서에 전자서명한다. 이러한 전자서명된 문서를 WAP 게이트웨이를 통해 웹 서버로 보내고 웹 서버에서는 다시 인증기관으로 서명된 문서를 보내어 문서를 검증하게 된다. 다음 [그림 2]는 이러한 구조를 보여주고 있다.



[그림 2] WPKI 환경에서의 전자서명 구조

2.2 XML 전자서명

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

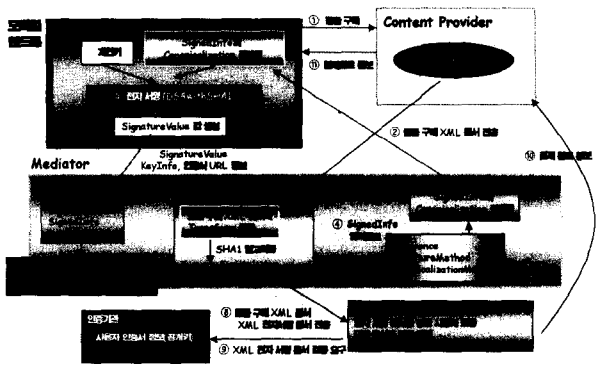
① Signature : XML 전자서명 문서의 부모 엘리먼트
② SignatureValue : SignatureMethod에 정의된 알고리즘을 적용하여 생성한 전자서명의 실제적인 값을 가지고 있다.
③ SignedInfo : Canonicalization 알고리즘, Signature 알고리즘, 또는 Reference를 포함한다.
④ CanonicalizationMethod : XML 문서를 정규화하기 위해 필요한 알고리즘을 포함한다.
⑤ SinatureMethod : 실제적인 서명값을 생성하기 위해 사용되는 알고리즘 명시
⑥ Reference : 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. 전자서명 시스템 설계 및 구현

3.1 XML 전자서명을 사용한 시스템

가. 무선 인터넷 환경에서의 XML 전자서명 시스템

무선인터넷 환경이 가지는 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 3]은 본 논문에서 제안하고자 하는 무선 인터넷 환경에서의 XML 전자서명 시스템 구조이며 무선 단말기, 컨텐츠 제공자, Mediator로 구성되어져 있다.



[그림 3] 무선 인터넷 환경에서의 XML 전자서명 구조

① 모바일 핸드폰
사용자가 물품을 구매하고 전자서명하기 위해 사용되는 수단이며 실제 서명에 필요한 SignatureValue를 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.

나. 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 DSA 알고리즘 중 전자서명은 다음과 같이 r과 s 값을 계산함으로써 이루어진다[5, 6, 9].

$$r = (g^{k} \bmod p) \bmod q$$
$$s = (k^{-1}(SHA^{-1}(M) + private\_key * r)) \bmod q$$

또한 r, s 값을 구하기 위한 연산처리를 Java Card에서 제

공하는 API를 이용하여 다음과 같이 구현하였다.

```
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);
```

② 전자서명 검증 애플리케이션

서명시 생성된 값을 사용하여 금융기관이나 서명을 확인할 필요가 있는 부분에서 서명값과 사용된 키 정보 그리고 공용키를 이용하여 검증한다. DSA에서 검증시 사용되는 알고리즘은 다음과 같다.

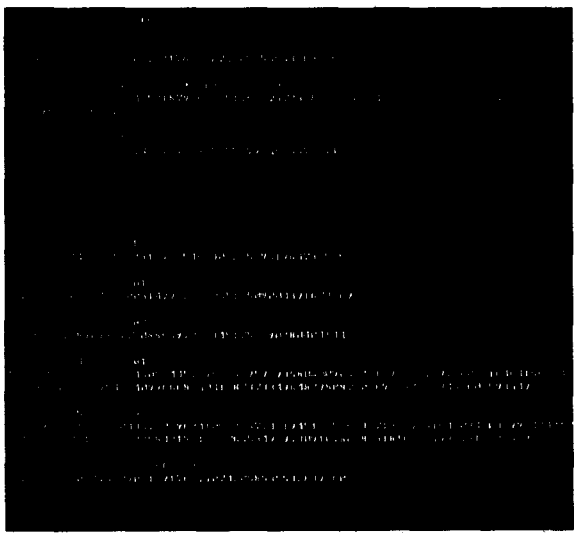
$$w = (s')^{-1} \bmod q$$
$$u1 = (SHA^{-1}(M') * w) \bmod q$$
$$u2 = (r' * w) \bmod q$$
$$v = ((g^{u1} * public\_key^{u2}) \bmod p) \bmod q$$

전자서명에 대한 검증 어플리케이션 역시 Java Card에서 제공하는 API를 이용하여 다음과 같이 구현하였다.

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

3.2 실행결과

본 논문에서 구현한 어플리케이션의 실행 결과는 다음 그림과 같다. 전자서명과 검증이 올바르게 수행되는 것을 볼 수 있다.



[그림 5] 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, PKI, XML 전자서명 기법들이 있지만, 아직까지 유·무선간의 인증기술들이 상호호환되지 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 사용할 수 있도록 자바 카드의 API를 이용한 전자서명 시스템을 설계 및 구현하였다. 자바 카드를 이용한 XML 전자서명은 무선 인터넷 환경에서도 XML 전자서명이 가능하고, 또한 전자상거래시 많이 사용하고 있는 XML 문서와의 상호 연동 가능성이나 유·무선 전자서명 시스템간의 상호 작용성을 높일 수 있으며, 기존 유선 인터넷에서 사용되는 XML 전자서명의 장점을 그대로 사용함에 따라 확장 가능한 전자서명 포맷을 제공할 수 있다.

향후 연구 과제로는 본 연구에서 제안하고 있는 시스템의 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, 한국정보처리학회 춘계 학술발표 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