모바일 환경에서 XML 전자서명 서비스를 위한 모듈 설계 및 구현

황경민* · 이재승** · 이성현** · 조태범* · 정회경*

*배재대학교 컴퓨터공학과 · **한국전자통신연구원

The Design and Implement of Module for XML Signature Service on Mobile Environment

Kyung-min Hwang* · Jae-seung Lee** · Seong-hyun Lee** · Tae-beom Cho* · Hoe-kyung Jung*

*Dept. of Computer Engineering, Paichai University · **ETRI

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

요 약

이동 통신기술의 발달로 모바일 환경에서 대량의 데이터 전송이 가능해졌고, 원활한 모바일 응용 서비스 개발을 위해 국내 모바일 폰에 WIPI(Wireless Internet Protocol for Interoperability) 플랫폼이 의무 탑재되고 있다. 이를 통해 개발된 어플리케이션은 WIPI가 탑재된 모바일에서 단말에 비종속적으로 상호운용이 가능하다. 현재 모바일 환경에서 전자상거래가 활발히 이루어지고 있으며 이는 XML(eXtensible Markup Language)을 기반으로 데이터를 처리하여 결제자의 서명인증 및 서명 부인방지를 통해 서비스되고 있다.

이에 본 논문에서는 WIPI 플랫폼을 기반으로 하는 XML 전자서명 모듈을 개발하여 WIPI가 탑재된 모바일에서 상호운용이 가능한 XML 전자서명 서비스를 위한 모듈을 설계 및 구현하였다.

ABSTRACT

The Large amounts of data were available to transfer on mobile environment in the development of mobile telecommunications technology. And WIPI(Wireless Internet Protocol for Interoperability) platform is being mounted obligations to develope mobile application services. The applications developed on WIPI platform is possible to interoperability on mobile mounted WIPI platform, so there are not demand on mobile device. Currently e-commerce service is actively on mobile environment. This service is offerd based on XML Signature(eXtensible Markup Language) which provide integrity, message authentication, and/or signer authentication services for data of any type, whether located within the XML that includes the signature or elsewhere. In this paper, we designed and implemented XML Signature service module which possible interoperability on mobile mounted WIPI platform.

키워드

XML, 전자서명, 모바일, WIPI

Ⅰ. 서 론

최근 모바일 단말 장치는 대량의 데이터를 처리할 수 있도록 고성능화되고 있으며 이동 통신 기술 또한 이를 서비스 가능하도록 발전하고 있다. 특히 모바일 단말 장치에서 전자서명을 통해 전자상거래를 이용할 수 있는 모네타 서비스 등이 제공되고 있으며 이를 통해 교통카드, 신용카

드, 모바일 뱅킹 서비스를 사용 가능하게 되었다. 그러나 서비스가 특정 단말장치와 해당 서비스를 이용하기 위한 전자칩을 사용해야 하기 때문에 일부 모바일 폰에서만 지원되고 있다[1,2].

이를 해결하기 위해 전자칩을 사용하지 않고 소프트웨어로 전자서명이 가능한 모듈의 개발이 필요하며 이는 WIPI 플랫폼을 기반으로 개발이 가능하다. WIPI는 모바일 단말 어플리케이션의 원활한 개발과 상호 운용성을 지원하기 위해 개발되었으며, 국내에서 생산되는 모든 모바일 단말 장치에 의무적으로 탑재토록하는 정책을 추진하고 있다. WIPI로 개발된 어플리케이션은 특정 모바일 단말에 종속되지 않으며 WIPI 플랫폼이 탑재된 모바일 단말 장치에서는 어떠한 제약 없이 상호운용이 가능하다.

이에 본 논문에서는 WIPI 플랫폼을 기반으로 전자결제 서비스를 개발하여 WIPI 플랫폼이 탑재된 모바일 단말 장치에서 사용 가능하도록 XML 암호화 및 전자서명 모듈을 설계 및 구현하였다.

II. 관련연구

2.1 XML 정규화

XML 정규화는 논리적으로 동일한 XML 문서를 물리적인 형태에서도 동일성을 보장하는 규칙이다[5]. 이때 XML 문서의 물리적 동일성을 보장하는 처리를 정규화라고 한다. XML 문서 정규화는 Canonical XML 1.0에 기술된 규칙과 절차에 의해 진행되며 해당 과정을 통해 만들어진 XML 문서를 정규 XML이라고 한다[3].

2.2 XML 암호화

XML 암호화는 XML 데이터를 암호화하고 그 결과를 XML로 표현하는 기술이다[4]. XML 암호화를 통해 다양한 유형의 데이터를 암호화 가능하며 암호화에 사용된 알고리즘과 암호화 키값을 명시한다. XML 암호화에 사용되는 엘리먼트의 구조는 그림 1과 같다.

XML 암호화는 EncryptedData 엘리먼트로 모든 것을 포함하는 구조로 이루어져 있으며 EncryptedData 엘리먼트는 Id, Type 속성 등을 가진다. Id 속성은 어플리케이션의 특정 처리를 위해 사용하거나 단일 XML 문서 내부에서 여러 개의 EncryptedData 엘리먼트를 구분하기 위해 사용하는 임의의 식별자로 사용되며 Type 속성은 원본 문서의 타입을 나타내기 위해 사용한다. ElementMethod 엘리먼트는 암호화에 사용한 알고리즘에 대해 algorithm 속성을 사용하여 기술한다. 또한 암호화에 사용된 키 값의 크기를 기술하는 KeySize 엘리먼트를 제공한다. XML 암호화에 사용되는 필수 암호화 알고리즘은 AES와 Triple-DES가 있으며, 본 논문에서는 이외에도 SEED, RSA, HMAC 알고리즘을 추가하였다. KeyInfo 엘리먼트는 CipherData 엘리먼트를 해독할 키를 얻을 수 있는 위치를 기술하며 XML Signature의 스키마를 import시켜 사용하도록 정의되어 있다. CipherData 엘리먼트는 CipherValue 엘리먼트라는 자식 엘리먼트를 통해 직접적으로 암호화된 데이터에 대해 base64 부호화를 통해 기술 가능하며, XML 문서내부가 아닌 외부에 존재하는 암호화 데이터에 대해서도 CipherReference 엘리먼트를 통해 표현이 가능하다. CipherReference 엘리먼트를 통해 암호화 데이터를 기술할 경우, URI 속성을 통해 암호화된 데이터의 위치를 기술한다.

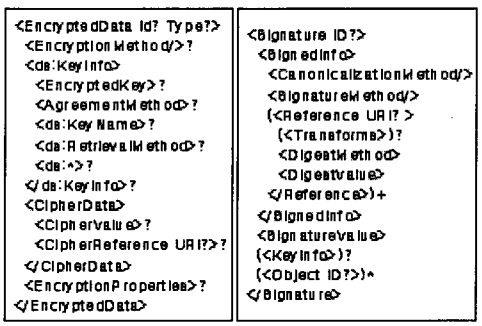

그림 1. XML 암호화 스키마 구조 (좌)
XML 전자서명 스키마 구조 (우)

2.3 XML 전자서명

XML 전자서명은 임의의 디지털 콘텐츠에 대한 디지털 서명을 표시하기 위해 쓰이는 XML 문법으로 다양한 유형의 데이터 타입에 대해 전자서명을 처리한다[5]. XML 전자서명 스키마의 구조는 그림 1과 같다.

XML 전자서명은 Signature 엘리먼트로 모든 것을 포함하는 구조로 되어 있으며 전자서명에 관련된 정보를 기술하는 SignatureInfo 엘리먼트와 서명된 데이터를 저장하는 SignaureValue 엘리먼트를 기본적으로 포함하도록 구성되어 있다. SignedInfo 엘리먼트는 전자서명에 관련된 정보를 기술하며, XML 정규화에 사용된 알고리즘을 명시하는 CanonicalizationMethod 엘리먼트, 전자서명에 사용된 알고리즘을 명시하는 SignatureMethod 엘리먼트, 서명에 사용된 Digest값과 Digest값 추출을 위해 사용된 알고리즘을 명시하는 DigestMethod 엘리먼트와, DigestValue 엘리먼트, 그리고 Digest관련 엘리먼트를 포괄하며 전자서명을 적용한 원본 문서의 위치를 기술하는 Reference 엘리먼트로 구성된다. XML 전자서명은 3가지 형식으로 나뉘는데 그 형식은 표 1과 같다. 동봉된 서명의 경우 원본 XML 문서 내의 특정 엘리먼트에 대해 Signature 엘리먼트가 추가되어 서명되는 경우이며, 동봉한 서명의 경우 서명 내에 Object 엘리먼트와 Id 속성을 통해 원본 문서를 기술하며, 이를 참조하기 위해 Reference 엘리먼트의 URI 속성

에 Object 엘리먼트의 Id 속성을 명시한다. 분리된 서명의 경우 원본 문서에도 서명이 포함되지 않고 서명 내부에도 원본 문서가 포함되지 않은 경우로서 서명외부에 존재하는 원본 문서를 서명하는 경우에 사용된다. 이때 Reference 엘리먼트의 URI 속성을 사용하여 외부에 존재하는 원본 문서의 경로를 기술한다.

III. 시스템 설계

본 시스템은 파일로 저장된 XML 파일을 읽어들여 XML 암호화와 XML 전자서명을 처리하도록 설계하였다. 이를 위해 전체 시스템은 파일 I/O 모듈, XML DOM Parser 모듈, XML 암호화 모듈, XML 전자서명 모듈, 암호화 모듈, 전자서명 모듈, Base64 부호화 모듈, XML 정규화 모듈로 구성하였다. 시스템 전체 구조는 그림 2와 같다.

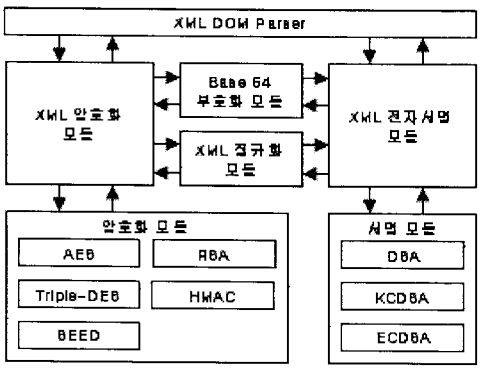

그림 2. 전체 시스템 구조

3.1 XML DOM Parser

외부로부터 XML 문서의 포인터를 전달받아 스트링 배열로 구성되어 있는 XML 문서를 DOM 파싱을 통해 메모리에 적재한다. 또한 XML DOM Parser는 효율적인 XML 문서의 관리를 위해 DOM Level 2 API를 지원하도록 설계되었다. 메모리에 적재된 XML 문서는 최상위 XML Document 정보의 포인터를 XML 암호화 모듈 또는 XML 전자서명 모듈에 전달한다.

3.2 XML 암호화 모듈

XML 암호화 모듈은 크게 암호화 콘텐츠 타입 분석 모듈과 암/복호화 알고리즘 처리 모듈, 키정보 처리 모듈로 구성된다. 암/복호화 알고리즘 처리 모듈에서 XML DOM Parser로부터 메모리에 적재된 XML Document를 전송받아 암호화를 진행한다. 먼저 전송받은 XML Document에서 암호화 또는 복호화를 진행하기 위해 암호화 타입을 암호화 콘텐츠 타입 분석 모듈을 통해 결정하며 해당 EncryptedData 엘리먼트의 Type 속성을 분석 및 생성한다. 다음으로 EncryptionMethod 엘리먼트를 통해 암/복호화에 사용할 알고리즘을 분석하며 이때 사용된 키정보를 KeyInfo 엘리먼트로부터 분석하여 암/복호화를 진행한다. 이후 암호화된 데이터는 Base64 부호화 모듈을 통해 부호화된다.

3.3 XML 전자서명 모듈

XML 전자서명 모듈은 전자서명/검증 처리 모듈, 키정보 처리 모듈, 전자서명 타입 분석 모듈, 원본 문서 Digest 추출 모듈로 구성되어 있다. DOM Parser로부터 메모리에 적재된 XML Document의 포인터를 전달받아 전자서명 서명/검증 처리 모듈에서 서명 및 검증을 수행한다. 먼저 XML 전자서명을 위해 XML 정규화 모듈을 통해 원본 XML 문서를 정규화 처리하고 전자서명 타입 분석 모듈을 통해 서명 타입을 enveloped, enveloping, detached로 분류하여 XML 문서를 생성 및 처리한다. 서명처리를 위한 원본 문서의 Digest 값 추출을 위해 Digest 추출 모듈로부터 Digest 값을 얻고 해당 값을 Base64 부호화 모듈을 통해 부호화한 뒤, DigestValue 엘리먼트에 텍스트 노드에 추가한다. 추출된 Digest 값은 다시 서명을 위해 사용되며 해당 Digest값을 통해 서명값을 추출한다. 추출된 서명값은 Base64 부호화 모듈을 통해 부호화된 후, SignatureValue 엘리먼트의 텍스트 노드에 추가된다. 이후 서명 타입에 따라 Reference 엘리먼트의 URI 속성을 결정하여 속성값을 명시한 뒤, 완료된 서명값을 검증을 통해 무결성 검사를 거친다.

3.4 암호화 모듈

XML 암호화 모듈에서 암호화 작업을 처리하기 위해 실제적으로 동작하는 알고리즘 모듈이다. 암호화 알고리즘은 필수적으로 필요한 AES, Triple-DES를 기본적으로 포함하고 있으며, 보다 다양한 알고리즘을 지원하기 위해 SEED, RSA, HMAC 알고리즘을 추가하였다. AES 알고리즘은 128비트, 256비트 블록 암호화를 지원하며, Triple-DES 알고리즘은 192비트 키(64비트 키 x 3개)를 지원하도록 설계하였다.

3.5 전자서명 모듈

전자서명에 사용되는 알고리즘으로써 전자서명에 필수요소인 DSA 전자서명 알고리즘과 KCDSA 알고리즘, ECDSA 알고리즘을 지원 가능하도록 설계하였다. 특히 KCDSA 알고리즘을 지원하기 위해 DSA 알고리즘에서 사용하는 SHA1 알고리즘 외에 HAS160 알고리즘을 추가하여 보다 안전하고 다양한 전자서명을 지원하였다.

3.6 Base64 부호화 / XML 정규화 모듈

바이너리 데이터를 전송 및 처리에 용이하도록 ASCII 코드의 64개의 부호를 사용하여 데이터를

표현하는 모듈이다. 이 모듈은 암호화 또는 전자서명을 통해 생성된 값을 부호화한다. 이는 XML 암호화 및 XML 전자서명에서 사용되는 필수요소이다. XML 정규화 모듈은 XML 암호화에서는 선택사항이며 XML 전자서명에서는 필수요소로 XML 문서의 의미는 동일할 수 있지만 표현되는 형태가 다양한 이유로 서명 변형에 영향을 주지 못하도록 설계된 모듈이다. 본 모듈에 입력된 모든 XML 문서 데이터는 UTF-8 유니코드로 부호화되며 XML 정규화의 규칙에 따라 처리된다.

Ⅳ. 시스템 구현

시스템 구현 환경은 인텔 x86계열의 IBM-PC를 기반으로 Windows XP Pro SP2 운영체제에서 개발하였다. 개발에 사용된 개발도구로는 SKT WIPI 1.2 SDK와 Microsoft Visual C++ 6을 사용하였다.

4.1 구현 시나리오

본 시스템을 사용하여 구매자가 쇼핑몰에서 물품을 선택 및 결제하고 해당 XML로 구성된 결제문서에 대해 서버를 통해 판매자에게 전송 및 서명을 검증하여 물품을 거래하는 가상의 시나리오를 구현하였다. 전체 시스템의 구현 시나리오는 그림 3과 같다.

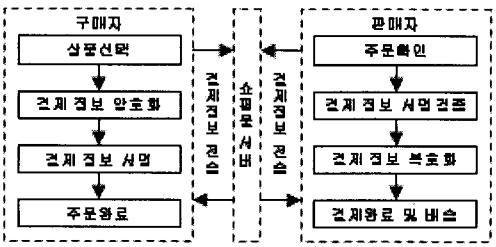

그림 3. 시스템 시나리오

4.2 시스템 구현

본 논문에서 설계한 시스템을 적용하여 구매자와 판매자를 구현하였으며 구매자와 판매자의 결제를 연결하는 쇼핑몰 서버를 구축하였다. 구매자는 쇼핑몰에 접속하여 물품을 선택하고 선택된 물품 정보와 함께 구매자의 결제 정보가 XML 문서로 생성된다. 이후 생성된 XML 문서에 기재된 결제정보를 보호하기 위해 암호화 알고리즘과 전자서명 알고리즘을 선택하여 결제정보를 암호화 및 전자서명을 진행한다. 이를 통해 최종 완성된 결제정보 XML 문서를 쇼핑몰 서버를 통해 판매자에게 전달한다. 판매자는 쇼핑몰 서버로부터 구매자의 결제 정보 XML 문서를 전송받아 해당 문서에 대한 서명 검증과 암호화된 결제정보에 대한 복호화를 진행한다. 서명 검증 및 복호화를 완료한 후 구매자의 결제정보를 확인하여 물품에 대한 배송을 진행한다. 서버는 구매자와 판매자 사이에서 결제 정보를 송수신시 해당 정보에 대한 서명 검증 중간에 진행하여 구/판매자간의 신뢰성 있는 데이터 전송을 보증하도록 구현하였다. 그림 4는 판/구매자에서 서명이 처리된 모습이다.

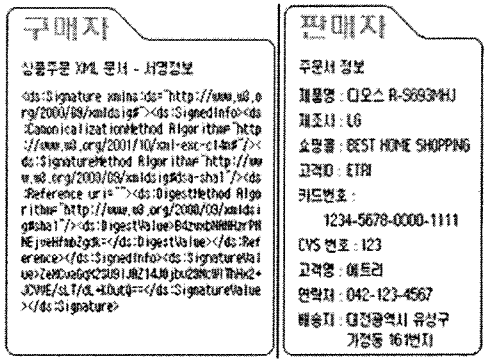

그림 4. 서명 처리된 판/구매자 모바일 정보

Ⅴ. 결 론

본 논문에서는 모바일 환경에서 전자서명을 원활히 지원하기 위해 WIPI 플랫폼이 탑재된 모바일 단말에서 사용가능한 XML 전자서명 모듈을 설계 및 구현하였다.

구매자와 판매자측 시스템 구현 시 키 생성 알고리즘을 사용하여 키 값을 생성하였을 경우 키 생성에 소요되는 시간이 길어져 사전에 생성된 키 값을 사용하여 서명 및 검증을 진행하였다. 또한 SEED, KCDSA, ECDSA 등의 다양한 암호화 알고리즘과 전자서명 알고리즘을 제공하여 보다 안전한 암호화 및 전자서명을 지원하도록 하였다.

XML 전자서명 모듈을 통해서 WIPI 플랫폼이 탑재된 모바일 단말에서는 단말의 기종에 독립적으로 사용이 가능하며 향후 모바일 단말을 통해 전자서명에 관련된 전자결제 시스템, 전자투표 등의 활용에 기여할 것으로 기대된다.

향후 연구로는 모바일 단말에서의 키 생성시 소요되는 시간을 단축하기 위한 방법에 대해 연구가 필요하다.

참고문헌

[1] 윤상흠·김현종, "무선인터넷 시장동향 및 WIPI의 역할", 전자공학회지 제30권 제11호 p122-131 2005. 4

[2] 김선자·김홍남, "모바일 플랫폼 발전 방향과 WIPI", 정보과학회지 제24권 제7호 p31-37, 2006. 7

[3] W3C, "Canonical XML", 2001. 5

[4] W3C, "XML Encryption", 2002. 12

[5] W3C, "XML Signature", 2002. 2