제18회 한국정보처리학회 추계학술발표대회 논문집 제9권 제2호 (2002.11)

무선 인터넷 환경에서 XML 전자서명 기법을 이용한 Mediator 설계

장창복, 이민희, 김동혁, 백주현, 최의인
한남대학교 컴퓨터공학과
e-mail:chbjang@dblab.hannam.ac.kr

Design Of Mediator Using XML Signature in Wireless Environment

Chang-Bok Jang, Min-Hee Lee, Dong-Hyuk Kim, Joo-Hyun Baek, Eui-in Choi
Dept of Computer Engineering, Han-nam University

요 약

무선 인터넷의 급속한 발전과 무선 단말기 성능의 발달로 인해 무선 단말기를 이용한 전자상거래(M-Commerce)가 활성화되고 있다. 따라서 전자상거래시 중요한 문제점으로 여겨지는 데이터 보안이나 사용자 인증 같은 기술이 M-Commerce 환경에서도 적용될 수 있는 연구가 현재 활발히 진행되고 있으며, 대표적인 연구로는 WPKI가 있다. 또한 유선 인터넷 환경에서의 전자상거래는 XML을 통한 문서교환 연구가 활발하게 진행 중에 있기 때문에 XML 전자서명에 관한 연구가 많이 이루어지고 있다. 따라서 본 논문에서는 무선 인터넷 환경에 XML 전자서명 기법을 적용하여 사용자 인증과 XML 문서 및 전자서명 시스템들 간에 상호 연동성을 제공할 수 있는 Mediator를 설계하였다. 본 논문을 통해 무선 인터넷 환경에서도 XML 전자서명 포맷을 제공하여 XML 문서를 이용한 전자상거래 범위를 무선 인터넷 환경으로 확대할 수 있으며, 기존 유선 인터넷 환경에서 사용되는 XML 문서 기반 전자상거래 시스템과도 서로 상호 연동 가능하다.

1. 서론

이동하기 쉽고 휴대가 간편한 무선 단말기의 성능 향상과 물리적 선의 한계를 극복할 수 있는 무선 인터넷 환경의 발달로 인해 무선 통신을 이용한 전자상거래(M-Commerce)가 활성화되고 있다. 이러한 전자상거래에서는 사용자 인증이나 데이터 보안 같은 기술이 아주 중요한 문제로 여겨지고 있기 때문에, 인증기관(CA: Certification Authority)으로부터 인증서를 발급 받아 거래문서에 전자 서명하여 사용자 신원을 확인하는 기술들이 연구되고 있다. 또한 최근에는 XML 문서를 이용한 전자상거래가 활성화되고 있기 때문에 사용자 인증분야에서 XML 전자서명 기법[1, 7]을 사용하기 위한 연구가 진행되고 있다. 이처럼 무선 인터넷에서도 무선 단말기를 이용하여 전자상거래를 하기 위해서는 사용자를 확인할 수 있는 전자서명 기술에 관한 연구가 필요하다. 하지만 무선 인터넷 환경에서 사용되고 있는 무선 단말기는 성능면이나 네트워크 환경면에서 기존 유선 인터넷에 비해 많은 제약사항을 가지고 있기 때문에 무선 단말기상에 데이터 처리 같은 연산 기능을 두기에는 어려운 점이 많다.

따라서 본 논문에서는 기존의 유선 인터넷 환경에서 사용되고 있는 XML 전자서명 기법을 무선 인터넷 환경에 적용하기 위하여 전자 서명의 핵심인 전자서명 값을 생성하는 부분은 무선 단말기에서 이루어지도록 하고 그 외의 XML 전자서명 문서를 생성하는 부분은 Mediator를 두어 처리하는 시스템을 설계하였다.

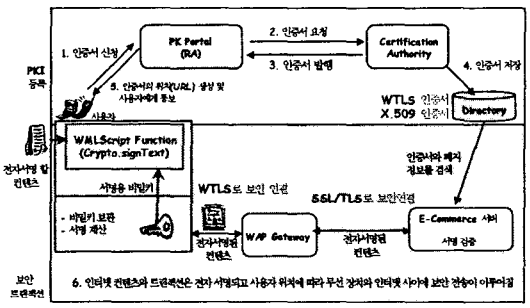
2. 관련 연구

무선 인터넷 환경에서 사용자 인증과 데이터 보안 관한 표준은 아직 완벽하게 확립되어 있지 않은 실정이며 현재 WAP에서 제안하고 있는 WPKI(Wireless Public Key Infrastructure)[6, 10]가 많이 연구되고 있다. 따라서 많은 무선 결제 시스템은 각각 서로 다른 인증 방법을 채

택하여 시스템을 구축하고 있으며 이러한 지불 시스템 및 업체들로는 Hermes[2], Paybox[3], Brokat[4], SK텔레콤[11], KTF[12] 등이 있다. 또한 유선 인터넷 환경에서는 XML 문서를 이용한 전자상거래가 많이 연구되고 있기 때문에 XML 문서에 전자서명 할 수 있는 XML 전자서명 기법에 관한 연구가 이루어지고 있다.

2.1 WPKI

WPKI는 무선 인터넷 환경에서 공개키 기반 인증 표준으로 새롭게 만들어낸 표준이 아닌 기존 유선 인터넷에서 사용되고 있던 PKI 방식을 무선 인터넷 환경에 맞게 최적화하여 확장시킨 것이다. 현재 WAP 포럼의 WPKI 표준이 가장 일반적으로 사용되고 있다. 다음 [그림 1]은 WPKI의 인증절차와 전자서명 절차를 보여주고 있다[6].



[그림 1] WPKI의 인증 및 전자 서명

① WPKI 인증 형식과 암호 알고리즘

WPKI에서 사용되는 인증 형식으로는 X.509 표준 인증서와 WAP에서 새롭게 제한한 WTLS 인증서 등이 있으며 암호 알고리즘으로 ECC(Elliptic Curve Cryptography) 알고리즘[8]을 새롭게 채택하여 인증서의 크기를 감소시키고 무선 단말기의 부하를 감소시켰다.

② WPKI의 전자서명

WPKI는 서명하려는 컨텐츠나 트랜잭션을 Crypto.signText 함수를 이용하여 전자서명한다. 이러한 전자서명된 컨텐츠나 트랜잭션은 WAP 게이트웨이를 통해 웹 서버(E-Commerce 서버)로 전송되고 웹 서버에서는 다시 인증기관으로 서명된 문서를 보내어 문서를 검증하게 된다.

2.2 XML Signature

XML 전자서명은 W3C의 XML-Signature WG(Working Group)에서 제정하였으며 현재 계속적인 표준화 작업이 이루어지고 있다. XML 전자서명 표준 문서에는 XML 전자 서명 문서를 생성하고 표현하기 위한 규칙과 구문처리를 명시하고 있다.

XML 전자서명 문서는 Signature 엘리먼트로 표현되는 다음과 같은 것들로 구성되어져 있다.

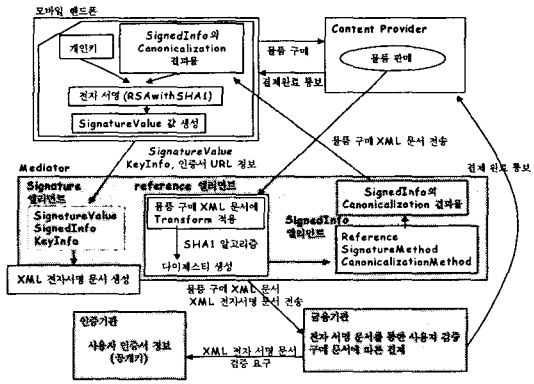
- Signature : XML 전자서명 문서의 부모 엘리먼트
- SignatureValue : SignatureMethod에 정의된 알고리즘을 사용하여 생성한 전자서명의 실제적인 값
- SignedInfo : Canonicalization 알고리즘, Signature 알고리즘, 또는 Reference를 포함한다.
- CanonicalizationMethod : XML 문서를 정규화하기 위해 필요한 알고리즘을 포함한다.
- SinatureMethod : 실제적인 서명 값을 생성하기 위해 사용되는 알고리즘 명시
- Reference : 선택적으로 서명문서에 포함시킬 수 있으며 ID를 통해 다른 곳에서 참조 할 수 있다.
- Transforms : 서명자가 메시지 다이제스트 객체를 어떻게 얻는지를 명시
- DigestMethod : 다이제스트 값을 생성하기 위한 다이제스트 알고리즘 명시
- DigestValue : DigestMethod를 통해 생성된 다이제스트 값 포함
- KeyInfo : 키 발생기를 통해 생성되는 키에 대한 정보 포함

3. 전자서명 시스템 설계

3.1 XML 전자서명을 이용한 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 다음과 같이 설계하였다.



[그림 2] 무선 인터넷 환경에서의 XML 전자서명 시스템

① 무선 단말기

사용자가 물품을 구매하고 전자서명하기 위해 사용되는 수단이며 실제 서명에 전자상거래가 발생할 경우 사용자의 인증을 위해 필요한 SignatureValue를 생성한다.

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 SignInfo 엘리먼트의 Canonicalization(정규화) 결과물을 전송한다. 최종적으로는 SignatureValue와 다른 정보들을 무선 단말기로부터 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.

나. 무선 단말기의 SignatureValue 어플리케이션 설계

무선 단말기에서 전자서명을 위한 SignatureValue 값을 계산하기 위한 알고리즘은 다음과 같다.

```
Trans_SignatureValue /* 생성된 SignatureValue를 다른
{                    정보와 전송하기 위한 데이터 구조 */
  String Signed_Value;     // 서명된 값을 저장
  String Signed_KeyInfo;   // 사용된 키 정보 저장
  String Signed_URLInfo;   // 인증서 위치 정보 저장
}
main() // 주 프로그램
{
String SignInfo_Canonicalization;
/* Mediator로부터 전송될 SignInfo 정규화 값을 저장하
   기 위한 변수 선언*/
SignInfo_Canonicalization = Trans_SignInfo();
   // Mediator로부터 전송된 SignInfo 정규화 값을 저장
KeyInfo Used_KeyInfo;   // 사용될 키 정보를 위한 변수
String Sign_Value; /* 전자서명되는 값을 위한 변수 선
                      언 */
String URL; // 전자서명시 필요한 인증서의 위치 정보
String KeyInfo_Name /* 전자서명시 사용되는 키 정보
                       변수 */
Sign_Value=Sign_Cryto_SignInfo(SignInfo_Canonicalization);
                // 전송된 SignInfo 정규화 값에 전자서명
Trans_SignatureValue.Signed_Value = Sign_Value ;
 // Mediator에 전송하기 위한 SignatureValue 값을 저장
Trans_SignatureValue.Signed_KeyInfo=KeyInfo_Name;
 /* Mediator에 전송하기 위한 사용된 Key 정보 저장 */
Trans_SignatureValue.Signed_URLInfo = URL;
                       /* 인증서 위치 정보를 저장 */
Trans_Mediator(Trans_SignatureValue);
// Mediator로 전송
}
```

다. Mediator 설계

무선 인터넷 환경에서 사용하고 있는 무선 단말기는 성능면이나 네트워크 측면에서 기존 유선 인터넷 환경보다 제약사항이 많다. 이러한 제한성으로 인해 무선 단말기내에 XML 전자서명 문서를 생성하고 처리하기에는 사실상 불가능하므로 무선 단말기에서는 전자서명에 필요한 서명 값을 생성하도록 하고 유선 인터넷에 Mediator를 두어 XML 전자서명 문서를 생성할 필요가 있다. 따라서 무선 단말기와 Mediator 간의 데이터 이동 및 Mediator에서 XML 전자서명 문서를 생성하기 위한 어플리케이션을 구현을 위해 데이터 구조 및 알고리즘을 다음과 같이 설계하였다.

① Mediator 어플리케이션 데이터 구조 및 알고리즘

Mediator내에서 XML 전자서명 문서를 생성하기 위한 데이터 구조 및 알고리즘은 다음과 같다.

```
Reference_Element   // Reference 엘리먼트 구조
{
String Ref_URL;        /* Reference 엘리먼트 참조 URL
                          정보 */
String Ref_Trans;      // XML 문서 Transform 변수
String Ref_DigestMethod;  // 다이제스트 생성 Method
String Ref_DigestValue;   // 생성된 다이제스트 값
}
SignInfo_Element          // SignInfo 엘리먼트 구조
{
String SignInfo_CM;       // 정규화 Method
String SignInfo_SM        // Signature Method
}
Signature_Element         // Signature 엘리먼트 구조
{
String Sign_Keyinfo;      // 서명시 사용된 키 정보
String Sign_SignatureValue; // 서명된 값
}
main()
{
String Payment_Doc;    // XML 문서 저장을 위한 변수
String Trans_Result;   // Transform한 후의 값 저장
String Digest_Trans;   // 다이제스트 값 저장
Payment_Doc=get(Payment.xml);
        /*지불 결제를 위한 XML 구매 문서를 획득 */
Trans_Result = Trans_XML(Payment_Doc);
          /* 획득한 XML 문서를 Transform 한다 */
Digest_Trans = Function_SHA1(Trans_Result)
/* Transform한 XML 문서를 해시함수를 통해 다이제스
   트를 생성 */
Reference_Element Ref;      //Reference 엘리먼트 생성
Ref.Ref_URL = get(string URL);
 /* 참조 URL을 획득하여 Reference 엘리먼트에 저장 */
Ref.Ref_Trans = get(string Transform);
 /* Transform 시 사용된 Method를 획득하여 Reference
```

```
    엘리먼트에 저장 */
Ref.Ref_DigestMethod = get(string DigestMethod);
 /* 다이제스트를 생성할 때 사용한 알고리즘을 획득하여
    Reference 엘리먼트에 저장 */
Ref.Ref_DigestValue = Digest_Trans;
/* 생성된 다이제스트 값을 Reference 엘리먼트에 저장 */
SignInfo_Element SignInfo; /*SignInfo 엘리먼트 생성 */
String Canonical_XML; /* XML 문서 정규화를 위한
                         변수 */
Canonical_XML = F_Canonical(Payment.xml)
                    /* 사용된 XML 문서를 정규화 */
SentToMobile(Canonical_XML);
   /* 무선 단말기로 정규화된 XML 문서 값을 전송 */
SignInfo.SignInfo_CM = get(CanonicalMethod);
                  /* 사용된 정규화 Method를 획득 */
SignInfo.SignInfo_SM = get(SignatureMethod);
                 /*사용된 signature Method를 획득 */
Signature_Element Sign; /* Signatue 엘리먼트 생성 */
Sign.Sign_KeyInfo = F_receive_key(); /* Keyinfo 값을
                                        획득 */
Sign.Sign_SignatureValue = F_receive_sign();
                    /* SignatureValue 값을 획득 */
String XML_Signature_DOC; /* XML Signature 문서를
                             위한 변수 */
XML_Signature_Doc=Create_XML_Signature(Ref,
SignInfo, Sign,); /* 생성된 각각의 엘리먼트를 이용하여
                     XML 전자서명 문서를 생성 */
SendToPayment(XML_Signature_Doc,Payment_Doc,
InfoURL)  /* 지급 결제를 위해 금융기관에 전자서명
      문서와 구매 문서 그리고 인증서 정보를 전송 */
}
```

3.2 무선 인터넷 환경에서 XML 전자서명 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

4. 결론 및 향후 연구과제

본 연구에서는 무선 인터넷 환경에서 Mediator를 통하여 XML 전자서명 기법을 사용할 수 있는 시스템을 설계하였다. 본 시스템을 통하여 무선 인터넷 환경에서도 XML 전자서명을 사용함으로써 현재 전자상거래시 많이 사용하고 있는 XML 문서와의 상호 연동 가능성 및 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 구현하여 시스템의 안정성 검증이 필요하며, 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
[10] 한국정보통신기술협회, http://www.tta.or.kr
[11] SK텔레콤, http://www.moneta.co.kr
[12] KTF, http://www.npaymagic.co.kr