모바일 단말기 상에서 안전한 인증을 위한 자바 기반의 PKI 시스템 연구

최 병 선[†] · 김 상 국[††] · 채 철 주[†] · 이 재 광[†††]

요 약

모바일 네트워크 환경은 언제 어디서나 네트워크를 사용하는 모바일 서비스를 편리하게 사용할 수 있도록 해준다. 그러나 언제 어디서나 서비스를 제공받을 수 있다는 것은 언제 어디서든지 정보가 누출되거나 왜곡될 위험성 또한 존재하기 마련이다. 특히, 프라이버시 문제가 해결되지 않고서는 우리 일상생활과 융합되어 편리함을 제공해주는 모바일 네트워크 환경이 오히려 모바일 네트워크 감시 체제를 구축하는 심각한 역기능을 초래하게 될 것이다. 모바일 단말기들은 크기와 모양이 다양하고 컴퓨팅 연산 능력이 적은 저성능 휴대 장치들이 많기 때문에, 컴퓨팅 연산이 많이 요구되는 공개키 암호 기술을 저성능 모바일 단말기에 적용하기는 힘든 상황이다. 이에 본 논문에서는 프라이버시 문제를 해결하면서, 컴퓨팅 연산 능력이 적은 저성능 모바일 단말기에 적용할 수 있는 자바 기반의 암호 모듈 및 PKI 기반의 사용자 인증을 제안하고자 한다. 국내 표준 암호 알고리즘(SEED, KCDSA, HAS160)과 인증서를 기반으로 세션키와 공개키를 조합함으로서 최소한의 암복호화 연산을 통해 인증 및 전자 서명을 제공하며, 이를 대표적인 모바일 단말기인 PDA 환경에서 세션키 분배 및 사용자 인증이 안전하게 이루어짐을 확인할 수 있었다.

키워드 : 모바일 단말기, 모바일 네트워크, 암호 알고리즘, 인증, 전자서명, 공개키 기반 구조, 인증서, 인증기관, 등록기관

A Study of Java-based PKI System for Secure Authentication on Mobile Devices

Byeong-Seon Choi[†] · Sang-Kuk Kim[††] · Cheol-Joo Chae[†] · Jae-Kwang Lee[†††]

ABSTRACT

Mobile network environments are the environments where mobile devices are distributed invisible in our daily lives so that we can conventionally use mobile services at any time and place. The fact that we can work with mobile devices regardless of time and place, however, means that we are also in security threat of leaking or forging the information. In particular, without solving privacy concern, the mobile network environments which serve convenience to use, harmonized without daily lives, on the contrary, will cause a serious malfunction of establishing mobile network surveillance infrastructure. On the other hand, as the mobile devices with various sizes and figures, public key cryptography techniques requiring heavy computation are difficult to be applied to the computational constrained mobile devices. In this paper, we propose efficient PKI-based user authentication and java-based cryptography module for the privacy-preserving in mobile network environments. Proposed system is support a authentication and digital signature to minimize encrypting and decrypting operation by compounding session key and public key based on Korean standard cryptography algorithm(SEED, KCDSA, HAS160) and certificate in mobile network environment. Also, it has been found that session key distribution and user authentication is safely done on PDA.

Key Words : Mobile Devices, Mobile Network, Cryptography Algorithm, Authentication, Digital Signature, Public Key Infrastructure, Certificate, CA, RA

1. 서 론

전 세계적인 인터넷의 폭발적인 발전과 보급으로 인하여 네트워크 상에서 이루어지는 전자 거래 또는 전자 결제, 전자정부 등의 사이버 생활 범위가 넓어지고 있다. 특히 무선 네트워크를 사용하는 모바일 네트워크 환경은 모바일 단말기의 눈부신 성능 향상과 더불어 무선 대역폭의 증가로 이전에는 생각하지 못했던 모바일 정보 서비스를 제공받을 수 있게 되었다. 모바일 단말기란 액정화면과 메모리 처리기를

※ 이 논문은 2007년도 한남대학교 학술연구조성비 지원에 의하여 연구되었음
† 준 회 원 : 한남대학교 컴퓨터공학과 박사과정
†† 정 회 원 : 한국과학기술정보연구원 지식정보센터 국내정보팀 선임연구원
††† 종신회원 : 한남대학교 컴퓨터공학과 교수
논문접수 : 2007년 6월 5일, 심사완료 : 2007년 8월 13일

가지고 있으며 손에 들고 다니면서 이용할 수 있는 단말기를 통칭한다. PDA, HPC, 스마트폰, 핸드폰 등 이러한 제품을 모바일 단말기라고 하고 좀더 넓게 보면 타블렛 PC나 포스트 PC를 모바일 단말기로 볼 수 있을 것이다. 지금까지 많이 사용하는 모바일 단말기는 PDA와 핸드폰이다. 하지만 현재까지 개발된 네트워크 관련 기술들은 모두 데스크 탑 PC 상에서 수 Mbps ~ 수백 Mbps의 넓은 대역폭을 가지며 일반적으로 신뢰성 있는 유선 네트워크를 기반으로 서비스 개발이 이루어져 왔다. 이에 무선 네트워크는 유선 네트워크에 비교할 때, 훨씬 제한적인 통신환경을 가지며 사용 대역과 이동성 등의 제한으로 인하여 낮은 대역폭과 낮은 연결 안정성 및 가능성, 높은 지연 특성을 가진다. 또한 무선 네트워크를 사용하는 모바일 단말기는 데스크 탑 PC에 비하여 CPU 성능의 제한과 낮은 메모리 용량, 사용전력 제한 등의 특성을 가지게 된다. 이로 인하여 유선 네트워크 환경과 비교할 때, 많은 보안 취약점을 가지고 있다. 즉, 기존의 유선 네트워크와 데스크 탑 PC 환경에서 제공하는 보안 서비스를 쉽게 적용할 수 없는 문제를 가지고 있다는 점이다[1]. 이에 본 논문에서는 모바일 단말기에 인증서를 사용하여 세션키와 공개키의 조합으로 효율적인 인증 및 전자서명 기능을 제공할 수 있는 PKI 기반의 인증 시스템을 연구하였다. 인증서는 개인 또는 기관에서 서명 및 암·복호화에 사용되는 공개키와 이에 대응한 개인키의 소유 증명을 확인해 주는 전자문서로써 각 구성원의 신원을 증명하기 위한 중요한 수단이다[2]. 더불어 국내 환경을 고려하여 국내 표준 암호 알고리즘인 SEED, KCDSA, HAS160과 대표적인 공개키 암호 알고리즘인 RSA, 해시 알고리즘인 SHA-1을 자바 기반의 암호 API로 구현하였다. 본 논문에서 제안된 국내 표준 암호 알고리즘 기반의 안전한 인증 및 전자서명 모듈은 모바일 네트워크 보안에 더욱 견고함을 더하여 줄 것이고, 컴퓨팅 능력이 낮은 모바일 단말기들을 대상으로 하는 모바일 네트워크를 이용한 서비스에 잘 부합될 것으로 판단되며, 향후에 개발될 서비스 이용자부터 서비스 기기까지의 통합적이고 단일화된 인증 및 접근제어 프레임워크 구축의 초석이 될 것으로 사려된다. 또한 안전성이 확보되지 않는 모바일 네트워크 서비스가 사용자로부터 외면을 받을 수밖에 없고 더욱이 모바일 네트워크 서비스에 따라 개인의 경제적 손실뿐만 아니라 프라이버시까지 위협받을 수 있으므로 제안된 PKI 기반의 인증 및 전자서명 서비스는 모바일 네트워크 기반의 서비스 활성에 이바지할 것으로 판단된다.

본 논문의 구성은 다음과 같다. 1장의 서론에 이어 2장에서는 본 논문에서 제안하는 인증 및 전자서명에 사용된 PKI를 설명하고, 3장에서는 모바일 단말기에 인증서를 발행하고 관리하는 CA와 이를 활용한 PKI 기반의 인증 및 전자서명 서비스 방식을 분석 및 설계하며, 4장에서는 이에 대한 구현 및 성능평가 결과를 설명한다. 마지막으로 5장에서는 결론을 도출한다.

2. 관련연구

2.1 PKI와 인증 서비스

인터넷 상에서 전자상거래 행위가 이루어지기 위해서는 비대면 특성을 보완하고 신뢰성을 보장하기 위한 거래 당사자 간의 신분 확인이 전제되어야 하며, 이는 인증, 무결성, 부인봉쇄 등의 서비스를 제공하는 전자서명 기술을 활용함으로써 해결가능하다. 전자서명 기술을 효과적으로 이용하기 위해서는 공개키 암호 방식이 필요하며, 공개키 암호 방식을 이용한 인증 방법을 구현하기 위한 기술적, 제도적 기반이 요구되는 이를 공개키 기반 구조(PKI: Public Key Infrastructure)라고 한다. 또한 공개키 기반 구조는 정보시스템 보안, 전자상거래, 안전한 통신 등의 여러 응용 분야에서 신원 확인이 용이하도록 하는 정책, 수단, 도구 등을 수립 및 제공하는 객체들의 네트워크 집합으로 볼수 있다[3][4]. 공개키 기반 구조에서는 거래 당사자의 신분을 증명해 주는 수단으로 인증서(Certificate)를 활용하고 있으며, 이를 관리하고 지원하기 위해서는 IETF는 RFC 문서를 통하여 표준으로 제정하고 있다[5][6][7].

2.2 X509 v3 인증서

전자서명은 물리적인 형태의 인감도장이나 수기로 생성된 서명과 같은 역할을 수행한다. 인증기관(CA: Certificate Authority)의 역할은 인감도장에 대한 인감증명서를 발급하는 동사무소와 동일하다. 여기서 CA는 사전에 정해진 방침에 따라서 거래 당사자의 신원을 증명하는데, 인증서를 발급 받고자 하는 자는 주민등록증과 같이 그의 신분을 증명할 신분증을 CA에게 제시하면 CA는 그의 신분에 관한 정보와 공개키를 담은 메시지를 생성한다. 이러한 메시지를 인증서라고 하며, CA는 이 메시지에 대해서 전자적으로 서명하여 인증서의 유효성을 보증한다. 인증서는 특정한 공개키가 특정한 개인에게 종속된다는 사실을 확인하는 수단을 제공하여 다른 사람이 특정인의 공개키를 도용하거나 공개키 자체를 변조하지 못하도록 한다. 최상위의 인증기관은 공개키는 사전에 널리 공개되어 있어야 한다[8][9][10]. X.509 v3 인증서는 X.509 v2 인증서에 비해 많은 새로운 개념들이 도입되었다. 근본적 변화는 확장자를 도입한 것이다. 이는 X.509 실현자가 그들의 용도에 적합하게 인증서 내용을 정의할 수 있게 하기 위함이다. 표준 확장자(standard extension)들은 인증서 정책 정보, 주체(subject) 디렉토리 속성, 인증 경로 제한, 확장된 인증서 폐지 목록(CRL : Certificate Revocation List) 기능들을 제공한다[11].

3. 모바일 단말기를 위한 PKI 시스템 설계

3.1 PKI 시스템

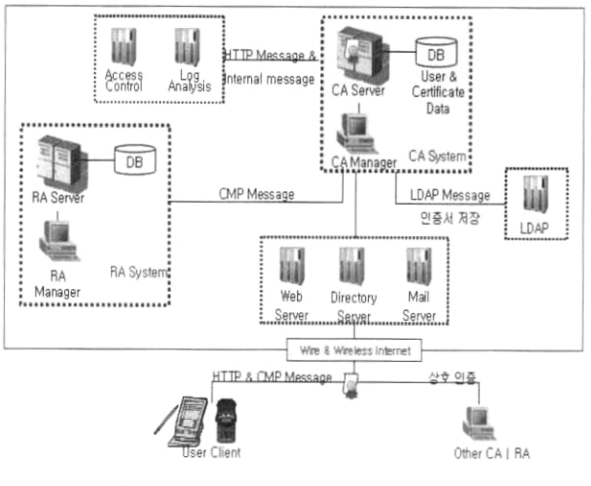
본 논문에서의 PKI 시스템은 오프라인상의 사용자 인감이나 서명을 공개키 알고리즘을 이용해서 전자적으로 구현한 사용자 인증 시스템이다. 본 시스템을 사용하는 사용자

는 인증, 무결성, 부인방지, 접근통제 등 인터넷 환경에서 요구되는 다양한 보안 서비스를 제공받게 된다.

3.1.1 구성 및 기능

본 논문에서 연구한 모바일 단말기를 위한 PKI 시스템은 (그림 1)과 같은 시스템 구성을 가지고 있다.

- CA Server : 인증서를 발급하고 관리하는 인증 시스템의 핵심으로 다양한 공개키 알고리즘을 통하여 사용자 인증서를 발급한다.
- RA Server : 사용자 정보를 등록하고 관리하는 시스템으로 CA 서버와 연계하여 사용자 인증서에 대한 발급 업무를 보조해준다.
- LDAP : CA 서버에서 발급한 인증서를 공표하기 위한 시스템으로 공개저장소의 개념을 포함한다.
- Admin Tool : CA 서버에 대한 운영 및 관리를 위한 관리자 전용 도구로 CA 서버에 대한 전반적인 운영을 제어할 수 있다.



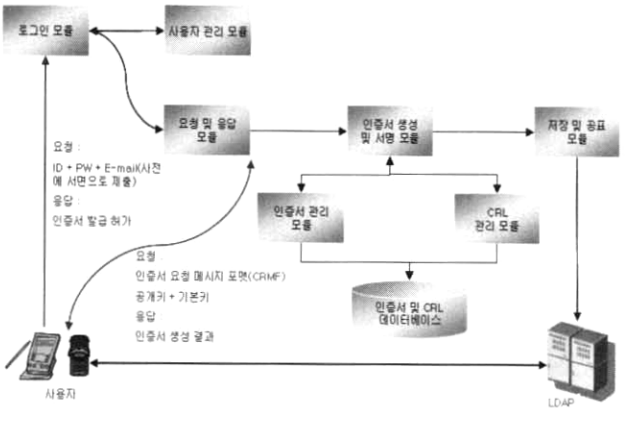
(그림 1) 모바일 단말기를 위한 PKI 시스템 구조도

3.1.2 CA 서버의 구성

본 논문에서 연구한 PKI 시스템에서 CA 서버가 가지는 역할은 절대적이라고 할 수 있다. CA 서버는 PKI 시스템의 근본을 이루는 사용자 인증서를 발행하기 위한 서버로, 이를 위해서 다양한 구성 요소를 가지게 된다. CA 서버의 역할 및 기능 구성은 (그림 2)와 같다.

3.2 제안하는 모바일 단말기를 위한 인증 시스템

본 논문에서 제안하는 인증시스템을 자체 구축한 CA에서 발급받은 인증서를 PDA와 같은 휴대단말기에 저장하고, 이를 세션키와 조합하여 안전한 로그인 기능을 제공한다. 인증서에서 사용하는 공개키 암호알고리즘은 본 논문에서 구현한 Java 암호 API 중, KCDSA와 RSA를 선택하여 발급받을 수 있으며, 세션키는 SEED 암호 알고리즘을 사용하여 생성한다. 다음 <표 1>은 본 논문에서 제안한 인증과정을 설계하는데 사용한 표기들이다.



(그림 2) CA 시스템의 모듈 구조도

〈표 1〉 사용자 인증 프로토콜 표기

표 기	의 미
E	암호화(Encryption)
D	복호화(Decryption)
CA	인증기관(Certificate Authority)
MC	모바일 클라이언트, 휴대단말기 사용자
MS	모바일 서버, 인증 서버 및 서비스 제공자
$CERT_{MC}$	모바일 클라이언트 인증서
$CERT_{MS}$	모바일 서버 인증서
SR_{MC}	MC가 생성한 난수(Secure Random 값)
SR_{MS}	MS가 생성한 난수(Secure Random 값)
PRI_{MC}, PUB_{MC}	모바일 클라이언트의 개인키와 공개키
PRI_{MS}, PUB_{MS}	모바일 서버의의 개인키와 공개키
secretkey	비밀키(Secret Key)
sessionkey	세션키(Session Key)
AutoInfo	인증이 성공했음을 포함하는 인증 메시지
SEED	국내 표준 대칭 암호 알고리즘(SEED)
RSA	비대칭 암호 알고리즘(RSA)
SHA-1	해시 알고리즘(Secure Hash Algorithm)
||	연접(concatenate) 연산자

모바일 네트워크에서 안전하게 정보를 전송하기 위해서는 먼저 클라이언트와 서버 또는 기기간 상호인증 및 키 동기화(세션키) 과정이 필요하다. 상호인증 및 세션키 설정 절차는 다음과 같은 절차로 수행된다.

3.2.1 Connection Request와 Challenge

Step 1. [MC -> MS] : 모바일 클라이언트(Mobile Client)가 모바일 서버(Mobile Server)로 접속을 요청한다. 이때 클라이언트는 자신의 인증서($CERT_{MC}$)를 서버로 전송한다.

Setp 2. [MC <- MS] : 서버가 E_SR_{MS}_secretkey와 E_secret_PUB_{MC}, $CERT_{MS}$를 클라이언트로 전송한다.

① 클라이언트의 연결요청과 인증서를 수신한 서버는 CA에게 인증서의 유효성 유무를 요청한다.

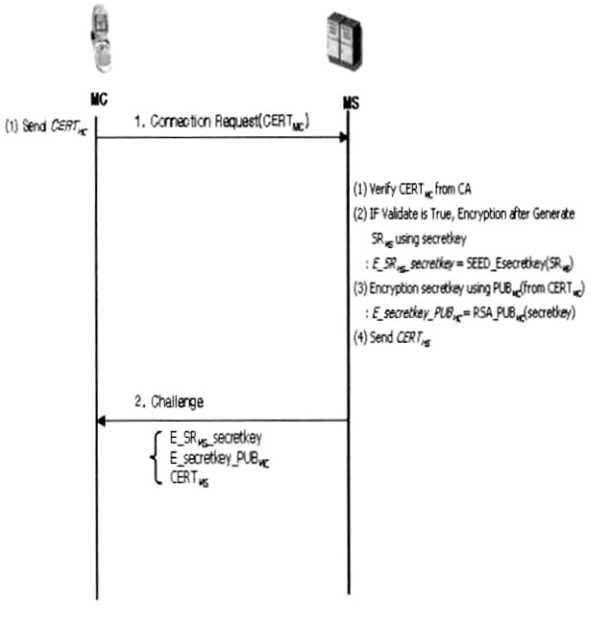
② 클라이언트의 인증서가 유효한 경우, 서버는 SecureRandom 함수를 이용하여 난수(SR_{MS})를 생성하

고, 이를 SEED 기반의 비밀키(secretkey)를 사용하여 암호화 한다($E\_SR_{MS}\_secretkey$).

③ secretkey를 안전하게 전송하기 위해, $CERT_{MC}$로부터 획득한 RSA 기반의 공개키(PUB_{MC})를 사용하여 암호화 한다($E\_secretkey\_PUB_{MC}$).

④ 서버는 자신의 인증서($CERT_{MS}$)를 클라이언트로 함께 전송한다.

다음 (그림 3)은 Step 1과 Step 2의 동작 과정을 보여주고 있다.



(그림 3) Step 1. Connection Request와 Step 2. Challenge

3.2.2 Response

Step 3. [MC -> MS] : 클라이언트가 E_sessionkey_PUB_{MS}와 E_SR_{MC}_secretkey를 서버로 전송한다.

① 서버로부터 인증서를 수신한 클라이언트는 CA에게 인증서의 유효성 유무를 요청한다.

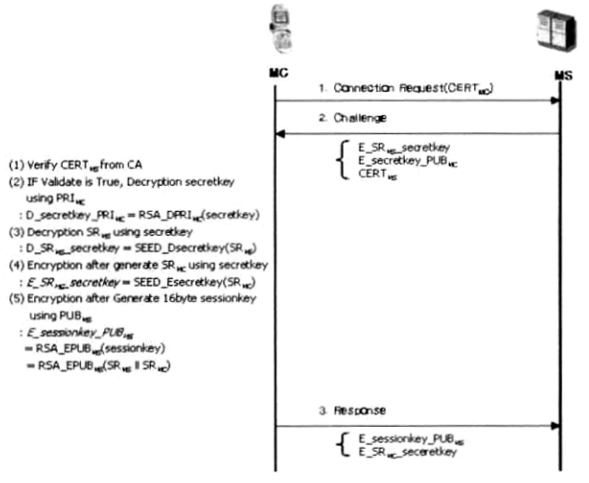
② 서버의 인증서가 유효한 경우, 클라이언트는 자신의 개인키(PRI_{MC})를 사용하여 서버로부터 수신한 secretkey를 복호화한다($D\_secretkey\_PRI_{MC}$).

③ 복호화한 secretkey를 사용하여 SR_{MS}를 복호화한다($D\_SR_{MS}\_secretkey$).

④ 클라이언트는 자신의 난수(SR_{MC})를 생성하고, 이를 secretkey로 암호화한다($E\_SR_{MC}\_secretkey$).

⑤ 클라이언트는 자신이 생성한 SR_{MC}와 복호화한 SR_{MS}를 연접($SR_{MS} \| SR_{MC}$)하여 16바이트(SEED는 128비트의 키를 사용)의 세션키(sessionkey)를 생성하고 이를 $CERT_{MS}$로부터 획득한 공개키(PUB_{MS})를 사용하여 암호화한다($E\_sessionkey\_PUB_{MS}$).

다음 (그림 4)는 Step 3의 동작 과정을 보여주고 있다.



(그림 4) Step 3. Response

3.2.3 Authentication Info

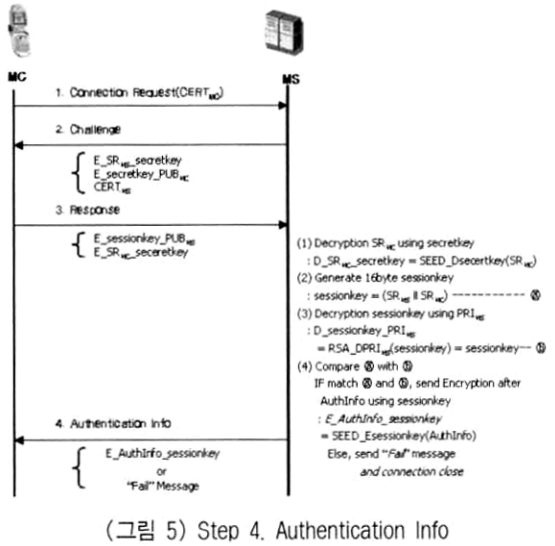
Step 4. [MC <- MS] : 서버가 인증 유무를 알려주는 E_AuthInfo_sessionkey 또는 Fail 메시지를 클라이언트로 전송한다.

① secretkey를 사용하여 SR_{MC}를 복호화한다 ($D\_SR_{MC}\_secretkey$).

② 복호화한 SR_{MC}와 서버 자신의 SR_{MS}를 연접하여, 16바이트 sessionkey를 생성한다($SR_{MS} \| SR_{MC}$).

③ 서버의 개인키(PRI_{MS})를 사용하여 클라이언트로부터 수신한 sessionkey를 복호화한다($D\_sessionkey\_PRI_{MS}$).

④ 서버는 ②에서 생성한 sessionkey와 ③에서 복호화한 sessionkey를 비교한다. 만약, 두 키가 일치한다면 sessionkey를 동기화하고 클라이언트에게 인증이 성공했음을 알리는 메시지를 동기화한 sessionkey를 사용하여 암호화한다($E\_AuthInfo\_sessionkey$). 그러나 두 키가 일치하지 않는다면, 인증이 실패했음을 알리는 메시지를 생성한다($Fail$).



(그림 5) Step 4. Authentication Info

위의 (그림 5)는 Step 4의 과정을 보여주고 있다.

3.2.4 Support of Application Service

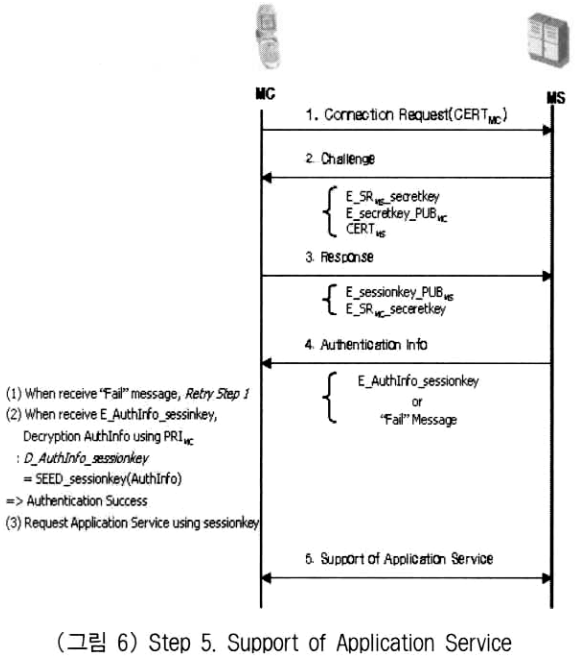
Step 5. [MC <-> MS] : 인증이 성공한 경우 서버에게 응용 서비스를 제공받을 수 있다.

① 서버로부터 "Fail" 메시지를 수신한 경우, Step 1부터 재시도 한다.

② sessionkey로 AuthInfo를 복호화하여 인증이 성공했음을 알게 된다(*D_AuthInfo_sessionkey*).

③ 동기화한 sessionkey를 사용하여 안전하게 메시지를 주고받을 수 있으며, 또한 서버의 응용 서비스를 제공받을 수 있다.

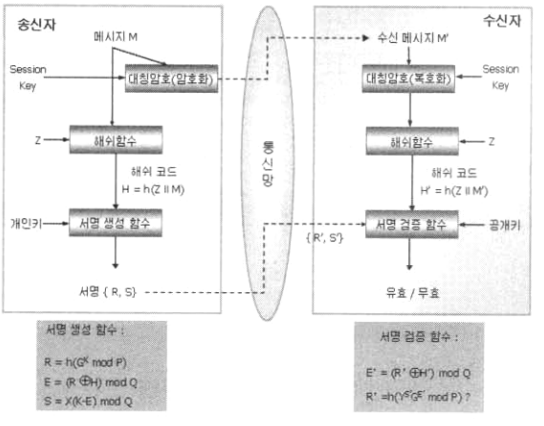
다음 [그림 6]은 Step 5의 과정을 보여주고 있다.



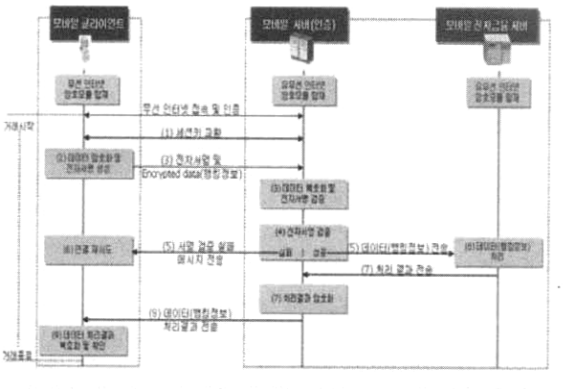
(그림 6) Step 5. Support of Application Service

3.3 안전한 데이터 전송 시스템

다음 (그림 7)과 (그림 8)은 KCDSA[12]를 이용하여 전자서명을 제공하는 뱅킹 데이터 전송 과정을 도식화한 것이다. 그림에서 알 수 있듯이, 모바일 클라이언트가 전송하는 뱅킹 데이터는 모바일 서버(인증 수행)에 의해 인증이 완료된 후, 모바일 전자 금융 서버에게 뱅킹 데이터가 전송되다. 모바일 인증전자 서명 및 검증은 기존의 KCDSA에서 제공하는 방법을 활용하고 있다. 다만 KCDSA가 메시지에 대한 암호화 기능을 제공하지 않기 때문에 본 논문에서는 인증 과정에서 동기화한 세션키를 활용하여, 메시지를 암호화하여 전송한다. 이때, 세션키는 16바이트로서 SEED에서 요구하는 키 길이와 동일하다. 따라서 모바일 클라이언트는 SEED 암호화를 적용한 뱅킹 데이터와 특정 디렉토리에 있는 has160KCDSA 서명 알고리즘을 가지고 있는 인증서를 활용하여 전자 서명을 생성하여 모바일 서버에게 전송한다.



(그림 7) KCDSA를 이용한 전자서명



(그림 8) 전자 서명을 이용한 뱅킹 데이터 전송 절차

이를 수신한 모바일 서버는 암호화된 뱅킹 데이터에 대하여 복호화를 수행하고, 모바일 클라이언트의 전자 서명을 검증을 하여 신원 확인을 수행할 수 있다. 이때 본 논문에서는 모바일 서버가 has160KCDSA 서명 알고리즘을 가지고 있는 인증서를 CA로부터 이미 다운로드 받은 상태로 가정하였다. 아니면, 전자 서명 전에 해당 인증서를 서버에게 전송하는 방법을 사용할 수도 있다. 본 논문에서의 전자 서명 기능은 뱅킹 데이터와 같은 민감한 데이터에 대하여 암호화를 수행함으로써, 제 3자에 의한 데이터 도청 및 가로채기를 방지하는 것이다.

4. 구현 및 성능 평가

본 논문에서 개발한 CA 및 보안 서비스, LDAP 등과 같은 전체 시스템은 IBM 호환 PC를 사용하여 각 모듈의 소스 코드를 작성하였으며, 마이크로소프트사의 Windows 2003 Server와 RedHat사의 리눅스 9을 통하여 시스템을 구축하였다.

또한, JDK 1.2 및 1.4[13]를 통하여 각종 API 및 인터페이스 등을 구현하였으며, 보안 서비스와 관련된 모듈은 Bouncycastle[14]의 핵심 API를 활용하여 구축하였으며, SEED와 KCDSA, HAS160을 추가하였다. 가장 중요한 특징

〈표 2〉 PKI 시스템 구축을 위한 환경

항 목		내 용
개발 API	Language	PDA : J2SETM v1.2 Server : J2SETM v1.4
	Cryptography API	Buncycastle 1.17 Crypto API
	EJB	EJB(Enterprise Java Beans) 2.1
구현 환경	개발 Tools	Kawa 3.22 JSP(Java Server Page)
	Hardware	Intel Pentium III 800MHz RAM 512MB Intel Pentium IV 2.4GHz RAM 512MB
	OS	Windows 2003 Server Windows XP Redhat Linux 9

〈표 3〉 PDA 환경

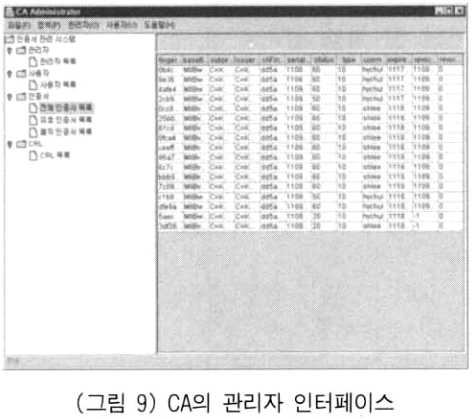
항 목		내 용
사용 기종	시스템 ROM	128MB
	시스템 RAM	128MB
	플래시 블록 크기	128KB
	OS 버전	Windows CE 4.21
	디스플레이	240×320
	프로세스	Intel(R) PXA270
자바 환경		Personal Java 1.1 (WINCE, ARM 프로세서용)

중의 하나는 현재 개발한 PKI 시스템은 PDA 등과 무선 단말기 환경을 고려하여 개발하였으나, 일반 유선 데스크 탑 환경으로 확장이 용이하다는 점이다. PKI 시스템을 구축 및 운영하기 위한 환경은 <표 2>와 같으며 클라이언트 시스템 환경, 즉 일반 사용자가 사용하는 PDA 환경은 <표 3>과 같다.

4.1 PKI 시스템 인터페이스

4.1.1 관리자 도구

관리자 도구는 CA에 대한 운영 및 인증서 발급 업무, 사용자 관리, 정책 설정 등과 관련한 업무를 수행하기 위한 인터페이스이다. 자바를 기반으로 스윙을 사용하여 구현하였다. 다음 (그림 9)는 관리자 도구의 인터페이스를 보여주고 있다.



(그림 9) CA의 관리자 인터페이스

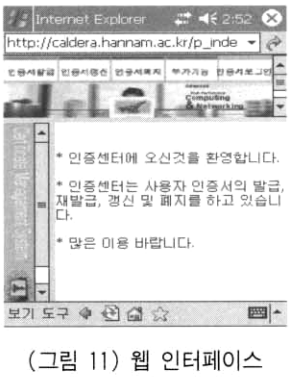
4.1.2 정책설정

정책은 CA 시스템을 운영하기 위한 핵심 정보를 설정하고 관리하기 위한 일종의 가이드라인이다. (그림 10)은 구현한 CA에서 적용되고 있는 정책의 일부 예이다.

(그림 10) CA의 정책 파일

4.1.3 사용자 웹 인터페이스

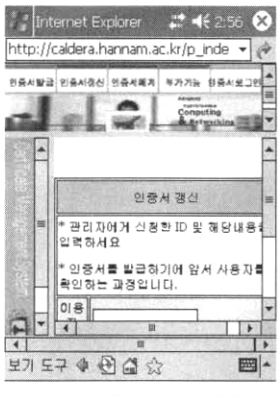
사용자 웹 인터페이스는 인증서 발급/재발급, 갱신, 폐지, 검증, 열람등과 같은 핵심 사용자 기능을 포함하고 있으며, 웹 기반으로 작성되어 있으며, 사용자의 단말기 환경을 고려하여 240*320에 최적화되어 있다. 다음 (그림 11)은 PDA에서 웹 인터페이스 화면을 캡쳐한 모습이다.



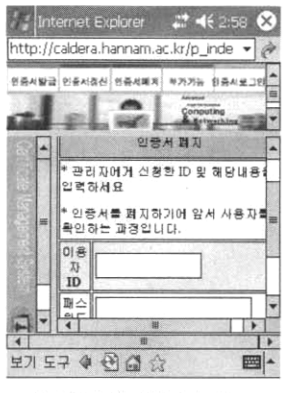
(그림 11) 웹 인터페이스

(그림 12) 인증서 발급

위의 (그림 12)는 PDA에서 인증서를 발급받는 과정을 보여주고 있다. 사용자는 서면으로 아이디와, 패스워드, 이메일 주소등을 포함하는 신청양식을 서면으로 제출하고, 관리자는 사용자의 신원을 확인한 후, 이를 등록한다. 등록이 완료되면 사용자에게 이메일로 이 사실을 통보하고, 사용자는 웹 인터페이스를 사용하여 인증서를 자신의 PDA로 발급받을 수 있다. 또한 자신의 데스크 톱 PC에서 인증서를 다운로드 받은 후, 이를 PDA로 다운로드 할 수도 있다. 다음 그림들은 웹 인터페이스를 통하여 제공되는 서비스인 인증서 갱신, 폐지, 검증 및 CRL 목록을 다운로드하는 과정을 보여주고 있다.



(그림 13) 인증서 갱신



(그림 14) 인증서 폐지

(그림 15) 인증서 검증

(그림 16) CRL 가져오기

다음 (그림17)과 (그림 18)은 PDA에 다운로드한 인증서를 보여주고 있다.

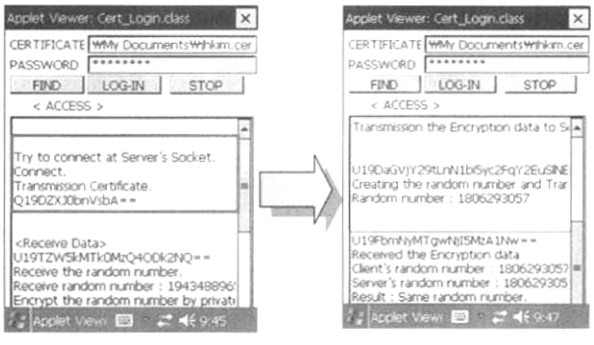
(그림 17) 인증서 관리 윈도우 실행

(그림 18) CA 인증서 정보

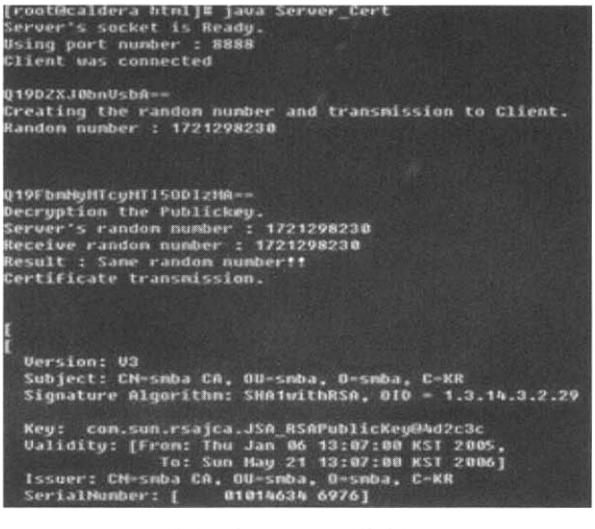
4.2 인증서 기반의 인증 테스트

본 논문에서 구현한 인증서 기반의 인증 구조는 (그림 19)와 (그림 20)에서 보는 바와 같이 비밀키와 공개키를 조합한 인증 시스템으로 공격자가 중간에 메시지를 가로챌 수 없으며, 이 과정을 통하여 안전하게 메시지를 송수신할 수 있는 세션키를 확립한다.

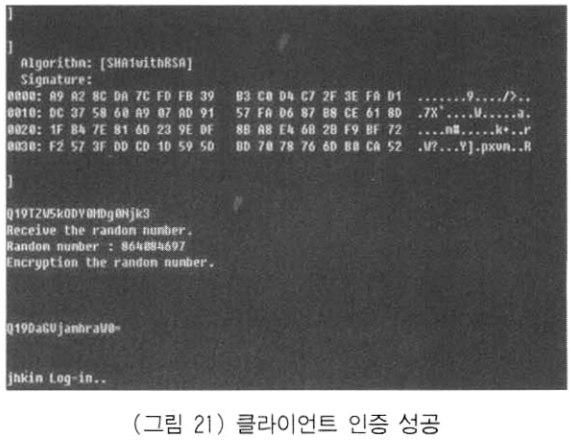
또한 다음 (그림 21)에서 보는 바와 같이 서버가 클라이언트를 인증하게 되면, 클라이언트에게 인증 완료 메시지를 전송하고 응용 서비스를 제공하게 된다.



(그림 19) 인증 과정(클라이언트)



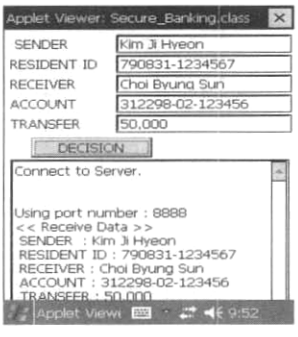
(그림 20) 인증 과정(서버)



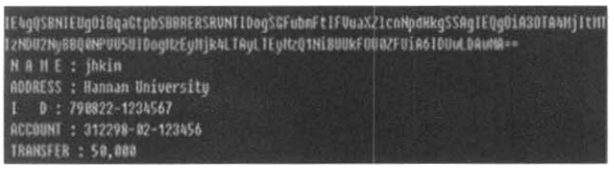
(그림 21) 클라이언트 인증 성공

4.3 안전한 데이터 전송 테스트

인증과정에서 동기화한 세션키는 클라이언트와 서버 간의 데이터 전송에 있어서 안전한 메시지 전송을 보안한다. 다음 (그림 22)와 (그림 23)은 모바일 뱅킹을 가정하여 안전한 계좌 이체 데이터 전송과정을 보여주고 있다. 세션키를 통하여 안전한 메시지 전송을 보장하고, 전자서명을 통하여 신원확인 및 부인방지를 제공하게 된다.



(그림 22) 뱅킹정보 전송



(그림 23) 뱅킹정보 수신

4.4 성능 평가 및 분석

4.4.1 응용연산 성능평가

암호 알고리즘의 성능을 평가하기 위해, 다음 <표 4>와 같이 동일한 암호 알고리즘에서 중요한 연산들이 속도를 PDA와 데스트 탑 PC 환경에서 테스트 하였다. 본 논문에서는 암호 연산에 사용하는 임의의 정수 클래스를 구현하였다. 기존의 JDK에서는 임의의 정수 클래스로서 BigInteger를 제공하지만, PDA에 사용되는 Personal Java에서는 이를 제공하지 않는다. 따라서 효율적인 암호화 연산을 위해서는 이러한 임의의 정수 클래스 구현이 필수적이라 하겠다. 구현한 임의의 정수 클래스는 JDK 1.4를 참조하여 구현하였다. 수행 시간은 동일한 연산을 1,000회 반복한 시간이며, 단위는 ms(1/1000초)이다. 처리 가능한 최대 자료형이 JDK1.4(PC)에서는 8 바이트 길이의 Long형이고 (Personal Java 1.1(PDA)에서는 2바이트 길이의 short형이다. 이러한 제한 때문에 본 논문에서 구현한 연산 클래스가 JDK1.4보다 소요 시간이 오래 걸린다.

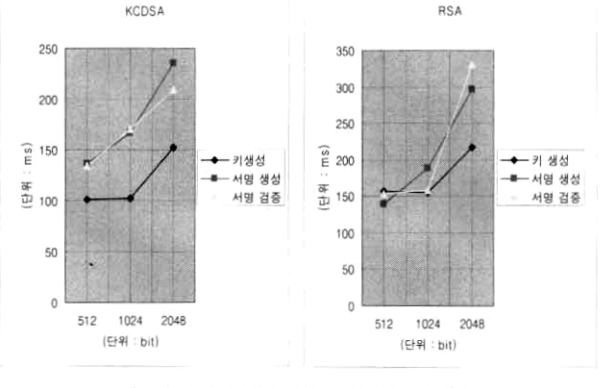
〈표 4〉 수행시간

(단위 : ms)

Method	PDA	PC
최대 공약수 x.gcd(y)	221	20
모듈러 지수 연산(x^y mod n) x.modPow(y, n)	130	71
승산 역원 (x^{-1} mod n) x.modInverse(n)	140	50

4.4.2 비대칭 암호 알고리즘

다음 (그림 24)는 본 논문에서 구현한 암호 API에 대한 수행 시간을 분석하기 위해 전자서명에 사용되는 KCDSA와 RSA에서 키 길이에 따른 키 생성 및 서명 생성과 검증 속도를 측정하여 성능을 평가한 것이다. 현재까지는 PDA와 같은 모바일 단말기의 하드웨어적 성능이 유선 네트워크를 사용하는 데스크 탑 PC 환경에 비해 현저히 뒤떨어지기 때문에, 키 생성, 암호화/복호화, 전자서명/검증에 소요되는 시간을 분석하여 최적의 성능을 발휘하는 암호 알고리즘을 선택하여야 한다. 향후 모바일 단말기의 성능이 향상된다면, 암호 알고리즘을 선택하는데 있어 보다 다양해지리라 생각된다. 키 생성 및 서명 생성과 검증에 있어서는 KCDSA가 RSA보다 빠른 속도를 보이고 있으나, RSA에 비해 전자 서명만을 제공할 뿐 암복호화 기능을 제공하지 않기 때문에, 본 논문에서는 세션키(SEED 알고리즘)를 이용하여 KCDSA가 암복호화 기능을 제공함으로써 안전한 메시지 전송을 제공하도록 하였다. 또한 KCDSA는 국내표준 전자서명 알고리즘으로서 국내환경에 필수적이며, 2006년 ISO 정보보안기술(JTC1/SC27) 국제표준화 회의에서 국제표준으로 확정되었다.

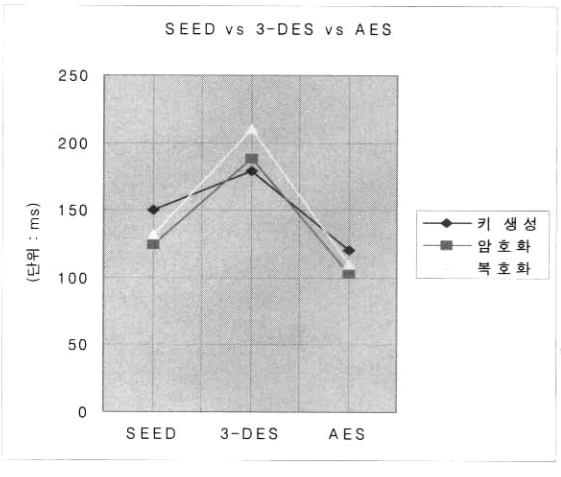


(그림 24) KCDSA와 RSA 성능 평가

4.4.3 대칭 암호 알고리즘

다음 (그림 25)는 대표적인 대칭키 알고리즘인 SEED와 3-DES, AES에 대하여 키 생성, 암호화 및 복호화 속도를 측정하였다. 여기에서는 성능평가를 위해 다음과 같은 제약사항이 있다. AES는 비록 세 개의 키 사이즈(128/192/256)를 갖지만, 한 개의 키 사이즈(128)를 가지는 SEED와 비교하기 위해, 두 알고리즘의 키 사이즈를 128비트로 한정하여 측정하였다. 그리고 3-DES의 경우 두 개의 키 사이즈(112/168)를 갖지만, SEED와 AES가 보다 작은 키임에도 불구하고 동일한 성능을 가지고 있음을 보이기 위해 키 사이즈를 168로 한정하여 측정하였다. 따라서 본 논문에서의 3-DES는 168비트(56비트의 크기를 가지는 3 개의 키를 사용)의 키를 사용하였다. 물론 키 사이즈가 클수록 보다 강력한 암호화 강도를 제공한다. 하지만, 휴대폰과 같은 적은 용량의 메모리로 커다란 암호학적 강도를 유지해야 하는 분야에 쉽게 적용하려면, 기본적인 암호학적 강도를 제공하면서 키 사이즈가 작고 빠른 수행속도를 가지는 암호 알고리즘을 선택하는 것이 중요하다. SEED(128)와 AES(128)는 3-DES(168)와 거의 동일한 암호학적 강도와 빠른 수행 속도(라운드 수가 3-DES에 비해 적음)를 제공한다. SEED가 비록 AES에 비해 동일한 키 사이즈를 가지면서도 수행속도

가 느리지만, 2005년 ISO/IEC 국제표준화 회의에서 국제표준으로 채택되었고, IETF에도 4건의 국제표준을 보유하고 있다. 또한 민수부문용 국내 표준 블록암호로 개발되어 현재 다양한 응용에서 사용되고 있어 국내환경을 고려할 때 필수적인 암호 알고리즘이라고 할 수 있다.



(그림 25) SEED와 3-DES, AES의 성능 비교

5. 결 론

급격히 발전하고 있는 인터넷을 통한 전자거래, 인터넷뱅킹, 전자문서 교환과 같은 서비스는 교환되는 메시지의 암호화와 함께 송·수신하거나 결제하는 사람의 신원에 대한 인증 문제가 매우 중요하다. 인증서는 개인 또는 기관에서 서명 및 암·복호화에 사용되는 공개키와 이에 대응한 개인키의 소유 증명을 확인해 주는 전자문서로써 각 구성원의 신원을 증명하기 위한 중요한 수단이다. 본 연구를 통해서 구현된 PKI 시스템은 모바일 단말기 사용자뿐만 아니라, 각 기관이 가지는 사용자, 주 활용 형태, 기관 특성 등에 맞게 구축할 수 있는 중·소규모의 인증 체계를 수립하는 것을 목표로 연구하였다. 또한 모바일 단말기가 가지는 하드웨어적 제약 사항을 극복하고자, 모바일 단말기에 적합한 인증서 관리 서비스와 자바 기반의 암호화 알고리즘을 설계 및 구현하였다. 또한 비밀키와 공개키를 조합하여 보다 안전한 인증을 제공할 수 있도록 하였으며, 세션키와 공개키의 조합을 통하여 안전한 전자서명을 제공할 수 있었다. 또한 국내 표준 암호 알고리즘인 SEED와 KCDSA를 모바일 단말기에 적용하여 테스트하여 보았다. 또한, 암호 알고리즘과 PKI 시스템 구축을 위한 핵심 클래스의 결합을 통해서 인증서를 발행 및 관리를 자유롭게 할 수 있는 PKI 체계를 구축하였다. 암호 API 및 PKI 클래스를 토대로 하는 PKI 시스템의 개발은 암호 알고리즘을 활용한 보안 서비스의 중요한 위치를 차지하고 있으며, 현재 모바일 네트워크 기반의 각종 서비스에서 강력한 보안 기능을 제공하는 부분으로, 각종 보안 서비스의 제공을 위해서 가장 먼저 구축되어야 할 부분이다. 본 논문에서 개발된 PKI 시스템은 기존 사용 제품들에 대항하여 독자적인 기술/상업적인 가치를 지니고 있으며, 향후 각종 보안 서비스의 제공에 있어서 선도적인 위치를 차지할 수 있을 것이다. 본 논문에서의 PKI 시스템은 자바 기반으로 개발되어 유형 정의를 시스템에 무관하게 정의하기 때문에 플랫폼에 독립적이고 이식성이 매우 높으며, 시스템에 무관한 2진 파일을 생성하는 인터프리터 언어이기 때문에 컴파일 언어에 가까운 속도와 시스템 독립성을 보장한다. 또한 자바는 포인터 개념이 없고 유형정의가 간단하여 실행 전에 클래스 파일을 이용한 프로그램의 검사가 가능하며, 실제로 웹 브라우저가 애플릿을 실행가 전에 보안검사를 수행하기 때문에 보안에 있어서 안전하다고 할 수 있다. 더불어, 개별 서비스에 대한 모듈 형식으로 구성되어 있어, 그 활용의 범위가 고정되지 않고, 다양한 시스템 및 서비스에 적용할 수 있는 장점을 가지고 있다. 향후 연구로는 이러한 보안 모듈을 WIPI 기반의 환경에 적용시켜 휴대폰과 같은 모바일 단말기에 PKI 서비스를 제공하는 것이다.

참 고 문 헌

[1] 윤종호, "무선 LAN 보안 프로토콜", (주)교학사, 2005.

[2] 원동호, "현대 암호학", 그린 출판사, 2004.

[3] 전문석, 유두구외 5명, "PKI", 도서출판 미래컴, 2003.

[4] 최용락, 소우영, 이재광, 이임영, "컴퓨터 통신 보안", 그린 출판사, 2005.

[5] IETF, "Internet X.509 Public Key Infrastructure Certificate and CRL Profile", RFC 2459, January 1999.

[6] IETF, "Internet X.509 Public Key Infrastructure Certificate Management Protocols", RFC 2510, March 1999.

[7] 류종호, 염흥렬, "인증서 관리 프로토콜(CMP)의 최근 동향", 정보보호학회지, 제 10권 제 4호, 2002. 12.

[8] RSA Data Security, Inc., "Public Key Cryptography Standards #1-12", June 3, 1991.

[9] IETF, "Internet X.509 Certificate Request Message Format", RFC 2511, March 1999.

[10] ITU-T, "Specification of Abstract Syntax Notation", X.208, 1988.

[11] 한국정보통신기술협회, "전자서명 인증서 효력정지 및 폐지목록 프로파일 표준", TTSS.KO-12.0013, 2001. 8.

[12] 김병천, "KCDSA 표준개정", 비시큐어, 2000. 12.

[13] http://java.sun.com/downloads/ea/

[14] Jess Garms, Daniel Somerfield, "Professional Java Security", 정보문화사, 2001.

최 병 선

e-mail : bschoi@netwk.hannam.ac.kr
2002년 한남대학교 컴퓨터공학과(학사)
2004년 한남대학교 컴퓨터공학과 (공학석사)
2004년~현재 한남대학교 컴퓨터공학과 (박사과정)
관심분야 : 정보보호, PKI, 시스템 보안

채 철 주

e-mail : cjchae@netwk.hannam.ac.kr
2004년 한남대학교 컴퓨터공학과(학사)
2006년 한남대학교 컴퓨터공학과(공학석사)
2006년~현재 한남대학교 컴퓨터공학과 (박사과정)
관심분야 : 네트워크 보안, 유비쿼터스 컴퓨팅, 시스템보안

김 상 국

e-mail : skkim@kisti.re.kr
1989년 인천시립대학교 전자공학과(학사)
1991년 한양대학교 전자계산학과 (이학석사)
2005년 한남대학교 컴퓨터공학과 (공학박사)
2001년~현재 한국과학기술정보연구원 선임연구원
관심분야 : 정보보호, 정보통신, BPMS

이 재 광

e-mail : jklee@netwk.hannam.ac.kr
1984년 광운대학교 전자계산학과(학사)
1986년 광운대학교 전자계산학과 (이학석사)
1993년 광운대학교 전자계산학과 (이학박사)
1993년~현재 한남대학교 컴퓨터공학과 교수
관심분야 : 정보보호, 네트워크 보안, 임베디드 시스템