모바일 환경에서의 XML 문서 디지털 서명 시스템

학일명* · 홍현우* · 이성현** · 이재승** · 정회경*

*배재대학교 컴퓨터공학과 · **한국전자통신연구원 정보보호연구단

XML Digital signature System based on Mobile Environment

Ri-Ming Hao* · Xian-Yu Hong* · Seong-hyun Lee** · Jae-Seung Lee** · Hoe-Kyung Jung*

*Dept. of Computer Engineering, Paichai University · **Information Security Research Division, ETRI

E-mail : *{hrm8216, honexianyu, hkjung}@pcu.ac.kr, **{duribun, jasonlee}@etri.re.kr

요 약

최근 모바일 단말기를 통하여 휴대폰 결제, 계좌 이체, 주식 투자 등의 금융서비스를 이용하는 사용자가 증가하고 있다. 모바일 전자상거래에서 데이터는 XML 문서형태로 전송, 교환되고 있다. 그러나 XML 문서는 해킹이나 악성코드로 공격받게 될 경우 일반적인 XML 문서만으로는 전자상거래의 보안요구를 만족시키기 어렵다. 특히 현재 국내에서 개발된 WIPI(Wireless Internet Platform for Interoperability)의 경우, 개방적인 플랫폼으로서 집중적인 공격에 대비해야 할 필요성이 있다.

이에 본 논문에서는 모바일 환경에서 XML 문서의 디지털 서명에 관련한 W3C 권고안의 요구사항에 따라 기존의 RSA(Rivest Shamir Adleman), DSA(Digital Signature Algorithm), KCDSA(Korean certificate Digital Signature Algorithm) 및 HMAC(Hash Message Authentication Code) 알고리즘을 사용하여 모바일 환경에서의 XML 문서 디지털 서명 시스템을 설계 및 구현하였다. 본 시스템은 국내 무선 인터넷 표준인 WIPI 플랫폼에서 테스트를 진행하였다.

ABSTRACT

Recently, More and more consumer enjoy the finance service such as settling, account transferring, stocks investment, and so via mobile device. In the mobile environment, data transferring between the devices is formatted as XML. However, the common XML file is exposed to the attack such as hacking and malignity code, to satisfy security of mobile environment is very difficult. The problem is more seriously at the open platform such as WIPI that is developed by our country. So there is enough reason to propose one system to protect the import data.

In this paper, we development the system to digital signature and signature the XML document in order to protect data, and the system is observing the recommendation of the XML Signature Syntax and Processing by W3C. When designing and composition the system, we use the digital signature algorithm RSA, DSA, KCDSA, and HMAC, etc. we test the system at the open WIPI platform.

키워드

모바일, 디지털 서명, XML, WIPI

Ⅰ. 서 론

최근 무선 인터넷 기술 및 하드웨어 기술의 발전과 더불어 무선단말기는 기존의 메모리용량, 처리속도 등의 제한에서 벗어나서 기존의 통화 외에 노래, 영화, 게임, 금융서비스 등 다양한 서비스를 제공하는 멀티미디어와 정보처리의 중심으로 부각되고 있다. 특히 모바일 금융서비스는 소비자들의 일상 금융활동에 큰 변화를 가져왔다. 모바일 환경에서 제공되는 금융서비스는 XML을 통해 데이터를 전송, 교환한다. XML 문서 보안에 대해서는 W3C에서 2002년 12월에 권고안을 발표하고 표준화 작업을 진행하고 있다 [1].

이에 본 논문에서는 모바일 환경에서 데이터 교환에 사용되고 있는 XML 문서를 서명시킴으

로서 중요한 데이터들의 보안성을 강화하는 디지털 서명 시스템을 설계 및 구현하였다.

II. 관련연구

2.1 XML 정규화

XML 문서가 하나의 어플리케이션에서 다른 어플리케이션으로 전송될 때 물리적 변화(라인 종료문자, 공백처리, 인코딩 등의 변화)가 일어날 수 있다. 이런 변화가 생긴 XML 문서는 원래의 텍스트와 다른 바이트열로 표현되기 때문에 그 텍스트의 서명이 확인되지 못한다. 따라서, W3C에서 Canonical XML 명세는 다음과 같은 규칙을 권고하고 있다.

- 속성값의 표준화
- 문자와 파싱된 엔터티 참조 대체
- XML 선언과 DTD 제거
- 공백 엘리먼트는 시작 태그와 종료 태그의 쌍으로 대체
- 문서 엘리먼트 외부의 공백과 시작 태그와 종료태그의 내부에 있는 공백 표준화
- 문자 내용의 모든 공백 보존
- 속성값 구분자는 이중 따옴표로 대체
- 속성값과 문자 내용의 특수 문자들은 문자 참조로 대체
- 엘리먼트에서 불필요한 네임스페이스 제거
- 각 엘리먼트에 디폴트 속성 추가
- 각 엘리먼트와 네임스페이스는 알파벳순으로 정렬
- 문서는 UTF-8로 인코딩
- 행 종료문자는 #xA로 대체

위의 규정들을 통해 의미적으로는 동일하지만 사용자들에 물리적으로 상이하게 변형된 XML 문서를 정형화 할 수 있다.

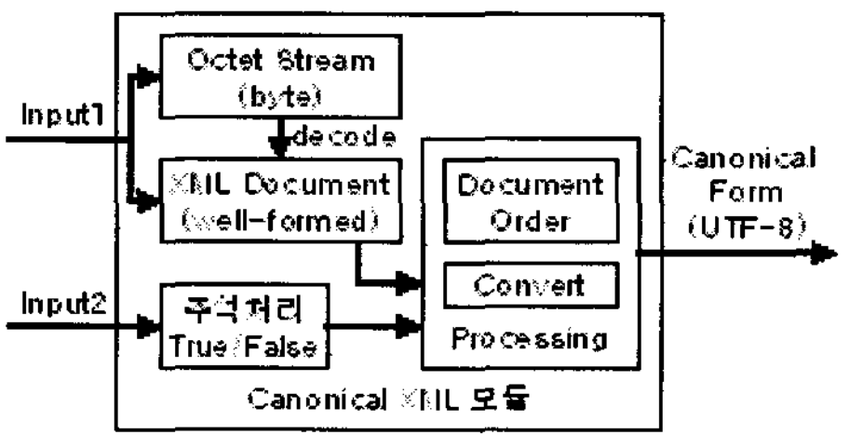

그림 5. 데이터 모델의 흐름

그림 1에서와 같이 Canonical XML 모듈은 두 개의 인자를 입력으로 받는다. Input1은 노드셋 또는 옥텟스트림으로 입력받는 방식에 대한 인자이고 input2는 주석 처리에 대한 부분으로 주석 포함 여부에 대한 인자이다. 첫 번째 인자를 받아들였을 때, 그 값이 옥텟스트림일 경우 XML 노드셋으로 변환되며 이 XML 문서는 well-formed 규칙만 충족하면 된다[2].

2.2 XML 디지털 서명

XML 전자서명은 W3C에서 지속적인 표준화 작업을 진행하고 있다. 워킹그룹의 목표는 디지털 콘텐츠에 대한 서명을 표현하기 위한 문법을 개발하고 해당 서명 연산 및 서명된 XML 문서를 검증하는 절차를 개발하는 것이다. 전자서명은 데이터 무결성 인증 그리고 부인 봉쇄와 같은 정보보호 서비스를 제공한다. 그림 2는 W3C에서 제안한 XML 문서의 디지털 서명 스키마 구조를 보여주고 있다.

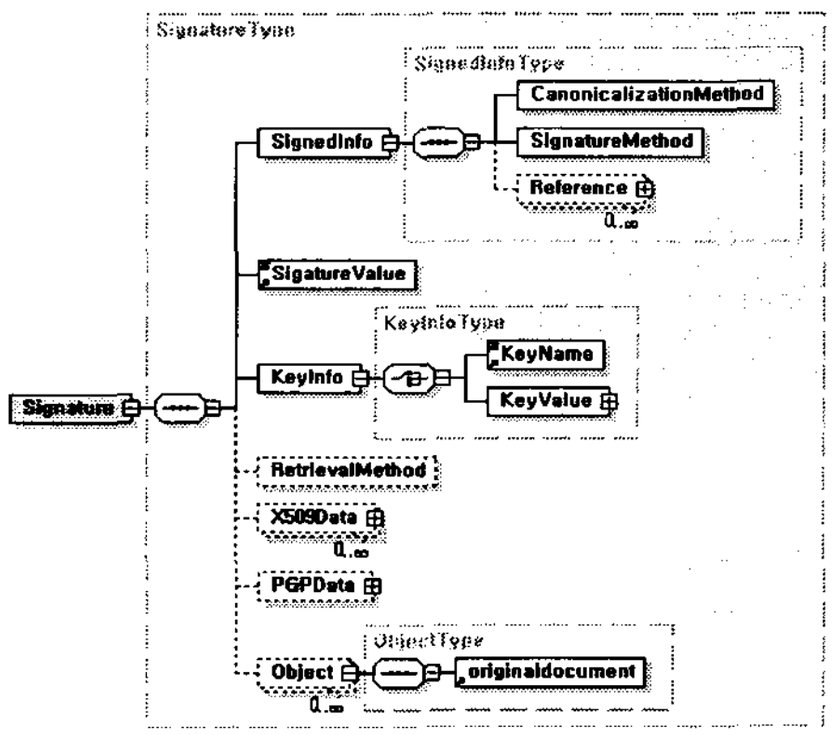

그림 6. 디지털 서명 스키마 구조

Signature 엘리먼트는 XML 전자서명의 루트 엘리먼트이다. SignedInfo 엘리먼트는 정규화 알고리즘, 서명 알고리즘, 그리고 한 개 이상의 참조값을 포함한다. SignatureValue 엘리먼트는 전자 서명의 실제 값을 담고 있는데, 이 값은 항상 base64 MIME 타입으로 인코딩된다. KeyInfo 엘리먼트는 수신자들이 서명 검증에 필요한 키를 얻을 수 있도록 해 주는 엘리먼트이다. Object 엘리먼트는 선택 사항으로써 모든 데이터를 담을 수 있으며 MIME 유형, ID, 인코딩 속성들을 포함할 수 있다. KeyInfo 엘리먼트는 KeyValue 엘리먼트와 KeyName 엘리먼트를 포함한다. KeyValue 엘리먼트는 서명을 확인하고 데이터를 복호화 하는데 사용하는 공개키의 실제 값을 포함하며 사용한 공개 키 알고리즘의 유형에 따라 RSAKeyValue 엘리먼트나, DSAKeyValue 등의 엘리먼트를 포함할 수 있다. KeyName 엘리먼트는 키를 식별하기 위해 사용하는 문자열을 포함한다[3].

III. 시스템 설계

본 시스템의 전체 아키텍처를 그림 3으로 표현하였다.

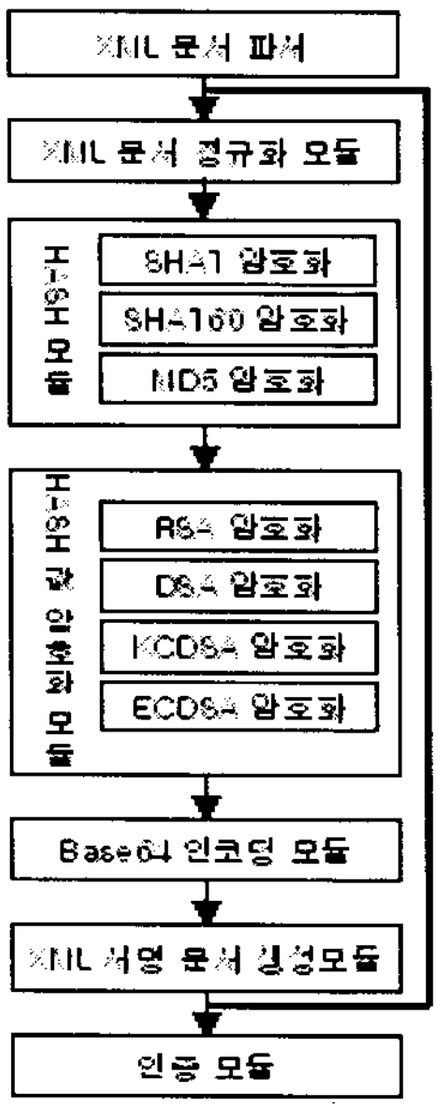

그림 7. 본 시스템의 아키텍처

본 시스템은 XML 문서를 수신 후 문서를 파싱하여 각 엘리먼트의 정보를 분석한다. 만약 문서에 포함된 엘리먼트들 중에 Signature 엘리먼트가 존재하지 않으면 시스템은 XML 디지털 서명 모드로 실행되고, Signature 엘리먼트가 존재하면 인증 모드로 실행된다. XML 문서 서명을 실행하기 위해서는 XML 문서를 그림 3의 절차에 따라 처리되어야 한다.

3.1 서명모드

본 시스템에서는 디지털 서명 및 인증될 XML 문서를 그림 4와 같은 구조의 스키마로 설계하였다.

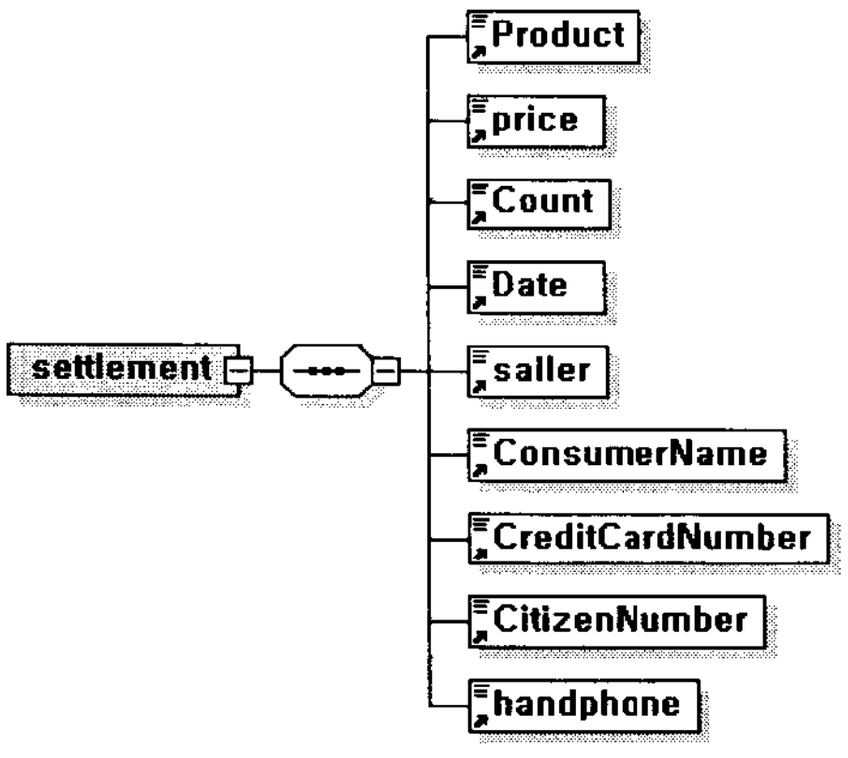

그림 8. 서명에 사용되는 XML 문서 스키마

본 서명 문서는 서명된 문서를 나타내고 있으며 상품명, 구매수량, 구매날짜, 결제금액, 결제화폐, 구매자 이름, 휴대폰 번호, 신용카드 번호 등의 엘리먼트를 가지고 있다. 서명 모드에서는 암호화하려는 데이터를 시스템 관리자가 지정할 수 있으며 제공된 스키마에 따라 자동 설정도 가능하다. 또한 디지털 서명에 사용될 블록 암호화 알고리즘도 시스템 관리자가 선택 가능하며 기본값으로 RSA 암호화 알고리즘이 설정되어 있다. 시스템은 암호화키를 생성하고 다시 데이터 암호화를 진행한다. 암호화된 데이터는 바이너리 데이터로서 XML 문서에 표현하기 위해 다시 BASE64로 인코딩되며 문서 생성 모듈에 전송된다. 표 1은 본 시스템에서 사용한 암호화 알고리즘들의 정보를 보여주고 있다[4].

표 1. 본 시스템에서 사용한 암호화 알고리즘

알고리즘	명칭
인코딩	BASE64
MAC	HMAC-SHA1
전자서명	RSAwithSHA1
전자서명	DSAwithSHA1
전자서명	KCDSASHA160
전자서명	ECDSASHA1
정규화	주석 없는 정규화
다이제스트	SHA1

암호화가 완료된 데이터는 문서 생성 모듈에 전송된다. 문서 생성 모듈은 그림 2의 스키마 구조를 참조하여 Signature 엘리먼트의 하위 엘리먼트인 SignatureValue 엘리먼트에 암호화 된 데이터를 포함시키고, KeyValue 엘리먼트의 하위 엘리먼트인 RSAKeyValue 엘리먼트에 RSA 공개키를 포함시켜 Signature 엘리먼트로 원본 XML 문서의 암호화될 엘리먼트를 대체한다.

3.2 인증 모드

인증 모드에서는 Signature 엘리먼트로부터 원본 XML문서의 Digest 값, Reference 알고리즘, 암호화된 데이터, SignatureMethod 알고리즘, CanoicalizationMethod에 사용한 Canonical XML 표준, KeyInfo 등의 정보를 추출하여 서명 인증모듈에 전송한다. 데이터 서명 인증 모듈은 먼저 HASH 값을 비교하고 RSA 공개키를 사용하여 암호화된 키를 인증한다. 암호화된 데이터는 Base64로 디코딩하여 인증을 수행하고 생성된 정보를 문서 생성모듈에 전송한다. 마지막으로 두 값을 비교하여 인증결과를 검증한다.

IV. 시스템 구현

모바일 XML 문서 디지털 서명 시스템은 INTEL x86 계열 CPU를 탑재한 IBM-PC 호환

컴퓨터와 Microsoft 사의 Windows XP SP2 운영체제가 설치된 PC에서 개발하였다. 개발도구는 Microsoft 사의 Visual C++ 6.0 SP6 이며, WIPI 모바일 환경의 개발을 위해 SKT IDE를 사용하였다. 테스트 환경은 SKT IDE 개발환경의 검증을 위해 SKT 에뮬레이터를 사용하였으며, XML 파서는 모바일 환경을 위하여 개발된 XmlParserDOM2를 사용하였다. 개발언어는 C 언어를 사용하였고 유저 인터페이스는 WIPI C API로 구축하였다[5].

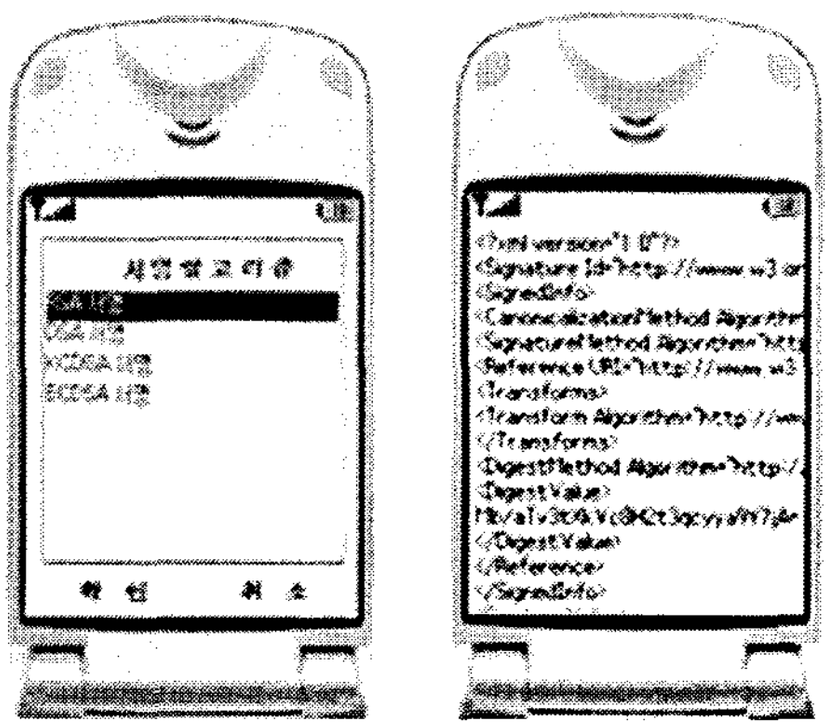

그림 9. 시스템의 디지털 서명 결과

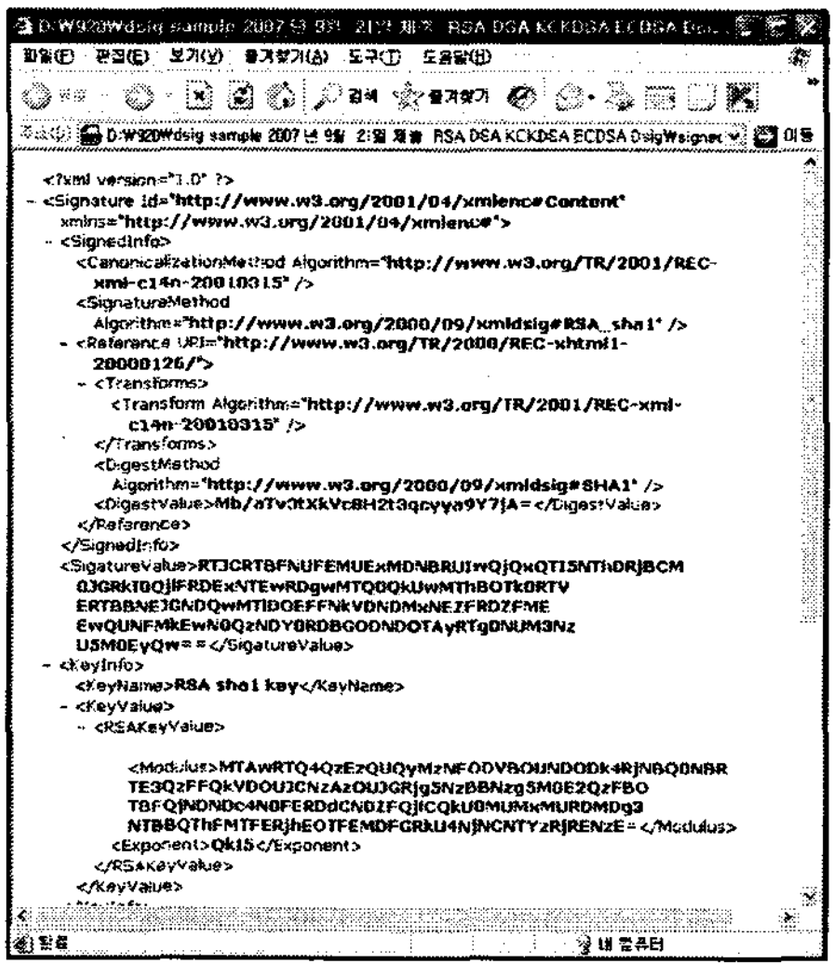

그림 10. 서명 결과 XML 문서

그림 5에서는 RSA_SHA1으로 처리된 디지털 서명 결과를 보여주고 있으며 그림 6은 서명 모듈에서 XML 문서를 생성하여 전송된 결과를 보여주는 XML 문서이다.

V. 결론

미래의 정보통신에서 대부분의 데이터 표현 및 전송은 XML 문서로 이루어 질 것이며, XML 기반 기술의 개발은 정보통신의 모든 분야의 기술에 접목되어 사용 될 것이다. 따라서 XML 기반의 디지털 서명 인증기술과 같은 원천기술 확보는 국가적으로 매우 중요하며 특히 모바일 플랫폼이 WIPI로 통합될 것을 대비하여 관련 소프트웨어의 개발이 시급하다.

이에 본 논문에서는 디지털 서명 인증기술의 국내외 동향분석 및 관련 포럼 표준화 동향 파악으로 최신 기술 동향을 분석하여 현재의 PC 환경 또는 모바일 환경에서의 데이터 교환 표준인 XML 문서 디지털 서명에 대한 연구를 진행하였다. 특히 본 연구는 모바일 환경에서의 보안성능을 향상시키고 모바일 플랫폼 상에서의 보안 기술을 확보하여 WIPI의 표준화 추진에 기여할 것으로 사료된다.

향후 연구 과제로는 모바일 단말 데이터 암호화와 상호 운용 가능한 디지털 서명 보안 시스템에 관한 연구가 필요하다.

참고문헌

[1] William Stallings, "Cryptography and Network Security", 2005
[2] W3C, "Canonical XML 1.0", 2001
[3] W3C, "XML-Signature Syntax and Processing", 2002
[4] Donald E. Eastlake, "Secure XML: The New Syntax for Signatures and Encryption", 2003
[5] 한국 무선인터넷 표준화 포럼, "모바일 표준 플랫폼 규격 V2.0.1", 2004