모바일 환경에서의 XML 전자서명을 이용한 암호화 시스템 설계

성 경†

요 약

무선 인터넷이 급속히 발전하고 모바일 폰의 성능이 발달함에 따라서 모바일 폰을 이용한 전자상거래가 활성화되고 있다. 이러한 모바일 폰을 이용한 전자상거래를 M-Commerce라고 한다. 또한 이러한 전자상거래시 가장 중요한 문제점으로는 데이터 보안이나 사용자 인증 기술이며, 이러한 기술에 관한 연구로 WPKI와 WTLS가 있다. 하지만 전자 문서를 모바일 폰에서 서명한 후 다시 메시지를 전송할 때 암호화 되지 않으면, 외부에 노출될 위험이 존재하고 있다. 따라서 본 논문에서는 모바일 환경에 XML 전자서명 기법을 적용하여 사용자 인증을 처리하고 처리한 문서를 암호화 하기 위한 시스템을 설계하였다. 본 논문을 통해 모바일 환경에서도 XML 전자서명을 제공할 수 있으며, 전자서명 문서를 암호화 함으로써 외부로부터의 위험을 예방할 수 있다.

키워드 : 확장성마크업언어, 전자서명, 모바일환경, 전자인증, 정보보안

A Design of Encryption System Using XML Signature in Mobile Environment

Kyung Sung†

ABSTRACT

Electronic commerce that use Mobile Phone according as the radio Internet develops rapidly and performance of Mobile Phone develops is activated. It is said that electronic commerce that use these Mobile Phone is M-Commerce. Also, the most important controversial point is data security or an user certification technology at these electronic commerce, there are research reactor WPKI and WTLS about this technology. However, when transmit message again after sign electronic documents in Mobile Phone, if do not encrypt, danger exists to be exposed to outside. Therefore, in this paper, designed system to encipher document that handle and handles user certification applying XML electronic sign technique in Mobile environment. Prevent of XML electronic sign in Mobile environment through this paper, and can stave off danger from outside by enciphering electronic sign document.

Keywords : XML, Digital Signature, Mobile Environment, Degital Authentication, Information Security

1. 서 론

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 문

† 정회원: 목원대학교 컴퓨터교육과 전임강사(교신저자)
논문접수: 2004년 6월 24일, 심사완료: 2004년 7월 13일

서를 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.

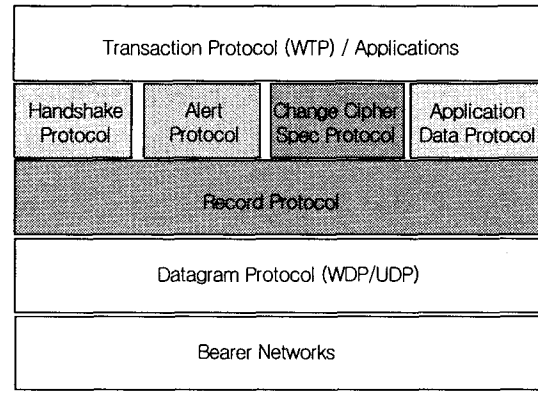
2. 관련 연구

모바일 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 채택하여 시스템을 구축하고 있으며 이러한 지불 시스템 및 업체들로는 Hermes[2], Paybox[3], Brokat[4], SK 텔레콤[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. WTLS

WTLS는 TLS(Transport Layer Security)라고 잘 알려진 인터넷 보안 프로토콜을 기반으로 한 Transport-level 보안 프로토콜이다. WTLS는 통신 중인 노드들을 인증할 수 있고, WML 데이터가 전송되어질 때 데이터의 무결성을 검사하고 암호화 할 수 있다. WTLS는 좁은 대역폭을 갖는 무선 네트워크상의 무선 단말기에서 사용되어지도록 최적화되었다. WTLS는 <그림 1>과 같이 암호 및 키 교환 알고리즘을 결정하고 공개키를 확보하며 키 교환 및 세션을 설정하는 Handshake Protocol과 Handshake의 성공과 새로운 암호규격의 사용을 통보하는 Change Cipher Spec Protocol, 그리고 Handshake에서 생성된 보안 파라미터를 이용하고 연결 상태를 적용하는 Record Protocol, 마지막으로 WTLS 전 구간에 걸쳐서 동작하며 수신한 데이터에 대한 경고 및 실패 메시지를 발생하고 응답해주는 Alert Protocol로 구성되어져 있다.



<그림 1> WTLS의 구조

따라서 WTLS는 PKI 기반 프로토콜과 암호화 기반 프로토콜로 구성되어져 있는 WAP 애플리케이션을 위해 다음과 같은 보안 서비스를 제공한다.

- 인증 : 온라인 상에서의 교환, 트랜잭션, 또는 자원의 접근 허락 같은 엔터티의 identity를 검사한다. WTLS는 PKI 기반이므로 전자서명이나 Private 서비스, 서버 또는 노드들의 인증에 공용키 인증 방식을 사용한다.
- Private : 도청이나 비허가된 접근을 방지한다. WTLS는 통신하고 있는 노드들 사이에서 WAP 데이터를 암호화 할 수 있는 능력을 가지

고 있으며 PKI 기반이기 때문에 통신하는 노드들 간에 서로 다른 암호화키와 인증을 사용하여 일대다 통신 암호화를 지원할 수 있다.

■ 무결성 : 전송되는 도중이나 저장장치에 있는 동안 사고나 다른 목적으로 인해 데이터가 간섭받지 않도록 하고, 수정되지 않음을 보장한다. WTLS는 데이터 수정을 추적할 수 있는 해싱 알고리즘 암호화 기술을 사용하는 데이터 fingerprint를 채택하였다.

■ 서비스 거부 공격의 방어 : 기존의 서비스 거부 공격을 좀더 어렵게 만든다. WTLS는 데이터가 반복되거나 성공적으로 검사되지 않을 경우 이러한 데이터를 추적하고 방출할 수 있는 서비스를 포함하고 있다.

2.2. XML 전자서명 기법

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

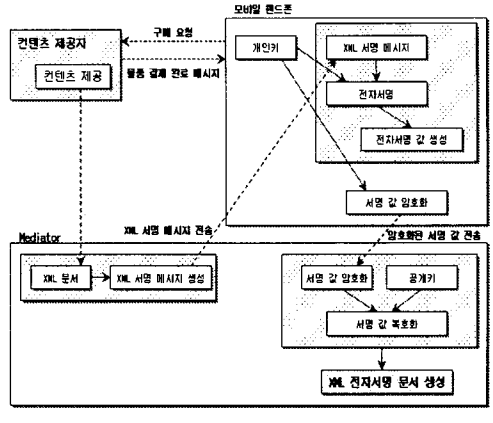
■ DigestValue : DigestMethod를 통해 생성된 다이제스트 값 포함

■ KeyInfo : 키 발생기를 통해 생성되는 키에 대한 정보 포함

3. XDSS(XML Digital Signature System) 설계

3.1. XDSS 시스템에서의 전자서명 및 암호화

모바일 환경은 기존 유선 인터넷 환경과는 다른 제한 요소를 가지고 있다. 따라서 본 논문에서는 XML 전자서명 값을 계산하여 처리과정을 무선 단말기에서 수행하도록 연산을 분산시켜 설계하였다. <그림 2>는 본 논문에서 제안하는 XML 전자서명 시스템 구조이다.



<그림 2> XML 전자서명 시스템

① 모바일 폰

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.

3.2. 모바일 전자서명 어플리케이션 설계

모바일 폰에서 전자서명을 위한 전자 서명 값을 계산하기 위한 알고리즘은 <그림 3>과 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 저장
하기 위한 변수 선언*/
SignInfo_Canonicalization = Trans_SignInfo();
// Mediator로부터 전송된 SignInfo 정규화 값을 저장
String KeyInfo_Name
/* 전자서명시 사용되는 키 정보 변수 */
String Sign_Value;
/* 전자서명되는 값을 위한 변수 선언 */
String URL;
// 전자서명시 필요한 인증서의 위치 정보
Sign_Value=Sign_Cryto_SignInfo(SignInfo_Canonicaliza
tion); // 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
}
```

<그림 3> XML 전자서명 알고리즘

3.3. XDSS 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 서명값을 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 <그림 4>와 같이 설계하였다.

```
String URL;
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 획득하
여      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 */
}
```

<그림 4> Mediator 어플리케이션 데이터 구조 및 알고리즘

3.4. 모바일 환경에서의 XML 전자서명 절차

본 논문에서 제안한 시스템에서 XML 전자서명 절차는 다음과 같다.

- 공개키와 개인키 알고리즘을 이용하여 키 다운로드
- 공개키를 통한 개인키 생성
- 생성된 개인키를 mediator에 공개키로 암호화하여 전송
- 개인키를 통한 서명 메시지 암호화

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 계산후 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 후 XML 서명 문서내의 다이제스트 값과 비교
  - 서명 검증 : SignedInfo Canonicalization 결과물 계산하고, 공개키와 SignatureValue를 가지고 복호화
⑥ 검증 완료 후 결제 완료
⑦ 사용자에게 결제 완료를 통보

3.5. 실행결과

본 논문에서 구현한 전자서명 어플리케이션의 실행결과는 <그림 5>와 같이 전자서명과 검증이 올바르게 수행되는 것을 확인할 수 있다.

<그림 5> 전자서명 및 검증결과

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.

참 고 문 헌

[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 International 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

성 경

1988 목원대학교 전자계산학과 (공학사)

1993 경희대학교 전자계산학과 (공학석사)

2003 한남대학교 컴퓨터공학과 (공학박사)

1994~2004 동해대학교 컴퓨터공학과 교수

2004~현재 목원대학교 컴퓨터교육과 전임강사

관심분야 : 정보보호 및 정보관리, 컴퓨터네트워크, 신경회로망, 컴퓨터교육

E-Mail: skyys04@mokwon.ac.kr