情 報 保 護 學 會 誌
第21卷 第1號, 2011. 2

모바일 혁명시대의 공인인증서 이용 현황 및 정책 방향

강 필 용*

요 약

'손안의 PC'로 비유되는 스마트폰의 등장 및 폭발적인 보급과 함께 온라인 정보서비스 패러다임이 모바일 환경으로 급속히 전환되고 있다. 이러한 모바일 환경은 시간 및 공간의 제약없이 정보서비스를 받을 수 있는 장점이 있는 반면, 상대적으로 취약한 보안 환경으로 인한 정보보호에 대한 우려도 증가하고 있다. 이에 사이버 인감증명서로 비유되는 공인인증서는 여전히 보편적인 신뢰수단으로 그 위상을 유지할 것으로 전망되고 있으며, 본 고에서는 모바일 환경에서의 공인인증서비스 현황 및 안전성·신뢰성 제고를 위한 정책 방향을 소개한다.

I. 서 론

스마트폰으로 대표되는 스마트기기의 확산으로 모바일 혁명이 현실화되고 있다. '손안의 PC'로 불리는 스마트폰은 휴대전화의 기능에 정보처리 기능 및 인터넷 연결을 통한 데이터 통신을 지원하는 모바일 기기로서, 사용자는 상시 휴대를 통해 시간 및 공간의 제약없이 인터넷에 연결하여 24시간 정보서비스를 이용할 수 있게 되었다.

최근의 방송통신위원회 발표[1]에 따르면, 국내의 스마트폰 가입자 수는 2010년 10월말 기준으로 525만명으로 전체 이동통신 가입자의 10.4%를 차지하고 있으며, 12월까지 총 630만대가 보급될 것으로 내다봤다. 또한, 2015년에는 누적 가입자가 3,500만명에 육박하여 전체 가입자의 64.3%를 차지할 것으로 예상했다. 또한, 태블릿 PC도 급속도로 보급('10년 10만대 → '12년 437만대 예상)되는 등 현재의 추세를 고려하면, PC로 대표되는 유선 환경의 상당부분을 스마트기기 기반의 모바일 환경이 대체할 것으로 전망된다.

한편, 이와 병행하여 보안에 대한 우려도 급속히 증가하고 있는데, PC와 비교해 다양한 접속경로 존재 및 잦은 응용 프로그램 설치, 24시간 구동되는 환경임에도 제한된 컴퓨팅 파워 및 배터리 용량 등으로 보안 프로그램 구동이 제약을 받는 등 근본적으로 취약한 보안 환경에 기인한다.

이러한 보안 위협에 대응하기 위해 단말 및 컨텐츠(응용 프로그램 포함)는 물론, 네트워크 및 서버 등 계층별로 전방위적인 보안 대응체계가 요구되고 있다.

본 고에서는 정보보호 기반에 해당하는 식별·인증 기능을 지원함으로써 전자금융서비스 등에 필수적으로 적용되고 있는 공인인증서를 중점적으로 살펴보고자 한다. 현재, 사이버 인감증명서로 비유되는 공인인증서는 서명자의 본인확인과 서명 내용의 무결성 및 부인방지 제공을 위한 신뢰수단으로 폭넓게 활용되고 있다.

높은 보안성을 요구하는 대표적인 모바일 서비스로는 스마트폰 뱅킹 및 증권거래 등 금융서비스와 전자민원 등 전자정부 서비스 이용을 들 수 있다. 최근의 추세를 보면, 스마트폰 소지자의 25% 이상이 뱅킹서비스에 가입하여 서비스를 사용하고 있는 등 이용자가 급격히 증가하고 있으며, 이에 기반한 전자정부 서비스도 점차 확대될 것으로 전망된다.

요컨대, 이 같은 중요 서비스 환경에서는 필수적으로 공인인증서 기반의 서비스가 구현되고 있으며, 본 고에서는 이러한 공인인증서 이용 현황 및 정책 방향을 소개함으로써 관련 분야의 응용서비스 개발 및 보안대책 수립에 참고할 정보를 제공하고자 한다.

본 고의 구성을 살펴보면, II장에서는 공인인증서 개념 및 현황을 소개한다. III장에서는 공인인증서 기반 모바일 응용서비스 동향을 살펴본 후, IV장에서는 안전성 및 신뢰성 제고를 위한 정책 방향을 소개한다. 마지

* 한국인터넷진흥원 전자인증팀 (kangpy@kisa.or.kr)

막으로 V장에서는 요약 및 향후 전망을 제시한다.

Ⅱ. 공인인증서비스 현황

본 장에서는 공인인증서에 대한 간략한 소개 및 이용 현황을 중심으로 살펴본다.

2.1 개요

1999년에 제정된 전자서명법 [2] 에 근거한 공인인증서는 일종의 사이버 인감증명서(서명용 개인키는 인감에 해당)로써 오프라인에서의 기명 서명과 동일한 법적 효력을 갖는다. 기술적으로는 비대칭키 암·복호화를 지원하는 PKI(Public Key Infrastructure)를 기반으로, 서명자 확인과 서명한 내용에 대한 무결성, 서명 사실에 대한 부인방지를 지원함으로써 사이버 환경에서의 본인 확인 및 결제서비스 등에 폭넓게 적용되고 있다.

2000년 2월에 최초의 공인인증기관(CA)이 지정된 이후, 총 5개의 공인인증기관이 지정·운영되고 있다.

공인인증기관에서 발급하는 공인인증서를 유형별로 정리하면 [표 2]와 같다. 즉, 발급 대상에 따라 개인과 법인으로, 이용 범위에 따라 용도제한용 및 범용으로 구분된다.

2.2 이용 현황

2010년 12월 기준으로 공인인증서는 총 2,371만건이 발급되어 이용되고 있다. 공인인증기관 간에는 중복발

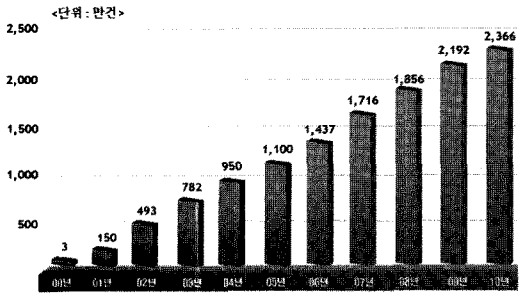
〔표 1〕 공인인증기관 현황

인증기관	지정일	홈페이지
한국정보인증(주)	2000. 2. 10	www.signgate.com
(주)코스콤	2000. 2. 10	www.koscom.co.kr
금융결제원	2000. 4. 12	www.kftc.or.kr
한국전자인증(주)	2001. 11 24	www.crosscert.com
(주)한국무역정보통신	2002. 3. 11	www.ktnet.co.kr

〔표 2〕 공인인증서 유형

구분	발급 건수	개인	법인
범용	279만건	4,400원	110,000원
용도제한용*	2,093만건	무료	별도계약

* 은행·증권·신용카드 등 허용된 용도에만 사용 가능



〔그림 1〕 공인인증서 발급 및 이용 추이

급이 가능한 점을 감안하더라도, 경제활동인구('10.12월 기준 2,453만명)의 96% 이상이 이용하고 있는 등 가장 보편적인 신뢰수단으로 인식되고 있다.

특히, 2002년 9월에 전자금융거래에 적용이 의무화된 이후, 인터넷 뱅킹의 보급과 함께 이용자가 급속하게 증가하였다. 최근에는 전자민원, 연말정산, 주택청약, 전자세금계산서 등 비금융 분야로 확산되고 있다.

한편, 이러한 공인인증서 발급체계를 활용한 부가 서비스로서 서버인증서, 기기인증서, 코드서명 인증서 등을 발급 [3] 하고 있으며, 본 고에서는 사람을 대상으로 한 부분에 중점을 두고 살펴본다.

2.3 스마트폰 환경에서의 이용기반 조성

본 절에서는 스마트폰 환경에서의 공인인증서 이용 기반의 조성을 위한 활동으로 기술규격 개정 및 공인인증서 공용 앱(App) 개발·보급에 대해 살펴본다.

2.3.1 기술규격 개발·보급

스마트폰 환경에서의 공인인증서 이용을 위한 기술규격으로는 '무선단말기에서의 공인인증서 저장 및 이용 기술규격' [4] 이 있으며, 모바일 환경에서 다양한 응용서비스간의 공인인증서 상호연동을 지원하기 위해 2010년 3월에 개정되었다. 주요 내용을 살펴보면, 저장매체별 저장위치 및 저장방식을 [표 3]과 같이 규정하였으며, 안전성 강화를 위해 암호 토큰 인터페이스 표준(PKCS #11)의 준용을 권장하고 있다.

이러한 기술규격을 기반으로, 아이폰과 안드로이드 및 윈도우 모바일 폰, 바다폰 등과 같은 스마트폰은 물론, 피처폰(일반 휴대전화)에서도 공인인증서 기반의 응용서비스를 제공할 수 있게 되었다.

〔표 3〕 저장매체별 공인인증서 저장위치 및 저장방식

저장매체	저장위치 및 저장형식
내장형 메모리	표준 인터페이스 함수(PKCS#11) 아이폰의 경우, 공인인증서 공용 앱(App)
외장형 메모리	드라이브명:\NPKI\인증기관 식별자
USIM (또는 IC칩)	(저장토큰) 별도로 정의한 스마트카드 파일 구성도 및 메모리맵 참조 (보안토큰) 표준 인터페이스 함수(PKCS#11)

현재, 스마트폰 뱅킹 및 증권거래 등 대부분의 은행 및 증권회사에서 본 기술규격을 적용한 공인인증서 기반의 다양한 응용서비스를 제공하고 있다.

2.3.2 공인인증서 이동 서비스 제공

모바일 환경에서의 공인인증서 이용의 일반적인 형태는 PC에 저장된 것을 스마트폰 등으로 복사·이동하여 사용하고 있다.

최상위 인증기관(Root CA)인 한국인터넷진흥원(KISA)에서는 기술규격 [5] 에 따른 실질심사를 통해 PC에 저장된 공인인증서를 스마트폰으로 이동·저장하는 서비스에 대한 안전성을 검증하고 있다.

현재, 일부 공인인증기관에서 스마트폰 상에서 직접 공인인증서를 발급·이용하는 서비스가 구현된 상태이며, 조만간 활성화될 것으로 전망된다.

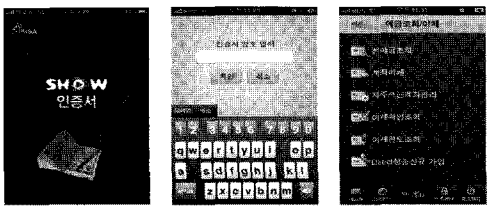
2.3.3 공용 앱 개발·보급

애플 아이폰의 경우, 폐쇄적인 운영체제(OS) 정책으로 인해 응용서비스별로 공인인증서를 보관·이용해야 하는 불편이 있었다. 즉, 응용서비스 수만큼 공인인증서가 요구되는 등 호환성을 제공하지 못한다.

이에 KISA 및 KT 공동으로 공인인증서 호환성 지원을 위한 공용 앱을 개발·보급하여, 아이폰 환경에서의 편리한 이용 기반을 조성하였다. 2010년 5월에 애플 앱스토어에 등록 후, 45만건('10.12월 기준)이 다운로드 되어, 은행 및 증권 등 다양한 응용서비스와 연계되어 사용되는 등 좋은 반응을 보이고 있다.

Ⅲ. 공인인증서 기반 서비스 동향

본 장에서는 모바일 환경에서의 공인인증서 기반 서비스 동향을 소개하기 위해, 가장 대표적인 서비스인 스마트폰 뱅킹서비스와 스마트 전자정부 서비스를 중심으로 살펴본다.



〔그림 2〕 공인인증서 공용 앱(Show 인증서) 실행 예

3.1 스마트폰 뱅킹서비스

2010년 1월, 금융감독원에 의한 스마트폰 보안조치 [6] 에 의해 기존의 PC 환경과 동일한 수준의 보안성 강화를 요구함에 따라 공인인증서 등의 적용이 의무화되었다. 그러나, 스마트폰 환경에서의 공인인증서 의무화는 신속한 신규 서비스 도입 및 정보보호 기술·업체간 공정한 경쟁을 저해한다는 일련의 주장에 따라 국무총리실 주재로 민·관 전문가가 논의한 결과, 공인인증서 외 안전성이 검증된 인증수단의 도입을 허용하는 한편, 30만원 미만의 소액결제는 공인인증서 없이도 바로 적용하기로 했다 [7].

현재, 금융감독원을 중심으로 관련 규정의 개정 [8] 및 세부평가기준 마련을 준비하고 있으며, 2011년 2월에 공개 및 설명회가 개최될 예정이다.

한편, 한국은행 보도자료 [9] 에 따르면, 국내 스마트폰 뱅킹 이용자는 아이폰, 갤럭시S 등 스마트폰 열풍에 힘입어 서비스 도입 1년여 만에 261만명('10.12월)에 이르는 등 급속히 증가하고 있다. 이러한 확산 추세를 고려하면, 점차 PC 기반의 인터넷뱅킹을 상당부분 대체할 것으로 예상된다.

이러한 사례는 공인인증서 도입은 스마트폰 뱅킹서비스 확산에 장애가 되지 않았음은 물론, 보안성 강화에 일조함으로써 서비스 확산에 기여하고 있음을 방증하고 있다. 공인인증서 관련 일련의 논의는 ActiveX로 상징되는 웹 접근성 문제에 기인하며, 실제 스마트폰 환경에서는 이러한 기술적 제약과 무관하게 공인인증서비스가 구현되고 있다.

3.2 스마트 전자정부 서비스

스마트 전자정부 서비스는 크게 일반 국민을 대상으

로 한 대민 행정서비스와 공무원을 대상으로 한 내부 행정서비스로 구분할 수 있다.

3.2.1 대민 행정서비스

일반 국민을 대상으로 하는 대민 행정서비스는 각종 민원 신청 및 상황 조회, 증명서 발급 등을 지원한다. PC 기반의 유선 환경과 동일하게 본인확인 수단으로 공인인증서가 활용될 수 있으며, 아직까지는 기존의 홈페이지를 모바일 환경에서 접속하는 수준의 서비스 지원을 중심으로 진행되고 있다.

진정한 모바일 서비스를 위해서는 각종 신청서류의 작성·신청, 증명서 발급, 고지서 수령·확인 및 즉시 납부 등을 스마트기기를 활용할 수 있어야 하며, 이러한 서비스를 가능하게 하는 것에는 공인인증서가 핵심 역할을 담당할 것으로 예상된다.

3.2.2 내부 행정서비스

내부 행정서비스 분야는 업무 효율의 개선을 위해 접근하고 있다. 즉, 시간 및 공간의 제약을 극복한 업무 수행을 통해 업무 효율의 극대화를 목표로 하며, 메일 및 게시판을 비롯하여 결재 및 현장업무 지원을 통해 가능하다.

아직까지 보안에 대한 우려로 [표 5]와 같이 제한된 서비스를 대상으로 단계적으로 진행되고 있지만, 검증된 보안대책이 마련되면 폭넓게 적용될 수 있을 것으로 전망된다. 유선 환경과 마찬가지로 외부 접속자의 신원확인 및 업무 내용에 대한 무결성·부인방지 등을 보장하기 위해 공인인증서(이 경우엔 행정전자서명용으로 공무원에게 발급된 인증서)가 가장 중요한 역할을 할 것으로 예상된다.

〔표 4〕 주요 모바일 대민서비스 현황

기관	서비스 내용
행정안전부	민원24
지식경제부	에너지다이어트, 지식경제용어사전
문화체육관광부	정책투데이
법무부	법아놀자
재정부	시사경제용어
특허청	특허검색, 재산용어사전, 특허수수료계산 등
코레일	아이 코레일(iKorail)
서울시	서울교통, 상상제안, 위치찾기, i Tour Seoul 등

〔표 5〕 스마트 전자정부 행정서비스 추진계획(안)

단계	대상	추진 서비스
1단계('10년)	행정안전부(시범적용)	간이 메모보고
2단계('11년)	전부처	메일, 전자결재 등
3단계('12년)	경찰, 소방, 복지 등	현장업무 지원서비스*

* 부처별 수요에 따른 선별 적용

Ⅳ. 정책 방향

본 장에서는 모바일 환경에서 공인인증서비스의 안전성 및 신뢰성 제고를 위해 추진되고 있는 암호체계 고도화, 안전한 저장매체 보급, 분실신고센터 운영 등 관련 정책을 소개한다.

4.1 암호체계 고도화

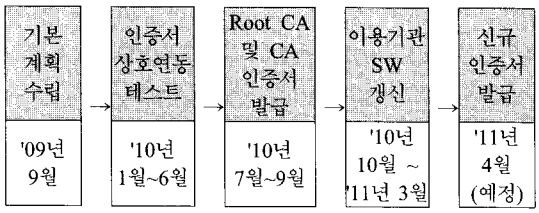
컴퓨팅 기술의 급속한 발달은 기존 암호체계의 안전성을 지속적으로 저하시키는 결과를 초래하고 있다. 국내외 암호전문기관에 의하면, 현행 공인인증서는 2013년 이후엔 안전성을 보장할 수 없으므로 암호체계 고도화를 통한 보안성 강화를 요구하고 있다[10, 11].

이에 행정안전부 및 KISA에서는 2009년부터 기본계획 수립 등 고도화 정책을 추진하고 있으며, 암호체계 고도화 내용은 전자서명키의 길이를 기존 RSA 1,024비트에서 2,048비트로 상향하는 한편, 해쉬 알고리즘도 기존 SHA-1에서 SHA-256으로 교체하는 것이다.

현재, 최상위 인증기관 및 공인인증기관의 발급체계 준비 후, 전자거래업체 등 이용기관의 준비작업이 진행중에 있다. 즉, 이용기관의 서버 단에서는 신규 인증서 식별·검증을 위한 기능을, 사용자 단에서는 인증서 기반의 서명을 위한 기능 모듈 등의 갱신이 필요하다.

〔표 6〕 암호체계 고도화 내용

구분	현행		변경	
	전자서명키	해쉬알고리즘	전자서명키	해쉬알고리즘
Root CA	2,048비트	SHA-1 (160비트)	2,048비트	SHA-256 (256비트)
CA	2,048비트	SHA-1 (160비트)	2,048비트	SHA-256 (256비트)
가입자	1,024비트	SHA-1 (160비트)	2,048비트	SHA-256 (256비트)



〔그림 3〕 공인인증서 이용 앱(Show 인증서) 실행 예

한편, 기존 인증서의 경우엔 유효기간(1년)까지 사용할 수 있으므로, 이용자 측면에서는 아무런 변화를 느끼지 않고 기존의 방식대로 서비스를 이용하게 된다.

공인인증서 암호체계의 고도화 추진경과는 다음의 [그림 3]과 같으며, 2011년 4월부터 신규 및 재발급 인증서를 대상으로 암호체계가 고도화된 신규 인증서가 발급될 예정이다.

한편, 2,048비트 알고리즘을 당장 적용할 수 없는 저사양 모바일 기기의 경우엔 기존의 인증서를 2013년까지 한시적으로 사용하게 된다. 향후 모바일 환경에서의 저사양 기기를 지원하기 위해 타원곡선암호(ECC) 등 경량화된 알고리즘[12] 도입 등을 통해 안정성을 강화한 암호체계를 이용할 수 있는 기반의 조성을 검토할 예정이다.

4.2 안전한 저장매체 보급

공인인증서비스의 안전성을 강화하기 위해서는 무엇보다 전자서명을 위한 개인키 유출을 원천적으로 방지하기 위한 저장매체의 안전성 개선이 요구된다.

유선 환경에서는 일반적으로 이용의 편리성으로 PC 하드디스크(HDD)에 저장하는 경우가 많으며, 최근 안전성 홍보를 통해 USB 등 이동형 저장매체를 이용하는 비율을 높이고 있다. KISA에서는 안전성 강화를 위한 보안토큰 평가·인증을 통해 안전한 저장매체 보급을 지원하고 있다.

스마트폰으로 대표되는 모바일 환경에서의 가장 이상적인 접근은 물리적으로 안전한 저장공간을 확보하는 것이다. 즉, 스마트폰을 분실하더라도 전자서명을 위한 개인키는 물리적으로 외부로 유·노출되지 못하도록 안전성을 강화할 필요가 있다.

이에 KISA에서는 범용가입자식별모듈(USIM)[13]에 공인인증서 탑재 및 이용을 추진하고 있으며, 빠르면 2011년 상반기에 관련 서비스를 이용할 수 있을 것으로 전망된다. USIM은 가입자 인증 및 과금, 보안 기능 등 다양한 서비스를 제공할 수 있도록 개인정보를 담은 스마트카드로서, 전자서명 프로세서를 내장하고 있는 등 기본적으로 공인인증서를 사용할 수 있는 기반을 제공하고 있다. 한편으로는 최근 주목받고 있는 스마트 SD(Secure Digital)카드를 기반으로 공인인증서의 안전한 저장 및 보안 기능의 효과적인 구현을 위한 시도도 추진되고 있다.

이처럼 KISA에서는 이통사 및 제조업체·보안업체와 관련 원천기술 개발·보급을 병행함으로써 안전한 저장공간 및 이용기술 확보를 추진하고 있다.

4.3 분실신고센터 운영

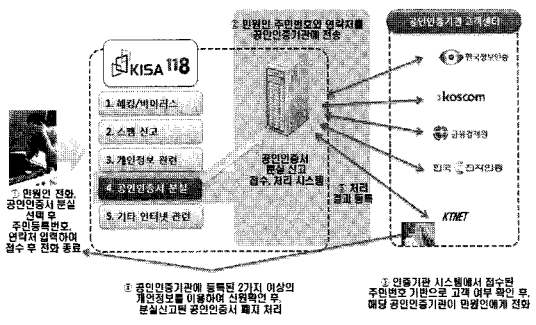
전자서명용 개인키를 PC HDD에 저장하는 경우, 상대적으로 해킹에 취약하므로 보안토큰 등 안전한 이동식 저장매체에 보관 및 이용할 것을 권장하고 있다.

반면에 이동식 저장매체를 이용하는 경우, 분실 위험도 증가하므로 대응책이 필요하다. 일반적으로 공인인증서 이용자는 발급한 인증기관 및 연락처를 모르는 경우가 많고, 특히 주말·야간 등 인증기관의 근무시간 외에는 신고체계가 운영되지 않는 문제점이 있다.

이에 대응하여 KISA에서는 ☎118 콜센터[14]와 연계한 분실신고센터를 2011년 3월부터 운영할 예정이다. 즉, 5개 공인인증기관을 대표해 통합 접수를 통해 24시간 신고체계 운영을 통해 분실로 인한 보안사고를 미연에 방지할 수 있을 것으로 기대된다.

V. 결 론

본 고에서는 스마트폰으로 대표되는 모바일 환경에



〔그림 4〕 공인인증서 분실신고센터 구성도

서의 공인인증서 이용 현황 및 안전성 · 신뢰성 제고를 위한 정책 방향에 대해서 살펴보았다.

최근의 스마트폰 보급 확산과 함께 다양한 응용서비스 이용의 활성화로 정보서비스 패러다임이 유선에서 모바일 환경으로 옮겨가고 있다. 스마트폰 보급 초기엔 공인인증서에 대한 오해 등으로 논란이 있었지만, 사이버 환경에서의 본인확인 및 무결성 · 부인방지 등의 보안성 제공을 위한 수단으로 여전히 폭넓게 활용될 것으로 전망된다. 요컨대, PC로 대표되는 유선 환경에서와 마찬가지로 스마트폰으로 대표되는 모바일 환경에서도 공인인증서는 보편적 신뢰수단으로서의 위상을 유지하는 한편, 지속적인 안전성 · 신뢰성 제고를 위한 접근을 통해 그 위상을 강화할 것으로 예상된다.

본 고에서는 이러한 노력의 일환으로 공인인증서 암호체계 고도화 및 안전한 저장매체 보급, 분실신고센터 운영 등 주요 정책 방향을 소개하였다.

향후 과제로는 편의성 제고를 위한 웹 접근성 개선 및 다양한 신규 모바일 기기로 이용 확대를 위한 인증서 탑재 · 이용기술 등 선제적인 연구개발이 필요하다.

참고문헌

[1] 스마트 모바일 시큐리티 종합계획, 방송통신위, 2010년 12월.

[2] 전자서명법, 법률 제10008호, 2010년 2월.

[3] 웹서버 보안, 코드서명, 보안메일용 인증서 발급 절차 가이드라인, 한국인터넷진흥원, 2011년 1월.

[4] 무선단말기에서의 공인인증서 저장 및 이용 기술규격, 한국인터넷진흥원, 2010년 10월.

[5] 무선단말기와 PC간 공인인증서 전송을 위한 기술규격(v2.0), 한국인터넷진흥원, 2010년 3월.

[6] 스마트폰 전자금융서비스 안전대책, 금융감독원, 2010년 1월.

[7] 전자금융거래 인증방법의 안전성 가이드라인, 국무총리실, 2010년 5월.

[8] 전자금융감독규정 시행세칙, 금융감독원, 2010년 8월.

[9] 2010년중 국내 인터넷뱅킹서비스 이용현황, 한국은행, 2011년 2월.

[10] Elaine Barker, William Barker, William Burr, William Polk, Miles Smid, "Recommendation for Key Management Part 1: General(Revised)", SP 800-57, NIST, March 2007.

[11] Elaine Barker, Allen Roginsky, "Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths", SP 800-131A, NIST, January 2011.

[12] N. Koblitz, "Elliptic curve cryptosystems", *Mathematics of Computation*, Vol.48, pp. 203-209, 1987.

[13] USIM, http://www.3gpp.org/-CT6-Smart-Card-Application-Aspects

[14] http://www.kisa.or.kr/customer/appeal/appeal_main.jsp

〈著者紹介〉

강 필 용 (Pilyong Kang)

비회원

1992년 2월 : 숭실대학교 컴퓨터학부 졸업

1996년 2월 : 숭실대학교 컴퓨터학과 석사

1998년 8월 : 숭실대학교 컴퓨터학과 박사

2001년 9월~2009년 7월 : 한국정보보호진흥원(KISA)

2006년 5월~2006년 11월 : 미국 카네기멜론대학교(CMU) 방문연구원

2009년 7월~현재 : 한국인터넷진흥원(KISA) 팀장

<관심분야> 시스템 및 네트워크 보안, 전자서명 등