情 報 保 護 學 會 誌
第 14 卷 第 6 號, 2004. 12

안전한 RFID/USN 환경을 실현하기 위한 디지털 통합인증서비스

윤 재 호*, 박 배 효*, 주 학 수*, 권 현 조*, 전 길 수*

요 약

RFID/USN 환경에서 정보보호의 취약성에 대응하기 위해서는 정보를 관리하는 데이터 서버에 접근하는 개체에 대한 인증뿐만 아니라 정당한 RFID 리더와 USN 노드임을 인증할 수 있어야 하는 등 전반적인 디지털 인증체계로의 기술 및 개념 변화가 병행되어야 한다. 즉, RFID/USN 환경에서는 정보화의 주체가 사람에서 사물 및 기기(이하 사물/기기)로까지 확대됨으로 인해서 정보를 다루는 주체의 정당성을 확인하는 인증 수단도 사람에서 사물/기기로 확대된다. 따라서 사물/기기 인증을 포함할 수 있도록 기존의 유무선 PKI 인증체계를 확장하고, 그 위에 실명보호 인증, 디지털 권한관리를 위한 속성인증, 그리고 디지털 문서의 증거 효력을 위한 관리 방법 등을 포함하는 디지털 통합인증서비스가 필요한 시점이다.

Ⅰ. 서 론

기존의 공인인증체계는 사람을 대상으로 전자서명 및 부인방지 서비스를 제공하는 것이 목적이었으므로, RFID/USN환경에서 대상이 되는 사물/기기에 대한 인증체계로 적용할 수는 없다. 사물/기기들에 대한 인증체계를 마련하기 위해서는 인증서 프로파일 및 검증체계의 변경 등 기존의 공인인증체계 전반에 걸친 변경이 이루어져야 하며 관련 규격개발 및 표준화, 인증기관 운영기술 개발 등이 마련되어야 한다. 공인인증체계의 인증기술을 이용하여, 개체가 RFID/USN 네트워크에 구축된 EPC-IS (Information Service)등과 같은 정보검색 서버 및 정보저장서버에 접근하기 위해서는 기존 공인인증체계와 XML 기반의 RFID/USN 인증체계의 연동도 필요한 시점이다. 현재 공인인증체계의 인증서는 사용자 신원확인 서비스를 제공할 수 있으나, 사용자의 익명성 보장/제어 기능을 제공하지는 못하며, 통신내역증명 및 증거보존 서비스, 사용자 권한관리를 위한 권한 인증서비스를 제공하지 못하는 등 그 한계가 있기 때문에 디지털 통합인증서비스는 그 필요성이 더욱 부각되고 있다.

또한 유비쿼터스 환경에서 센서, 정보 가전 등의 디바이스가 네트워크 접점으로 새로이 등장함에 따라 공격대상이 증가하고 예상치 못한 공격유형이 발생할 가능성 증대되고 있으며, 디바이스에 대한 공격의 영향이 네트워크로 확대될 가능성이 있으므로 네트워크 접점으로서의 다양한 디바이스에 대한 안전성 제고가 필요하다.

Any where, Any time, Any service를 위해 다양한 센서, 정보가전 등이 전자태그 등으로부터 수집하여 전송하는 정보량이 증가하게 되는데, 초소형 센서 등 디바이스는 저전력, 낮은 계산능력, 작은 메모리 등 하드웨어적인 제약으로 보안강도가 낮은 기술이 탑재되므로 정보 전송시 외부공격으로부터 기밀성을 보장할 수 없다. 따라서 유비쿼터스 환경에 적합한 위·변조 및 유출 방지 기술 확보가 필요하며 정보유통의 안전성과 신뢰성을 확보하기 위한 법·제도의 정비도 필요하다. 또한, 센싱 및 무선통신을 통한 일시적이고 잦은 연결이 많은 유비쿼터스 네트워크 환경은 응용서비스 연속성을 저해할 우려가 있기 때문에 유비쿼터스 네트워크 환경에서 응용서비스 이용자의 안전성과 편리성을 동시에 만족시키고 서비스의 연속성을 보장할 수 있는 체계 구축도 필요하다.

본 고에서는 상기에 서술된 RFID/USN 환경에서 정보보호 필요성과 위협요인에 대처하기 위한 방안으로 관련 국외동향과 디지털 통합인증서비스에 대해 다루고자 한다.

* 한국정보보호진흥원({jhyoon, parkbh, hsju, hckwon, kschun}@kisa.or.kr)

Ⅱ. 국외동향

1. 미국

미국은 9.11테러를 계기로 본토안보부(Department of Homeland Security)를 신설하고(2003. 3월), 부내에 IAIP(Information Analysis and Infrastructure Protection)에서 정보보호업무 담당하고 있다. IAIP의 임무는 주요기반시설에 대한 취약점평가 및 보호계획의 수립, 사이버공격의 분석·경고·대응, 긴급복구에 대한 기술지원, 정보보호 연구개발 촉진과 자금지원 등 사이버공간 정보보호를 위한 국가전략(National Strategy to Secure Cyberspace)을 발표하고 국가차원의 정보보호 추진체계 정비를 수행하고 있다[1].

본토안보부(DHS)는 유비쿼터스 첨단기술을 8개 분야로 나누어 개발하고 있으며 첨단 보안기술관련 프로젝트는 ATO(Advanced Technology Office) 등에서 나누어 진행 중에 있다. ATO(Advanced Technology Office)에서는 특수 서명 감지(Unique Signature Detection)[1] 등의 프로젝트가 진행 중이다.

이외, 차세대 보안기술 개발을 위해 대학 및 민간 연구기관의 다양한 프로젝트가 현재 진행 중에 있다. 펜실베니아 대학에서는 유비쿼터스 네트워크 환경에서의 이동통신 보안환경 구축 프로젝트 추진 2001년 5월에 시작한 5년간의 프로젝트 MUSE를 수행 중에 있으며, 암호전문회사인 NTRU社는 전자태그(RFID)와 비접촉형 스마트카드 등과 같은 제한된 컴퓨팅 환경에서 동작하는 초경량 암호기술을 탑재한 GenuID 제품을 개발하였다.

1.1 암호인증기술관련 동향

미국은 'E-Authentication 프로젝트' 추진을 통해 사용자 인증 신뢰등급에 적합한 시스템의 안전기준을 마련하고 이에 따라 사용자 인증시스템의 구현기술 지침을 마련 중이며, SUN사, HP사 등을 중심으로 서로 다른 서비스에 등록한 별도의 Identity를 체인으로 연결함으로써 다른 Identity를 가지고 있더라도 통합인증을 수행할 수 있는 Federated Identity 솔루션을 개발 중이다. 또한, 미국 BBN 연구소는 2002년 9월부터 2004년 9월까지 DARPA IXO NEST 프로그램으로부터 예산을 지원받아 "TinyPK" 프로젝트를 추진하였다. TinyPK란 원 프로젝트 명 "Lightweight Security for Wireless Networks of Embedded Systems"을 대신하여 사용되고 있으며 Tiny Public key를 의미한다. 프로젝트의 주요목표는 버클리대에서 개발한 센서플랫폼 MICA Motes에 RSA기반의 경량화된 개체 인증 및 키교환 방식을 개발하는 것으로, 저전력 센서 디바이스의 무선 네트워크용 보안 서비스를 목적으로 하고 있다.

VeriSign사는 공급망을 위한 EPC[2] Network 서비스를 도입하여 EPC Network를 위한 Root ONS 서비스(Local ONS, EPC Information Service, EPC Discovery Service, EPC Trust Service)를 포함하여 EPC Application Developers Program운영으로 EPC Network와 연동을 위해 필요한 기술 정보를 제공하고 있다. 또한, EPC Starter Service를 통해 EPC Network 사용자에게 추가개발 없이 EPC Network를 사용할 수 있도록 하는 서비스를 제공하고 있다. VeriSign은 EPC 관련 정책에 영향력은 없으며 단지 EPCglobal의 정책에 따라 EPC Network 운영하고 있으나, 기존의 X.509 인증서를 이용한 PKI기반 보안네트워크를 이용하여 EPC 네트워크의 Trust 서비스를 제공하고 있다[1].

2. 유럽

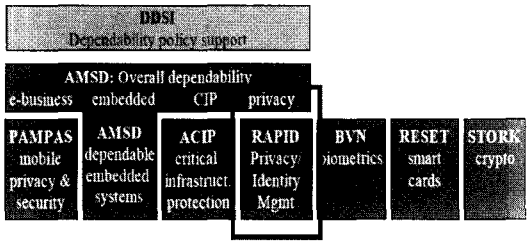
유럽은 정보보호 구심점 역할을 담당할 '유럽 네트워크 및 정보보호 기구(ENISA : European Network and Information Security Agency)'를 유럽공동체내에서 네트워크 및 정보보호 강화를 위해 2004년 3월에 설립하였으며, 2008년까지 5년간 24백만 유로를 예산으로 책정하고 있다. 이 기구는 회원국과 협력을 통한 네트워크 및 정보보호 강화로 인터넷 이용 활성화에 기여하며, 네트워크와 정보보호 관련문제의 해결을 위한 중심적인 역할을 수행한다.

2.1 암호인증기술관련 동향

유럽은 유비쿼터스 컴퓨팅 및 네트워크 환경의 도래에 따른 유럽차원의 종합적이고 체계적인 로드맵을 수립하고 있다. "eEurope 2005 실행계획"에서 정보신뢰(Dependability) 구축의 필요성을 제시함에 따라 미래 정보화 사

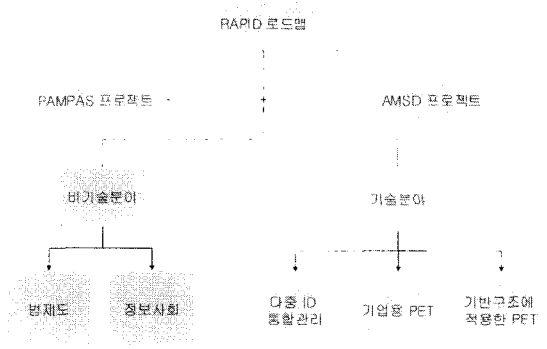
1) 아군과 적군의 전투 장비 또는 무기 등을 구별하여 선택적으로 공격할 수 있도록 이들의 장비 또는 무기를 식별할 수 있는 기술인 "유비쿼터스 signature의 유무를 판별하는 기술

2) EPCglobal은 EAN(European Article Number) International과 UCC(Uniform Code Council)가 공동으로 설립한 비영리 표준 기구. EPC Network의 표준 개발 및 운영감독을 하며 전세계 EPC 번호 등록 서비스를 담당



〔정보신뢰 로드맵〕

※ PAMPAS : Pioneering Advanced Mobile Privacy And Security
RAPID : Roadmap for Advanced Research in Privacy and Identity Management
STORK : Strategic roadmap for crypto



〔RAPID 로드맵〕

회를 위한 정보신뢰 로드맵을 개발, 정보신뢰 로드맵 중에서 이용자의 프라이버시 및 보호에 관한 프로젝트는 PAMPAS 프로젝트와 RAPID 프로젝트가 있으며, 사용자 프라이버시 보호를 위한 기반기술인 암호기술에 대한 로드맵을 수립한 STORK 프로젝트가 있다.

PAMPAS 프로젝트는 이동통신환경에서의 사용자 프라이버시 보호를 위한 로드맵을 개발('01년~'03년)하는 것으로 무선단말기의 계산능력 제한으로 인한 고비도 암호 및 무결성 메커니즘 내재의 어려움 등 현재 무선통신 환경의 문제점을 인식하고 이러한 문제점을 해결하여 진정한 유비쿼터스 네트워크 시대를 맞이하고자 이동통신 보안 기반기술, 응용기술, 네트워크 기술, 플랫폼 관리 기술 등으로 구분하여 로드맵 제시하는 프로젝트이다.

STORK 프로젝트는 미래 정보사회의 프라이버시 보호를 위한 핵심보안기술인 암호기술의 로드맵을 수립했다('02년~ '03년). 전자화폐, 전자선거, 이동 단말기간 암호통신 등 정보사회에서 활용되고 있는 또는 활용이 예상되는 암호 신기술을 분류하고 이 분류에 따라 발전방향을 제시하고 또한, 유비쿼터스 네트워크 시대에 최대 이슈가 되고 있는 이용자 프라이버시 보호를 위한 PET(Privacy Enhancing Techniques)의 핵심기술로 암호기술 연구의 중요성을 부각하고 있다. STORK 프로젝트 결과를 토대로 유럽 미래 정보사회의 신뢰성 강화를 위한 암호기술을 접목한 워터마킹 구현 프로젝트인 ECRYPT(European Network of Excellence for Cryptology - '04년~'08년, 총 750만 유로) 프로젝트를 추진하고 있다.

RAPID 프로젝트를 통해서는 Federated Identity 체계에서의 사용자 프라이버시 보호를 강화할 수 있는 로드맵을 개발, 법·제도, 사회, 기술 분야로 구분하여 각 분야별 로드맵을 제시하고 있다.

이 프로젝트에서는 기존의 ID 통합관리기술이 익명성을 제대로 보장하지 못한 문제점을 보완하고자 PET 기술을 활용하여 주소, 위치, 수준별 서비스 등에 대한 프라이버시를 보장하고 이용자의 ID, 개인정보 등을 서비스 제공자에게 드러내지 않고도 서비스에 대한 정당한 권한을 획득할 수 있는 사용자 프라이버시를 강화한 ID 통합관리 체계 구축을 목표로 하고 있다.

3. 일본

일본 내각총리실 산하 IT전략본부는 'e-Japan 전략II 가속화계획'을 발표(2004. 2.)하였다. 이 계획은 2003년 발표된 e-Japan 전략II을 가속화하여 2005년까지 세계 최첨단 IT국가의 건설이 목표로 안전하고 안심할 수 있는 네트워크사회 구축을 위한 정책과제를 도출하고 아시아를 중심으로 하는 IT분야의 국제협력전략, 정보보호 정책강화, 콘텐츠 정책 추진, IT 제도개혁, 평가의 반영, 전자정부·전자자치단체의 추진 등 6개 중점분야를 선정하고 있다. 또한, 2004년 상반기에 아시아 국가와의 협력강화를 중심으로 하는 IT관련 국제정책의 기본방향을 설정, 안전한 IT의 활용을 위해 공공분야·주요 인프라의 정보보호강화 대책 수립과 정보보호 인적기반의 확충 계획을 수립하고 있다.

일본 총무성에서는 제2기 IT혁명 추진을 위해 2010년 유비쿼터스 네트워크 사회를 목표로 한 「u-Japan 구상」을 발표하였으며, 이는 2010년까지 경제 활성화를 향한 중점시책으로 2010년 87.6조엔의 경제효과와 120.5조엔의 경제 파급효과를 예상하고 있다. 이를 위해 IT정책에서(Information Technology) ICT정책으로(Information & Communication Technology) 전환하고 2005년 중점시책을 다음과 같이 정리하고 있다.

• 일본 ICT환경의 이용증가와 함께 급증하는 개인정

보 유출, 바이러스 감염, 사이버범죄 등에 대비하여 신속하고 유연한 대응책 마련

- 신뢰성 높은 네트워크 확보를 위한 기반 정비를 위해 사이버공격 탐지기술, 본인확인을 위한 인증기술, 바이러스 대응기술, 정보의 안전한 유통을 위한 암호기술 등의 연구개발 실시
- 개인정보보호를 위한 스팸메일 대책, 개인정보보호를 위한 제도, 가이드라인 시행, 소비자 불만 DB를 개선하여 총무성 홈페이지에 개재하고 적극 반영하는 등의 제도 개선
- 일상생활 공간의 안전확보를 위해 전자태그 이용의 고도화, 활성화를 위한 연구, 센서네트워크 기술 연구, e-Health를 위한 네트워크 환경정비 실시
- 지역사회 안전확립을 위해 소방방재 ICT네트워크 고도화, 중앙정부·지방정부·주민 간 방재정보 공유시스템 개발을 통해 신속하고 효율적인 광역방재 체계 구축
- 안전한 ICT환경구축을 위한 위성시스템 개발, 차세대 GIS(Geographic information system, 3차원 지리정보시스템) 실용화를 향한 정보통신 기술 연구

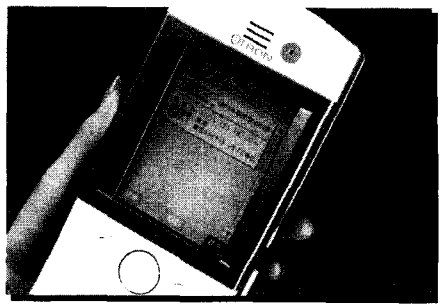
3.1 암호인증기술관련 동향

일본 노무라종합연구소는 '유비쿼터스 네트워크를 선도하는 정보통신기술 로드맵'에서 Identity 통합관리 기술을 유비쿼터스 환경의 차세대 보안기술의 하나로 선정하였고, 일본 총무성은 RFID에서의 프라이버시 데이터 보호를 위한 가이드라인을 마련 중에 있다. 또한, 사물/기기 인증(디지털 ID)과 자격/권한 인증(디지털 Right)을 제공하기 위하여 일본 T-엔진 포럼에서 운영하는 u-ID 센터를 통하여 사물식별코드인 유비쿼터스 ID (ucode)와 보안 플랫폼인 eTRON 기술을 개발하고 있다[2].

3.2 u-ID 센터의 사물식별코드 및 검색 서비스

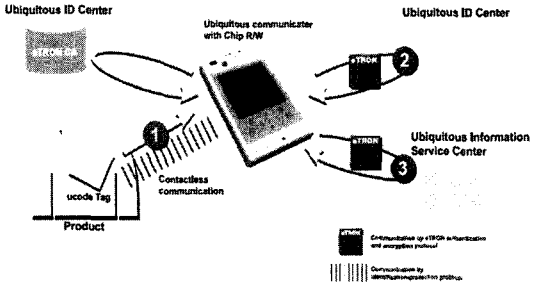
일본 uID 센터는 2003년 3월 설립되어 사물식별코드인 ucode를 발행하고, 코드 운용방식 확립 및 물품정보 검색서비스를 위한 보안기술 연구를 주된 활동으로 하고 있다. 또한 보안을 위한 기반 인증기관인 eTRON CA를 운영하며 사물식별 검색서비스의 안전성을 제공하고 있다.

uID 센터가 제공하는 사물식별 검색서비스의 주요 구성요소로는 사물 식별코드(ucode), ucode태그, 유비쿼터스 커뮤니케이터, uID 레졸루션 서버, 물품정보 서비스 서버, eTRON CA가 있다.



〔유비쿼터스 커뮤니케이터〕

- 사물 식별코드(ucode) : 실세계 사물을 유일하게 식별하기 위하여 제안한 코드체계로서 128, 256, 384비트 등 128비트 단위로 길이 확장이 가능하고 기존의 바코드, ISBN, IP주소, 전화번호 등과 호환성 있음
- ucode 태그 : 사물식별 코드(ucode)를 유비쿼터스 커뮤니케이터(UC)에 전달하는 역할을 하는 디바이스로 식별방법, 메모리접근방법, 암호화기법, 전력제공 방식에 따라 크게 9가지 클래스로 나뉘어 제공됨
- 유비쿼터스 커뮤니케이터(UC) : ucode 태그에서 ucode를 읽어 사용자에게 물품정보 검색서비스를 제공하는 통신기기로 무선랜, 블루트스 등 외부 네트워크와 연결되어 있음
- uID 레졸루션 서버(Ubiquitous ID Resolution Server) : ucode와 관련된 물품정보를 가지고 있는 데이터베이스의 위치를 알려주는 분산 디렉토리 시스템
- 물품정보 서비스 서버(Production Information Service Server) : ucode와 관련된 물품정보를 저장하는 데이터베이스



〔물품정보 검색서비스 아키텍처〕

- uID 센터(eTRON CA) : eTRON ID 인증서 생성 및 폐지를 통하여 PKI 기반의 암호화 및 인증서비스 수단 제공

① UC는 상품에 부착되어 있는 ucode 태그에 저장된 ucode를 무선 또는 광학적 방식으로 읽음
② UC는 uID 레졸루션 서버에 접근하여 ucode에 해당하는 상품정보를 저장하고 있는 물품정보 서비스 서버의 위치를 전송받음
③ UC는 물품정보 서비스 서버에 접근하여 물품정보를 획득하고 이를 사용자에게 보여줌

UC가 ucode 태그를 읽는 과정에서 태그에 저장된 정보 누출과 물품검색 서비스 과정에서 허락되지 않은 사용자의 물품정보 획득을 막기 위해서 uID 센터에서는 공격자가 ucode를 식별하는 것을 막는 프로토콜인 Identification Protection communications protocol (IPCP) 및 eTRON 보안기술을 제공하고 있다.

eTRON은 유비쿼터스 환경에 맞도록 일본에서 개발한 운영체제인 트론을 위한 보안 플랫폼이다. 애초 DRM(Digital Right Management) 등 안전한 정보 유통환경을 구축에 사용된 보안기술로서, RFID/USN 환경에서는 물품정보 검색서비스의 핵심으로 동작한다. eTRON은 UC가 uID 레졸루션 서버와 물품정보 서비스 서버에 접근하여 안전한 정보 교환을 위해서 반드시 거치는 상호인증기술을 지원하며 상호인증에 필요한 사물 식별코드는 eTRON 칩에 보관된다. eTRON 칩은 물리적 보안기능(스마트카드와 유사한 물리적 보안, Tamper Proof) 및 데이터 위·변조 방지 기능을 갖추고 있으며, 아래의 보안기능을 제공한다.

- 상호인증 : eTRON 디바이스 식별 수단으로 e-TRON ID를, eTRON 디바이스간 상호인증 수단으로 eTRON ID 인증서 이용하며, eTRON ID 인증서는 uID 센터에 구축되어 있는 인증기관(eTRON CA)에서 발급한다.
- 접근제어 : eTRON 디바이스에 접근하는 사용자 인증 : PIN 번호, 원타임 패스워드 등이며, eTRON 디바이스의 데이터 보호 : eTRON ID 기반 임의적 접근통제 기능을 제공하며, 이를 위해 접근통제 목록(ACL)을 발행서버에서 생성·관리
- 안전한 데이터 송수신 : TRON 디바이스간 통신을 위하여 보안 채널을 형성하기 위한 암호프로토콜인 eTP(entity Transfer Protocol)를 사용함

Ⅲ. 안전한 RFID/USN 기반 조성을 위한 디지털 통합인증서비스 및 PKI 기반의 정보보호 기술연구

1. 디지털 통합인증서비스

디지털 통합인증서비스는 RFID 태그 혹은 USN 노드가 가진 정당한 데이터(Right Data)를 적기적소(Right Time, Right Place)에 정당한 사람(Right People) 또는 정당한 기기(Right Device)에게 연결시켜 주는 기술 및 서비스를 말한다. 이를 위해 전자거래 주체에 대한 식별(Digital ID), 해당 주체의 권한과 자격을 확인(Digital Right), 거래 후 전자적인 증거를 확보(Digital Evidence)할 수 있는 포괄적인 디지털 증명 체계가 필요한 것이다.

1.1 디지털 ID

디지털 ID란 사이버 공간상에서 부여되는 다양한 신원정보를 말한다. 사이버 공간은 실제의 직접대면이나 대화를 통하는 방법과는 달리 가상의 공간에서 상대방의 ID와 실체를 자신이 가지고 있는 정보에 의한 신뢰를 바탕으로 통신을 하고 있다. 따라서 각국에서는 신뢰기반의 RFID/USN 환경에 적합한 다중 ID 통합관리 및 인증체계의 연구가 활발히 진행되고 있다.

1.2 디지털 ID의 증명

사이버 공간상의 사람(개인, 법인)은 물론, 유비쿼터스 환경에서 새로운 전자거래 주체로 등장하게 되는 모든 사물에 대하여 신뢰성 있는 신원 증명 기능은 반드시 필요하다. 정보가전, RFID 태그, 생체센서 등 유비쿼터스 환

〔디지털 통합인증서비스〕

경의 새로운 전자거래 주체를 대상으로 한 디바이스 인증 서비스는 디바이스 인증기관과 디바이스 제작사간의 연계를 통하여, 디바이스 제작 단계에서 인증서를 디바이스에 내장하는 형식으로 제공될 수 있으며, 디바이스에 내장된 인증서를 편리하고 안전하게 갱신할 수 있는 체계 마련도 병행되어야 한다.

또한, USN 등 유비쿼터스 환경에서 서비스 제공자에게 실명을 노출하지 않으면서 신원을 확인받아 서비스를 이용할 수 있도록 하는 실명보호 인증서비스의 제공도 필요한데, 실명보호 인증기관은 사용자의 실명을 확인한 후, 가상의 신원정보에 대한 증명 기능을 제공하는 실명보호 인증서를 발행함으로서 구현될 수 있다. 실명보호 인증서 발행 시 응용서비스의 필요에 따라 뒤에 설명될 디지털 Right 증명 기능을 활용하여 추가적인 속성 증명 기능의 통합 제공도 가능하다. 익명성을 악용하여 사이버 공간상의 범죄자 실명을 숨기는 경우, 이를 추적하여 실제 신원을 확인할 수 있는 체계도 마련되어야 한다.

1.3 디지털 Right

디지털 Right란 특정 정보에 대한 접근, 사용 또는 소유 등의 권한 정보를 말하며, 이러한 디지털 Right의 증명은 디지털 ID 증명을 통해 확인된 사람 또는 사물에게 특정한 자격이나 권한 등의 소유 여부를 확인하고 이를 신뢰성 있게 증명하는 것을 말한다. 유비쿼터스 환경에서 보다 안전하고 차별화된 서비스를 제공하기 위하여 신원이 확인된 전자거래 주체에 대하여 자격이나 권한 등 추가적인 속성증명 서비스 제공하며, 전자거래 주체의 자격, 권한 등 속성 정보의 신뢰성을 확인할 수 있는 기관과 연계하여 속성인증서 발급 체계를 구축할 수 있다. 전자거래 주체의 다양한 속성에 대한 신뢰성 있는 증명기능을 이용하여, 응용서비스 이용자별로 차별화된 서비스 제공이 가능하며 의료서비스 등 특화된 서비스 제공자의 자격에 대한 증명을 통해 신뢰성 있는 응용서비스의 구현이 가능하다.

1.4 디지털 Evidence

디지털 Evidence는 전자거래 사실 및 내용을 사후에 증명할 수 있는 정보를 말한다. 전자거래 증명기관을 통하여 거래 사실 및 내역을 증명함으로써 전자거래와 관련한 분쟁을 효율적으로 해결할 수 있는 기반을 마련하는데 그 목적이 있다. 이는 유비쿼터스 환경에서 전자거래 정보의 양적인 확대와 함께 대량의 전자거래 증명 정보를 효율적으로 생성·관리할 수 있는 기술 개발의 필요성이 증대됨에 따라, 전자거래 증명 기능을 신뢰성 있게 제공할 수 있는 독립적인 거래증명기관을 구축·운영하기 위함이다. 장기간에 걸쳐 거래사실 및 내역에 대한 증명이 요구되는 응용서비스를 위하여 증거보존 서비스가 제공되는데, 현재의 전자서명이 제공하는 전자문서 작성자 확인 및 무결성 검증 기능을 장기간 보장할 수 있는 기술을 개발하고 이에 기반하여 전자거래 증거보존기관을 구축·운영하여야 한다.

1.5 One ID, Any Service

디지털 Evidence의 증명은 디지털 ID와 디지털 Right에 대한 신뢰성 있게 확인된 상대방과 전자거래를 수행한 후, 전자거래 사실 및 내역에 대한 증명 기능을 수행하거나 장기간 전자적인 증거를 보존하는 등의 기능 제공을 말한다. 이는 궁극적으로 한 번의 인증 수행만으로 유비쿼터스 응용서비스를 편리하게 이용할 수 있는 "One ID, Any Service" 실현이 목적이며, 신원증명, 속성증명 등을 위한 사용자 인증정보를 통합적으로 관리할 수 있는 디지털 크리덴셜 표준 개발이 필수적이다. 디지털 크리덴셜(Digital Credential) 이란 신원·권한 증명을 위해 사용하는 전자 증명서로서 전자서명 인증서, 속성 인증서 등을 포괄하며 익명성, 추적성, 일회성, 유일성 등의 부가기능을 가질 수 있다.[3,4]

"One ID, Any Service"를 구현을 위해 역할기반 접근통제기술, 디지털증명 UI(User Interface), 인증정책 관리기술 등 관련 요소기술 개발이 필요하고, "One ID, Any Service"를 구현함에 있어서 특정 서버에 사용자 행위패턴이 수집되어 개인정보 침해가 발생하지 않도록 사용자에게 인증절차 통제권을 부여해야 한다. 차세대 웹서비스 구현 시 디지털 증명기능을 활용하여 편리한 사용자 인증환경 등을 지원할 수 있도록 "웹서비스 보안 프레임워크" 개발도 병행되어야 한다.

2. PKI를 이용한 정보보호기술

2.1 ID 기반의 인증기술 연구

RFID/USN 환경에서 사물 및 기기간의 안전한 통신을 위해서 상대 기기에 대한 인증과 키 분배는 반드시 필요하다. 특히 사람이 아닌 사물에 대한 인증과 키 분배를 위해서는 사물을 유일하게 식별할 수 있는 식별체계를 이용하여야 한다. 이러한 인증과 키 분배를 위해서 기존의 공개키 기반의 인증체계를 사용한다면, 상대 기기를 인증하기 위해서는 무엇보다 공개키가 공개되는 것을 필수적으로 하기 때문에 공개키 디렉토리가 별도로 필요하며, 인증기관에 의한 공개키 인증서 발행이 필요하다. 한

편 공개키를 사용하여 통신을 할 때 키 사이즈가 비밀키 통신에 비하여 엄청 커지게 되어 키 관리의 문제라든지, 키를 따로 관리해야 하는 3자 개입의 문제가 발생되게 된다.

공개키 기반구조에 비해 ID기반 암호시스템을 이용하면 키 관리문제가 훨씬 쉬어진다. ID기반 암호시스템의 기본개념은 Shamir가 1984년에 처음 제안한 것으로 공개키 인증서를 이용하는 대신 사용자의 이메일, 전화번호 등을 이용하여 공개키를 생성하는 방법이다. 이는 공개키를 관리하는 공개키 디렉토리를 없애 키 관리를 훨씬 단순하게 하는 이점을 제공한다. 1984년 이후로 많은 ID기반 암호시스템들이 제안되었으며 전자메일, 무선 이동 애드혹(Ad-hoc) 네트워크 등 다양한 응용환경에 적용을 시도하고 있다.

RFID/USN 환경에서의 사물/기기의 사물식별코드(EPC, ucode, IP address 등)를 ID로 생각한 인증모델은 공개키의 관리가 이루어져야 하는 CA기반 인증모델보다 키 관리 측면에서 용이할 수 있으며, 기존 RSA기반 방식의 서명길이보다 짧은 서명길이의 구현이 가능하다. 또한, ID기반 시스템에서 이용되는 Weil pairing 맵의 특성을 이용하면 효율적인 batch verification 특성과 같은 전자서명의 구현도 가능함에 따라, 이에 대한 향후 연구가 진행되어야 할 것으로 판단된다[5].

2.2 경량 정보보호 기술 및 규격 개발

2.2.1 경량 PKI 중심의 정보보호 기술

앞에서 서술한 디바이스 인증기술, 속성인증기술, 실명보호 인증기술 등을 구현하기 위해서는 이를 뒷받침하기 위한 다양한 기술의 개발이 필요하고, 이 기술들의 근간에는 제한된 네트워크 환경 및 이동성과 휴대성, 분산 환경의 강조로 인한 경량화된 기술이 요구된다.

먼저 다양한 매체에 적용 가능한 경량 암호기술 개발이 시급하다. RFID 태그 등과 같이 배터리 전력에 한계가 있고 아주 작은 소형 프로세서를 사용하는 초경량·저전력 계산환경에서 고속의 암호연산이 가능한 차세대 암호원천기술의 개발은 필수요소이다. 아울러 기존의 암호알고리즘을 어떻게 구현하느냐에 따라 처리속도 및 메모리 크기가 변화되므로 이에 대한 연구개발도 필요하다. 또한, 해킹이나 비밀키의 분실 등으로 비밀키가 노출되었을 때 피해를 최소화할 수 있도록 전방보호, 후방보호 등의 특성을 갖는 암호화 기술 개발과 기존의 양자간 암호기술을 확장하여 그룹키 교환, 브로드캐스트 암호 등 다자간 암호기술 개발도 필요하다. 특히, 유비쿼터스 네트워크의 정보유통 환경에 적합한 키로밍 기술, 웹서비스 기반 키관리 기술은 기술 개발자의 보안조건과 이용자의 편의성을 동시에 만족하는 유용한 기술들이다. 이외에 암호화된 개인정보 DB를 복호화하지 않고도 필요한 통계수치를 산출해 낼 수 있는 DB 암호화 기술도 필요한 기술이다. 웹 서버 운영자들은 서비스 이용자의 민감한 개인정보를 안전하게 관리하기 위해 정보를 저장한 DB를 암호화하여 보관하나, 현재의 DB 암호화 기술로는 웹 운영에 필요한 통계수치를 파악하기 위해 DB 전체를 복호화해야 하기 때문에 필요 이상의 개인정보가 노출 될 수 있기 때문이다.

둘째, 경량화된 인증서의 검증기술개발이 필요하다. CRL, OCSP, SCVP등의 기술은 CA 혹은 신뢰된 검증기관과의 통신에 의해서만 확인될 수 있는 정보이다. 하지만, RFID/USN의 경우 기기에 따라서 인증서 체인구성과 개별적 검증이 기기 자체 혹은 네트워크에 의해 원천적으로 차단될 수 있다. 이를 위한 경량화된 검증기술의 연구는 반드시 필요하다.

셋째, 실시간 환경을 만족하는 통신프로토콜의 개발이다. 유선PKI와 무선PKI의 경우 전자서명메시지 및 암호화 메시지의 실시간 특성은 많은 부분 고려되지 않았다. E-mail이나 전자서명메시지, 암호메시지 등은 검증자에 의해 메시지 수신 후 실시간 응답이 필요없는 Non-interactive 통신 프로토콜에 의존해 왔다. 하지만, RFID/USN의 경우 기기들 간의 메시지 교환은 실시간에 이루어 져야 하는데, 이는 PKI 각 개체 간에 주고받는 메시지는 실시간으로 작성 및 검증되어야 한다는 것이다. 이때 시간차가 날 경우 네트워크 및 기기 간에 심각한 문제를 일으킬 수 있다. 이를 위한 동기화 기법은 논외로 한다.

2.2.2 기술 규격 개발 및 표준화

앞 절에서 설명한 경량 PKI의 기술은 경량 인증서 및 경량 메시지 코딩 기법, 경량 처리모듈에 의해 기술규격에 따라 구현되어야 한다. 경량 인증서의 경우 기존의 X.509v3 인증서와 RFC3280 인증서, WAP Cert, WTLS 인증서, X9.68(Part II)등의 각 인증서 필드들을 면밀히 검토하여 각 기기의 특성을 아우를 수 있는 인증서 형태를 공인인증기관 및 벤더들과 도출하여 규격화해야 한다. 이러한 인증서의 형태 연구는 새로운 기술이 필요하지 않으나, 각 단체간의 협의를 도출한다는 절차를 거쳐야 하므로 때에 따라선 더욱 어려운 작업이 될 수 있다. 또한, 개발되지 않은 새로운 인증서 필드의 필요성은 관련 PKI기술을 선도할 수 있는 좋은 기회가 될 것이다.

2.3 기타 정보보호 기술

이외에 유비쿼터스 네트워크 환경에 대비하여 BcN, USN, 홈네트워크 등 차세대 정보통신 기반의 멀티미디어 컨텐츠 보호기술과 멀티미디어 컨텐츠의 불법유통을 방지하기 위한 핑거프린팅 기술, 워터마킹 기술 등 컨텐츠 위·변조 방지기술, 이기종 디바이스, 다양한 u-어플리케이션 간 상호운용성을 보장하는 멀티미디어 컨텐츠 보호기술 개발 등이 요구되고 있다.

특히, 유비쿼터스 네트워크 환경의 특성을 고려한 보안기술로 사물간의 자율적 의사소통을 통해 공간-사물-컴퓨터-사람을 연계하는 유비쿼터스 네트워크 환경에서 이용자의 자연어 인식 기술, 분산형 접근제어기술 및 정보가전, 센서 및 디바이스 사이에서 통신되는 메시지의 위·변조 검증(MAC) 기술은 바로 응용할 수 있는 실용적 기술이 된다.

또한, 유비쿼터스 환경에 적합한 능동형 보안관리 기술로 센서 등 디바이스의 보안기능에 대한 무결성을 자체적으로 점검하고 결과를 자동 보고(Reporting)하는 보안기능 자동검사 기술의 개발도 필요하다.

3. 디지털통합인증 시범사업 개발 전망

디지털 통합인증프레임 기반의 디지털 ID, 디지털 Right, 디지털 Evidence 서비스 실현을 위해서는 실생활에 직접적으로 필요한 시범사업 발굴이 필요하다. 시범서비스의 예는 다양하지만, 디지털 ID 인증을 통하여 디바이스간의 정보교류 서비스, 온라인 의료서비스에서 의사, 간호원 등의 자격 및 권한을 보장하는 디지털 Right, RFID/USN 환경에서 수많은 사물/기기들간의 트랜섹션을 보장하는 Digital Evidence 등을 생각할 수 있다. 또한, 현재 한국전산원에서 추진하고 있는 RFID 시범사업의 결과를 기반으로 보안 시범사업을 연속화하는 방법을 모색할 수 있을 것이다. 하지만 급변하는 IT환경을 고려해 볼 때, 향후 2~3년간 산업의 동향을 파악하여 보안 서비스를 필요로 하는 분야를 발굴하는 것이 중요하리라 판단된다.

Ⅳ. 결 론

현재 다양한 개체인증을 수용할 수 있는 통합인증 서비스 개발이 VeriSign사를 중심으로 처음 시도되고 있는 시점이므로 국내 기술개발 및 연구에 좀 더 많은 관심을 기울인다면, 관련 기술 분야를 이끌 수 있는 리더로서 RFID/USN 환경에 적합한 디지털 통합인증서비스 기술을 선도할 수 있으리라 판단된다. 즉, 국내 인증관련 인프라 기술은 국외에서 성공사례로서 모델이 될 만큼 국제적으로 인정받고 있어 이러한 기술력을 바탕으로 RFID/USN 환경에 적합한 통합인증 기본 모델 및 상세모델을 단기에 개발함으로써 국제 경쟁력을 제고할 수 있고, 기존의 인증서비스를 RFID 태그, 리더 등 기기에 대한 인증으로 확대하여 익명인증서비스, 내용증명서비스 등 신규서비스를 창출함으로써 국내 정보보호시장의 제2의 성장기를 가져올 수 있으며, 프라이버시 침해 논란으로부터 벗어나 RFID/USN 산업 활성화에 초석을 마련할 수 있을 것으로 보인다.

국외에서는 사물/기기 인증서비스가 아직 준비단계에 불과하고 익명인증, 내용증명 서비스는 준비하고 있지 않아 해외시장을 선점할 수 있는 기회가 될 수 있다. 또한, RFID/USN 환경을 위한 통합인증기반을 마련함으로서 고의에 의한 RFID 정보삭제, 정보유출을 통한 산업스파이 활동, 모조품 불법유통 등의 RFID/USN 정보화 역기능을 방지함으로써 건전한 RFID/USN 산업 활성화에 기여하리라 생각된다.

참 고 문 헌

[1] VeriSign, "The EPC Network : Enhancing the Supply Chain", Jan. 2004, http://www.verisign.com/static/002109.pdf

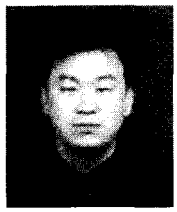
[2] uidcenter, "uID Technology", http://www.uidcenter.org/english/technology.html

[3] Gerrit Bleumer, "Credentials", ACM, February 2003

[4] IETF RFC 2828, Internet Security Glossary, 2000

[5] D. Boneh, M. Franklin, "Identity-based Encryption from the Weil Pairing", SIAM J. of Computing, Vol. 32, No. 3, pp. 586-615, 2003

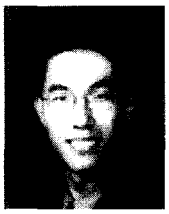
〈著 者 紹 介〉



윤 재 호 (Jaeho Yoon)
정회원

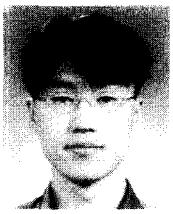
1997년 02월 : 인하대학교 전자공학과 학사
1999년 09월~2000년 11월 : MSc IT Security in University of Westminster(London) 수료

2002년 09월~2004년 08월 : 세종대학교 소프트웨어 공학과 석사
1997년 02월~1998년 12월 : (주)현대엔지니어링 FA Sensor 설계팀원
2000년 12월~현재 : 한국정보보호진흥원(KISA) 암호인증기술팀 연구원
〈관심분야〉 RFID/USN 정보보호, PKI, 암호프로토콜



박 배 효 (BaeHyo Park)
정회원

1997년 2월 : 한국과학기술원(KAIST) 전기 및 전자공학과 학사
2002년 8월 : 광주과학기술원(GIST) 기전공학과 석사
2002년 7월~현재 : 한국정보보호진흥원 연구원
〈관심분야〉 RFID/USN 정보보호, 암호프로토콜, 통합인증기술



주 학 수 (Hak Soo Ju)
정회원

1997년 8월 : 고려대학교 수학과 학사
1999년 8월 : 고려대학교 수학과 석사
2001년 8월 : 고려대학교 수학과 박사과정 수료
2001년 9월~현재 : 한국정보보호진흥원 연구원
〈관심분야〉 암호학, 공개키암호, 응용보안프로토콜, RFID/UNS 정보보호

권 현 조 (Hyun Jo Kwon)
정회원

1997년 2월 : 성균관대학교 정보공학과 학사
2000년 8월 : 성균관대학교 정보통신대학원 석사
1997년 1월~1997년 7월 : (주)나라계전기술연구소 연구원
1997년 7월~현재 : 한국정보보호진흥원 연구원
〈관심분야〉 키관리, 암호프로토콜, RFID/USN 정보보호

전 길 수 (Kilsoo Chun)
종신회원

1991년 2월 : 서강대학교 수학과 이학사
1993년 2월 : 서강대학교 대학원 수학과 이학석사
1998년 2월 : 서강대학교 대학원 수학과 이학박사
1998년 10월~1999년 9월 : 서강대학교 기초과학연구소 박사후 연구원
2001년 3월~2001년 6월 : 서강대학교 컴퓨터학과 연구교수
2001년 7월~현재 : 한국정보보호진흥원 암호인증기술팀장
〈관심분야〉 암호학, 정보보호, RFID/USN 정보보호