情 報 保 護 學 會 誌
第19卷 第6號, 2009. 12

유비쿼터스 환경에 적합한 기기인증체계 구축

이 상 원*, 김 정 희*, 황 보 성*, 전 길 수*

요 약

유비쿼터스 환경으로 네트워크 환경이 진화함에 따라 다양한 기기가 정보제공의 주체로 등장하고, 이에 따른 정보보호의 중요성이 증대되고 네트워크에 참여하는 기기에 대한 신뢰된 인증체계의 필요성이 요구되고 있다. 현행 사람 중심의 공인인증체계의 안전·신뢰성에 준하는 기기인증을 위해 추진되고 있는 기기인증체계 구축현황을 소개한다.

Ⅰ. 서 론

네트워크 환경이 유비쿼터스 환경으로 진화함에 따라, 사람뿐만 아니라 홈디바이스, 지능형 로봇, 휴대단말기 등 다양한 기기가 정보제공 주체로 등장하고 이러한 추세는 지속적으로 확대될 것으로 예상된다. 기기의 이용 증대와 더불어 기기에 대한 정보보호 중요성이 증대 및 이에 따른 네트워크에 참여하는 기기에 대한 신뢰된 인증체계의 필요성 또한 요구되고 있다

하지만, 현행 사람 중심의 공인인증체계는 u-City, u-Health 등에 참여하는 다양한 기기를 식별하고 인증하는데 어려움이 있다. 기기에 대한 진위성 확인 및 인증이 이루어지지 않아 비인가된 기기를 통해 서비스가 제공될 경우, 유비쿼터스 서비스의 신뢰성에 직접적인 위협 및 다양한 피해를 유발할 수 있다. 이러한 위협 및 피해에 대응하고 네트워크에 접속하는 기기의 진위성 및 네트워크 접속 권한을 확인하기 위해 기기인증서의 이용이 요구되고 있으며, 실제 케이블TV 셋탑박스, 휴대단말기 등에 기기인증서를 이용하는 사례가 점진적으로 증가하고 있는 추세이다.

국내의 경우, 1999년 전자서명법 제정을 통해 공인인증체계를 구축하고 그 이용자 수도 2천만 명에 달하고 있다. 하지만, 공인인증서는 발급대상을 사람 및 법인으로 한정하고 이에 대한 신뢰된 인증체계만을 구축함에 따라 기기에 대한 인증체계 및 절차는 미흡한 사항이다. u-City 등의 국가정보화 사업 등을 통해 다양한 기기가 도입되고 비인가된 기기에 대한 인증문제가 대두되면서 국내에서도 기기에 대한 인증의 필요성이 증가하고 있다.

이에 본고에서는 기존 공인인증체계의 안전·신뢰성에 준하는 기기인증체계 구축을 위해 u-City 사업을 대상으로 추진되었던 기기인증 시범사업과 현재 진행되고 있는 기기인증 체계 구축현황을 소개한다.

Ⅱ. 기기인증 이용현황

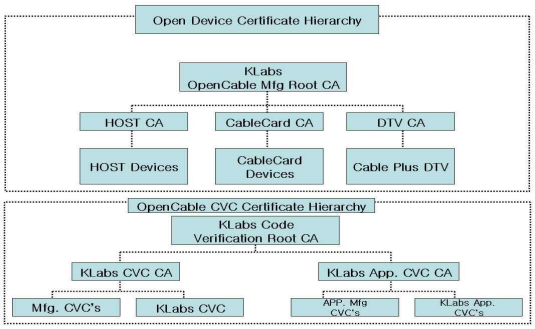
네트워크 연결기기에 대한 진위확인 및 데이터의 암호화 등을 위해 도입되고 있는 기기인증의 국내외 이용현황을 소개하고, 기기인증서와 관련한 기술표준 및 이용기술을 검토함으로써 기기인증체계의 구축배경을 살펴본다.

2.1. 기기인증 이용현황

방송사업자는 방송서비스 전송 시 셋톱박스가 복제되지 않은 정당한 기기인지를 확인할 필요가 있는데, 현재 셋톱박스의 기기인증은 케이블카드 간의 통신 시 각 개체의 불법복제 방지를 위한 인증으로 업계표준인 OpenCable의 규격에 기반하고 있다. 현재 한국디지털케이블연구원(KLabs)이 국내 케이블사업 분야의 최상위 인증기관으로서 미국의 CableLabs와 업무협력을 통

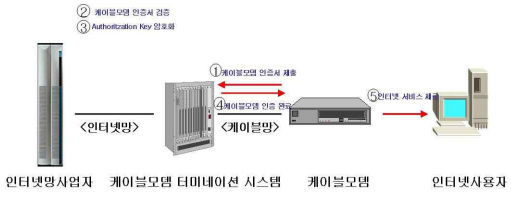
* 한국인터넷진흥원 전자인증팀 ({swlee, kimjh, hbs2593, kschun}@kisa.or.kr)

해 PKI 기기인증서를 발급하며, 공인인증기관 한국정보인증은 KLabs의 위탁인증기관으로서 디지털 케이블 셋톱박스와 이에 플러그인(plug-in) 되는 케이블카드의 기기인증을 위한 PKI 인증서를 발급하고 있다.



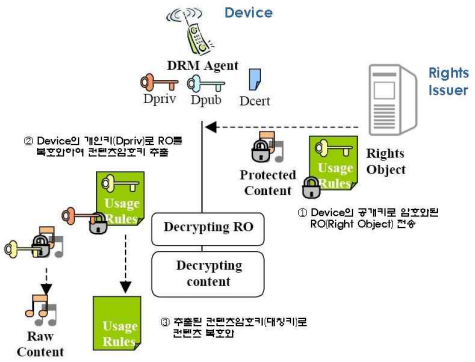
[그림 1] 국내 셋톱박스 인증체계

유선방송망에서 인터넷망을 운용하는 사업자들은 사용자들에게 인터넷서비스 제공 시 케이블모뎀이 복제되지 않은 정당한 기기인지에 대한 확인이 필요하다. 미국의 경우, VeriSign사가 케이블모뎀과 케이블모뎀 터미네이션 시스템 간 기기인증을 위해 PKI인증서를 발급하고, 케이블모뎀 터미네이션 시스템은 케이블모뎀이 제출한 케이블모뎀 PKI인증서를 검증하여 케이블모뎀이 정당한 기기인지를 확인하는 모델이 서비스 중이다. 케이블모뎀 인증을 위한 PKI인증서 프로파일 및 관련된 규격은 케이블모뎀 업계표준인 Data Over Cable Service Interface Specification(DOCSIS)에서 정의하고 있으며, 케이블모뎀 PKI 인증서는 케이블모뎀 내 비휘발성 메모리 내 보안영역에 저장되고 이용되어진다. DOCSIS 기반의 케이블 모뎀 PKI 인증서는 중앙집중식과 분산식 모델을 통해 발급·관리 될 수 있다.



[그림 2] 케이블모뎀 인증절차

CMLA(Content Management Licensing Administrator)는 Intel, Nokia, MEI/Panasonic, Samsung 4개의 회사가 모여서 만든 무한책임회사(LLC)로서, 저작권발급자(Right Issuer)로부터 모바일기기까지 안전한 방법으로 콘텐츠를 배포하기 위한 OMA(Open Mobile Alliance) DRM 2.0 규격의 신뢰모델이다. OMA DRM 2.0에서는 PKI기반으로 Right Issuer와 Device간에 Content 보호를 위한 end-to-end protocol을 정의하고 있으며, CMLA는 이를 지원하기 위해 인증(Certification)체계 인증서 및 CRL 발급에 대한 규격을 정의하고 있다. 이동통신사업자는 암호화된 컨텐츠와 컨텐츠암호키를 휴대폰의 공개키로 암호화하여 전송한다. CMLA 인증서를 탑재한 정당한 휴대폰(신원확인)은 이동통신사업자가 송신한 메시지를 복호화하여 컨텐츠암호키를 추출하게 된다. 마지막으로 휴대폰은 컨텐츠암호키를 이용하여 컨텐츠 복호화 후 컨텐츠를 이용할 수 있게 된다.



[그림 3] CMLA의 PKI 기기인증서 이용절차

WiMAX는 WiMAX를 지원하는 단말기(노트북, 휴대폰 등 휴대용 기기)에 기기인증서비스를 제공하여 정당한 기기 여부 확인 및 암호화 통신을 지원하며, 현재 VeriSign사에서 WiMAX 장비에 대한 기기인증서를 발급 중이다. WiMAX에서는 여기에 접속하기 위한 단말기가 정당한 기기인지 확인이 필요하며, 이때 WiMAX 관련 단말기 제조사는 WiMAX 포럼으로부터 기기 형식승인을 획득한 후, VeriSign사로부터 기기인증서를 발급받게 된다. 제조사는 WiMAX 단말기 제조 시 VeriSign사로부터 발급받은 기기인증서를 기기에 탑재하여 단말기를 출시한다. WiMAX 단말기가 WiMAX 서비스에 접근 시, WiMAX 서비스에 접근 가능한 기기인지 여부를 상호 확인하고, 이를 기반으로 암호화통신

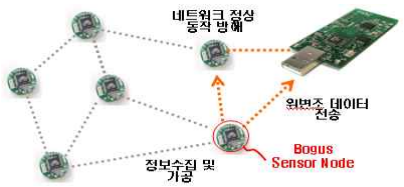
을 수행한다.

[그림 4] WiMAX 인증서비스

2.2. 기기인증체계 구축 필요성

전자정부서비스가 고도화되고 유비쿼터스 네트워크 기술의 발전됨에 따라 인증을 필요로 하는 대상이 사람과 사람에서 기기와 기기, 기기와 사람으로 확대되었다. 이러한 기기들 간의 인증 등이 안전하고 신뢰성 있게 이루어지기 위해 보안성이 강화된 기기인증체계의 구축 및 적용방안의 마련이 필요하게 되었다.

유비쿼터스 환경은 사람뿐만 아니라 홈디바이스, 지능형 로봇, RFID 등 기기와 사물이 네트워크를 통해 모두 연결되며, 이에 따라 컴퓨팅 공간과 물리적 공간간에 끊김없는 서비스 제공을 위해 기기간 신뢰된 인증기술이 핵심요소이며 서비스 활성화를 위해 해결해야할 필요가 있다. 기존의 공인전자서명 인증체계는 사람을 대상으로 하고 있어 기기에 대한 신뢰된 인증기반이 미흡하였다. 기기에 대한 인증이 이루어지지 않아 비인가된 기기를 통해 서비스가 제공될 경우, u-health 등에서 인간 생명에 치명적인 위협을 초래할 수도 있다. 기기의 진위성 인증에 대한 기술 및 인식 부재로 u-City, u-Health 등 u-IT 서비스에서 기기에 대한 인증이 부족한 것이 지금의 현실이다.



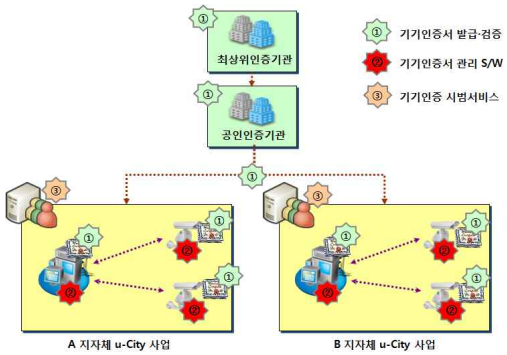
[그림 5] 가짜 센서를 이용한 공격

따라서 전자정부서비스, u-City, u-Health 등 정보화 사업 등에 도입되는 기기의 안전한 이용기반 마련을 위해 기기인증체계의 구축이 필요하다. 네트워크에 참여하는 다양한 기기를 식별하고 진위를 판단할 수 있는 신뢰된 기기인증체계를 구축하고, 향후 유비쿼터스 서비스에 이용될 다양한 기기에 대한 기기인증서비스 제공을 위한 기반 마련이 필요하다.

Ⅲ. 기기인증 시범사업

앞에서 살펴본 바와 같이 네트워크에 연결되는 기기에 대한 정보보호 수준 제고를 위해 신뢰된 기기인증체계 구축의 필요성이 증대되었다. 이에, 신뢰된 국가 기기인증체계 구축을 위한 요구사항 도출 등을 위해 기기인증 시범사업을 추진하게 되었다. 기기인증 시범사업은 국가정보화 사업에 도입된 기기의 안전성 문제 지적에 따라 네트워크 카메라를 대상기기로 선정하고 기기인증서 적용을 추진하였다.

3.1. 기기인증 시범사업 개요



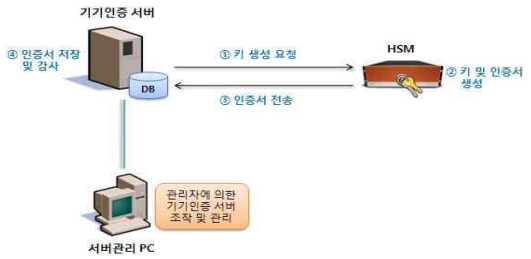
[그림 6] 기기인증 시범사업 추진범위

u-City 구축사업을 통해 다양한 기기들이 도입되고 있으나, 인가되지 않은 기기로 인한 문제점이 존재하였다. 이러한 지적에 따라 u-City 사업을 대상으로 기기에 대한 상호인증 등을 수행하도록 하는 기기인증 시범사업을 시행하게 되었다.

기기인증 시범사업은 u-City 사업에 도입되는 네트워크 카메라를 대상으로 기기인증 시험발급 체계를 구축하는 것으로, 기기인증서 시험발급 및 검증시스템의 구축과 기기인증서 처리 소프트웨어의 개발, 기기인증서의 적용 및 테스트, 기기인증 요구사항 도출 등을 수행하였다.

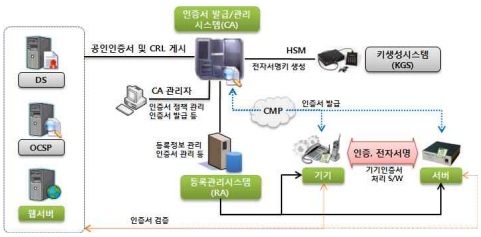
3.2. 기기인증 시범사업 구축

기기인증서 시범서비스 지원을 위해 기기인증서 시험발급 시스템을 구축을 진행하였다. 최상위인증기관과 공인인증기관의 기기인증서 시험발급 및 검증시스템을 기존의 인증시스템과는 별도로 추가 구축하고 네트워크 카메라에 탑재될 기기인증서를 발급할 수 있는 체계를 갖추었다.



[그림 7] 최상위인증기관 기기인증서 시험발급 시스템

공인인증기관은 기존 인증시스템의 전자서명 및 해쉬 알고리즘의 개선 및 기기인증서 대량발급 기능, 웹을 통한 기기인증서 공고기능 등을 추가 개발하여 기기인증 시험시스템을 구축하였다. 인증기관은 네트워크 카메라 제조사로부터 기기정보를 받아 기기인증서를 발급하고 발급된 기기인증서와 비밀키를 기기인증서 처리 소프트웨어와 함께 기기내에 적용하였다.



[그림 8] 공인인증기관 기기인증시스템 구성도

기기인증서 시범사업 내에서 기기인증서의 관리, 전자서명의 생성 및 검증, 응용서버와의 상호인증 등을 수행하는 소프트웨어인 기기인증서 처리 소프트웨어를 직접 구현함으로써 기기에서의 기기인증서 처리능력과 소프트웨어 구현 범위 등의 요구사항을 도출할 수 있었다.

구분	PC	기기
프로세서	Intel, AMD 등 범용 프로세서	ARM, MPIS 등 임베디드 프로세서
운영체제	윈도우 계열	Embedded Linux 등 임베디드 운영체제
실행파일 크기	2 ~ 6MB	700 KB
개발도구	MFC, C/C++ 범용 컴파일러	Cross Compiler - ARM Linux Compiler 등 전용 컴파일러

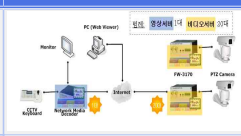
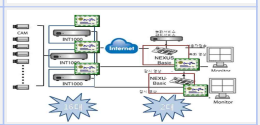
[그림 9] 기기인증서 처리 소프트웨어 비교

3.3. 기기인증서 시범적용

기기인증서 시범사업을 통해 u-City 사업을 수행하고 있는 3개 지방자치단체에 대해 기기인증서를 발급하고 기기인증서 처리 소프트웨어를 탑재하여 기기인증서비스를 적용하였다.

기기인증서의 발급 및 전자서명의 생성·검증 등을 수행하여 기기의 성능에 따른 기기인증서 처리 소프트웨어의 처리능력을 테스트하였다. 기기인증서가 각각 탑재된 네트워크 카메라와 응용서버를 대상으로 기기인증서 기반의 상호인증을 적용하였으며, 실제 필드의 네트워크 카메라 기기에 기기인증서를 적용하여 필드 테스트를 진행하였다.

[표 1] 기기인증서 적용 현황

사업 및 관련기관	시스템 구성	사업 수행내용
"u-방범서비스" (충남 연기군)		- 기기인증 랩 테스트 - 기기인증서 발급·탑재 - 기기인증 필드 적용
"u-Safety 통합시스템" (인천광역시)		
"u-2011 육상로드조성" (대구광역시)		

3.4. 기기인증 요구사항 및 대응방향

기기인증서 발급시스템을 갖추고 기기인증서 처리 소프트웨어를 통해 기기인증서를 시범적용해 본 결과

제도적, 기술적, 운영적인 면에서 기기인증에 대한 다양한 요구사항이 도출되었다.

우선 기기인증에 대한 제도적 요구사항으로 기기인증서비스에 대한 법적인 요구사항을 마련하여 기기인증서 발급절차에 대한 신뢰성을 확보하고, 기기인증기관의 관리 및 감독 체계를 마련하는 것이 필요하다는 것이다.

두 번째 기술적 요구사항으로 기기인증서의 유효기간, DN 명, 전자서명 및 해쉬 알고리즘과 이용용도, 기기인증서의 발급 및 탑재 기술과 안전한 저장방식에 대한 연구가 필요하다. 장기간 사용되는 기기의 특성에 따라 장기간의 안전성을 가지는 전자서명 알고리즘의 사용이 권고되며, 기기의 고유정보를 포함하도록 DN를 구성할 수 있어야 한다. 또한 다량으로 발급되는 기기인증서의 탑재관련 기술, 기기인증서와 비밀키의 안전한 저장 기술, 기기인증서의 검증과 관리 절차마련 등 기기인증서에 수반되는 다양한 기술의 개발이 요구되어진다.

마지막으로 운영적인 요구사항으로 기존의 공인인증체계와는 분리된 별도의 기기인증체계의 구축이 필요하며, 기기인증시스템 및 소프트웨어에 대한 안전성 점검 등이 요구된다. 기기인증서비스를 위한 별도의 심사와 점검을 통해 안전성을 확보하여야 한다.

Ⅳ. 기기인증체계 구축현황

기기인증서 시범서비스를 통해 도출된 요구사항 및 대응방향을 바탕으로 현재 기기인증서비스의 안전성 제고를 위한 기기인증체계 구축을 추진하고 있다. 기기인증체계 구축은 최상위인증기관 기기인증시스템의 구축, 기기인증서비스 안전성 확보방안 마련, 기기인증서비스 이용확대 방안 수립으로 나누어 추진하고 있다.

4.1. 최상위인증시스템 구축

최상위인증기관 기기인증시스템 구축 주요내용으로는 기기인증서 발급 및 검증서비스 제공을 위한 장비의 도입과 기기인증서 발급에 따른 인증 소프트웨어의 기능 개선을 추진한다. 기존의 인증시스템과는 별도의 시스템으로 구축되며 기기인증서 발급을 위해 필요한 전자서명키 생성 및 보호를 위한 장비 또한 별도로 도입된다.

4.2. 기기인증서비스 안전성 확보방안 마련

기기인증기관의 기기인증관련 시스템, 기기에 탑재되는 기기인증서 처리 소프트웨어, 제조업체 등의 기기인증서 주입 소프트웨어 등에 대한 구현 및 운영에 대한 가이드라인을 개발을 진행하고 있다. 기기인증 구현 가이드라인의 경우 인증기관 인증시스템, 기기인증서 처리 소프트웨어, 주입소프트웨어 등이 갖추어야 할 기능을 나열하고 이를 구현하기 위해 필요한 사항을 기술하게 될 것이다. 또한 운영 가이드라인은 기기인증기관의 시설 및 장비에 대한 기준을 언급하고 이에 대한 운영에 관한 사항을 기술하게 된다.

기기에 탑재되는 기기인증서를 이용하고 관리하기 위해 마찬가지로 기기에 탑재되는 기기인증서 처리 소프트웨어의 안전성 및 신뢰성을 검증할 필요가 있으며 이를 위해 기기인증서 처리 소프트웨어 구현적합성 평가도구 개발을 추진하고 있다. 구현적합성 평가도구는 기기인증서 처리 소프트웨어에서 필요로 하는 암호알고리즘의 적합한 구현 및 기기인증서의 이용·관리기능 등을 평가할 수 있는 소프트웨어이다.

기기에서 일반적으로 기기인증서와 비밀키는 메모리에 저장되게 되어 기기의 운영체제의 취약성으로 인한 문제발생시 기기인증서와 비밀키가 외부로 유출되는 사고가 발생할 수 있다. 이를 방지하기 위해 기기인증서 유출방지 보호기술 연구를 진행하고 있다. 기기인증서비스 이용환경에서의 기기인증서 및 비밀키의 저장방식을 조사하고 분석하고, 유출방지를 위한 보호기술의 개발현황을 조사하여 기기인증서와 비밀키의 암호화 및 유출방지 등의 보호기술 적용방안을 제시하고자 한다.

4.3. 기기인증서 이용확대 방안 수립

미래에 도입되어 사용하게 될 신규 IT기기에 대해 기기인증서를 적용할 수 있는 방안을 연구하기 위해 국내외 기기인증서비스가 도입되어 운영되고 있는 현황을 조사하고 이를 통해 기기인증서비스의 도입전망을 예측하고자 한다. 또한 기존의 u-City, u-health 등의 국가정보화 사업을 통해 도입되었던 기기 현황을 분석하고 도입추세에 대한 분석을 병행하고 있다.

기기인증서비스가 도입된 기기와 기기인증서비스가 적용되지 않은 신규 기기에 대한 도입 추세분석과 함께

기기인증 관점에서 기기에 대해 위협분석을 실시하고 이를 통해 요구사항을 도출함으로써, 다양한 기기에 적용할 수 있는 기기인증서비스 모델과 기준을 마련할 수 있을 것이다. 또한 기기인증서비스에 대한 법 개선방향을 수립하고 개선안을 마련하고 있다.

기기인증서의 이용을 확대하기 위한 방안 중 하나로 경량화된 기기인증서 상태확인 방안을 연구한다. 기존의 CRL과 OCSP는 비실시간성, 통신 트래픽 부하 등의 문제점을 안고 있다. 기기인증서의 상태확인에 있어서 이러한 문제점을 해결하여 보안성과 성능을 보장할 수 있는 방안 마련을 진행하고 있다. 두 번째로, 기기인증의 환경과 특성 상 사용자의 개입없이 기기인증서가 갱신 또는 재발급될 필요가 있다. 이를 위해 네트워크 기기환경을 감안하여 기존에 설치된 기기인증서를 자동갱신 및 재발급할 수 있는 방안을 연구하고 있다. 마지막으로 폐쇄망 및 열악한 네트워크 환경을 고려하여 기기인증서를 검증할 수 있도록 기기인증서 검증 Agent 기술 연구를 진행하고 있다. CRL 및 OCSP 등의 접속이 불가능한 폐쇄된 내부망에서 기기가 이용될 때 기기인증서의 유효성을 검증하기 위해 검증대행 기술의 연구가 진행 중이다.

Ⅴ. 결 론

유비쿼터스 서비스 환경에서 다양한 환경과 기기를 통해 이루어지는 서비스가 증가하고 확대됨에 따라 기기간의 인증이 중요한 문제로 이슈화되었다. 기기에 대한 진위성 확인과 인증이 이루어지지 않는 경우 치명적 위협을 초래할 수 있으며, 유비쿼터스 환경의 끊김없는 서비스 제공을 위해 기기간의 인증은 반드시 필요하다. 기기인증이란 네트워크 환경에 접속 가능한 다양한 유무선기기에 대한 인증을 의미하며, 유비쿼터스 환경에서는 모든 기기들의 협력에 의해 실제 통신이 이루어지므로 정상적인 통신을 위해서는 기기의 진위를 확인하는 인증이 중요한 문제가 된다.

기기인증 시범사업을 통해 u-City에 적용되는 네트워크 카메라에 대해 기기인증서를 발급하고 적용함으로써 기기인증에 대한 다양한 요구사항을 도출할 수 있었다. 도출된 기기인증 요구사항과 이를 분석한 대응방향을 바탕으로 본격적인 기기인증체계 구축이 진행 중에 있다. 기기인증체계 구축사업을 통해 최상위인증기관 기기인증시스템이 구축되고, 기기인증서의 안전성 확보를 위한 기기인증 관련 가이드라인 개발 및 기기인증서 처리 소프트웨어 구현적합성 평가도구 개발, 기기인증서 및 비밀키의 유출방지 기술 연구가 진행된다. 또한 기기인증서 이용확대를 위해 기기인증서 상태검증의 경량화 방안, 기기인증서의 자동갱신 및 재발급 방안 연구, 제한된 네트워크 환경에서의 기기인증서 검증방안 연구를 진행하고 있다.

기기인증서 관련 기술의 개발과 기기인증 제도화 추진 등을 통해 신뢰된 기기인증서 이용기반이 구축되면, 기기간의 진위성 확인 및 상호간의 인증이 보다 안전하게 이루어질 것으로 전망된다.

참고문헌

[1] “기기인증 시범서비스 결과보고서”, 한국정보보호진흥원, 6. 2009.
[2] “기기인증서비스의 안전성 제고를 위한 기기인증체계 구축” 제안서, 행정안전부, 3. 2009.
[3] “유비쿼터스 환경에서의 기기인증을 위한 기술 연구”, 한국정보보호진흥원, 11. 2008.
[4] http://www.klabs.re.kr, 한국디지털케이블연구원
[5] http://docsis.org, DOCSIS : Data Over Cable Service Interface Specifications
[6] http://www.cm-la.com /, Content Management License Administrator
[7] http://www.wimaxforum.org/, WiMAX Forum

<著 者 紹 介>

이 상 원 (Sang-Won Lee)

2004년 2월 : 한국정보통신대학원 대학교 석사
2004년 4월~2006년 5월 : (주)하이닉스반도체 사원
2006년 6월~현재 : 한국인터넷진흥원 주임연구원
<관심분야>정보보호, PKI

김 정 희 (Jung-Hee, Kim)

정회원

1997년 2월 : 중앙대학교 산업정보학과 졸업
1999년 2월 : 중앙대학교 산업정보학과 석사
1999년 1월~8월 : 한국정보보호센터 연구원
1999년 9월 ~ 2001년 8월: (주)쌍용정보통신 사원
2001년 9월~현재 : 한국인터넷진흥원 선임연구원
관심분야 : PKI, RFID 정보보호, 시스템개발방법론

황 보 성 (Bo-Sung Hwang)

2001년 2월 : 순천향대학교 전산학과 석사
2001년 1월~현재 : 한국인터넷진흥원 선임연구원
관심분야 : 정보보호, PKI

전 길 수 (Kilsoo Chun)

종신회원

1991년 2월 : 서강대학교 수학과 이학사
1993년 2월 : 서강대학교 수학과 이학석사
1998년 2월 : 서강대학교 수학과 이학박사
1998년 10월~1999년 9월 : 서강대학교 기초과학연구소 박사후 연구원
2001년 3월~2001년 6월 : 서강대학교 컴퓨터학과 연구교수
2001년 7월~현재 : 한국인터넷진흥원 팀장
<관심분야> 암호학, PKI, ID관리