무선 인터넷 환경에서 XML 전자서명 기법을 이용한 전자서명 시스템

장창복° 김동혁 백주현* 이민희 최의인
한남대학교 컴퓨터 공학과
한국전산원*
{chbjang°, dhkim, mhl, eichoi}@dblab.hannam.ac.kr
Bbaek@nca.or.kr*

Digital Signature System Using XML Signature in Mobile Environment

Chang-Bok Jang° Dong-Hyuk Kim Joo-Hyun Baek* Min-Hee Lee Eui-In Choi
Dept. of Computer Engineering, Hannam University
National Computerization Agency*

요 약

무선 인터넷의 급속한 발전으로 인해 무선 단말기를 이용한 전자상거래(M-Commerce)가 활성화되고 있다. 이러한 전자상거래에서는 데이터 보안이나 사용자 신원 확인 같은 인증이 유·무선 인터넷 환경 모두 중요한 기술로 인식되고 있기 때문에 무선 인터넷에서의 WPKI나 유선 인터넷 환경에서의 XML 전자서명 같은 연구가 활발히 진행되고 있다. XML 전자서명은 XML문서를 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 제안하였다. 본 논문을 통해 무선 인터넷 환경에서도 확장 가능한 XML 전자서명 포맷을 제공할 수 있다.

1. 서 론

무선 단말기가 물리적인 선을 통해 네트워크를 사용해야 하는 한계가 없고 이동하며 가지고 다닐 수 있을 만큼 작기 때문에 무선 통신을 이용한 전자상거래가 활성화 되고 있다. 이러한 무선 단말기를 이용한 E-Commerce 트랜잭션을 Mobile Commerce 또는 M-Commerce 라고 한다. 기존의 유선 인터넷 사용자들은 전자상거래시 자신이 실제 거래 당사자임을 확인시키기 위해 인증기관(CA: Certification Authority)으로부터 인증서를 발급 받고 이 인증서를 통해 거래문서에 전자서명하는 방법을 사용하고 있으며 최근 XML 문서를 이용한 전자상거래가 활발히 연구되고 있기 때문에 XML 전자서명 기법[1, 7]을 사용하기 위한 연구가 진행되고 있다. 이처럼 무선 인터넷에서도 무선 단말기를 이용하여 전자상거래를 하기 위해서는 전자서명을 위한 절차 및 방법에 관한 연구가 필요하다.

본 논문에서는 기존의 유선 인터넷 환경에서 사용되고 있는 XML 전자서명 기법을 무선 인터넷 환경에 적용하여 유선 인터넷 환경의 XML 문서와 상호 연동 가능한 전자서명 시스템을 제안한다.

2. 관련 연구

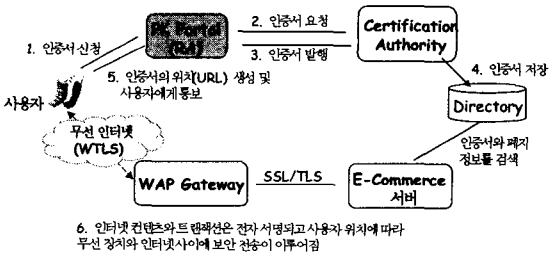
무선 인터넷 환경에서 데이터 보안 및 인증에 관한 연구로는 WAP의 WPKI(Wireless Public Key Infrastructure)[6]가 대표적인 기술이다. 하지만 이러한 인증 기술은 아직까지 완벽한 표준이 확립되어 있지 않은 상태이기 때문에 많은 지불결제 시스템에서는 표준이 확립되지 않은 상태로 지불 시스템을 구현하고 있다. 지불 시스템들로 Hermes[2], Paybox[3], Brokat[4] 같은 것이 있다. 또한 유선 인터넷 환경에서는 XML 문서를 이용한 전자 상거래 연구가 활발하게 이루어지고 있고 이러한 XML 문서에 전자서명 할 수 있는 XML 전자서명 기법에 관한 연구가 이루어지고 있다.

2.1 WPKI

WPKI는 PKI를 구현하기 위해 새롭게 만들어낸 표준이 아닌 무선 환경을 위해 기존의 PKI 방식을 최적화하여 확장시킨 것이다. 무선 네트워크 상에서는 WAP 포럼의 WPKI 표준이 가장 일반적으로 사용된다[6].

① WPKI 구조와 데이터 흐름

사용자가 서비스 제공자와 보안 통신을 하거나 트랜잭션에 전자서명을 하기위해서는 PKI에 등록한 뒤 인증서를 발급받아야 한다. 다음 [그림 1]은 이러한 처리를 보여주고 있다.



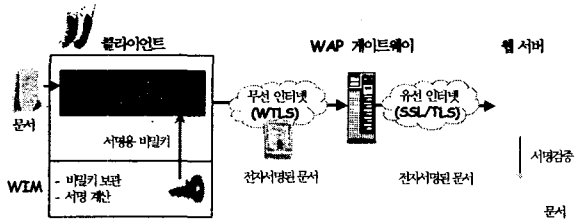
[그림 1] WPKI의 구성요소 및 인증서 발급 절차

② WPKI 인증 형식과 암호 알고리즘

WPKI 인증 형식으로는 표준인 X.509 인증과 서버측 인증을 위해 새롭게 제한한 WTLS 인증 형식을 사용하며 ECC (Elliptic Curve Cryptography) 알고리즘[8]을 통해 인증 크기를 감소시켰다.

③ WPKI의 전자서명

WAP에서 제안하고 있는 WPKI는 무선 단말기에 저장된 비밀키와 서명하려는 문서를 WMLSCrypt의 Crypto.signText 함수를 이용하여 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[6].

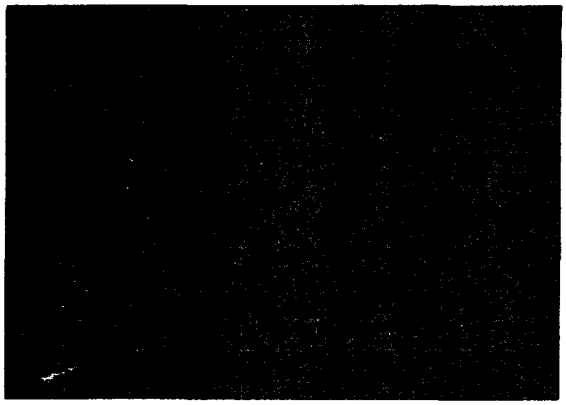


[그림 2] WPKI 환경에서의 전자서명 구조

2.2 XML 전자서명

XML 전자서명은 W3C의 XML-Signature WG(Working Group)에서 제정하였으며 2002년 2월 현재 "Recommendation" 상태로 존재하여 계속적인 표준화 작업이 이루어지고 있다. 이 문서에는 XML 전자 서명 문서를 새롭게 생성하고 표현하기 위한 규칙과 구문처리를 명시하고 있다.

XML 전자서명 문서는 Signature 엘리먼트로 표현되는 다음과 같은 구조를 갖는다.



[그림 3] Signature 엘리먼트 구조

① Signature : XML 전자서명 문서의 부모 엘리먼트
② SignatureValue : SignatureMethod에 정의된 알고리즘을 사용하여 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

3.1 무선 인터넷 환경의 제한요소

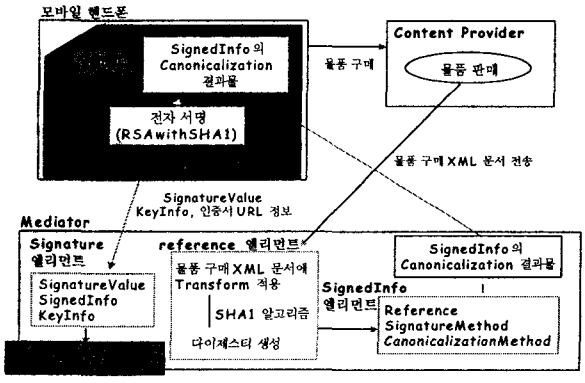
현재 무선 네트워크의 발전으로 M-Commerce가 활성화되어 많은 보안 기술 및 인증 기술 연구가 이루어지고 있다. 하지만 무선 인터넷은 무선 단말기와 환경의 특성으로 많은 제한요소[5]를 가지고 있어 유선 인터넷 환경의 보안, 인증 기술을 그대로 적용하기에는 사실상 불가능하다. 무선 인터넷 환경이 가지는 제한 요소로는 다음과 같다.

- 좁은 대역폭
- 덜 강력한 CPU
- 적은 메모리 량
- 데이터와 프로그램을 위한 적은 저장장치 크기
- 작은 디스플레이

3.2 XML 전자서명을 사용한 시스템 설계

가. 무선 인터넷 환경에서의 XML 전자서명 시스템

무선인터넷 환경이 가지는 제한 요소로 인하여 기존 유선 인터넷 환경에서 XML 전자서명을 클라이언트에서 모두 처리했던 것처럼 무선단말기에서 처리하기에는 사실상 불가능하다. 따라서 본 논문에서는 XML 전자서명 과정 중 전자서명 값을 계산하는 부분만 무선 단말기에서 수행하도록 연산을 분산시켜 설계하였다. 다음 그림은 본 논문에서 제안하고자 하는 무선 인터넷 환경에서의 XML 전자서명 시스템 구조이며 무선 단말기, 컨텐츠 제공자, Mediator로 구성되어져 있다.



[그림 4] 무선 인터넷 환경에서의 XML 전자서명 구조

① 무선 단말기

사용자가 물품을 구매하고 전자서명하기 위해 사용되는 수

단이며 실제 서명에 필요한 SignatureValue를 계산하는 부분이다.

② 컨텐츠 제공자(Content Provider)

유선 인터넷 환경에서 컨텐츠 제공을 담당하며 사용자와 전자 상거래가 이루어진다.

③ Mediator

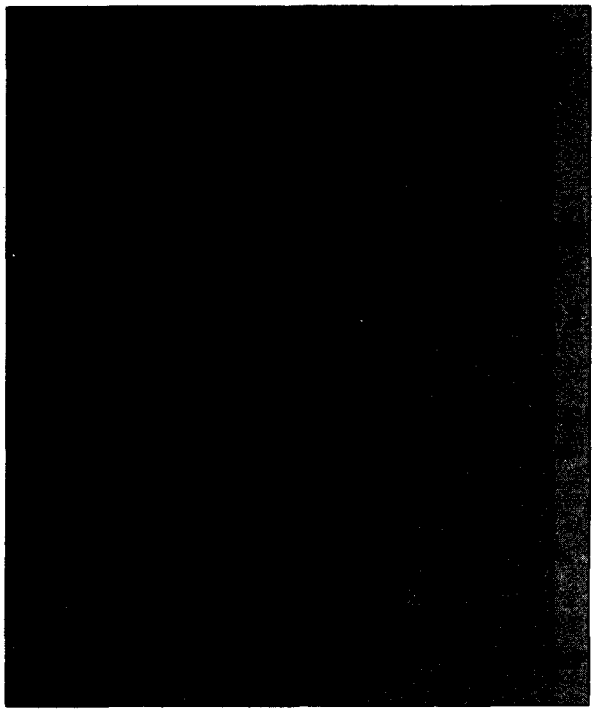
전자상거래시 XML 전자서명 문서에 필요한 각각의 엘리먼트를 생성하며 무선 단말기에 SignInfo의 Canonicalization 결과물을 전송한다. 최종적으로는 SignatureValue와 다른 정보들을 무선 단말기로부터 전송받아 XML 전자서명 문서를 생성한다.

나. 프로그램 알고리즘 및 전자서명 알고리즘

무선 단말기에서 SignatureValue 값을 계산하기 위한 프로그램과 계산된 값을 전송하기 위한 데이터 구조를 설계할 필요가 있다.

① SignatureValue 프로그램 알고리즘

SignatureValue를 계산하기 위해 사용되는 프로그램의 알고리즘은 다음과 같다.



② 전자서명 알고리즘

전자서명 알고리즘은 전자서명할 문서중 SingInfo 엘리먼트를 정규화하여 생성된 값과 개인 키를 함께 사용하여 전자서명 값을 생성할 때 사용된다. 본 논문에서는 RSA 알고리즘[9]을 사용한다.

다. XML 전자서명을 사용한 무선 인터넷 환경에서의 서명절차

본 논문에서 제안한 시스템 구조에서 전자서명을 하기 위한 절차는 다음과 같다.

① 사용자는 인증서를 발급 받음
② 사용자가 상품을 구매
③ XML 구매 문서를 Mediator에 전달
④ XML 서명 문서 생성을 위한 작업
- Reference 엘리먼트 생성
- SignedInfo 엘리먼트 생성
- SignedInfo Canonicalization 결과물 단말기 전송

⑤ 무선 단말기 스마트 카드 내 연산
- 개인키를 이용한 SignatureValue 계산

⑥ SignatureValue와 KeyInfo 등을 Mediator에 전달
⑦ Signature 엘리먼트 생성
⑧ XML 서명 문서 작성
⑨ XML 서명 문서와 구매 문서를 인증 기관에 전송
⑩ 인증기관에서는 비교 검사
- 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

⑪ 인증 완료 후 결제 완료
⑫ 사용자에게 결제 완료를 통보

4. 결론 및 향후 연구 과제

본 연구에서는 무선 인터넷 환경에서 XML 전자서명 기법을 사용할 수 있는 시스템을 설계하였으며, 무선 인터넷 환경에 XML 전자서명을 사용함으로써 전자상거래시 많이 사용하고 있는 XML 문서와의 상호 연동 가능성이나 전자서명 시스템간의 상호 작용성을 높일 수 있고 기존 유선 인터넷에서 사용되는 XML 전자서명의 장점을 그대로 사용함에 따라 확장 가능한 전자서명 포맷을 제공할 수 있다.

향후 연구 과제로는 본 연구에서 제시하고 있는 시스템 구조를 실제 환경에서 구현할 필요가 있으며, 전자서명 알고리즘으로 무선 인터넷 환경을 위해 제안된 ECC(타원 곡선) 알고리즘을 제안한 시스템에 적용시키는 연구가 필요하다.

참고문헌

[1] XML-Signature Syntax and Processing, W3C, 12 February 2002
[2] Hermes - A Lean M-Commerce Software Platform Utilizing Electronic Signatures, Sebastian Fishmeister, IEEE. Hawaii Internation Conference on system Sciences, January 7th 10, 2002
[3] Brokat. WWW Site. http://www.brokat.com
[4] Paybox. WWW Site. http://www.paybox.de
[5] Mobile Electronic Commerce: Emerging Issues, Aphrodite Tsalgatidou, Procs of EC-WEB 2000, pp.477-486
[6] WPKI(Wireless Public Key Infrastructure), Version 24 Apr 2001
[7] XML/EDI 와 XML 전자서명 통합 시스템의 설계, 장우영, 유승범, 장인걸, 차석일, 신동일, 신동규, 2001년 한국정보처리 학회 춘계 학술발표 제 8권 제 1호, pp.407-410
[8] Elliptic curve cryptography on smart cards, Henna Pietiläinen, Helsinki University of Technology, 2000
[9] A method for obtaining digital signatures and publickey cryptosystems, R.L.Rivest, A.Shamir, L.Adleman, ACM, 21(2), February 1978