무선 인터넷을 위한 전자거래 시스템의 공증서비스

박동규* · 황유동*, 김학범** · 최길수**

순천향대학교 정보기술공학부*, 장미디어인터렉티브**

The Authentication Service of E-Commerce System for Mobile Internet

Park Dong-Gue* · Hwang Yu-Dong*, Kim Hak-Bum** · Choi Gil-Soo**

Department of Information and Technology Engineering, College of Engineering

SoonChunHyang University*, Jang Media Interactive**

요 약

휴대폰 및 PDA의 급속한 보급에 따라 무선 인터넷을 통한 전자 거래에 대한 관심이 증대하고 있다. 하지만 작은 대역폭과 낮은 기기 성능등 무선 환경이 갖는 한계는 무선 인터넷을 통한 전자 거래의 발전에 장애 요인이 되고 있다. 본 논문에서는 무선을 이용한 전자거래 시스템에서 공증 서비스를 제공함으로 온라인 결재에 대한 적법한 법적인 절차를 마련할 뿐만 아니라 거래에 대한 안전성 및 신뢰성을 제공하는 시스템을 구성 하고자 한다.

1. 서 론

오프라인 거래에서는 누구나 거래에 대한 영수증을 받고 또 그 영수증이 법적인 효력을 지니고 있지만 온라인 거래시스템에서는 아직 그런 제도 장치가 없었다. 따라서 온라인 결재 시스템을 이용한 사람이라면 결재에 대한 영수증 및 그 영수증의 법적인 제도장치에 대한 필요성을 느끼고 있다.

또한 휴대폰 및 PDA의 급속한 보급에 따라 무선 인터넷을 통한 전자 거래에 대한 관심이 증대하고 있다. 하지만 작은 대역폭과 낮은 기기 성능 등 무선 환경이 갖는 한계는 무선 인터넷을 통한 전자 거래의 발전에 장애 요인이 되고 있다.

본 논문에서는 무선을 이용한 전자거래 시스템에서 공증 서비스를 제공함으로 온라인 결재에 대한 적법한 법적인 절차를 마련할 뿐만 아니라 거래에 대한 안전성 및 신뢰성을 제공하는 시스템을 구성 하고자 한다.

2. 전자 공증 서비스

2. 1. 전자 공증 서비스의 개요

공증인은 신청인으로부터 송신된 전자문서의 성립과 내용을 심사하고 공증 문을 전자 서명하여 신청인에게 송신하고 보관함으로써 기존의 공증을 전자화 할 수 있으며, 전자서명이 제공하는 무결성의 특징을 이용하여 인증기관 등의 객관적 제3자를 통한 전자문서의 내용증명이 가능하다.

2.2 전자 공증 서비스의 이용가능 분야

전자 공증 서비스를 제공하거나 사용할 수 있는 서

비스의 종류로는 공공, 기업, 커뮤니케이션 및 디지털 컨텐츠 보호 의 4가지 측면으로 분류 할 수 있으며 각 분류에 대한 세부 적용 가능한 분야를 도식도로 나타내었다.

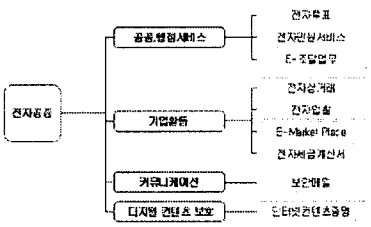

그림 1 전자공증 서비스의 이용가능 분야

2.3 전자 공증 서비스의 선행 요구조건

2.3.1 PKI 기반 기술

전자 공증 서비스를 이용하기 위해서는 전자서명, 암.복호화 기술, 인증서 관련 기술 및 각종 PKI 관련 기술이 요구된다. 이런 기술은 거래의 무결성 , 인증, 기밀성, 부인불가 등의 요구조건을 제공하기 위해서 사용되는 기술이며 각 기능에 대한 요구조건을 충분히 만족시킬 수 있는 정도의 강도 및 비도를 가지고 있는 기술들이 선정되어 적용되어야 한다.

2.3.2 표준 적합성

공증 시스템은 다양한 분야에서 여러 방면으로 적용 가능한 시스템이므로 향후에 예상되는 시스템의 확장 및 규격화 표준화에 주의를 기울여야 한다. 현재는 공증 서비스에 대한 어떠한 규정도 없는 관계로 시스템 구성요소인 PKI 기반 기술에만 국제 표준을 적용하여 시스템을 구성해야 한다.

2.3.3 법적 효력

공증시스템의 궁극적인 목적은 법적인 효력을 지니는 것이다. 현재 서비스 되고 있는 많은 인증관련 절차도 결국은 법적인 효력의 해석 여부에 따라서 선택되이지고 이용되고 있기 때문에 공증 서비스의 확장 및 이용도 결국은 법적인 제도 및 효력이 바탕이 되어야 만 한다.

3. 구현

3.1. 구현 환경

① 개발 환경

PDA : Windows 2000에서 WinCE용 VC++

서버 : SunOS jupiter 5.9 Generic sun4u sparc SUNW,Ultra-60

DB : Oracle 8.1.5

② 테스트 및 운영환경

PDA : WinCE Ver3.0 Emulator, samsung NEXIO S-150, IPAQ 3630

서버 : SunOS jupiter 5.9 Generic sun4u sparc SUNW,Ultra-60

DB : Oracle 8.1.5

3.2 구현 예

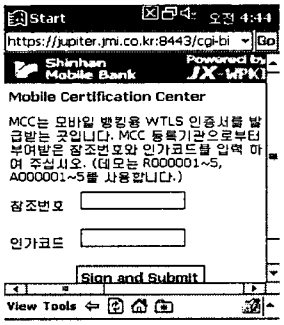

그림 2. 인증서 요청 화면

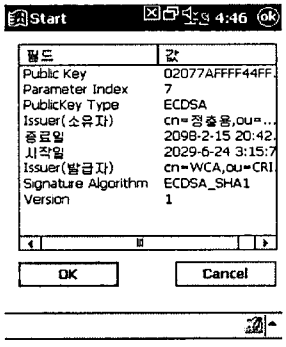

그림 3. 인증서 보기 화면

3.3. 구현 프로그램의 장점

① ECC용 인증서를 사용한 장점

- 서명은 SignedContent를 이용하고 ASN을 사

용하지 않으므로 시스템에 부하가 적음
- 인증서는 WTLS 인증서를 사용하여 용량이 작고 인증서 parsing이 단순하다.
- ECDSA를 사용하여 RSA보다 성능이 우수하다.
- 키 사이즈가 작고 인증서도 크기가 작으므로 통신 데이터량이 적다.

② JX-ECC의 성능 속도

구 분		ECC용 인증서(sec)	RSA용 인증서(sec)
Key 생성 시간	Pentium II	0.005	1.64
	Win CE	0.010	5.14
	Cellvic PDA	4.88	2.563
전자 서명 시간	Pentium II	0.005	0.10
	Win CE	0.011	0.24
	Cellvic PDA	5.03	250
Key 검증 시간	Pentium II	0.011	0.37
	Win CE	0.022	0.008
	Cellvic PDA	9.9	7.723

표 2 JX-ECC의 성능

③ 적용한 ECC 알고리즘의 장점
- Key 사이즈가 작아 암호모듈의 경량화와 속도 증가의 효과
  * ECC 160bit의 키는 RSA 1024bit와 동등한 암호화 수준을 제공.
  * 보다 큰 길이의 키가 사용될 경우 두 시스템 키의 비율은 상대적으로 증가
- 암호 알고리즘 중 가장 강력한 보안성을 확보
- 메모리 공간의 감소와 처리 효율의 증가.
  * 자원 사용과 처리용량이 제한적인 이동전화, PDA등에 적합
- RSA의 단점을 보완할 수 있는 유일한 솔루션

④ 공증 서비스
- 무선 환경에서 전자공증 서비스를 제공한다.
- DVCS 시스템을 이용하여 전자 공증에 대한 검증 서비스를 제공할 수 있다.
- 무선에 적용 가능하도록 설계된 DVC를 클라이언트에 전송하여 준다.
- 영수증 형태의 거래에 대한 결과값을 클라이언트가 저장하고 보관할 수 있다.

⑤ DVCS 시스템이 무선에 적합한 이유
- ECC 인증서로 서명한 요청 메시지는 1.3K 정도의 크기이고 응답 메시지인 DVC 는 2K 정도의 작은 사이즈로서 무선에 적합하다.
- 무선에 적용 가능한 간단한 프로토콜이다.
- 무선에 최적화된 JX-ECC 모듈을 사용하여 성능 및 속도가 PC 버전과 별 차이가 없다.

⑥ 기존의 응용 서비스와의 차별화
- 기존의 시스템은 결과 값을 저장하는 정도의 서비스만 제공하므로 법적인 문제가 있을 경우에만 특별한 프로세스로 검증에 대한 서비스를 제공하고 있다. 하지만 본 시스템은 사용자의 편의성 및 신뢰성을 제공하기 위하여 무선으로 거래확인에 대한 결과 및 공증에 대한 요청이 있을 경우 언제 어디서든지 서비스를 제공할 수 있다는 장점이 있다.
- 무선 환경에 적합한 ECC 인증서를 이용한 시스템이다.

4. 결론

본 연구에서는 무선 인터넷을 이용한 전자 거래 시스템의 공증 서비스를 위하여 ECC인증서를 이용한 시스템을 개발하였다. 개발된 시스템에서는 인증서의 유효성 검증을 위하여 DVCS 시스템을 도입하여 공증에 대한 검증서비스 또한 제공한다.

DVCS의 VSD 서비스를 이용할 경우에는 다음과 같은 문제점들이 고려되어야 할 것이다.

* 폐기 또는 효력 정지된 인증서로 싸인한 경우
* 효력 정지에 대한 서비스를 위해서는 과거의 모든 CRL을 관리 해야 하는 문제점
* 전자서명한 데이터에 시간(Time Stampping)에 대한 증명이 요구되는 문제점
  - 공증서비스의 법적인 효력여부
* 공증 서비스가 일부 특정 대상에 대한 서비스의 차원에서 벗어나기 위해서는 공증 서비스의 법적인 효력에 대한 정의 및 규정이 선행되어야 한다.

5. 참고문헌

1] ISTF-017-R1, 무선 인증서 요청형식 프로토콜 표준, 인터넷보안기술포럼, 2003. 5.
2] WAP WMLScript Crypto Library, WAP-161-WMLScriptCrypto-200106220-a, 2001.6.20
3] ISTF-Draft_014, 무선 WTLS 인증서 프로파일 표준, 인터넷보안기술포럼, 2002. 4.
4] ISTF-Draft_015, 무선 전자서명 알고리즘 표준, 인터넷보안기술포럼, 2002.4
5] WAP Wireless Transport Layer Security Proposed. WAP-261-WTLS-20010406-p, 2001. 4. 6.
6] Standards for Efficient Cryptography, SEC 1: Elliptic Curve Cryptography version 1.0, 2000.
7] RFC 2630, Cryptographic Message Syntax, IETF, 1999.
8] TTAS.KO-12.0016, 무선 전자서명 인증서 프로파일 표준, TTA, 2002.
9] TTAS.KO-12.0017,무선 전자서명 인증서 효력정지 및 폐지목록 프로파일 표준, TTA-120017, TTA, 2002.
10] TTAS.KO-12.0021 (2002), 무선 전자서명 알고리즘 표준, TTA, 2002.