암호/인증/권한관리

1. 개요

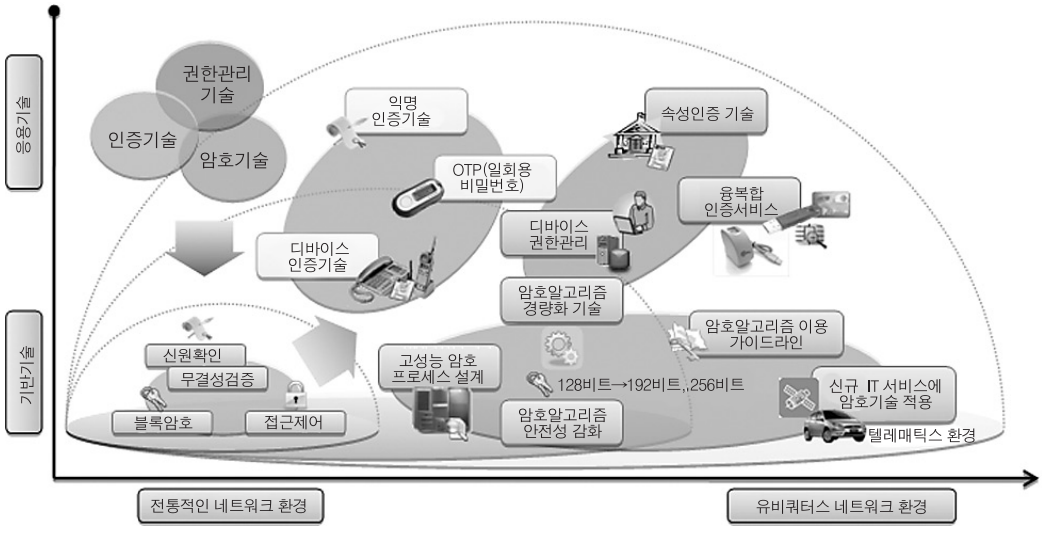
1.1. 기술개요

1.1.1. 중점기술 및 표준화 대상항목의 정의

• 중점기술의 정의

정보보호분야의 암호 · 인증 · 권한관리 기술은 인터넷 등 사이버 환경에서 다양한 정보를 안전하고 신뢰성 있게 접근 · 이용 · 유통하기 위한 기반 기술로써, 정보의 안전한 송수신을 위한 프리미티브 기술인 암호기술과 사용자의 신원확인 및 유통되는 정보에 대한 무결성을 보장하기 위한 인증기술, 불법적인 정보접근을 통제하기 위한 권한관리 기술로 구분. 또한, 최근 사이버 해킹 기술의 급속한 발전과 유비쿼터스 환경의 도래에 따라 사회적으로 요구되고 있는 안전성의 강화 및 경량화된 암호 · 인증 · 권한관리 기술을 포함

- 암호기술은 사이버 환경에서 정보의 안전한 송수신(즉, 비밀성 및 무결성 등 지원)을 위한 프리미티브 기술로써 다양한 디바이스가 어우러진 유비쿼터스 환경에서 활용 가능한 경량화된 암호 기술, 다양한 보안 프로토콜에서 블록 암호 알고리즘을 사용하기 위한 운영 모드, 클라우드 컴퓨팅, 스마트 그리드 등 새로운 정보통신 서비스 환경에서의 키관리기술, 암호알고리즘 활용 및 적용방안을 포함하고 있음
- 인증기술은 사이버 환경에서 적법한 사용자를 식별하기 위한 신원확인을 비롯하여 유통되는 정보의 무결성을 보장하는 기술임. 일반적인 ID/패스워드와 같이 사용자의 신원확인 기술에서부터 다양한 단말기의 진위성 여부를 보장하기 위한 디바이스 인증기술, 익명의 사용자를 추적할 수 있는 익명 인증기술, 매번 비밀번호를 변경하는 OTP(One Time Password) 인증 기술 등을 포함하고 있음
- 권한관리기술은 인터넷상에서 유통되고 있는 정보에 대한 접근 시 적법한 권한을 가지고 있는지 여부를 판단하기 위한 기술로써, 해당 사용자에 대한 권한을 인증수단에 포함하는 속성 인증 기술, 하드웨어 기반의 접근제어 기술, USIM 등 다양한 접근제어 수단을 제공하는 디바이스에 대한 권한관리 기술 등을 포함하고 있음



• 표준화 대상항목의 정의

구 분	표준화 대상항목	표준화 내용
암호	유비쿼터스 환경에 적합한 경량 암호 알고리즘	유비쿼터스 환경을 구성하는 다양한 정보통신기기의 정보처리 및 전송의 안전성 보장 및 소형기기에 적합한 경량화된 암호 알고리즘(키 생성 및 암 · 복호화 과정 등)을 제시
	블록암호 알고리즘 운영모드	다양한 보안프로토콜에서 블록암호를 활용하기 위한 운영모드 및 운영모드 선택을 위한 지침을 제시 ※ IPsec 프로토콜에서의 SEED 운영모드 사용규격 등 국제 표준화 추진 중
	응용서비스에서의 암호 알고리즘 활용 방법	VoIP, IPTV, IPSec 등 네트워크 프로토콜과 클라우드컴퓨팅, 스마트그리드, 텔레매틱스, RFID/USN 등 다양한 응용서비스의 안전성 강화를 위한 규범적인 암호 알고리즘 적용 및 활용 지침을 제시※ 예를들어, 스마트그리드 환경에서의 암호 알고리즘 적용 등 보안대책 수립 및 보안기능 구현시 본 표준을 참조하여 작업
인증	다양한 인증수단에 대한 보안성 검증 프레임워크	다양한 인증수단에 대한 안전성 및 신뢰성 검증을 위한 위험분석 기반의 보안성 검증 프레임워크를 정의 ※ 즉, 인증수단별 보증수준 검증을 위한 기준 및 절차 등 제시
	디바이스 인증 기술 및 응용	인터넷 전화기, CCTV, 휴대단말기, 지능형 가전 등 정보통신망에 연결된 다양한 디바이스에 대한 식별 · 인증 등 신뢰된 인증 서비스를 제공하기 위한 기반 및 응용기술을 정의
	일회용패스워드(OTP) 인증 기술 및 응용	인터넷 서비스의 안전성 강화를 위해 일회용 패스워드(OTP)를 활용한 응용기술[1] 개발과 다양한 인증 프로토콜에 OTP를 적용하기 위한 보안 프로토콜 확장기술[2]을 정의 * 1) OTP를 활용한 부인방지 기술, 거래연동 인증기술 등 2) OTP-TLS, OTP-EAP, OTP-Kerboeros 등
	일회용패스워드(OTP) 인증 시스템 보안 요구사항	OTP 기반 인증서비스를 제공하는 인터넷 서비스 사업자가 보안성을 유지하기 위한 세부적인 보안 요구사항*을 정의하고, 타 서비스 또는 시스템과 상호 연동성을 보장하기 위한 응용 프로그램 인터페이스 등 구현 요구사항을 정의 * OTP 기기 및 인증시스템, 보안 알고리즘, 생성 알고리즘 등
	익명성을 보장하는 인증 기술	웹사이트 회원가입 및 성인인증 등 서비스 이용의 프라이버시 보장을 위해 가명 또는 익명을 사용할 수 있도록 보장하는 한편, 익명성 남용을 방지하기 위한 익명인증체계(익명인증서 프로파일, 프로토콜, 검증 등) 및 익명에 대한 추적기술 등을 정의
	바이오정보를 이용한 전자서명 기술	인증서 대여 등 기존의 공개키 기반 전자서명 기술의 단점을 보완하기 위해 지문, 홍채 등 바이오정보를 포함한 전자서명 인증기술 및 이용 효율성 제고 방안 정의
권한관리	기기 관리자 및 소유자간의 권한관리 기술	정보통신망에 연결된 다양한 디바이스에 대한 식별 · 인증 및 권한부여를 위해 디바이스를 관리하는 기기 관리자 및 소유자의 디바이스에 대한 권한관리 모델 및 시나리오, 기기 식별체계 등을 정의
	통합 권한관리 프레임워크 및 응용 서비스	다양한 정보시스템에 적용된 서로 다른 권한관리 체계의 연계 및 통합관리를 위한 프레임워크 정의 및 이에 기반한 응용 서비스 구현을 위한 지침을 제시
	사용자 권한관리를 위한 인증기술 및 응용	속성인증서 프로파일, 관리 · 운용 및 검증 프로토콜, 사용자 인터페이스 기술 등 속성인증서를 활용하여 사용자에 대한 권한을 관리하기 위한 기술을 정의

• **표준화 대상항목의 그린 ICT 관련성 및 녹색기술수준**

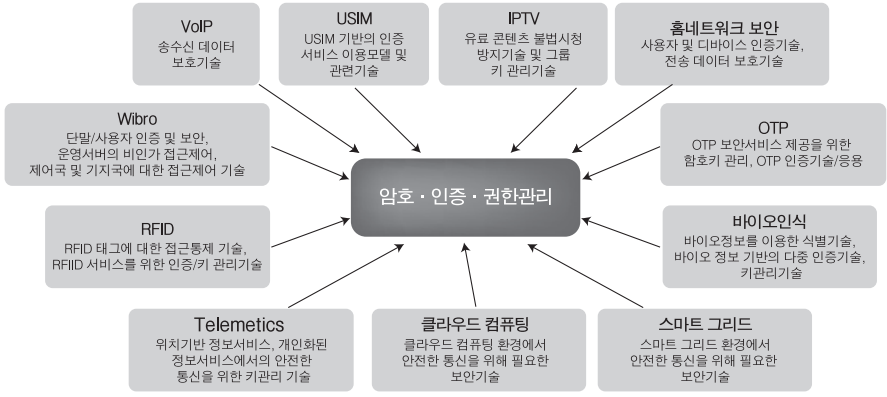
- 응용서비스에서의 암호알고리즘 활용 방법 중점기술은 온라인을 통한 재택근무, 화상회의 등을 안전하게 제공하기 위한 방법으로 물건의 소비 감소, 인간의 이동 감소, 물류의 이동감소, 업무 효율화 증대를 통해 에너지 절감 및 이산화탄소(CO2) 감축이 가능하며, 연구결과에 따르면 EU 근로자 10%의 재택근무시 연간 2,217만톤의 CO2 감축이 예상됨(ETNO, 2006)
- 또한, 스마트그리드를 통해 주택용 에너지관리시스템, 에너지 절약형 상점시스템 등 u-센서 기반 에너지 고효율 서비스 모델 확산으로 전력 · 에너지 감소를 실현하여 냉난방 전략의 40% 이상 절감 예상(WWF, 2008)
- 사이버 환경에서의 다양한 인증 및 권한관리 기술의 활성화는 오프라인에서의 대면확인 및 물리적 인증매체 사용을 대체함으로써 물리적인 이동 및 폐기물의 감소는 물론, 업무 효율의 극대화 및 공간 효율화에 크게 기여할 것으로 기대됨

표준화 대상항목		물건의 소비 감소	전력 · 에너지 소비 감소	인간의 이동 감소	물류의 이동 감소	공간 효율화	폐기물 감소	고 효율화 (업무 효율화)	그린 ICT와 연관 특징 (CO_2 배출 감소효과)	녹색기술수준
암호	유비쿼터스 환경에 적합한 경량 암호알고리즘	-	○	-	-	-	-	○	경량화 알고리즘으로 전력소비감소와 에너지 감소로 CO2 배출 감소	-
	블록암호 알고리즘 운영모드	-	-	-	-	-	-	-	-	-
	응용서비스에서의 암호 알고리즘 활용 방법	◐	◐	◐	◐	○	○	◐	암호 알고리즘 활용을 통해 사이버 환경에서 안전한 응용서비스를 제공함으로써 종이 사용량 및 이동 감소를 통해 에너지 소비를 줄일 수 있음	-
인증	다양한 인증수단에 대한 보안성 검증 프레임워크	○	-	○	-	-	○	-	온라인 인증수단 확산으로 대면 인증 및 인증매체의 감소로 인간의 이동 및 폐기물 감소	-
	디바이스 인증 기술 및 응용	○	-	○	-	-	○	◐	인증 매체의 감소와 이동감소, 폐기물이 감소, 고효율화	-
	일회용패스워드 (OTP) 인증 기술 및 응용	○	-	○	-	-	○	○	보안카드와 같은 인증 매체의 감소로 폐기물이 감소와 고효율화	-
	OTP 인증 시스템 보안 요구사항	-	-	○	-	-	-	○	-	-
	익명성을 보장하는 인증 기술	-	-	○	-	-	-	-	-	-
	바이오정보를 이용한 전자서명 기술	-	-	○	-	-	◐	-	인증 매체의 감소로 폐기물이 감소	-
권한관리	기기 관리자 및 소유자간의 권한관리 기술	-	-	○	○	-	-	-	-	-
	통합 권한관리 프레임워크 및 응용 서비스	○	-	○	-	-	○	○	인증 매체의 감소로 폐기물이 감소	-
	사용자 권한관리를 위한 인증기술 및 응용	-	○	○	-	-	-	○	권한관리를 통해서 프로세서 사용시간 절약 및 이동감소로 고효율화	-

〈범례〉 -(관련없음) ○(소) ◐(중) ●(대)

1.1.2. 연관기술 분석

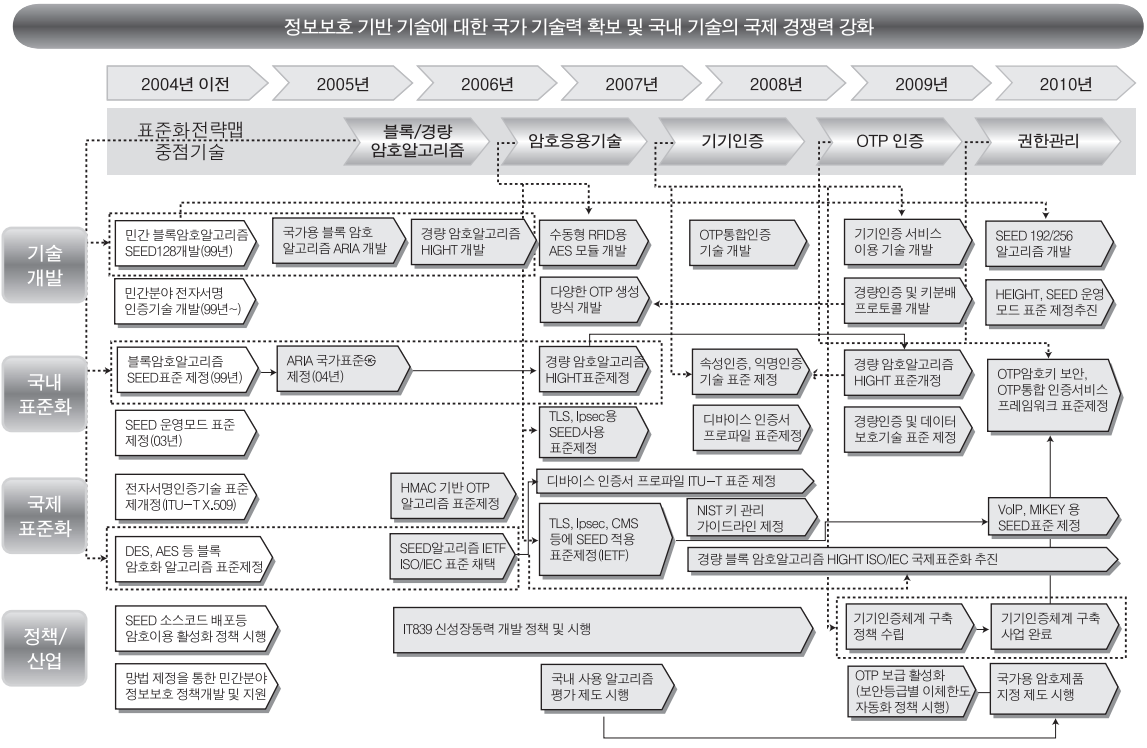
• 연관기술 관계도



• 연관기술 분석표

연관기술	내 용	표준화기구/단체		표준화수준		기술개발수준	
		국내	국외	국내	국외	국내	국외
RFID	RFID 태그의 접근을 제어할 수 있는 인증 및 키 관리 기술	TTA/USN 포럼	IETF, ITU-T	표준제정	표준안 제정검토	상용화	상용화
IPTV	IPTV 서비스에서의 유료콘텐츠의 불법시청 및 복제를 방지하기 위한 기술	TTA	IETF, ITU-T, IETF	표준안 개발/검토	표준안 개발/검토	상용화	상용화
홈 네트워크 보안	안전한 홈 네트워크 서비스를 제공하기 위해 홈 내부 및 원격 사용자에게 보안서비스를 제공하기 위한 기술	TTA/홈 네트워크 보안포럼	ITU-T	표준안 개발/검토	표준안 개발/검토	구현	구현
VoIP	VoIP 단말기, 중계장비간의 송 · 수신 데이터에 대한 보호 기술	TTA	IETF	표준제정	표준제정	상용화	상용화
Wibro	와이브로 서비스에서의 단말 및 사용자에 대한 인증기술 및 제어국 · 기지국의 접근을 제어할 수 있는 기술	TTA	IEEE	표준제정	표준제정	상용화	구현
바이오인식	얼굴, 지문, 홍채 등 사람의 고유한 특성인 바이오정보를 사용하여 서비스 이용자의 신원확인 및 인증하는 기술	TTA	ITU-T, ISO/IEC SC37	표준제정	표준제정	상용화	상용화
Telemetics	위치정보 시스템과 무선 통신망을 이용한 텔레매틱스 환경에서 안전한 통신을 위한 키 관리 기술	TTA	IETF, ITU-T	표준안 개발/검토	표준안 개발/검토	구현	구현
USIM	3세대 이동통신 단말기에 이용되는 스마트카드인 USIM에 공인인증서비스를 제공하기 위한 기술	TTA	3GPP, OMA	표준안 개발/검토	표준안 개발/검토	구현	구현
OTP	일회용 패스워드로써 포털사이트의 로그인, 금융거래 시에 이용되는 인증기술	TTA	ITU-T, IETF	표준안 개발/검토	표준안 개발/검토	상용화	상용화
클라우드 컴퓨팅	클라우드컴퓨팅 환경에서 안전한 통신을 위해 필요한 보안기술	TTA/클라우드 컴퓨팅포럼	ITU-T	표준안 개발/검토	표준안 개발/검토	상용화	상용화
스마트그리드	스마트그리드 환경에서 안전한 통신을 위해 필요한 보안기술	TTA/스마트 그리드 정보통신 융합포럼	ITU-T, ISO/IEC, ZigBee	표준안 개발/검토	표준안 개발/검토	구현	구현

1.2. 중점기술의 년도별 주요현황 및 이슈



• **기술개발 주요현황 및 이슈**

- 1999년 KISA를 중심으로 민간용 블록 암호 SEED 128 개발
- 1999년~민간 공인인증서비스 제공을 위한 전자서명인증 기술 개발
- 2004년 국가용 블록 암호 ARIA 알고리즘 개발
- 2005년 국정원 및 산 · 학 · 연 공동으로 경량 블록 암호 알고리즘(HIGHT) 개발
- 2006년 ETRI에서 수동형 RFID용 AES 모듈 개발
- 2006년~2008년 스마트카드, 바코드, 음성신호 및 그래픽 등을 이용한 OTP 생성 방식 개발
- 2007년 금융보안연구원에서 OTP 통합인증 기술 개발
- 2007년 KISA에서 암호 이용 가이드라인과 각 분야별 활용방안에 대한 가이드라인 개발
- 2008년 USN환경의 경량 인증 및 키분배 프로토콜 개발
- 2008년 u-인증 서비스 도입 및 이용 기준 개발
- 2009년 KISA를 중심으로 민간용 블록 암호 알고리즘 SEED 192/256 개발
- 2009년 익명 PKI 시스템 및 서비스 요소 기술 설계
- 2009년 KISA에서 기기인증을 위한 최상인 인증시스템 구축 및 2010년 정부용 인터넷전화기에 기기인증서 탑재
- 2010년 신규 IT 환경을 지원하기 위한 효율적인 암호 알고리즘 구현기술 개발
- 2010년 OTP를 이용한 대칭키 기반의 부인방지 프로토콜 개발

- 2010년 ETRI에서 익명성 제어 가능한 그룹 서명 기반 익명 인증인가 암호 프리미티브 개발

• **국내표준화 주요현황 및 이슈**

- 1999년 SEED 블록암호 알고리즘 TTA 표준 제정
- 2003년 SEED 운영모드 TTA 표준 제정
- 2004년 ARIA 블록암호 알고리즘 국가 표준(KS) 제정
- 2004년 차량용 ITS 응용 단말기 인터페이스에 대한 TTA 표준 제정
- 2006년 차량-인프라 간 통신에 대한 TTA 표준 제정
- 2006년 텔레매틱스 단말 소프트웨어 플랫폼 인터페이스에 대한 TTA 표준 제정
- 2006년 HIGHT 블록 암호 알고리즘, TLS용 SEED 사용 표준, IPsec용 SEED 사용 표준, CMS를 위한 추가암호 알고리즘 SEED 등 TTA 표준 제정
- 2007년 속성인증, 익명인증, 홈네트워크 인증 기술 등에 대한 TTA 표준 제정
- 2008년 경량화된 블록 암호알고리즘 HIGHT 개정
- 2008년 수동형 RFID 경량 인증 및 데이터 보호 프로토콜에 대한 TTA 표준 제정
- 2008년 USN에서 센서노드간 경량 인증 및 키분배 프로토콜에 대한 TTA 표준 제정
- 2009년 OTP 암호키 관리 보안요구사항, OTP 통합인증서비스 프레임워크, OTP 인증 서비스를 위한 보증레벨에 대한 TTA 표준 제정
- 2010년 블록암호알고리즘 SEED 및 HIGHT의 운영모드 등 TTA 표준 제정 추진
- 2010년 기기인증서 프로파일, 기기인증서 효력정지 및 폐지 목록 프로파일, 기기인증서 DN 정의, 디렉토리 스키마, 전자서명 알고리즘 파라미터 표준화 추진 후 제정 예정
- 2010년 OTP 응용프로그램 인터페이스, OTP 기기 보안요구사항, OTP 비밀키 컨테이너 등 표준 제정 추진
- 2010년 익명 인증 서비스 프레임워크, 그룹 서명 기반의 익명 인가 프레임워크 표준 추진

• **국제표준화 주요현황 및 이슈**

- 2005년 ISO/IEC 18033-3 : 블록암호 알고리즘에 SEED 추가하는 표준 개정
- 2005년 IETF에서 SEED 블록 암호 알고리즘 표준 제정(RFC 4009, RFC 4269(개정))
- 2005년 IETF에서 CMS에서의 SEED 암호 알고리즘 사용 표준 제정(RFC 4010)
- 2005년 IETF에서 TLS, IPsec, IKE용 SEED 사용 표준 제정(RFC 41623, 4916, 4615)
- 2005년 IETF에서 HMAC 기반의 일회용패스워드 알고리즘 표준 제정(RFC 4226)
- 2007년 IETF에서 EAP와 일회용패스워드 프로토콜을 결합한 표준 제정(RFC 4793)
- 2007년 ITU-T에서 홈네트워크에 적용 가능한 디바이스 인증서 프로파일 표준 제정(X.1112)
- 2007년~현재 ISO/IEC에서 경량 암호블록 암호 알고리즘(HIGHT) 표준 추진
- 2007년 NIST 키관리 가이드라인(NIST Publication 800-57) 개발
- 2008년~현재 ITU-T에서 OTP 기반 인증 서비스 관리 프레임 표준 추진(X.sap-3, '10.12월 제정예정)
- 2009년 IETF에서 추적가능한 익명인증 기술 표준 제정(RFC5636)
- 2009년 ITU-T에서 전자상거래를 위한 익명인증 가이드라인 표준 추진(X.sap-5)
- 2010년 ISO/IEC에서 그룹서명 및 익명인증 기술 표준 추진

- 2010년 IETF에서 VoIP용 SEED 사용 표준 제정(RFC 5669)
- 2010년 IETF에서 MIKEY에서의 SEED OID 추가 표준 제정(RFC 5748)
- 2010년 IETF에서 IPSEC에서의 SEED 운영모드 추가 표준 추진
- 2010년 ISO/IEC에 JTC1 SC27/WG2 그룹서명 기반의 익명 기술 표준화 추진

• **정책/산업 주요현황 및 이슈**

- 1999년~현재, 전자서명법 제정 및 공인인증서 이용 활성화 정책 수립 및 추진
- 2000년~현재, SEED 소스코드 배포를 통한 암호 이용 활성화 사업 추진
- 2001년 정보통신망 이용촉진 및 정보보호 등에 관한 법률 기반으로 민간분야 정보보호 관련 정책 개발 및 지원
- 2004년~2006년 텔레매틱스 기반 응용기술 개발 및 정책 추진
- 2005년 정부에서 IT839 신성장동력 기술 개발 추진 정책 수립
- 2006년 국내 상용 암호모듈 평가 제도(KCMVP) 시행
- 2008년 유비쿼터스 환경에 적합한 기기 인증체계 구축을 위한 정책 수립
- 2008년 전자금융거래를 위한 보안등급별 이체한도 차등화 정책 시행(1등급 매체: OTP, 보안토큰)
- 2009년 국가용 암호제품 지정제도 시행
- 2009년 기기인증서비스의 안전성 제고를 위한 기기인증체계 구축 완료
- 2010년 정부기관용 인터넷전화에 대한 기기인증서 발급 추진
- 2010년 공인인증서 외 다양한 인증수단의 도입 및 활성화를 위한 전자금융거래 감독규정 개정

1.3. 추진경과 및 중점 추진방향

• **추진경과**

- Ver.2008에서는 정부의 정책추진의지, 산업체의 요구사항, 국제표준화 동향, 그리고 파급효과 등을 고려하여 정보보호를 암호 · 인증 · 권한관리, 개인정보보호 · ID관리, 네트워크 및 시스템 보안, 응용보안 · 평가인증 등 4개 분야로 구분하여 정리하였으며, 암호 · 인증 · 권한관리 분야에서는 암호키관리, 암호응용기술, 익명인증, H/W기반 접근제어 등 4개의 중점표준화 항목을 선정함

- Ver.2009에서는 Ver2008에서 선정한 중점 표준화 항목 이외에 정부의 정책추진의지 및 국내 산업체 요구사항, 국내외 보안시장 트렌드 등을 고려하여 추가적으로 디바이스 분야를 중점 표준화항목으로 선정함. 또한, 최근 유비쿼터스 환경에서 안전한 정보전송을 보장하기 위해 필요한 경량화된 암호응용기술의 개발 요구가 증가됨에 따라 관련 표준화 및 기술개발 동향 등을 추가함

- Ver.2010에서는 기존 Ver.2007~Ver.2009에서 선정한 표준화 대상 항목과는 다르게 암호기술, 인증기술, 권한관리 기술별로 표준화 대상 항목을 추가 발굴하여 선정함. 특히, 그린 IT기술, 디바이스 인증기술 등 최근 정부정책 추진방향 및 신규 IT 서비스 분야에 적용 가능한 세부 아이템 위주로 표준화 대상항목을 추가 선정. 이에 따라, 안전성이 강화된 블록암호 알고리즘 및 경량 암호알고리즘 기술, 암호알고리즘 이용 가이드라인, 모바일 등 디바이스 인증기술, OTP 인증 기술 등 총 15개의 표준화 대상항목을 선정함

- Ver.2011에서는 Ver.2010에서 선정한 중점 표준화 항목을 기반으로 신규 IT 서비스 분야와 응용 환경에 적용 가능한 세

부 항목 위주로 표준화 대상항목을 추가 선정. 이에 따라 다양한 응용서비스에서 암호 알고리즘을 활용하기 위한 방안과 다양한 인증수단에 대한 보안성 검증 프레임워크, 통합 권한관리 프레임워크 등을 추가하여 총 12개의 표준화 대상항목을 선정함

• 버전별 중점기술의 변천

구 분	Ver.2008	Ver.2009	Ver.2010	Ver.2011
암호	- 암호알고리즘 - 암호 키 관리 - 암호 응용 기술	- 암호알고리즘 - 암호 키 관리 - 암호 응용 기술	- 유비쿼터스 환경에 적합한 경량 암호알고리즘 - 블록 암호알고리즘 기술 - 응용서비스에서의 암호 알고리즘 활용 방법 - 텔레메틱스 환경에서의 암호 키 관리 기술 - 암호알고리즘 이용 가이드라인 - 고성능 암호프로세서 설계	- 유비쿼터스 환경에 적합한 경량 암호알고리즘 - 블록암호 알고리즘 운영모드 - 응용서비스에서의 암호 알고리즘 활용 방법
인증	- PKI (Public Key Infrastructure) - 익명 인증 - 무선망 인증	- PKI (Public Key Infrastructure) - 익명 인증 - 디바이스 인증	- 모바일 환경에서의 인증서비스 모델 및 인증기술 - 인터넷 전화 등에 이용 가능한 디바이스 인증 기술 및 응용 - 일회용패스워드(OTP) 인증 기술 및 응용 - OTP 인증 프레임워크 - 익명성을 보장하는 인증 기술 - 바이오정보를 이용한 전자서명 기술	- 다양한 인증수단에 대한 보안성 검증 프레임워크 - 디바이스 인증 기술 및 응용 - OTP 인증 기술 및 응용 - OTP 인증 시스템 보안 요구사항 - 익명성을 보장하는 인증 기술 - 바이오정보를 이용한 전자서명 기술
권한관리	- PMI(Privilege Management Infrastructure) - HW 기반 접근제어	- PMI(Privilege Management Infrastructure) - HW 기반 접근제어	- 기기 관리자 간의 권한 관리 응용 기술 - 융복합 인증 서비스 모델 - 사용자 권한관리를 위한 인증 기술 및 응용	- 기기 관리자 및 소유자간의 권한 관리 기술 - 통합 권한관리 프레임워크 및 응용 서비스 - 사용자 권한관리를 위한 인증기술 및 응용

• 중점 추진방향

- 컴퓨터와 네트워크 기술이 융합된 유비쿼터스 환경에서는 다양한 디바이스들이 활용되고 이러한 디바이스를 통해서 어느 곳에서나 정보의 소통이 용이함에 따라 작고, 경량이며, 값싸고, 이동 가능한 디바이스에 적용 가능한 암호 기술에 대한 표준화를 중점적으로 추진

- 최근 클라우드컴퓨팅을 비롯하여 스마트그리드 등 신규 융합 IT서비스가 확산됨에 따라 안전한 서비스를 제공을 위한 암호 알고리즘의 활용 방안이 중요. 이에 따라, 응용서비스 분야에서의 암호 알고리즘 활용 방안에 대한 표준화를 중점적으로 추진

- 고유의 네트워크 환경에서 점차적으로 유비쿼터스 환경으로 전환되고 있는 시대흐름에 따라서 기존에 사람위주로 수행하던 암호 · 인증 · 권한관리 기술이 인터넷 전화(VoIP), IPTV, 홈가전, CCTV 등 다양한 디바이스로 점차 확대되어 감에 따라 디바이스 인증, 경량화된 암호 기술 등 유비쿼터스 환경에 적합한 기술에 대한 표준화를 중점적으로 추진

- 최근의 불법 게시물 및 악성 댓글 등 사회적으로 문제가 되고 있는 온라인 게시문화를 개선하기 위한 정보보호 기술에 대한 관심이 점차 높아짐에 따라, 평상시에는 익명성을 보장하다가 불법 또는 악의적인 댓글 게시 시 게시자의 신원을 파악

할 수 있는 익명인증 기술에 대한 표준화 추진

- 기존 정보시스템에 대한 인증 방식이 단순 패스워드 또는 인증서 등에 한정하여 수행되었다면, 최근에는 일회용 패스워드(OTP), 바이오인식 등 다양한 인증 수단 및 방식이 혼용되어 사용되므로, 해당 기술의 지속적인 표준화와 병행하여 인증 수단별 보증수준 검증을 위한 기준 및 절차 등 검증 프레임워크 개발을 추진함

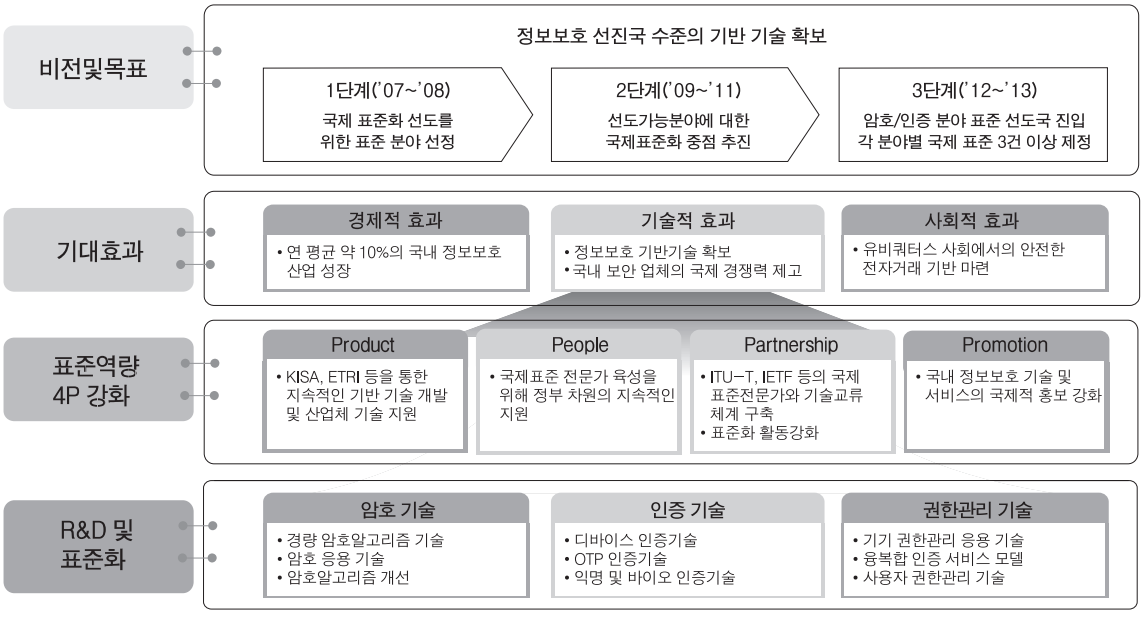
- 최근 전자금융거래의 인증방식에 대한 공인인증서 의무화 규제완화에 따라 공인인증서와 동등한 안전성을 갖는 다양한 인증방식의 도입이 검토되고 있으며, 바이오인식 기반의 인증기술 및 부인방지 기능을 추가한 OTP 등 다양한 기술개발이 진행되고 있음

- 또한, 인터넷뱅킹, 온라인증권 등 금융 분야의 안전한 전자거래 보장을 위해 기존 보안카드의 안전성을 강화한 OTP 인증기술에 대한 프레임워크 및 응용 기술 분야에 대한 표준화도 중점적으로 추진

- 유비쿼터스 환경의 발달과 함께 정보제공의 주체로 등장한 다양한 정보통신기기에 대한 식별 · 인증 및 권한관리의 중요성이 대두됨에 따라 이를 위한 표준화를 추진

- 전자정부 등 대규모 조직에서 서로 다른 인증 및 권한관리 체계를 표준화 없이 도입 · 운영하다 보니 보안수준에 따른 차별적인 관리의 어려움 및 기관별 보안 솔루션의 중복 도입 등의 문제가 발생하고 있음. 이에 다양한 정보시스템 및 서비스의 보안수준에 따른 신뢰수준 관리, 통합인증 및 정보자원에 대한 접근권한 제어, 사용이력 기록 등을 지원하기 위해 통합 권한관리 프레임워크의 표준화를 추진

1.4. 표준화의 Vision 및 기대효과



1.4.1. 표준화의 필요성

◦ 암호 · 인증 · 권한관리 분야는 인터넷상에서 안전한 정보의 전송 및 이용을 위해 반드시 필요한 정보보호 기반 기술로써 인프라 성격을 띠고 있기 때문에 정보보호 시스템의 상호호환성, 인터넷 이용자의 안전성 및 신뢰성 보장을 위해 해당 기반 기술에 대한 표준화가 필요

◦ 또한, 국제 표준화는 정보보호 제품에 대한 국제 통상 문제를 해결하는 역할을 수행할 수 있기 때문에 국내 정보보호 기술의 국제적 위상 제고 및 국내 정보보호 제품의 국내외 경쟁우위 확보를 위해 암호 · 인증 · 권한관리 기술에 대한 국제 표준화가 필요

- 암호 · 인증 · 권한관리는 정보보호에서 기반이 되는 기술이며, 다양한 IT기반 서비스에서 유통되는 정보의 기밀성, 무결성을 보장하기 위해 출시되는 정보보호제품의 국제간 호환성을 확보를 위해서는 이러한 기반 기술에 대한 표준화가 필요
- 국내에서는 암호, 인증, 권한관리 기술과 관련하여 지금까지 다양한 표준화가 이루어져 왔음. 특히 암호알고리즘의 경우, SEED, KCDSA, HAS-160 등을 포함하여 차세대 암호로서 HIGHT, FORK256 등 컴퓨팅 및 정보보호 기술의 변화에 따라 기술개발 및 표준화를 추진하여 왔음. 또한, 최근 클라우드 컴퓨팅, 스마트그리드 등 새로운 정보통신 환경에서 활용하기 위한 암호 기술에 대한 표준화가 필요
- 우리나라는 MEF(Major Economies Forum on Energy and Climate)를 통해 스마트그리드 선도국가로 선정됨. 스마트그리드 환경은 국가의 기반시설인 전력과 밀접한 연관을 가지고 있음. 따라서 보안상 심각한 문제가 발생할 경우, 전력을 사용하는 다른 시설에 막대한 피해를 초래할 수 있음. 이에 따라, 안전한 스마트그리드 환경을 구축하기 위해서는 경량화된 암호 및 인증기술에 대한 표준화가 필수적임
- 클라우드컴퓨팅 환경은 인터넷을 통해 하드웨어와 소프트웨어를 아웃소싱 형태로 공유하므로, 보안상 문제가 발생할 경우 개인 및 기업의 중요 정보가 외부에 노출될 수 있음. 따라서 클라우드컴퓨팅 환경에서 안전한 통신을 위한 암호 및 키 관리 기술의 표준화가 필수적임
- 인증기술의 경우는 국내뿐만 아니라 세계적으로 활용도가 높은 PKI 기술을 기반으로 지속적인 국제 표준화 추진이 필요함. 특히, 세계적으로 유례를 찾아보기 어려울 정도로 확산된 공인인증서 분야를 중심으로 관련 응용기술에 대한 국제 표준화 추진 노력이 필요함. 최근, 인터넷 이용확산과 맞물려 인터넷 역기능에 대한 우려가 제기되고 있어 이를 개선하기 위한 인증기술 표준화 역시 요구됨
- OTP 인증기술의 경우 해외에서는 美RSA사와 OATH(Open AuTHentication) 단체가 양립하여 기술 개발 및 표준화를 수행하고 있으나 상호연동성에 대한 고려가 없어, 다수의 OTP 기기를 사용하여야 하는 불편함이 있음. 따라서, 세계 최초로 통합인증서비스를 제공하는 국내의 OTP 통합관리 원천기술을 기반으로 세계 표준의 주도적인 추진이 가능함
- 최근 인터넷상에서 악성 댓글, 불법 게시물 등에 따른 피해가 확산됨에 따라 인터넷 역기능 예방 및 대응을 위해 익명인증 및 추적 등 다양한 기술개발 및 표준화가 요구되고 있음
- 최근 유비쿼터스 환경의 가속화로 인터넷전화, CCTV, 홈디바이스, 지능형 로봇, RFID 등 다양한 기기가 연결되어 정보제공 주체로 따라, 이들에 대한 안전성 및 신뢰성 강화를 위해 식별 · 인증 및 권한관리를 위한 표준화 추진이 요구되고 있음

• 전통적인 인증기술을 강화한 멀티팩터 인증기술의 출현 및 도입의 확산으로 이들에 대한 보안성 검증을 위한 기준 및 절차가 요구되는 한편, 다양한 정보시스템 및 서비스에 대한 보안수준에 따른 차별적인 통합인증 및 권한관리를 위한 표준화 추진이 요구되고 있음

1.4.2. 표준화의 목표

◦ 암호 기술과 관련해서는 국내에서 개발한 암호 알고리즘을 다양한 응용서비스에서 적용할 수 있는 적용표준 개발을 추진하여 2012년까지 각 분야별 국제표준 1건 보유
◦ 인증 및 권한관리 기술과 관련해서는 현재, 표준화가 미미한 분야인 익명인증, 디바이스 인증, OTP 인증 등에 대해 ITU-T 및 IETF 표준화 추진(2012년까지 국제표준 5건 보유)

• 암호기술의 경우, 국내에서 개발한 블록 암호 알고리즘, 해쉬 알고리즘, 스트림 암호 알고리즘 등에 대해 스마트그리드, 클라우드 컴퓨팅 등 새로운 정보통신 환경뿐만 아니라 신규 IT서비스에서 활용할 수 있도록 운영모드, 키 관리기술 등을 국제표준으로 추진하고, 이미 표준화되어 국제적으로 널리 활용되고 있는 기술을 국내표준으로 반영

• 인증기술의 경우, 2008년까지 익명인증 기술, 속성인증 기술 등에 대한 국내 표준화를 추진. 또한 2008년부터 익명인증 프로토콜에 대한 국제 표준을 개발하고 있으며, 2009년 8월 추적 가능한 익명인증서 기술에 대한 국제 표준화(IETF)가 완료됨. 2010년 ISO/IEC에 그룹서명기반의 익명인증기술에 대한 국제표준화가 진행중임. 또한 디바이스 인증 기술의 경우 디바이스 인증서 프로파일에 대한 국내 및 국제표준이 2008년 완료되었으며, 2009년부터는 기기인증체계의 수립을 통한 유비쿼터스 환경에 적합한 인증기술에 대한 국내 표준을 선행적으로 추진하고 2010년 이후에는 국제 표준화 추진

• 또한, 다양한 인증수단에 대한 안전성 및 신뢰성 검증을 위해 위험분석 기반의 보안성 검증 프레임워크에 대한 국내외 표준화를 추진함으로써, 다양한 서비스 환경 및 보안수준에 적합한 인증수단을 자율적으로 선택 · 도입할 수 있는 기술경쟁 환경의 조성에 기여

• OTP, 바이오인식 등 하드웨어 기반의 인증 및 권한관리 기술과 관련해서는 2009년부터 국내 표준 제정을 목표로 선행 추진하고, 2010년 이후부터 ITU-T를 통해 국제 표준화 추진 예정. 또한, 아직 국제적으로 관련 기술 표준화가 활성화 되어 있지 않기 때문에 주도적인 표준 개발을 통해 표준특허 획득에도 노력 예정

• 다양한 정보시스템 및 서비스의 보안수준에 따른 신뢰수준 관리, 통합인증 및 정보자원에 대한 접근권한 제어, 사용이력 기록 등을 지원하기 위해 행안부에서 전자정부지원사업의 일환으로 수행하는 사업을 바탕으로 통합 권한관리 프레임워크에 대한 표준화를 추진

1.4.3. Vision 및 기대효과

◦ 국내 암호 · 인증 · 권한관리 등 정보보호 기반기술에 대한 국내외 표준화 추진을 통해 국내 정보보호 기술의 이용확대 기반 마련
◦ 암호 · 인증 · 권한관리 기술에 대한 보급 확대 및 산업 적용을 통해 안전하고 신뢰할 수 있는 u-사회 구축에 기여

- 암호 · 인증 · 권한관리 기술의 경우 정보보호 제품의 기반 기술이므로 지속적인 원천기술 확보 및 표준화를 통해 해당 제품의 호환성 확보를 통한 국제 경쟁력 강화 및 국내 산업 육성에 기여
- 암호 · 인증 · 권한관리 관련 기반 기술의 경우 국제적으로 표준화가 이미 활발히 진행된 상태이긴 하지만 유비쿼터스 사회에 적용 가능한 경량화된 암호응용기술 및 인증기술의 경우 국내에서 선도가 가능하기 때문에 관련 기술에 대한 국제표준화 우선 추진을 통해 국제표준화 선점 및 IPR 확보에 기여
- u-사회에서는 다양한 형태의 정보보호 시스템이 존재하게 되므로 이러한 정보보호 제품에 적합하도록 암호 · 인증 · 권한관리 기술을 제공함으로써 안전하고 신뢰할 수 있는 u-사회 구축에 기여
- 전통적인 인증기술을 강화한 멀티팩터 인증기술의 출현으로 안전한 전자거래의 환경이 조성되어 있으며, 이를 기반으로 사용자의 편의성을 크게 개선할 수 있는 통합인증기술이 국내 기술로 선도가 가능한 상황으로, 국제 표준화 및 IPR 확보를 통해 관련 산업분야의 국제 경쟁력 확보를 기대

2. 국내외 현황분석

2.1. 시장 현황 및 전망

2.1.1. 국내 시장 현황 및 전망

가) 암호기술

- 한국인터넷진흥원(KISA)이 발간한 2009년도 국내 지식정보보호산업 시장 및 동향조사에 따르면 2009년 국내 정보보호 산업의 전체 시장규모는 8,072억으로 2008년도 7,388억원보다 9.2% 성장한 것으로 조사되어 전체적인 경제 상황이 열악한 가운데 비교적 높은 성장률을 보임

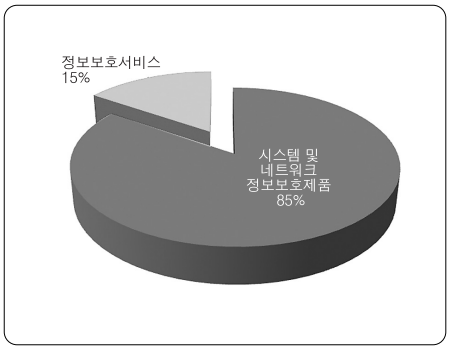
- 이 중 시스템 및 네트워크 정보보호제품은 2008년의 5,898억원보다 9.6% 증가한 6,463억원으로 나타났으며, 정보보호 서비스는 7.9%로 성장한 1,608억원으로 조사됨. 시스템 및 네트워크 정보보호제품의 전체 비중은 80.1%를 차지하였으며 정보보호서비스는 19.9%를 차지함

〈정보보호산업의 매출현황〉

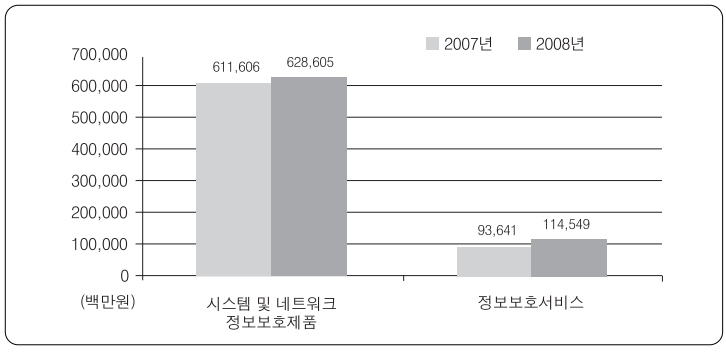
(단위 : 백만원)

구 분	2008년	2009년	증감률(%)	매출비중(%)
시스템 및 네트워크 정보보호 제품	589,850	646,373	9.6	80.1
정보보호 서비스	149,029	807,223	7.9	19.9
합계	738,879	772,412	9.2	100.0

※ 출처 : 한국인터넷진흥원, 2009 국내 지식정보보호산업 시장 및 동향조사



〈정보보호산업의 분류별 매출 비중 현황〉



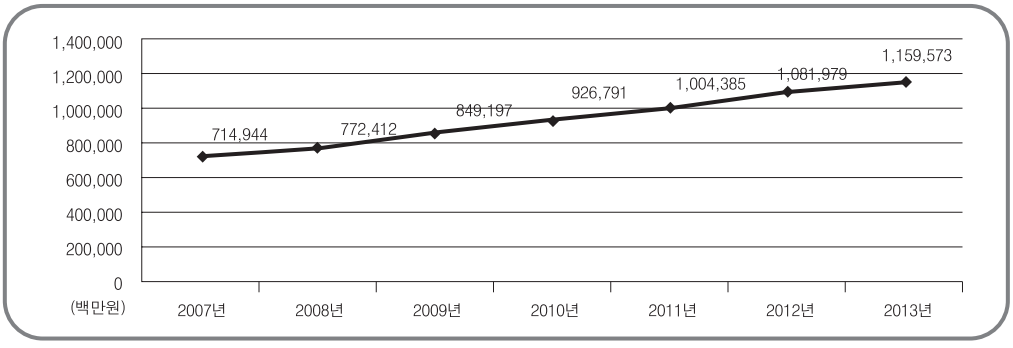
〈정보보호산업의 분류별 매출액 현황〉

- 정보보안기업의 2009년도 총 매출액은 807,223백만원으로 전년도 매출액 738,879백만원보다 68,344백만원(9.2%) 증가함. 향후 정보보안기업 전체의 매출액을 추정한 결과, 2010년도 매출액은 912,205백원까지 증가할 것으로 예산되며, 2008년부터 2014년에는 7년간의 연평균성장률(CAGR : Compound Annual Growth Rate)이 10.3%로 매출액이 지속적으로 상승하여, 2008년부터 738,879백만원에서 2014년 1,332,133백만원에 이를 것으로 전망

〈정보보호산업의 분류별 매출 전망〉 (단위 : 백만원)

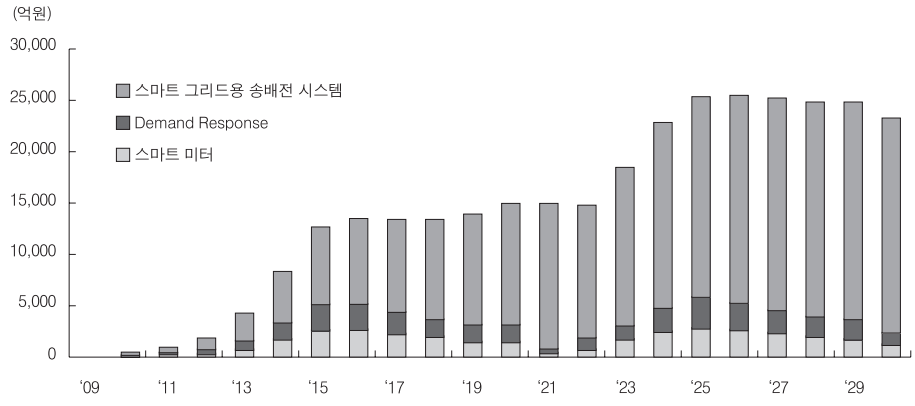
구 분	08년	09년	10년	11년	12년	13년	14년	CAGR(%)
시스템 및 네트워크 정보보호제품	589,850	646,373	736,194	826,015	915,836	1,005,657	1,095,478	10.9
정보보호 서비스	149,029	160,850	176,011	191,172	203,333	221,494	236,655	8.0
합 계	738,879	807,223	912,205	1,017,187	1,122,169	1,227,151	1,332,133	10.3

※출처 : 한국인터넷진흥원, 2009 국내 정보보호산업 시장 및 동향조사



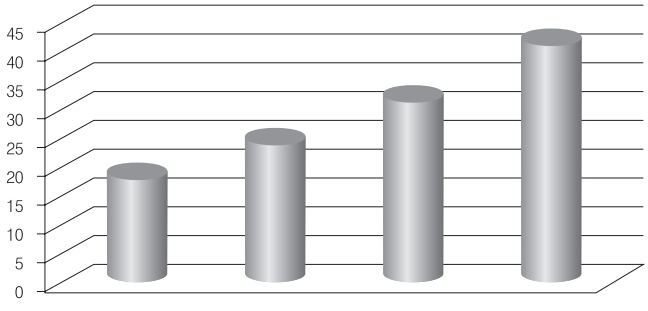
〈정보보호산업 시장 및 동향조사〉

- 정보보호제품 및 시스템에 암호 알고리즘을 탑재 · 적용하는 경우, 해당 시스템의 보안 및 안전성 수준을 만족할 수 있는 알고리즘의 종류나 키 길이 등이 선택되어야 함. 이를 위해 국가정보원 IT보안인증사무국에서는 "전자정부법" 제 27조 및 시행령 제35조에 따라, 국가 · 공공기관이 도입하는 정보보호제품에 대한 안전성 확인을 위한 보안적합성 검증제도를 시행하고 있음
  - 최근 급속도록 증가하고 있는 정보보호제품 중 암호기반 제품의 경우 국가암호정책과 직결됨을 감안하여 국가 · 공공기관 도입기준을 구체화하여 국가용 암호제품 지정제도를 신설하여 운영 중임. 암호기능을 주요 보안 기능으로 하는 제품으로, PKI 제품, SSO 제품, 디스크/파일/문서암호화 제품, 구간 암호화 제품, 메일 암호화 제품, 키보드 암호화 제품, 하드웨어 보안토큰 등이 국가용 암호제품 지정제도의 대상 제품군으로 포함됨
- 스마트그리드 관련 송배전 분야 중전기 시장 규모를 전망해 보면, 내수 시장은 2020년에 연간 1.2조원, 2030년에 2.1조원의 시장이 형성될 전망임



〈스마트그리드 중전기 내수 시장 전망, 출처 : 키움증권〉

• KT경제경영연구소에 따르면 2009년 1조 9,000억원이었던 국내 클라우드 컴퓨팅 관련 시장은, 2012년에 최대 4조 2,000억원에 달하고 연평균 약 30.3%의 증가율을 기록할 것으로 전망함



구 분	2009	2010	2011	2012	연평균증가율
시장규모	19	25	32	42	30.3%

(주)2010년~2011 수치는 CAGR 대입하여 산출 자료: KT경제경영연구소

〈국내 클라우드 컴퓨팅 시장전망〉

나) 인증 기술

• 시스템 및 네트워크 정보보호 제품의 소분류별 매출현황 중 공개키기반구조는 2008년도 매출액 37,055백만원에서 2009년도 40,711백만원으로 9.9%의 증가를 보이고, 인증제품의 경우 2008년도 매출 6,160백만원에서 2009년도 7,010백만원으로 13.8%의 증가를 보인다. 하지만 전체 시스템 및 네트워크 정보보호 제품의 매출에서 인증제품 및 공개키기반구조가 차지하는 비중은 7.4%에 불과함

〈시스템 및 네트워크 정보보호 제품의 매출 현황〉 (단위: 백만원)

구 분	2008년	2009년	증감률(%)	매출비중(%)
공개키기반구조	37,055	40,711	9.9	6.3
인증제품	6,160	7,010	13.8	1.1

※ 출처 : 한국인터넷진흥원, 2009 국내 지식정보보호산업 시장 및 동향조사

• 정보보호 서비스의 소분류별 매출 현황 중 인증서비스는 2008년 24,551백만원에서 2009년 26,548백만원으로 8.1% 증가

〈정보보호 서비스의 매출 현황〉 (단위: 백만원)

구 분	2008년	2009년	증감률(%)	매출비중(%)
인증서비스	24,551	26,548	8.1	16.5
인증제품	6,160	7,010	13.8	1.1

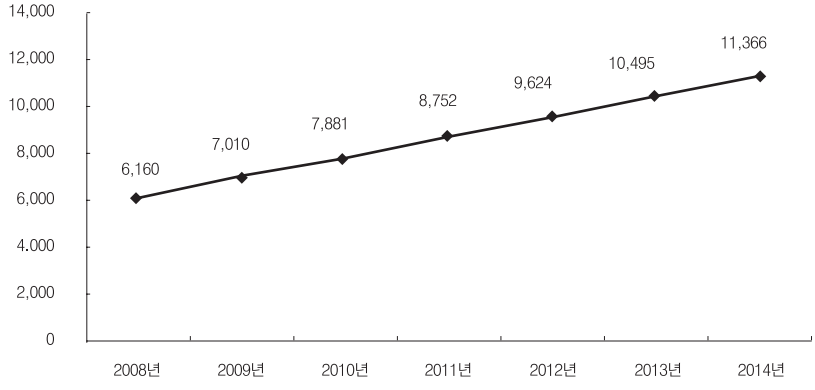
※ 출처 : 한국인터넷진흥원, 2009 국내 지식정보보호산업 시장 및 동향조사

• 인증제품의 매출액은 2009년 7,010백만원으로 850백만원(13.8%) 증가하였으며, 연평균성장률(CAGR) 10.7%로 지속적으로 증가하여 2014년에는 총 매출액이 11,366백만원에 이를 것으로 예상된다. 특히 1회 입금 규모에 따라 정해진 기준이 좀 더 맞아진 2008년 이후부터 인증제품에 대한 수요가 더 늘어난 것으로 추정됨. 금융권을 중심으로 새롭게 부각되고 있는 사용자인증 수단인 일회용비밀번호(OTP)와 더불어 H/W 토큰(HSM) 시장이 지속적으로 성장할 것으로 전망

〈인증제품의 매출 전망〉 (단위: 백만원)

구 분	2008년	2009년	2010년	2011년	2012년	2013년	2014년	CAGR(%)
보안 스마트카드	2,810	2,940	3,113	3,286	3,458	3,631	3,804	5.2
H/W 토큰	2,700	3,200	3,689	4,177	4,666	5,154	5,643	13.1
OTP	650	870	1,080	1,290	1,499	1,709	1,919	19.8
합계	6,160	7,010	7,881	8,752	9,624	10,495	11,366	10.7

※ 출처 : 한국인터넷진흥원, 2009 국내 지식정보보호산업 시장 및 동향조사



※ 출처 : 한국인터넷진흥원,
〈2009 국내 지식정보보호산업 시장 및 동향조사〉

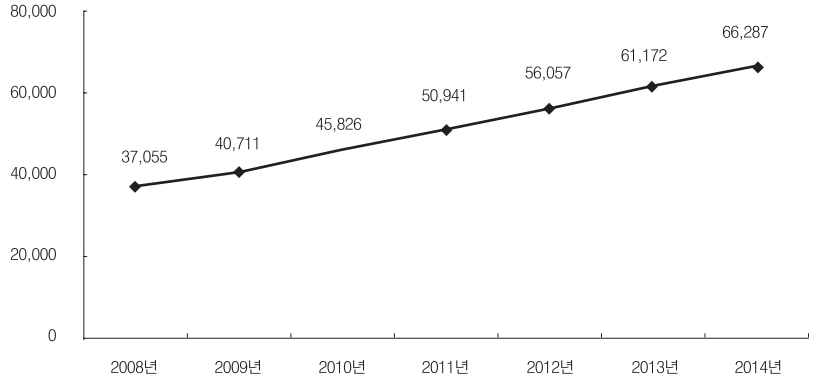
- 보안 스마트카드는 일반카드와는 달리 반도체 칩을 내장하여 방대한 양의 데이터를 저장할 수 있으며, 보안성이 뛰어나 향후 다양한 분야에서 지속적으로 활용될 것으로 전망됨. 보안 토큰 및 OTP의 경우 금융기관에서 보급단계 및 의무 시행과 같은 국가적 제도를 통해 시장이 동반 성장이 전망됨
- 1990년대 말부터 기업뱅킹을 위해 금융권에서는 OTP 기기를 도입하여 사용하였으며, 2007년도 6월말 OTP 통합인증센터가 오픈한 이후에 은행, 증권권역을 포함하여 국내 58개 금융기관에서 전자금융거래 등에 하드웨어 OTP기기를 사용하고 있음. 또한 현대자동차 및 김앤장, 기업은행 등의 기업에서도 기업내부망 접근권한 부여, 내부보안 및 사용자 인증을 위해서 OTP 기기를 이용하고 있으며 2009년 확대보급 단계를 거쳐 2010년부터는 제품 사용이 일반화 단계에 이를 것으로 예상됨
- 2008년 4월 "보안등급별 이체한도 차등화 정책" 시행에 따라 보안 1등급 매체인 OTP 발급자수는 꾸준히 증가하여 2010년 7월 OTP 기기의 발급자수가 400만명을 돌파하였으며 전자금융거래에서 OTP 인증은 계속 늘어날 전망임. 모바일 OTP의 경우엔 웹 포탈 및 온라인 게임 서비스 등에서 사용자 인증 수단으로 서비스되고 있으며, 현재 약 100만명 정도가 사용 중에 있고 계속 늘어나는 추세임
- 현재 국내 금융권에서는 OTP 통합인증센터를 구축하여 전자금융거래에 통합인증서비스를 이용하고 있으며, 향후 민간분야로의 전이가 기대됨. 한편, 공공분야에서도 정부통합인증센터를 구축하여 OTP를 포함한 다양한 인증수단을 통한 서비스를 제공하고 있음

• 공개키기반구조의 2009년도 매출액은 40,711백만원으로 2008년도 매출액 37,055백만원보다 3656백만원(9.9%) 증가하였음. 연평균성장률(GAGR) 10.2%의 성장추세를 꾸준히 유지하여 2014년도는 66,287백만원으로 예상됨. 최근 유비쿼터스 환경, 무선환경 등 다양한 분야에서 인증서 이용 등이 필요함에 따라 공개키기반구조의 시장매출이 꾸준하게 증가할 것으로 예상됨

〈공개키기반구조의 매출 전망〉 (단위: 백만원)

구 분	2008년	2009년	2010년	2011년	2012년	2013년	2014년	CAGR(%)
공개키기반구조(PKI)	37,055	40,711	45,826	50,941	56,057	61,172	66,287	10.2

※ 출처 : 한국인터넷진흥원, 2009 국내 지식정보보호산업 시장 및 동향조사



※ 출처 : 한국인터넷진흥원, 2009 국내 지식정보보호산업 시장 및 동향조사

• 무선/모바일 보안의 20098년도 매출액은 4,050백만원으로 전년도 매출액 3,057백만원에 비해 993백만원(32.5%) 증가하였으며, 연평균성장률(CAGR) 25.7%로 매년 상승하여 2014년에는 12,080백만원의 매출에 이를 것으로 전망됨. 무선/모바일 보안은 비즈니스 프로세스를 지원하는 형태로 점차 발전하고 있어 수요 증대가 확대될 것으로 예상됨

〈무선/모바일 보안의 매출 전망〉 (단위: 백만원)

구 분	2008년	2009년	2010년	2011년	2012년	2013년	2014년	CAGR(%)
무선/모바일 보안	3,057	4,050	5,656	7,262	8,868	10,474	12,080	25.7

※ 출처 : 한국인터넷진흥원, 2009 국내 지식정보보호산업 시장 및 동향조사

- 현재, 스마트폰 환경에서 지원되고 있는 인증서비스는 크게 3가지가 있음. 하나는 인증서를 활용한 뱅킹, 증권, 신용 확인, 입찰 등이며, 2009년 현재 관련 서비스 이용자는 150만명이 넘어서고 있으며 스마트폰 사용 일반화의 원년인 2010년에는 대폭 상승할 것으로 예상됨. 두번째는 게임사이트 및 기업 등에서 사용되고 있는 모바일 OTP로 가입자가 100만명을 넘어서고 있음. 마지막으로 각종 사이트의 회원 가입시 신원확인과 중복 가입 방지, 과금 등을 목적으로 사용되고 있는 SMS 인증이 있음
- 3G폰의 보급이 확산 되면서 USIM에 금융 솔루션 탑재가 되고 있으며 2010년 대용량 USIM이 출시되어 다양한 솔루션 탑재가 가능하며 대용량 USIM기반의 인증서 및 모바일 OTP관련 솔루션이 개발 중임. 그러나 방통위의 결정으로 USIM의 완전 개방이 이루어졌음에도 통신사들이 자체 규격 및 기술을 반영하여 제한을 가하고 있으므로 금융 솔루션을 개발 중에 있어 폐쇄 정책으로 이어질 수 있음. 결국, 이를 막기 위해서 USIM에 대한 부분은 반드시 표준화를 거쳐 기술 추가 및 서비스 추가가 필요한 상황임
- USIM이 활성화 되고 다양한 서비스가 USIM에 포함될 경우 교통카드, 신용카드, 각종 사용자 인증 기술 등이 휴대폰을 비롯한 다양한 휴대기기에서 구현이 되고 있음. 특히 해외에서 NFC USIM기술이 확보되어 있기는 하나 접촉 위주의 서비스인 반면, 국내에서는 교통카드처럼 비접촉으로 사용되는 경우가 많아서 이를 기반으로 한 기기간 인증까지도 향후 도입/확산될 가능성이 높음

• 2009년 바이오인식 시장은 지난해 대비 23.9% 성장한 733억원 규모를 형성하였으며, 2013년까지 14.9%의 연평균성장률(CAGR)을 기록하며 1,234억원에 달할 것으로 전망됨

〈바이오인식의 매출 전망〉 (단위: 백만원)

구 분	2008년	2009년	2010년	2011년	2012년	2013년	GAGR(%)
지문인식	54,773	68,119	78,577	89,036	99,494	109,953	14.0
안면인식	1,263	1,636	2,761	3,887	5,013	6,138	33.9
정맥인식	2,126	2,028	2,347	2,666	2,986	3,305	9.3
홍채인식	1,026	1,528	2,167	2,806	3,445	4,084	29.0
합계	59,188	73,310	85,852	98,395	110,937	123,480	14.9

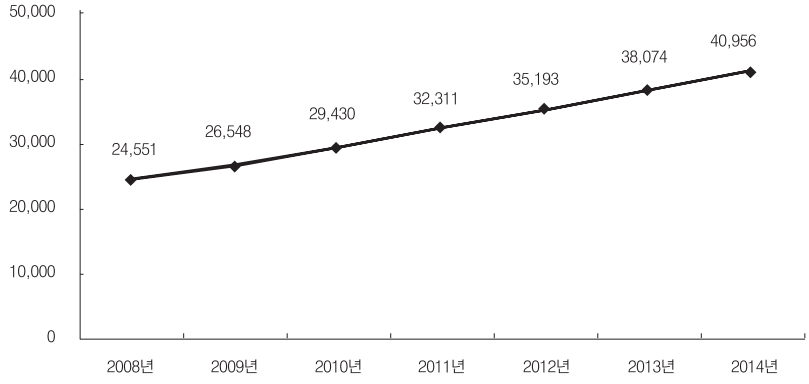
※ 출처 : 한국인터넷진흥원, 2009 국내 지식정보보호산업 시장 및 동향조사

• 인증서비스의 2009년도 매출액은 26,548백만원으로 2008년 매출액 24,551백만원보다 1,997백만원(8.1%) 증가한 것으로 분석됨. 연평균성장률(CAGR) 8.9%로 매년 성장하여 2014년도에는 40,956백만원에 이를 것으로 전망됨

- 유비쿼터스 환경에 참여하는 다양한 기기 및 정보를 위한 신뢰된 융 · 복합 인증서비스 제공이 필요함에 따라 향후 거래인증서비스, 기기인증서비스, 공인전자문서서비스의 시장 수요가 크게 증가할 전망임

〈인증서비스의 매출 전망〉 (단위: 백만원)

구 분	2008년	2009년	2010년	2011년	2012년	2013년	2014년	CAGR(%)
인증서비스	24,551	26,548	29,430	32,311	35,193	38,074	40,956	8.9



※ 출처 : 한국인터넷진흥원,

〈2009 국내 지식정보보호산업 시장 및 동향조사〉

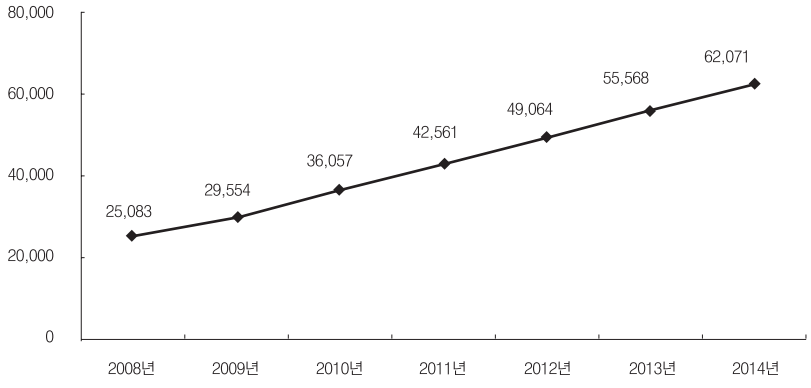
다) 권한관리 기술

• 권한관리는 개인정보보호와 기업정보보호 등이 주요시되는 보안추세에 힘입어 2009년도 매출액은 29,554백만원으로 2008년도 매출액 25,083백만원에 비해 4,471백만원(18.3%) 상승하였으며, 연평균성장률(CAGR) 16.3%로 지속적으로 성장하여 2014년에는 총 매출액 62,071백만원에 이를 것으로 예상됨

• 권한관리 시장은 개인정보보호 및 내부통제강화 이슈와 맞물려 금융기관, 공공기관, 산업기술을 보유한 기업들을 중심으로 수요가 더욱 확산될 것으로 전망됨

〈권한관리의 매출 전망〉 (단위: 백만원)

구 분	2008년	2009년	2010년	2011년	2012년	2013년	2014년	CAGR(%)
네트워크 접근제어(NAC)	10,200	12,592	15,778	18,965	22,151	25,338	28,524	18.7
통합접근관리(EAM)	1,890	1,600	1,907	2,213	2,520	2,826	3,133	8.8
싱글사인온(SSO)	5,886	5,130	5,639	6,148	6,657	7,166	7,675	4.5
통합계정관리(IM/IAM)	7,107	10,232	12,733	15,235	17,736	20,238	22,739	21.4
합계	25,083	29,554	36,057	42,561	49,064	55,568	62,071	16.3



※ 출처 : 한국인터넷진흥원,
〈2009 국내 지식정보보호산업 시장 및 동향조사〉

- 최근 홈네트워크 및 스마트 그리드 등 유비쿼터스 환경을 위한 많은 원격 기기들이 IP망 및 내부 네트워크로 연결되기 시작하면서 기기 인증 및 접근자 인증에 대한 이슈가 생겨나고 있음. 2005년에는 홈네트워크 인증 프레임워크를 ETRI에서 개발하였고 최근에는 KISA에서 기기 인증을 위한 인프라 및 표준화 작업을 진행하고 있음
  - 특히, 최근에 스마트 그리드 논의가 진행되면서 발전소 장비에서 가정의 전력량계에 이르기까지 각종 기기에 대한 원격 제어 및 통신이 필요하게 됨에 따라 이를 위한 표준이 2014년까지 정부에 의해 개발될 예정임. 특히 스마트 그리드를 비롯하여 ITS(Intelligent Transportation Systems), IBS(Intelligent Building System), SCADA(Supervisory Control And Data Acquisition) 등이 IP상에 노출될 경우 대부분이 국가 기반 설비이거나 주요 산업시설이어서 이에 대한 적절한 보안체계 구축이 필요한 상황임
  - 그러나, 현재 적용된 설비에는 권한관리가 포함되어 있지 않으며 암호화도 적용되어 있지 않음. 보안이 아예 적용 불가한 경우도 있어 개방에 있어 새로운 적용 방법 검토 및 재고와 보안체계 구축 및 권한 분리가 필요한 상황임
- 융복합 인증 서비스 시장의 경우 단순히 정보보호 서비스와 관련되기 보다는 인터넷 뱅킹과 모바일뱅킹, 인터넷 쇼핑 등 각종 전자거래의 증가와 스마트폰 등 다양한 단말기의 사용, 센서네트워크와 무선 메쉬 네트워크, 홈네트워크 서비스 등 유비쿼터스 환경을 위한 새로운 서비스의 등장으로 더욱 다양화되고 복잡화된 정보 시스템에 적응하기 위하여 융복합 인증 서비스가 적용되므로 그 시장 규모를 정보보호 서비스로 제한할 수는 없음

2.1.2. 국외 시장 현황 및 전망

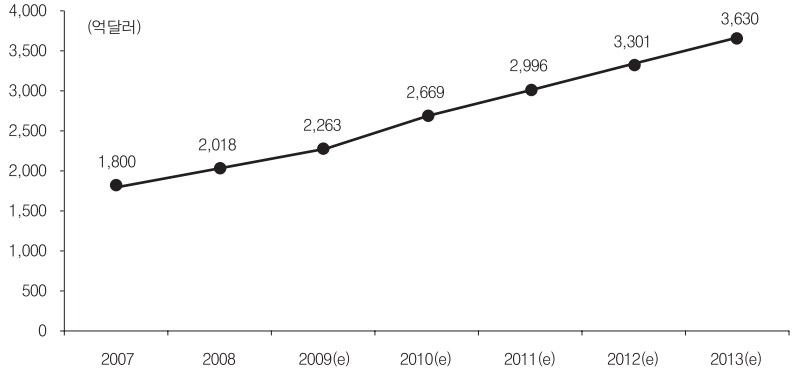
가) 암호기술

- 전자정보센터에 따르면 전 세계 지식정보보안 시장규모는 2007년 1,800억달러 규모에서 연평균 12.66% 상승하여 2013년에는 3,630억달러 규모에 이를 것으로 전망

〈전 세계 지식정보 보안시장 전망〉 (단위: 백만달러)

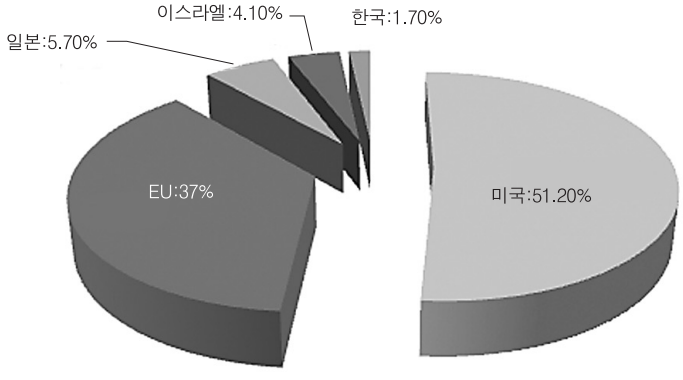
구 분	2007년	2008년	2009년	2010년	2011년	2012년	2013년	CAGR
시장규모	1,800	2,018	2,263	2,669	2,996	3,301	3,630	12.66%

전세계 지시정보 보안시장 전망(2007~2013)



※출처 : 전자정보센터, 2009

• 전세계 지식정보보안 산업은 미국과 EU 등 2개 지역이 전세계 시장의 88%를 점유하는 전형적인 글로벌 독과점 산업이며, 일본과 이스라엘이 나머지 시장을 분할하고 있음

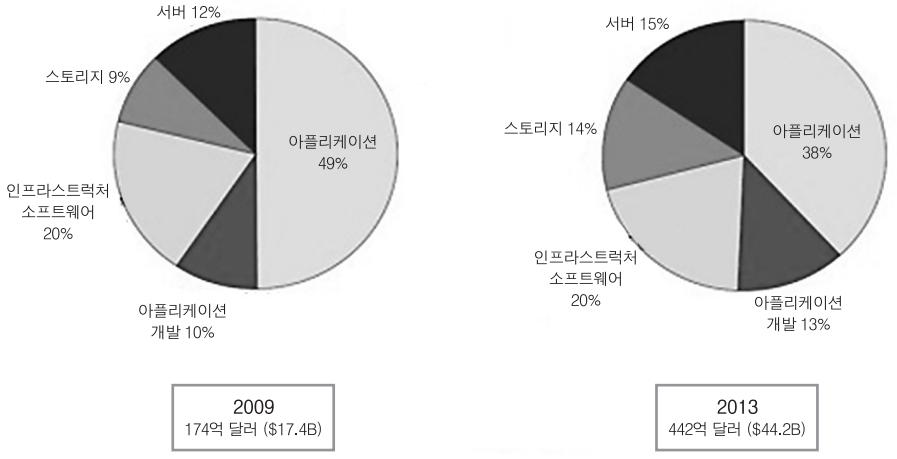


〈전세계 지식정보보안 산업 시장점유율〉

※ 출처 : 지식경제부, Securing Knowledge Korea 2013

• 최근 IDC 보고서에 따르면 미국 스마트 그리드 관련 지출액이 연평균 15.1%씩 증가, 2013년 180억 규모에 달할 것이라고 전망하며, 전력사의 사이버 보안부문 투자도 증개해 사이버 보안 시장규모는 2009년 12억 달러에서 2015년 37억 달러로 성장할 것으로 전망

• '09년 IDC 시장 보고서에 따르면 클라우드 컴퓨팅 시장은 대기업 위주로 빠른 성장을 하고 있음. IDC는 클라우드 컴퓨팅이 이제 초기 시장 형성 수준을 넘어 활성화 단계로 돌입했으며, '09년 이 시장 규모는 174억 달러에 이른다고 전함. 더불어 클라우스 시장이 향후 5년간 엔터프라이즈 시장 중심으로 고성장해 '13년에는 '09년 대비 2.5배 수준인 442억 달러 시장을 형성할 것으로 전망함



〈세계 클라우드 컴퓨팅 시장 규모〉

나) 인증 기술

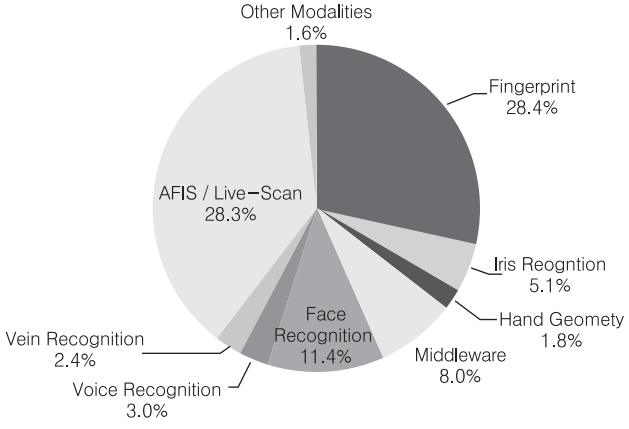
- IT 시장 조사 기관인 IDC는 세계정보보호시장 규모 및 전망 보고서인 "Worldwide and U.S. Security Services 2006 · 2011 Forecast and Analysis" 발표하였음(2008.1). 이 보고서에 따르면 2006년부터 2011년까지 세계정보보호시장은 약 15% 성장할 것으로 전망하였으며, 전자 정보 센터에 따르면 2007부터 2013년까지 세계정보보호시장은 약 12.6% 성장 할 것으로 전망함. OTP, 보안토큰 등 개인용 휴대보안기기에 탑재되는 사용자 인증 및 접근 관리(IAM) 소프트웨어는 로그온 및 패스워드 관리를 강화하여 컴플라이언스와 커버넌스 환경에서 필요로 하는 신뢰성을 제공할 것으로 전망하고 있음

- 해외에서는 국내와 같이 공인인증서 인프라가 잘 갖추어져 있거나 활용도가 높은 국가를 찾아보기 어려움. 그로 인하여 모바일 환경에서 인증서를 활용한 서비스가 지금까지 알려져 있지 않음. 그러나 RIM사의 블랙베리에서 메시지 보안을 ID기반 암호화를 적용하면서 새로운 트랜드가 생겨나기 시작함. 공개키를 비롯한 보안 프로토콜을 연구하는 분야에서는 주요 연구 과제로 자리 잡기 시작함. 그러나 국내에서는 스마트폰 사용률의 급격한 성장에 의해 모바일 공인인증서를 활용하는 서비스 분야가 현재 급격한 성장률을 보이고 있으며, 그에 대한 연구가 활발하게 이루어짐
  - 국내처럼 활발하지는 않지만 SMS 인증도 역시 널리 사용이 되고 있음. 그러나 해외의 경우 USIM의 이동성이 보장되고 있기 때문에 USIM을 활용한 특정 통신사에 의한 기능 추가나 기술 선도가 거의 이루어지기 어려운 현실임. 결국, 글로벌한 표준화의 연구와 표준 반영이 있기 전에는 새로운 기술 반영이 있기 어려우며, 동시에 필요성이 인정되면 오히려 더욱 빨리 표준화가 진행될 가능성도 높다고 할 수 있음

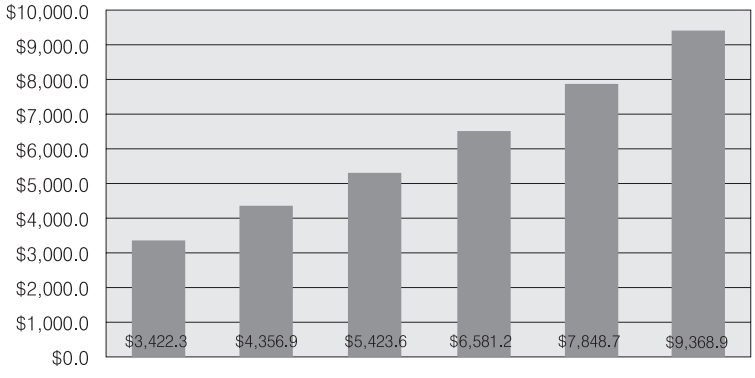
- 2002년 FFIEC(미국 연방금융기관 검사협의회)에서 발표한 인터넷뱅킹 사용자 인증 가이드라인에서 2-factor 인증 및 OTP 사용을 권고함에 따라, 미국의 BoA(Bank of America), Citibank를 비롯하여 싱가폴 HSBC, 일본, 호주, 유럽의 주요은행들이 전자금융거래에 2-factor 인증 도구로 모바일 OTP 및 하드웨어 OTP 기기를 활용하고 있음. 또한, 미 국방성에서도 사용자 인증 및 접근통제 권한 부여를 위해 OTP를 활용하고 있음. 인터넷 및 모바일 전자상거래 및 온라인 교육, 의료 서비스에서도 사용자 인증을 위해 활발히 사용되고 있으며 계속 서비스가 확대될 전망

- 싱가폴 등에서는 전자금융거래를 위한 OTP서비스를 구축중이며, 국내에서 개발하고 있는 OTP 인증 프레임워크와 유사한 모델을 구현 중에 있음. 해외 OTP 인증 프레임워크 사례들은 일반적으로 특정 벤더에 의한 단일 OTP 인증 프레임워크가 제공되고 있는 현실임. 향후 개발도상국의 전자정부나 해외 금융권에서의 강한 인증 수단으로서 OTP 인증프레임워크 및 2-Factor 인증 수단의 확대가 전망됨

• International Biometric Group의 Biometric Market and Industry Report 2009-2014에 따르면 총 매출에서 차지하는 비율이 지문인식 28.4%, 얼굴인식 11.4%, 홍채인식 5.1%, 음성인식 3.0%, 정맥인식 2.4% 등으로 조사되었음. 2009년 3,422.3백만달러 매출에서 매년 증가하여 2014년 9,368.9백만달러의 매출을 달성할 것으로 전망



〈2009년 바이오인식 기술 매출 전망〉



〈연간 바이오인식 산업 매출 전망(2009 ~ 2014)〉

※ 출처 : International Biometric Group의 Biometric Market and Industry Report 2009-2014

다) 권한관리 기술

• 2007년부터 2013년까지 세계정보보호시장은 약 12.6% 성장할 것으로 전망되고 서비스부문 매출이 연평균 17.4% 성장하여, 2006년 170억 달러 규모에서 2011년 379억 달러 규모로 증가하여 전체시장 성장을 견인할 것으로 예측

• IAM(Identity and Access Management)시장은 2011년까지 연평균 10.7% 성장할 것이며, SVM(Security and Vulnerability Management) S/W는 2006년 19억 달러 규모에서 연평균 18.4% 성장하여 2011년 44억 달러 규모로 성장할 전망

• IDC의 조사에 따르면 일본의 정보보호 시장은 정보보호 소프트웨어, 어플라이언스, 서비스 등으로 나누는데, 그 중에서 서비스 부분이 가장 많은 성장을 하는 것으로 전망하고 있음. 이것은 국내 정보보호 부분에서도 마찬가지이며 최근에 정보보호 소프트웨어 보다는 보안관제 등과 같은 서비스 부분이 많이 강화되고 있는 것이 그 예임

〈각 국가별 GDP 대비하여 정보보호 시장 규모〉

(단위 : 백만 엔)

구 분	Hardware	Software	Service	합계	GDP 대비 시장규모
세계	13,598	7,346	17,170	38,114	0.08%
미국	5,837	3,333	8,449	17,619	0.13%
일본	356.5	1,623	5,016	6,995.5	0.16%

2.2. 기술개발 현황 및 전망

2.2.1. 국내 기술개발 현황 및 전망

가) 암호기술

• 유비쿼터스 환경에 적합한 경량 암호알고리즘

- 900MHz RFID 기술의 경우, ETRI, 삼성전자 등에서 수동형 태그칩을 리더칩을 개발하였으나(2007년), 보안 기술이나 경량 인증 기술이 포함되어 있지 않음. 그러나, ETRI에서는 AES 모듈을 수동형 RFID 태그칩에서 사용이 가능할 정도의 저전력 설계/구현을 완료하였으며(2006년), 이를 수동형 RFID 태그칩에 내장하여 경량 인증 및 암호를 수행할 수 있을 것으로 전망함
- RFID/USN같은 유비쿼터스 환경에 적합하도록 암호 설계부터 경량을 고려하여 만들어진 암호로는 국내 HIGHT(HIGh security and light weigHT) 64비트 블록암호 알고리즘이 있으며(2005년), 2006년 12월 TTA 표준으로 제정되었으며, 2009년 6월 ISO/IEC 국제 블록 암호 알고리즘으로 표준화를 추진 중에 있음
- 상기와 같이 유비쿼터스 환경에 적합한 경량 암호알고리즘에 대한 기술개발 경향은 기존의 암호 알고리즘은 구현 설계 관점에서 저전력화하는 방향과 원천적으로 경량 디바이스에 적합하도록 새로운 암호 알고리즘을 설계하는 방향, 이렇게 두 가지 방향으로 진행 중에 있음

• 블록 암호알고리즘 운영모드

- 국내에서는 2000년 초부터 128비트 키 길이를 지원하는 128비트 SEED 암호 알고리즘과 128/192/256 비트의 키를 지원하는 128비트 ARIA 암호 알고리즘을 개발하여 민간 · 정부의 전자성거래, 금융, 무선통신 등에 활용됨. 최근에는 RFID 및 USN과 같은 초경량 구현 환경에 적합한 블록암호의 개발이 관심을 끌고 있는데, 국내에서 그러한 목적으로 개발된 블록암호 HIGHT가 개발됨
- 이렇게 국내에서 자체 개발한 블록 암호알고리즘을 다양한 보안프로토콜에서 활용할 수 있도록 NIST(National Institute of Standards and Technology) 에서 정의한 운영모드 기반으로 하여 활용하는 방안을 마련하고 있음

• 응용서비스에서의 암호 알고리즘 활용 방법

- 원천기술인 암호 알고리즘을 개발하는 한 후에 개발한 블록 암호 알고리즘의 활성화 제고를 위해 VoIP, IPTV, 클라우드컴퓨팅, 스마트그리드, 텔레매틱스, RFID/USN 등 다양한 서비스 및 인프라에 적용할 수 있는 활용 방안을 마련하고 있음
  - VoIP 기술은 음성통화를 IP망을 통해서 이용하는 새로운 통신기술로 인터넷을 통해 전송되는 데이터를 도청하거나 다른 사용자의 계정으로 무료 통화를 하는 등 보안위협이 발생 할 수 있음. 이에 VoIP 환경에서 안전한 통신을 SRTP(Secure Real-time Transport Protocol)에서의 SEED 암호 알고리즘을 활용할 수 있는 방법을 개발함
  - IPTV 기술은 IP망을 통해 방송이나 통영상 콘텐츠, 정보 등을 TV와 이동 단말에 제공하는 통신/방송 융합 서비스로서, 기존의 인터넷 망에서 발생할수 있는 도청, 데이터 위변조, 비인가자의 데이터 사용 등의 보안위협에 취약함. 이에 IP망에서 전송되는 데이터가 안전하게 전송될 수 있는 보안기술의 개발이 필요하므로 이러한 응용 서비스를 고려한 SEED 암호 알고리즘 활용 방법을 개발하고 있음
  - 스마트그리드 기술은 IT 기술과 전력망 기술을 결합한 통신/전력 융합 서비스로서, 기존의 인터넷 망에서 발생할 수 있는 도청, 데이터 위변조, 비인가자의 데이터 사용 등의 보안위협에 취약함. 이에 IP망에서 전송되는 데이터가 안전하게 전송될 수 있는 보안기술의 개발이 필요하므로 이러한 응용 서비스를 고려한 보안 기술이 연구되고 있으나, 아직 초기 단계임
  - 클라우드컴퓨팅 기술은 인터넷을 통해 하드웨어와 소프트웨어를 아웃소싱 형태로 공유하는 것으로, 여러 대의 단말을 통해 분산형 컴퓨팅 환경을 구축하는 개념임. 정보 및 자원이 네트워크상에 분산되어 존재함에 따라 외부로부터의 공격에 항상 노출되어 있음. 이에 IP망에서 전송되는 데이터가 안전하게 전송될 수 있는 보안기술의 개발이 필요하므로 이러한 응용 서비스를 고려한 보안 기술이 연구되고 있으나, 아직 초기 단계임

나) 인증 기술

• 다양한 인증수단에 대한 보안성 검증 프레임워크

- 전자금융거래 등 사이버 환경에서 이용자 및 거래행위 등에 대한 인증 강화를 위한 요구사항의 증가에 따라 다양한 인증수단이 개발 및 적용되고 있음. 날로 발전하는 해킹기술 등으로 단일 인증수단만으로 모든 보안 요구사항을 만족하기 어려우므로 여러 인증수단을 조합하여 적용하는 것이 필요하지만, 이들간 보안수준을 객관적으로 검증하기 위한 프레임워크의 부재로 인해 적절한 인증수단의 선택 및 객관적인 검증이 어려운 상황임

• 디바이스 인증 기술 및 응용

- 최근 유비쿼터스 환경 가속화로 사람뿐만 아니라 인터넷전화, CCTV, 홈디바이스, 지능형 로봇, RFID 등 다양한 기기가 네트워크를 통해 연결됨에 따라 기기가 서비스 주체로 등장하고 있어 행정안전부 및 인터넷진흥원을 중심으로 이들 기기에 대한 신뢰된 기기인증체계가 2009년 말에 추진되어 유비쿼터스 환경에 적합한 인증기술 및 제도 연구 등 향후 다양한 디바이스에서 인증서비스 제공을 위한 신뢰된 인증체계 구축을 위한 사업을 추진 중에 있음
- 디바이스 인증기술은 제조되는 임베디드 기기의 수량 및 특성을 고려하여 집중형, 분산형과 같은 인증체계의 구축이 고려되어야 함. 디바이스 인증을 위해 디바이스 인증서에 대한 프로파일 경량화, 디바이스 인증서를 등록하고 발급하는 기술, 디바이스 인증서와 개인키를 디바이스에 주입하고 관리하는 기술, 디바이스 내에 탑재되어 있는 디바이스 인증서를 자동으로 갱신 또는 재발급하는 기술, 디바이스 인증서 검증을 위한 검증의 경량화 및 상태검증의 경량화 및 암호 프로토콜의 경량화 등이 진행되고 있음

• 일회용패스워드(OTP) 인증 기술 및 응용

- 국내에서는 (주)미래테크놀로지사가 하드웨어 OTP 기기를 생산 및 판매하여 국내 금융권 등에 납품하고 있으며, (주)이니텍, (주)에이티솔루션 등에서 리니지게임, 싸이월드, 한게임등의 국내 주요 온라인 게임 및 포탈사이트에 모바일 OTP 서비스를 제공하고 있음
- 전통적인 일회용패스워드 인증기술을 확장하여 보안성을 강화하는 새로운 형태의 OTP 보안기술이 금융보안연구원과 국내 OTP 업체를 중심으로 지속적으로 개발되고 있음. 거래정보와 연계하여 거래서명을 하는 거래연동 OTP, 부인방지 기능을 제공하는 OTP, USIM 기반 OTP 등의 다양한 응용기술 개발 및 관련 시제품 개발이 진행되고 있음
- 최근에는 USIM을 이용한 모바일 OTP에 대한 기술개발이 진행되고 있으며, 하드웨어 OTP에 준하는 보안성과 휴대성을 동시에 만족시킬 수 있어 이동통신사 및 OTP 업체간의 합종연횡이 조만간 가시화될 것으로 보임
- 시각장애인을 위한 보이스 OTP 기술, 바코드와 모바일 OTP를 결합한 결제 솔루션 등 OTP를 응용한 기술 및 서비스 개발이 활발히 이뤄지고 있음

• 일회용패스워드(OTP) 인증 시스템 보안 요구사항

- 2007년 금융보안연구원의 OTP통합인증센터가 구축된 이후로 OTP 통합인증을 위한 프레임워크 표준 개발이 진행되어 오고 있으며, OTP를 활용하여 인증서비스를 제공하는 인터넷 서비스 제공자, OTP 업체등을 대상으로 한 OTP기기 및 인증시스템의 보안 요구사항에 대한 지속적인 표준 기술 개발이 진행되고 있음

• 익명성을 보장하는 인증 기술

- 최근 인터넷상에서 악성 댓글, 불법 게시물 등에 따른 피해가 확산됨에 따라 인터넷 역기능 예방 및 대응을 위해 다양한 기술 개발의 필요성이 대두되고 있음. 이를 위해, 기본적으로 인터넷 게시판 등에서 익명성을 보장하면서 범죄 등의 수사 목적으로 해당 게시자의 신원을 확인할 수 있는 익명인증기술에 대한 요구가 증가되고 있음
- 인터넷 실명제에 적용할 수 있는 익명 인증뿐만 아니라 무선 인터넷에서 간편하게 사용할 수 있는 인증방법들에 대한 연구가 필요할 것으로 전망
- 현재, 익명 인증은 ETRI와 산학공동으로 그룹서명 기반의 익명ID 기술이 연구개발 중으로 익명ID 발급을 위해 공개키 기반 구조가 사용되고 있으며, 익명 인증 기술 및 서비스 등이 학술적인 단계에서 연구가 이루어지고 있으나, 상용 서비스는 이루어지고 있지 않음. ETRI의 익명인증기술은 익명인증인가 암호프리미티브 실용화 설계, 안전성검증 및 구현이 완료하였고 익명암호 프리미티브기반 익명인증인가(PKI) 시스템 핵심요소 기술개발 및 실용화 가능성 검증 완료하였음
- 2008년부터 한국인터넷진흥원에서 익명인증서 프로파일에 대한 국제 표준화를 IETF PKIX WG에서 추진하여 2009년 8월에 IETF 표준으로 채택(RFC 5636: Traceable Anonymous Certificate)되었음
- 최근 인터넷상에서 악성 댓글, 불법 게시물 등에 따른 피해가 확산됨에 따라 인터넷 역기능 예방 및 대응을 위해 다양한 기술 개발의 필요성이 대두되고 있음. 이를 위해, 기본적으로 인터넷 게시판 등에서 익명성을 보장하면서 범죄 등의 수사 목적으로 해당 게시자의 신원을 확인할 수 있는 익명인증기술에 대한 요구가 증가되고 있음
- 한국인터넷진흥원(KISA)에서 가명 기반의 추적 가능한 익명인증서 이용 기술에 대한 국내(TTA, 2008년)/국제(IETF, 2009년) 표준화 제정
- ETRI는 익명성 제어가 가능한 그룹서명 기반의 익명인증 기술을 연구개발 중이며 이는 웹 인증 · 인가 및 전자상거래 과정에서 불법적 개인정보 수집유출 및 행적 추적을 막고, 법 · 제도 변화에 유연하게 대응가능한 프라이버시 증강형 암호 원천 기술로써 기존에 연구차원으로 진행되어온 그룹서명 기술들에 비해 다양한 실제 서비스에 적용 가능한 연구 진행

중. 또한, 실제 서비스에 적용할 수 있는 수준의 요구 사항 도출을 통하여 익명 인증 기술의 실용화 및 국내외 표준화 추진 (TTA, ITU-T, ISO/IEC)

• 바이오정보를 이용한 전자서명 기술

- 바이오정보에 기반을 둔 전자서명 키 생성 및 전자서명 알고리즘이 연구되고 있음. 하지만 아직 바이오정보를 이용한 전자서명 키 생성 기술은 초기 연구단계로서, 기술적인 측면에서의 안정적인 구현 가능성 및 안전성 평가방안 등의 개발이 필요

다) 권한관리 기술

• 기기 관리자 및 소유자간의 권한관리 기술

- 유비쿼터스 환경 하에서의 서비스 주체로 등장한 기기에 대해 2009년부터 기기인증서가 발급되어 이용되고 있으며, 기기를 이용하는 기기 소유자 또는 기기를 실질적으로 관리하는 관리자에 대한 권한관리 기술이 요구됨. 기기인증서의 경우 신원확인 후 기기관리자에 대해 인증서가 발급되며, 기기인증서와 연관되어 관리되도록 하고 있으나, 기기 관리자 및 소유자에 대한 권한관리 기술은 현재 연구되고 있으나 아직 초기 단계임

• 통합 권한관리 프레임워크 및 응용 서비스

- 최근 행안부에서는 다양한 정보시스템 및 서비스별로 보안수준에 따른 차별적인 관리 및 행정서비스 연계성 강화를 위해 통합인증 및 권한관리체계의 구축 · 운영을 추진하고 있음. 이를 통해 서비스 수준에 따른 신뢰수준 및 계정관리, 통합인증 및 정보자원에 대한 접근권한 관리, 사용이력 기록 등을 지원할 예정으로, 2009년 시범서비스 구축을 통해 2012년까지 전자정부는 물론, 전체 행정 · 공공분야에 도입을 추진하고 있음
- 즉, 서비스 및 보안수준에 따라 범정부 차원의 단일인증(SSO) 및 권한관리체계가 도입될 것으로 예상되며, 성공적으로 추진되면 민간분야에도 확산될 수 있을 것으로 기대됨

• 사용자 권한관리를 위한 인증 기술 및 응용

- 공개키 기반구조에서 사용되는 인증서는 상대방의 신원확인을 위한 기능은 지원하지만, 임무, 지위, 역할 등과 같은 다양한 속성에 대한 정보를 기반으로 하는 인증 기능의 제공에는 한계가 있음. 이에 따라, 공개키 기반구조와 함께 권한, 임무, 지위, 역할 등의 속성정보에 대한 인증을 제공하는 별도의 기반구조가 필요하게 되었음
- 2001년부터 PMI 모델 등을 개발하는 등 속성 정보를 안전하게 생성, 관리, 검증할 수 있는 방법에 대한 연구가 활발히 진행되어 옴. 현재 PMI 기능들은 접근제어 제품, EAM, 포털 관리 및 e-비지니스 시스템 등에 끼어 들어가는 형태로 동작하고 있지만, 앞으로는 XML 기반으로 발전할 것으로 전망. XML 기반은 단기적으로 거래 당사자 및 사업 파트너 간 정보 접근을 위하여 문법, 구문 등에 대한 동의가 이루어지고 장기적으로는 XML 표준화를 통하여 한층 더 역동적 사업 관계가 가능하도록 지원할 것임

2.2.2. 국외 기술개발 현황 및 전망

가) 암호기술

• 유비쿼터스 환경에 적합한 경량 암호알고리즘

- 컨테이너에 적용되는 능동형 RFID 보안을 위하여 미국의 Savi, 컴 등의 회사가 컨테이너 보안 시스템 개발을 주도하고 있음. 그러나, 여기에 사용되는 보안 기술은 새로운 경량 암호알고리즘이라고 보기는 어려우며, 기존의 다양한 표준에서

사용을 권고하고 있는 암호 알고리즘을 경량 구현하여 적용하고 있음

- VeriSign은 RFID 정보를 안전하게 저장할 수 있는 Secure EPC network 인프라를 개발 진행 중이나, 이는 인프라 네트워크 측면에서 보안이라 경량 암호를 사용하지는 않을 것으로 전망됨
- TI(Texas Instruments)사에서 자체적인 경량 대칭키 암호 알고리즘을 사용하여 DST RFID 태그칩을 개발하였으나, RSA security사와 Johns Hopkins 대학 등에서 이에 대한 취약성을 보고하였음
- USN 환경에서는 TinyOS기반의 TinySec 및 TinyECC에 대한 연구가 진행 중이며, 주로 ECC 암호 알고리즘은 저가의 USN 센서 노드에서 구현 가능하도록 경량 구현설계를 하였음

• 블록 암호알고리즘 운영모드

- NIST에서는 다양한 IT환경에서 블록암호를 활용할 수 있는 운영모드를 개발 중이며, 현재까지 정의된 운영모드에는 ECB, CBC, OFB, CFB, CTR, CCM, GCM, XCBC 등이 있음
  ※ ECB(Electronic Code Book), CBC(Cipher Block Chaining), OFB(Output FeedBack), CFB(Cipher FeedBack), CTR(Counter), CCM(Counter with CBC-MAC), GCM(Galois/Counter Mode), XCBC(eXtended Cipher Block Chaining mode)

• 응용서비스에서의 암호 알고리즘 활용 방법

- 미국, 일본, 유럽의 일부 선진국들은 NIST, NTT, ECRYPT 등을 기반으로 AES, Camellia, Blowfish 등 암호 알고리즘 개발하였으며, 네트워크 장비, 시스템 운영체제, IPsec 등의 어플리케이션에 적용 할 수 있도록 암호 알고리즘 탑재 제품 및 시스템에 대한 개발을 추진하고 있음
  ▫ 미국의 경우, NIST를 기반으로 암호 알고리즘이 활용 될 수 있도록, AES, 3TDES(Triple DES) 등이 탑재된 제품을 개발. TLS, S/MINE, IPsec, IEEE 802.11i 등에 적용될 수 있도록 기술을 개발하여 IETF, ISO/IEC, IEEE, ESTI 등에서 국제 표준화를 추진 중임
  ▫ 일본의 경우, 3GPP의 UMTS(Universal Mobile Telecommunication System), SSL/TLS, S/MINE 등에서 Camellia, KASUMI, MISTY1 등의 알고리즘이 활용될 수 있도록 하였으며, 국외에서 활용될 수 있도록 ISO/IEC, ITEF 등의 국제 표준화를 추진 중임

나) 인증 기술

• 다양한 인증수단에 대한 보안성 검증 프레임워크

- CC(Common Criteria) 등 일반적인 정보시스템에 대한 보안성을 평가하기 위한 기준 및 절차는 존재하지만, 사이버 상에서 이용자 및 거래행위 등에 대한 인증을 위한 수단에 특화된 보안성 검증 및 선택을 위한 지침은 미흡한 상황임
- 전자금융거래 등 온라인상에서의 다양한 유형의 거래행위가 증가함에 따라 인증수단에 대한 요구사항도 증가하는 추세이므로, 이들간 보안수준을 정의 및 검증할 수 있는 프레임워크의 수요 및 중요성도 증가하고 있음

• 디바이스 인증 기술 및 응용

- 미국의 경우, VeriSign사가 케이블모뎀과 케이블모뎀 터미네이션 시스템 간의 기기인증을 위해 PKI기기인증서를 발급하고, 케이블모뎀 터미네이션 시스템은 케이블모뎀이 제출한 케이블모뎀 PKI기기인증서를 검증하여 케이블모뎀이 정당한 기기인지를 확인하는 모델이 서비스 중
- 케이블모뎀 인증을 위한 PKI기기인증서 프로파일 및 관련된 규격은 케이블모뎀 업계표준인 Data Over Cable Service

Interface Specification(DOCSIS)에서 정의하고 있으며, 케이블모뎀 PKI 기기인증서는 케이블모뎀 내 비휘발성 메모리 내 보안영역에 저장되고 이용됨

- 액시스 및 소니 등의 CCTV 제조업체는 네트워크 카메라의 디바이스 인증을 위해 PKI 기기인증서를 이용하고 있으며, 카메라의 PKI 기기인증서를 통해 화상정보에 대한 전자서명을 생성 · 전송하여 해당 카메라를 인증하고, 이미지 위 · 변조여부를 확인
- 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 중. WiMAX 관련 단말기 제조사는 WiMAX 포럼으로부터 기기 형식승인 획득한 후, VeriSign사로부터 기기인증서를 발급

• 일회용패스워드(OTP) 인증 기술 및 응용

- 국외의 경우 RSA사, VASCO사, ActiveIdentita사, Incard사, Idenetita사, Toppan Forms사 등에서 카드형 및 토큰형 OTP기기, 모바일/소프트웨어 OTP를 개발하여 미국, 유럽, 일본, 홍콩 등의 금융권과 기업 내부망 접근, 전자상거래, 유무선 통신 접속 및 사용자 인증 등에 서비스 하고 있음
- 영국 등 유럽지역의 금융기관을 대상으로 EMV(Europay, Master Card, VISA Card) 등이 연합한 지급결제 표준인 CAP(Chip Authentication Program) 기술의 이용이 점차적으로 확대되고 있음. 해당 표준기술은 수신자 계좌번호, 거래금액 등의 거래정보와 OTP 정보를 연계한 인증기술로서 사용자 PC가 해킹된 상태에서도 안전하게 이체 및 결제할 수 있는 특징이 있음

• 일회용패스워드(OTP) 인증 시스템 보안 요구사항

- OTP 관련된 인증 프레임워크의 개발은 주로 표준화 단체에서 개발되고 있으며, VeriSign 등이 참여하고 있는 OATH(Open AuTHentication) 단체에서 OTP를 포함한 PKI 공인인증서, 바이오 인증에 관련된 서비스를 통합하는 구조인 OATH 레퍼런스 아키텍처라는 범용인증 프레임워크를 개발하고 있음
- 또한, OTP 인증 프레임워크에 대한 개발이 국내 금융보안연구원에 의해 2008년부터 ITU-T의 안전한 응용서비스(Q7/SG17)분야에서 추진되고 있으며, 2010년 말에 X.sap-3 최종 표준 제정을 목표로 하고 있음

• 익명성을 보장하는 인증 기술

- 전자투표는 대표적인 익명성을 보장하는 인증기술 응용으로써 누가 누구에게 투표하였는지 익명성이 보장되어야 하며, 투표자는 한번만 투표할 수 있도록 인증되어야 함. 투표자의 익명성 노출과 투표결과의 조작이 가해질 수 있다는 우려를 불식시키기 위해 무기명 비밀투표를 보장할 수 있는 전자투표시스템을 구축하여 누가 누구를 선택했는지 알 수 없도록 설계해야 하며, 외부로부터의 개입을 기술적으로 차단할 수 있도록 설계되어야 함
- 전자투표는 투표소 전자투표(Poll Site E-Voting), 키오스크 방식의 전자투표(Kiosk E-Voting), 원격 인터넷 투표(Remote Internet E-Voting)로 구분됨. 전세계적으로 30여개 국가가 전자투표를 실시하고 있으며, 투표소 전자투표(PSEV), 원격 인터넷 전자투표(REV) 방식을 적용하여 사용함
- 미국은 Dan Boneh 등을 중심으로 한 익명암호이론 연구 및 미래 인터넷을 위한 익명네트워크 기술연구(FIND)를 진행, EU는 IDEMIX, PRIME 등 프로젝트로 익명 크리덴셜 기반의 익명인증기술에 대한 연구를 수행하고 있음
- ISO는 JTC1 SC27 WG2(Anonymous Authentication)에서 그룹서명 기반의 익명인증 표준화를 추진하기로 의결하고(2009년 10월), TCG는 익명으로 TPM 기기를 인증하는 기술 표준화가 진행 중임
- 익명성을 보장하는 인증 기술은 조건부 추적성을 제공하는 그룹 서명 중심으로 연구되어 옴. 특히 2004년 Stanford대학

에서 VSC(Vehicle Secure Communication)에서 요구하는 통신량을 만족할 수 있는 수준의 짧은 그룹 서명 기법 등을 연구한 바 있으며, IBM에서 제안한 익명 인증 기법은 TPM Group의 DAA(Direct Anonymous Attestation)에 적용됨

- 현재는 관련 기술의 상용화를 위해 익명 인증을 제공하면서도 연산량과 통신량을 줄이기 위한 방법, 익명성을 제어하는 방법, 유효하지 않은 키에 대해 효율적으로 키를 폐기하고 이를 확인할 수 있는 방법 등에 대해 연구가 진행되고 있음

• 바이오정보를 이용한 전자서명 기술

- Mytec Technology에서 개발한 Bioscrypt는 기존의 특징점 중심의 지문인식 알고리즘에 비해 푸리에 변환과 Biometric encryption, 해쉬 과정을 추가한 독창적인 알고리즘을 개발, 다양한 응용분야를 제공하고 있음. 특히 이 알고리즘은 바이오 정보를 바탕으로 하여 일종의 키 정보를 유도할 수 있음. Bioscrypt 기술인 경우 지문정보에 대한 입력 후 키를 생성하지만, Bioscrypt 기술은 사용자 인증 및 메시지 인증부분이 취약하기 때문에 이를 개선한 새로운 전자서명 키 생성 기법이 필요함
- AK Jain, S. Prabhakar, L. Hong, and, S. Pankaniti에 의해 개발된 Fingercode는 J. Daugman 박사의 Iriscode를 모티브로 하여 생성된 것으로 지문의 융선방향을 각도에 따를 마스크를 이용하여 정보를 추출해 내는 방법이 있음. 이에 추가적으로 Peter Orvos가 제안한 바이오 인식 기술과 전자서명의 연계방법이 연구되고 있음. 이것은 공개키 기반 구조를 바탕으로 스마트카드에 저장된 Fingercode를 이용하여, 숨겨진 개인키 정보를 복구하도록 하는 방법임
- 2001년 Janbandhu와 Siyal이 제안한 바이오인증 전자서명 방식은 RSA와 DSA 공개키 기반 전자서명 알고리즘을 사용하는 기법에 해당함. 특히, John Daugman의 IrisCode에 근간하여 512바이트의 바이오 인식 데이터를 가정함. 하지만 바이오 인식 샘플에서 비롯되는 정보가 결정적이거나 혹은 충분한 오류정정을 통하여 결정적인 값으로 항상 복원될 수 있도록 가정하고 있음. 따라서 현실적으로 구현하는 데는 많은 어려움이 있는 기법이라고 할 수 있음
- 2002년 R. Nagpal과 S. Nagpal에 의해 제안된 바이오 인식 전자서명은 RSA 알고리즘에 기초하고 있음. 특히, 이 기법은 사용자의 망막, 홍채, 그리고 지문 등 세 가지 바이오정보를 이용하는 다중 바이오 인식 방식임. 따라서 다양한 입력장치를 요구하게 됨

다) 권한관리 기술

• 기기 관리자 및 소유자간의 권한관리 기술

- 케이블 모델 등에 이용되는 기기인증서는 기기에 대한 관리자가 웹 포털에 로그인 후, 기기에 대한 인증서를 발급받도록 하는 등 발급절차 권한에 대해서 언급되고 있음. 하지만, 기기에 탑재된 인증서가 주로 기기 간의 암호화 통신, DRM, 기기 자체에 대한 인증 등에 이용되기 때문에 기기 관리자 및 소유자에 대한 권한관리 기술은 아직 연구가 미진한 상태임

• 통합 권한관리 프레임워크 및 응용 서비스

- 전통적인 인증기술을 강화한 멀티팩터 인증기술의 출현으로 안전한 전자거래 및 결제를 위한 환경을 조성하고 있으며, 이를 기반으로 사용자의 편의성을 크게 개선할 수 있는 통합인증 및 권한관리의 필요성이 증가하고 있음. 국내외적으로 SSO로 대표되는 인증 및 권한관리 솔루션이 도입되고 있으나, 표준화 수준은 미흡하여 단일 도메인 내에서만 적용되고 있음. 특히, 보안수준에 따른 차별적인 인증 및 권한관리 부분은 중요성에 비해 기술개발 및 보급 수준은 미흡한 상황임

• 사용자 권한관리를 위한 인증 기술 및 응용

- 국외의 PMI 관련 제품개발은 국내에 비해 많이 활성화되어 있으나, 아직 많은 정보보호업체에서 제공하고 있는 권한관리 기능이 국내와 마찬가지로 기존의 PKI를 확장하거나 PMI 관련 기술을 자사에 커스터마이징하여 적용하고 있음

- 그러나 일부 업체에서 제공하는 PMI 제품은 국제 표준을 정확히 준수하고 있으며, 다른 업체들도 점차 이러한 표준화를 준수하고 있음. 이미 선도적인 다국적 정보보호업체의 경우에는 PMI관련 표준을 준수하는 제품들을 개발하여 여러 업계에 공급하고 있으며 현재 이러한 권한 관리 제품을 다른 보안 솔루션과 통합한 제품을 집중적으로 연구 및 개발을 하고 있음
- PMI 관련 제품으로서는 Baltimore Technologies사의 SelectAccess, Entrust Technologies사의 Entrust GetAccess, RSA Security사의 ClearTrust, Netegrity사의 SiteMinder 등이 있음

2.2.3. IPR 보유현황 및 확보가능분야

가) 암호기술

• 유비쿼터스 환경에 적합한 경량 암호알고리즘

- 국내 경량 암호 기술 관련 특허 출원은 ETRI, KISA, 고려대학교 등에서 경량 암호 구현설계 및 경량 암호 알고리즘에 대한 특허를 확보하고 있으나, 전체적으로 IPR 보유가 미비한 상태임. 그러나, RFID/USN 환경이 점차 확대됨에 따라, 경량 암호 기술에 대한 IRP 등록이 증가할 것으로 예상됨. 국내에서 IPR 확보가 가능한 분야로는 능동형/수동형 RFID 태그 환경에서 사용 가능한 경량 암호 기술 등이 있음

• 블록 암호알고리즘 운영모드

- 국내 블록 암호 알고리즘 관련 특허출원은 ETRI, KISA, 드림시큐리티 등에서 암호키관리 기술 및 시스템 구현 등과 관련한 특허를 확보하고 있음. 컴퓨터 기술의 발달로 공격기법이 지능화됨에 따라 알고리즘의 안전성 강화를 위한 연구가 지속적으로 이루어지고 있으므로, 암호 알고리즘 관련하여 국내외 표준화 추진 및 관련 IPR 확보는 가능할 것으로 사료됨

• 응용서비스에서의 암호알고리즘 활용 방법

- 암호 기술은 원천기술로 개발되어 IPR을 수행하기도 하지만, 암호 알고리즘은 보안 기능을 제공하기 위해 무선 통신, 시스템 보안 등 다양한 분야에 하나의 요소를 제공하는 기술로 활용되고 있으며, 이에 관련된 응용 서비스 IPR이 많이 존재하고 있음
- 최근 클라우드컴퓨팅, 스마트그리드, VoIP, IPTV와 같이 민감한 데이터 및 개인 정보를 안전하게 보호하기 위한 정보보호 기술에 대한 관심이 높아짐에 따라, 이에 적합한 암호 알고리즘의 응용에 관련된 IPR 발굴 노력이 필요함

〈암호 기술 관련 주요 특허〉

출원번호	출원일자	등록번호	공고일자	출원인	발명의 명칭	진 행 상태
10-2007-0109230	2007.10.29	10-0860970-00-00	2008.09.24	한국정보통신주식회사	통신 프로토콜 스택의 스위칭 기능을 이용한 이종의 무선 통신망에 대한 종단간 보안 통신을 위한 단말장치	등록
10-2007-0009901	2007.01.31	10-0874706-00-00	2008.12.18	KISA	초경량, 저전력 환경에 적합한 암호화 방법	등록
10-2007-7003426	2007.02.13	10-0883442-00-00	2009.02.05	인텔 코포레이션	온라인 서비스를 사용하여 직접 증명 비밀키를 디바이스에 전달하는 방법	등록
10-2007-0013973	2007.02.09	10-0896743-00-00	2009.04.30	성균관대학교 산학협력단	P3P를 위한 보안 시스템 및 그 보안 방법	등록
10-2007-0070448	2007.07.13	10-0906404-00-00	2009.06.30	삼성에스디에스 주식회사	소모품의 복제 방지 장치 및 방법	등록
10-2008-0039171	2008.04.28	10-0888075-00-00	2009.03.03	인하대학교 산학협력단	개인별 대칭키를 이용한 멀티캐스트를 위한 암호화 및 복호화 시스템	등록
10-2007-0020166	2007.02.28	-	-	씨투아이소프트(주)	수신자 제한을 위한 암호화/복호화 방법	공개
10-2007-0025139	2007.03.14	-	-	삼성전자주식회사	컨텐트의 조건부 복호화 방법 및 그 장치	공개

출원번호	출원일자	등록번호	공고일자	출원인	발명의 명칭	진 행 상태
10-2007-0033780	2007.04.05	-	-	삼성전자주식회사	UMS 기기의 컨텐츠를 보호하기 위한 방법 및 장치	공개
10-2007-7016930	2007.07.23	-	-	인터디지탈 테크날러지 코포레이션	무선 통신 시스템에서 가변 시큐리티 레벨을 제공하기 위한 시스템 및 방법	공개
10-2007-7017423	2007.07.27	-	-	가부시키가이샤 오크 죠호 시스템	파일의 암호화 · 복호화 방법, 장치, 프로그램 및 이 프로그램을 기록한 컴퓨터 판독 가능한 기록 매체	공개
10-2007-0092388	2007.09.12	-	-	(주)왈도시스템	음성 및 데이터 서비스를 통합적으로 제공하는 위성 통신 시스템 및 보안 기능 제공 방법	공개
10-2007-0099045	2007.10.02	-	-	(주) 엘지텔레콤	이동통신 단말기를 이용한 금융서비스 처리 시스템 및 그 제어방법	공개
10-2007-0108485	2007.10.26	-	-	삼성전자주식회사	대칭키 암호 프로세싱 장치 및 방법	공개
10-2007-0108466	2007.10.26	-	-	경희대학교 / 산학협력단	IPv6 네트워크에서 인접 노드의 탐색 메시지를 송수신하는 방법	공개
10-2007-0108757	2007.10.29	-	-	주식회사 케이티프리텔	웹환경에서 공유된 키를 이용한 데이터 송수신 방법 및 시스템	공개
10-2007-0002793	2007.01.10	-	-	이인섭	다국어 텍스트 문자열 암호화를 위한 대칭키 암호 알고리즘 보완 방법	공개
10-2007-0112923	2007.11.05	-	-	김도하	일회성 난수 테이블 대칭키 시스템	공개
10-2007-0112469	2007.11.06	-	-	ETRI	프라이버시를 보장하는 암호화와 복호화를 이용한 파일 공유 방법 및 시스템	공개
10-2007-0114402	2007.11.09	-	-	ETRI	수동형 RFID 태그의 암호화 연산 장치	공개
10-2007-0115504	2007.11.13	-	-	삼성전자주식회사	도전 응답 기반의 RTT 검사 방법, 장치 및 그 방법을 기록한 컴퓨터로 읽을 수 있는 기록 매체	공개
10-2007-7026698	2007.11.16	-	-	텔레콤 이탈리아 소시에떼 퍼 아찌오니	무선 통신 단말기에서 ＳＩＭ 카드에 의한 주변 장치의 관리 방법 및 이 방법을 이행하기 위한 주변 장치	공개
10-2007-0122687	2007.11.29	-	-	ETRI	베타 전개를 이용한 순서 보존 수치 데이터 암호화 시스템 및 방법	공개
10-2007-0125472	2007.12.05	-	-	ETRI	보안모듈 프로그램을 보호하기 위한 디지털 케이블 시스템 및 그 방법	공개
10-2007-0127977	2007.12.11	-	-	ETRI	RFID시스템에서 대칭키 암호화 기반 통신 데이터 보호 방법과 이를 수행하기 위한 리더 및 태그	공개
10-2007-0131205	2007.12.14	-	-	ETRI	원 타임 패스워드를 사용하는 관리 서버 예약 접속 방법, 클라이언트 및 시스템	공개
10-2007-0136398	2007.12.24	-	-	삼성전자주식회사	마이크로어레이의 정보 암호화/복호화 방법 및 시스템	공개
10-2008-7016970	2008.07.11	-	-	인터디지탈 테크날러지 코포레이션	노드에서 유저 데이터를 보호하는 방법 및 시스템	공개
10-2008-0073866	2008.07.29	-	-	한국정보통신 서비스 주식회사	휴대 인터넷 통신망을 이용한 카드결제 보안처리 시스템	공개
10-2009-7007749	2009.04.15	-	-	인터디지탈 테크날러지 코포레이션	그룹 단위 비밀키 발생	공개
10-2009-7008709	2009.04.28	-	-	지멘스 악티엔게젤샤프트	키관리 프로토콜을 보호하기 위해 대칭키를 제공하는 방법	공개
20-1996-0042519	1996.11.27	-	-	기아자동차 주식회사	차량의 타코 그래프	공개
10-1996-0070294	1996.12.23	-	-	기아자동차 주식회사	자동차의 비상용 운행기록장치	공개
10-1997-0069817	1997.12.17	-	-	현대자동차 주식회사	차량 운행 정보 기록장치	공개
10-1999-0043763	1999.10.11	-	-	현대자동차 주식회사	차량 주행 기록 데이터 수집장치	공개
10-2003-0036813	2003.06.09	-	-	(주)카젤	텔레매틱스 기기를 이용한 자동차 보험 고객 관리 시스템 및 방법	공개
10-2003-0079010	2003.11.10	-	-	현대자동차주식회사	차량간 통신을 이용한 긴급구조신호 송신 및 수신방법	공개

나) 인증 기술

• 다양한 인증수단에 대한 보안성 검증 프레임워크

- 아직까지 사이버 상에서의 다양한 인증수단별 객관적이고 체계적인 보안수준 산정을 위한 검증 프레임워크에 대한 표준 및 특허 등은 존재하지 않으며, 이러한 프레임워크가 개발될 경우 국내외 표준화가 가능할 것으로 판단됨

• 디바이스 인증 기술 및 응용

- 홈네트워크 및 디바이스에서의 인증 방법에 대해서는 국내 특허가 출원되어져 있긴 하지만, 그 외 신규 디바이스에 대한 인증 기술에 대한 특허는 존재하지 않음. 신규 IT서비스에 적용되는 디바이스별로 서비스 모델이 확정될 경우, 각 디바이스별 또는 디바이스 인증 관련 기반 기술에 대한 특허 출원은 가능할 것으로 판단됨

〈디바이스 인증기술 및 응용 관련 주요 특허〉

출원번호	출원일자	등록번호	공고일자	출원인	발명의 명칭	진 행 상태
10-2004-0015172	2004-03-05	10-2005-0089660	2005-09-08	엘지전자 주식회사	디지털 방송의 인증 방법(Certificate method of digital broadcasting)	등록
10-2008-7027064	2007-04-04	10-2009-0031853	2009-03-30	퀄컴 인코포레이티드	ＦＬＯ 디바이스를 인증하는 방법 및 장치(METHOD AND APPARATUS FOR ENABLING FLO DEVICE CERTIFICATION)	등록
10-2007-0096534	2007-09-21	10-2009-0030878	2009-03-25	엘지전자 주식회사	인증 상태 정보 처리 방법 및 방송 수신 장치(method of processing certificate status information and apparatus for receiving a broadcasting signal)	등록
10-2007-0034364	20070406	10-2007-0100179	2007-10-10	에이디파워 주식회사	전력기기 인증 방법 및 그 시스템 (Electric power device certification method and System thereof)	등록

• 일회용패스워드(OTP) 인증 기술 및 응용

- 현재 국내외에서 OTP와 관련한 응용기술들이 특허로 많이 출원되어 있는 상태이며, 시간동기화 방식 및 시도-응답 방식 등을 이용한 OTP 생성알고리즘부터 얼굴영상을 이용한 OTP 알고리즘, 그래픽을 이용한 OTP 알고리즘, OTP를 활용한 유무선 통신 사용자 인증 방식, 스마트카드를 이용한 OTP 생성방식, 모바일 뱅킹 및 텔레뱅킹 전자금융 활용방안 등 다수의 기술 특허들이 출원되어 있음. 현재 출원되어 있는 주요 OTP 인증기술 관련 국내특허는 아래와 같음
- 편리하면서 강한 인증을 제공하는 OTP 인증기술은 유비쿼터스 환경에서 다양한 분야의 IT 기술에 접목하여 사용할 수 있기 때문에 앞으로도 국내외 특허 출원이 활발할 것으로 예상됨

〈OTP 인증기술 관련 주요 특허〉

출원번호	출원일자	등록번호	공고일자	출원인	발명의 명칭	진 행 상태
10-2004-0044628	2004.06.16	10-0668387-0000	2007.01.12	(주)에스케이 텔레콤	일회용 암호방식을 이용한 통합 인증 시스템과 그 구축 방법	등록
10-2005-0070994	2005.08.03	10-0548638-0000	2006.02.02	(주)하이스마텍	스마트카드를 이용한 원타임 패스워드 생성 및 인증방법 그리고 이를 위한 스마트카드	등록
10-2006-0025093	2006.03.18	10-0791485-0000	2008.01.04	(주)코아보이스	음성신호를 이용한 OTP 보안 인증시스템 및 그 보안 인증방법	등록
10-2006-0036090	2006.04.21	10-0830969-0000	2008.05.20	(주)프럼나우	ＯＴＰ를 이용한 금융거래 방법 및 시스템	등록
10-2006-0039162	2006.05.01	10-0755212-0000	2007.09.04	(주)미래테크놀로지	오티피 발생용 아이씨 칩이 내장된 휴대폰을 이용한시간 동기 방식 오티피 생성 및 인증시스템과 그 방법	등록

출원번호	출원일자	등록번호	공고일자	출원인	발명의 명칭	진 행 상태
10-2006-0042411	2006.05.11	10-0813659-0000	2008.03.14	(주)케이에스넷, (주)씨앤앰	ＯＴＰ 생성 기능을 구비한 셋탑 박스 및 이를 이용한 전자상거래 시스템 및 방법	등록
10-2006-0084508	2006.09.04	10-0675259-0000	2007.01.29	김동규	오티피코드가 부가된 바코드 인증 시스템 및 그 방법	등록
10-2007-0020553	2007.02.28	10-0844195-0000	2008.07.04	(주)민인포	그래픽 오티피를 이용한 사용자 인증 방법	등록
10-2007-7027029	2007.11.20			뱅크오브 아메리카	일회용 비밀번호 신용／직불 카드	공개
10-2007-0112532	2007.11.06	10-0835260-0000	2008.06.10	(주)미래테 크놀로지	메모리해킹 방지를 위한 인터넷뱅킹 제어방법과 이에 사용되는 오티피토큰장치	등록

• 일회용패스워드(OTP) 인증 시스템 보안 요구사항

- OTP를 이용한 인증 시스템과 상호 연동성을 보장하기 위한 통합인증 프레임워크 등에 대한 특허가 금융보안연구원을 중심으로 등록 예정이며, 2010년내에 USIM기반 모바일 OTP 및 대칭키 기반 부인방지 기능을 제공하는 OTP기술에 대한 특허 출원 예정임

〈OTP 인증 시스템 보안 요구사항 관련 관련 주요 특허〉

출원번호	출원일자	등록번호	공고일자	출원인	발명의 명칭	진 행 상태
10-2008-0099425	2008.10.10			금융보안연구원	오티피 통합 인증 처리 시스템과 그 제어 방법	등록

• 익명성을 보장하는 인증 기술

- 프라이버시 침해 및 개인정보 유출 등의 사회문제가 발생하고 있어, 이를 해결하기 위한 익명성 기반의 정보보호기술에 대한 핵심기술개발이 필요하게 됨. 익명인증 및 익명권한관리 플랫폼 기술 등의 개발을 통하여 익명인증 원천 IPR 확보 및 상용화 원천기술 개발이 추진되고 있음

〈익명성을 보장하는 인증기술 관련 주요 특허〉

출원번호	출원일자	등록번호	공고일자	출원인	발명의 명칭	진 행 상태
2009-0032432	2009.04.14	10-2010-0085809 (공개번호)	2010.07.29	ETRI, 인하대학교	불확정 전송 방법을 기반으로 하는 가명 인증 시스템 및 그 방법	공개 (출원)
2008-0124847	2008.12.09	10-2010-0066169 (공개번호)	2010.06.17	ETRI	익명 인증을 이용한 개인 정보 관리 시스템 및 방법	공개 (출원)
2009-0024569	2009.03.23	10-2010-0062814 (공개번호)	2010.06.10	ETRI	조건부 추적이 가능한 익명 서비스 시스템	공개 (출원)
2008-0117164	2008.11.25	10-2010-0058697 (공개번호)	2010.06.04	박영민, 중앙대학교	프라이버시 보호와 서비스 차별화를 위한 분류 가능한 익명성 제공	공개 (출원)
2009-0061805	2009.07.07	10-2010-0053426 (공개번호)	2010.05.20	ETRI	권한 분산형 가명 인증서 처리 시스템	공개 (출원)
2009-0008162	2008.07.17	10-2009-0008162 (공개번호)	2009.01.21	인텔 코오퍼레이션	이선형 맵들로부터 의 직접적인 익명의 증명을 위한 장치 및 방법	공개 (출원)
2007-0025518	2007.03.15	10-0857991-00-00	2008.09.03	케이티, 서울대학교	선택적 익명 인증서 서비스 제공 방법 및 시스템	등록
2006-7025556	2006.12.04	10-2007-0040755 (공개번호)	2007.04.17	프랑스 텔레꽁	리스트 서명을 생성하기 위한 방법과 시스템	
2007-0048106	2007.05.17	10-0901693-00-00	2009.06.02	ETRI	동시 수행 환경에서의 링 인증 방법	등록

• 바이오정보를 이용한 전자서명 기술

- 바이오정보를 이용한 인증기술은 다수의 특허가 등록되어 있으며, 바이오정보를 이용한 키생성 및 전자서명 기술은 연구 중에 있어 향후 관련된 특허가 등장할 것으로 기대됨

〈인증 및 권한 기술 관련 특허〉

출원번호	출원일자	등록번호	공고일자	출원인	발명의 명칭	진 행 상태
10-2001-7011564	2001.09.11	10-0718086-0000	2007.05.08	톰슨 라이센싱	디지털 홈 네트워크를 위한 범용 복사 방지 시스템에서 액세스 관리 방법 및 디바이스	등록
10-2002-0039155	2002.07.06	10-0878764-0000	2009.01.08	삼성전자주식회사	사용자의 익명성보장을 위한 무선 랜 시스템 및 사용자의 익명성 보장방법	등록
10-2002-0000514	2002.01.04	10-0412041-0000	2003.12.09	삼성전자주식회사	시큐러티 프로토콜의 기능을 수행하는 홈 게이트웨이 및그 방법	등록
10-2002-7007813	2002.06.18	10-0833828-0000	2008.05.26	퀄컴 인코포레이티드	중매인의 사기 가능성을 감소시키면서 익명의 사용자를 인증하는 방법	등록
20-2006-0009059	2006.04.05	20-0422918-0000	2006.07.26	강만제	휴대용 단말기의 사용자 인증(S I M) 카드 커넥터	등록
10-2006-0069969	2006.07.25	10-0813006-0000	2008.03.06	한국전자통신연구원	방송 통신 융합 프레임워크 환경에서 엠펙-21 알이엘 및알디디를 이용한 라이센스 제공 시스템	등록
10-2006-7014702	2006.07.21			코닌클리케 필립스 일렉트로닉스 엔.브이.	콘텐츠로의 액세스를 인증하는 방법	공개
10-2007-7008144	2007.04.10			코닌클리케 필립스 일렉트로닉스 엔.브이.	조건적 액세스를 제공하는 방법	등록
10-2008-7002018	2008.01.25			코닌클리케 필립스 일렉트로닉스 엔.브이.	키 블록 기반의 인증 장치 및 방법	공개
10-2008-7010512	2008.04.30			프리바스피어 아게	사용자 인증 방법 및 디바이스	공개

다) 권한관리 기술

• 기기 관리자 및 소유자간의 권한관리 기술

- 기기인증과 관련한 기술 및 응용은 다수의 특허가 등록되어 있으나, 기기인증서와 관련한 기기 관리자 및 소유자간의 권한관리 기술은 연구 중에 있어, 향후 특허가 등장할 것으로 기대됨

• 통합 권한관리 프레임워크 및 응용 서비스

- 전통적인 인증기술을 강화한 멀티팩터 인증기술의 출현으로 안전한 전자거래의 환경이 조성되어 있으며, 이를 기반으로 사용자의 편의성을 크게 개선할 수 있는 통합인증 및 권한관리 기술이 국내 기술로 선도가 가능한 상황으로, 국제 표준화 및 IPR 확보를 통해 관련 산업분야의 국제 경쟁력 확보가 기대됨

• 사용자 권한관리를 위한 인증기술 및 응용

- 국내의 경우 IPR 확보가 매우 미흡한 편이며, 국외의 경우 다수의 IRP이 확보되어 있음. 국내의 경우 "속성 인증서를 이용한 유비쿼터스 디바이스 도메인 인증 방법" 등의 특허가 출원된 상태이며, 국외의 경우 "METHOD FOR ISSUING ATTRIBUTE CERTIFICATE FROM AN LDAP ENTRY" 등의 특허가 출원된 상태임

2.3. 표준화 현황 및 전망

2.3.1. 국내 표준화 현황 및 전망

가) 암호기술

• 유비쿼터스 환경에 적합한 경량 암호알고리즘

- 1999년에 KISA와 국내 암호전문가들이 128비트 블록 암호알고리즘을 개발하고 국내 정보통신단체표준(TTA)로 제정되었으며, 2005년부터는 국제 표준화 기구인 ISO/IEC, IETF에서 블록 암호 알고리즘 표준으로 제정됨. 최근 암호 알고리즘 활용성 강화를 위해 2009년 256비트를 지원하는 SEED 256 암호 알고리즘을 개발하고 국내외 표준화를 추진 중임
- 2004년에 ETRI 부설연구소(NSRI) 주도 하에, 산 · 학 · 연이 모여 경량 환경 및 하드웨어에서의 효율성을 향상시킨 블록 암호 알고리즘 ARIA를 개발하였으며, 2004년 12월 지식경제부에 의한 국가표준(KS)으로 제정되었음. 최근 ISO/IEC의 국제 표준화 기구에서 블록 암호 알고리즘으로 표준화를 추진 중임
- 2005년에 저전력 · 초경량을 요구하는 컴퓨팅 환경에서의 기밀성을 제공하기 위해 KISA, ETRI 부설연구소 및 고려대가 공동으로 64비트 블록 암호 알고리즘을 개발하여, 2006년 정보통신단체표준(TTA)으로 제정되었으며, 2009년 6월 ISO/IEC 블록 암호 알고리즘으로 국제 표준화 추진 중임
- SEED 128 블록 암호 알고리즘의 경우, 2005년부터 SEED 알고리즘이 활용 가능한 IPsec, TLS, CMS를 위한 SEED 암호 알고리즘 관련 표준을 개발하여 정보통신단체(TTA)으로 제정되었음

• 블록암호 운영모드

- 국내에서 개발한 SEED, HIGHT 등 블록 암호 알고리즘이 다양한 보안프로토콜에서 활용할 수 있도록 NIST에서 정의한 운영모드를 기반으로 국내 표준화 추진 중임

• 응용서비스에서의 암호 알고리즘 활용 방법

- 최근 유비쿼터스 등 저전력 · 초경량의 환경에서 적용 가능한 암호 알고리즘에 대한 개발이 지속적으로 이루어질 것으로 판단됨. 개발 알고리즘이 적용 가능한 응용서비스에서의 암호 알고리즘 활용 방법에 대한 표준이 개발될 것으로 판단됨
- ISO/IEC JTC1/SC31을 중심으로 수동형 RFID 보안 기술에 대한 표준화 진행 중이며, 이는 우리나라와 오스트리아가 주축이 되어 진행되고 있음. 또한, 모바일 RFID 환경에 적합한 프라이버시 보호 기술에 대한 표준화도 진행 중에 있으며, USN 보안 기술의 경우, ITU-T SG17과 ISO/IEC JTC1/SC6를 중심으로 표준화가 진행 중에 있음

〈암호 기술 관련 TTA 표준현황〉

분 야	표준번호	제목	표준상태	년 도	비 고
암호	TTA.KO-12.0001	부가형 전자서명 방식 표준 - 제2부 : 확인서 이용 전자서명 알고리즘	제정 완료	1998	KCDSA
	TTAS.KO-12.0011/R2	해쉬함수표준 - 제2부 : 해쉬함수알고리즘표준(HAS-160)	개정 완료	2005	
	TTAS.KO-12.0004	128비트 블록암호알고리즘 표준	제정 완료	1999	SEED
	TTAS.IS-10181.4	개방시스템 상호접속-개방시스템에서의 보안 골격-제4부:부인방지	제정 완료	1999	ISO/IEC 10181 -4, X.813
	TTAS.KO-12.0001/R1	부가형 전자서명 방식 표준 - 제 2 부 : 인증서 기반 전자서명 알고리즘	개정 완료	2000	KCDSA
	TTAS.KO-12.0011/R2	해쉬함수표준-제2부 : 해쉬함수알고리즘표준(HAS-160)	개정 완료	2005	
	TTAS.KO-12.0015	부가형 전자서명 방식 표준-제3부 : 타원곡선을 이용한 인증서 기반 전자서명 알고리즘	제정 완료	2001	EC-KCDSA
	TTAS.IF-RFC2631	Diffie-Hellman 키합의 방식	제정 완료	2003	
	TTAS.KO-12.0025	블록암호알고리즘 SEED의 운영모드	제정 완료	2003	
	TTAS.IF-RFC3217	3-DES와 RC-2 키 싸기	제정 완료	2005	
	TTAS.IF-RFC3394	AES 키 싸기 알고리즘	제정 완료	2005	
	TTAS.KO-12.0004/R1	128비트 블록암호알고리즘 SEED	개정 완료	2005	
	TTAS.KO-12.0011/R2	해쉬함수표준-제2부 : 해쉬함수알고리즘표준(HAS-160)	개정 완료	2005	
	TTAS.IF-RFC3370	암호 메시지 규격에서 사용되는 알고리즘	제정 완료	2005	
	TTAS.KO-06.0102	텔레매틱스 단말-TSP 서버간 서비스 프로토콜 Stage 1: 요구기능	제정 완료	2005	
	TTAS.KO-06.0117	텔레매틱스 단말 소프트웨어 플랫폼Stage2 : 요구기능	제정 완료	2006	
	TTAS.KO-12.0039	해쉬함수 알고리즘 FORK-256	제정 완료	2006	
	TTAS.KO-12.0040	64비트 블록암호알고리즘 HIGHT	제정 완료	2006	
	TTAS.IF-RFC3369	암호 메시지 규격	제정 완료	2006	CMS
	TTAS.KO-12.0041	스트림암호알고리즘 TSC-4	제정 완료	2006	
	TTAR-12.0001	MD5 메시지-다이제스트 알고리즘	제정 완료	2006	
	TTAS.IF-RFC4196	IPsec을 위한 SEED 암호알고리즘	제정 완료	2006	
	TTAS.IF-RFC4162	TLS를 위한 SEED 암호알고리즘	제정 완료	2006	
	TTAS.IF-RFC4010	CMS를 위한 추가암호 알고리즘 : Part1 SEED	제정 완료	2006	
	TTAS.IF-RFC3565	CMS를 위한 추가암호 알고리즘 : Part2 AES	제정 완료	2006	
	2004-008	패스워드 기반의 공개키 암호기술 표준(AMP)	폐지	2008	
	TTAS.KO-12.0040/R1	64비트 블록암호알고리즘 HIGHT	제정 완료	2009	
	TTAK.KO-12.0102	기업의 정보보호를 위한 암호정책 수립 지침	제정 완료	2009	
	TTAK.KO-12.0114	TLS에서의 ARIA 암호알고리즘 운영 방법	제정 완료	2009	
	TTAK.KO-12.0115	SRTP에서의 ARIA 암호알고리즘 운영 방법	제정 완료	2009	
	2009-1467	블록암호알고리즘 SEED의 운영모드	제정 예정	2010	

〈암호 기술 관련 KS 표준〉

분 야	표준번호	제목	등록일
암호	KSX6513-5	금융 거래 카드-집적 회로 카드를 사용하는 금융 거래 시스템의 보안 -제5부: 알고리즘의 사용	2002-07-31
	KSX6315-1	금융-메시지 인증을 위한 승인된 알고리즘-제1부: DEA 알고리즘	2002-07-31
	KSXISOIEC9979	정보기술-보안기술-암호 알고리즘 등록절차	2003-11-26
	KSXISOIEC13888-1	정보기술-보안기술-부인 봉쇄-제1부: 일반	2003-11-26
	KSXISOIEC11770-1	정보기술-보안기술-키 관리-제1부: 기본 틀	2003-11-26
	KSXISOIEC13888-2	정보기술-보안기술-부인봉쇄-제2부: 대칭 암호기법을 이용한 메커니즘	2003-11-26
	KSXISO10126-2	금융업-메시지 암호화 절차(도매금융)-제2부: DEA알고리즘	2003-12-06
	KSXISO10126-1	금융업-메시지 암호 절차 (도매금융)-제1부: 일반 원리	2003-12-06
	KSXISOIEC15946-3	정보기술-보안기술-타원형 곡선에 기반한 암호기술-제3부: 키 설정	2003-12-29
	KSXISOIEC9797-2	정보기술-보안기술-메시지 인증 코드-제2부: 전용 해쉬 함수를 이용한 메커니즘	2003-12-29
	KSXISOIEC15946-1	정보기술-보안기술-타원형 곡선에 기반한 암호기술-제1부: 일반	2003-12-29
	KSX6922-2	지불 시스템을 위한 IC 카드 규격-제2부: 보안 및 키 관리	2003-12-30
	KSX1208-2	정보기술-보안기술-N비트 블록암호 알고리즘을 이용하는 해쉬함수	2003-12-31
	KSX1205	정보기술-보안기술-n비트 블럭암호 알고리즘의 운영모드	2003-12-31
	KSX1211-2	정보 보안의 부인 봉쇄-제2부: 대칭 암호 기법을 이용한 메커니즘	2004-06-23
	KSX1209	정보 보안의 암호 알고리즘 등록 절차	2004-06-23
	KSX1210-1	정보 보안의 키 관리-제1부: 기본 틀	2004-06-23
	KSX1206	블럭 암호 알고리즘을 사용한 데이터 무결성 기법	2004-06-23
	KSX1204-3	정보 보호 기법-실체 인증-제3부: 디지털 서명 기법을 이용한 메커니즘	2004-06-23
	KSX1204-1	보안기술의 실체인증 기법-제1부: 일반모델	2004-06-23
	KSX1213	128비트 블록 암호 알고리즘 ARIA	2004-12-30
	KSXISO11568-2	금융-키 관리(소매 금융)-제2부: 대칭 암호화 방식을 위한 키 관리 기법	2004-12-30
	KSXISO11568-3	금융-키 관리(소매 금융)-제3부: 대칭 암호화 방식을 위한 키의 수명 주기	2004-12-30
	KSXISO10202-3	금융 거래 카드-집적 회로 카드를 사용하는 금용 거래 시스템의 보안-제3부: 암호 키 관련성	2005-06-30
	KSXISOIEC10118-2	정보기술-보안기술-해시함수-제2부: n-bit block cipher를 사용한 해시 함수	2005-12-21
	KSX6923-3	비접촉식 전자화폐 단말기용 지불SAM 규격-제3부: 지불SAM의 암호 알고리즘	2006-10-31
	KSX6924-3	선불IC카드-KS X 6923 대응 사용자 카드-제3부: 암호 알고리즘	2006-10-31
	KSXISOIEC9797-1	메시지 인증 코드-제1부: 블록암호를 이용한 메커니즘	2006-12-11
	KSXISO13492_2001	은행업무-키관리 관련 자료요소(소매금융)	2006-12-11
	KSXISOIEC9797-1	메시지인증코드-제1부: 블록암호를 이용한 메커니즘	2006-12-11
	KSXISOIEC10118-4:2001	정보기술-보안기술-해쉬함수-제4부: 법 연산을 이용하는 해쉬함수	2006-12-11
	KSXISO8731-2_2001	금융-메시지 인증을 위한 알고리즘-제2부: 메시지인증 알고리즘	2006-12-11
	KSXISOIEC11770-2	정보기술-보안기술-키 관리-제2부: 대칭 기법을 이용한 메커니즘	2006-12-26
	KSXISOIEC9798-4	정보기술-보안기술-실체인증-제4부: 암호학적 확인 함수를 이용한 메커니즘	2006-12-26
	KSXISOIEC9798-2	정보기술-보안기술-실체인증-제2부: 대칭형 암호 알고리즘을 이용한 메커니즘	2006-12-26
	KSXISOIEC18033-4	정보기술-보안기술-암호 알고리즘-제4부: 스트림 암호	2006-12-26
	KSXISOIEC18033-3	정보기술-보안기술-암호 알고리즘-제3부: 블록 암호	2006-12-26
	KSXISOIEC18033-1	정보기술-보안기술-암호 알고리즘-제1부: 일반	2006-12-26
	KSXISOIEC10118-3:2001	정보기술-보안기술-해쉬함수-제3부: 전용 해쉬 함수	2006-12-26
	KSX1208-1	정보기술-보안기술-해시함수-제1부: 일반	2006-12-26
	KSXISO11568-5_2001	은행업무-키 관리(소매 금융)-제5부: 공개키 암호를 위한 키 수명 주기	2006-12-29
	KSXISO13491-1_2001	금융업-보안 암호화 장치-제1부: 개념, 필요요건 및 평가방법	2006-12-29

나) 인증 기술

• 다양한 인증수단에 대한 보안성 검증 프레임워크

- 사이버 상에서의 다양한 인증수단별로 활발한 표준화가 진행되고 있으나, 이들간 보안성 정의 및 검증을 위한 절차 등은 정립되지 않은 상황임. 다양한 거래유형 및 위험수준에 따른 적절한 인증수단의 선택을 위한 객관적인 보안수준의 정의 및 검증을 위한 프레임워크 및 적용 지침 등에 대한 표준화 수요가 증가할 것으로 전망됨

• 디바이스 인증 기술 및 응용

- TTA 정보보호기반 프로젝트 그룹(PK501)을 통해 향후 유비쿼터스 환경에 적합하도록 사람에 대한 인증뿐만 아니라, 기기를 포괄하는 인증기술 관련 표준화가 추진되고 있으며 지속적으로 표준화 수요가 증가할 것으로 전망됨

분 야	표준번호	제목	표준상태	년 도	비 고
기기인증	TTAS.KO-12.0052	홈네트워크 등에 적용 가능한 디바이스 인증서 프로파일	제정완료	2007	-
	2010-049	기기인증서 프로파일	검토중	2010	2010년 제정예정
	2010-1347	기기인증서 효력정지 및 폐지목록 프로파일	검토중	2010	
	2010-1345	정보통신기기 식별을 위한 기기인증체계 DN 정의	검토중	2010	
	2010-1346	기기인증서 이용을 위한 전자서명 알고리즘 파라미터 정의	검토중	2010	
	2010-1348	기기인증체계 내에 정보구성을 위한 디렉토리 스키마 정의	검토중	2010	

• 일회용패스워드(OTP) 인증 기술 및 응용

- 2009년 TTA의 정보보호기반 프로젝트그룹(PG501)에서 OTP 암호키 관리 보안요구사항이 표준 제정되었으며, 2010년에 추가적으로 1건이 제정될 예정임. 2010년 이후에도 매년 1~3건의 OTP 관련 표준이 개발될 전망임

분 야	표준번호	제목	표준상태	년 도	비 고
OTP	TTAK.KO-0100	일회용패스워드(OTP) 암호키 관리 보안요구사항	제정완료	2009	-
	2009-826	일회용패스워드(OTP) 키컨테이너	검토중	2008	2010년 제정예정

• 일회용패스워드(OTP) 인증 시스템 보안 요구사항

- 2009년 TTA의 PG501과 PG504에서 OTP 통합인증 서비스 프레임워크와 OTP 인증 서비스를 위한 보증 레벨과 응용 가이드라인에 관한 표준이 제정되었으며, 2010년에는 OTP 토큰 보안요구사항과 OTP 응용 프로그램 인터페이스가 표준으로 제정될 예정임. 2010년 이후에도 매년 1~3건의 OTP 관련 표준이 개발될 전망임

분 야	표준번호	제목	표준상태	년 도	비 고
OTP	TTAK.KO-0128	일회용패스워드(OTP) 통합인증 서비스 프레임워크	제정완료	2009	-
	TTAK.KO-0120	일회용패스워드(OTP) 인증 서비스를 위한 보증 레벨	제정완료	2009	-
	2010-048	일회용패스워드(OTP) 응용 프로그램 인터페이스	검토중	2010	2010년 제정예정
	2009-1466	일회용패스워드(OTP) 기기 보안 요구사항	검토중	2009	2010년 제정예정

• 익명성을 보장하는 인증 기술

- 2008년에 TTA의 정보보호기반 프로젝트그룹(PG501)에서 표준화를 추진하여, 2009년말 "추적 가능한 익명 인증서 이용 기술"이 표준으로 채택됨. 해당 표준은 추적 가능한 가명 기반의 익명인증서 이용기술을 다루고 있으며, 추적 가능성을 위해 등록대행기관과 인증기관의 역할을 분리하여 익명성을 보장하면서 추적 가능한 익명인증서 이용기술을 정의함
- 2010년에 같은 프로젝트그룹에서 익명성을 제어할 수 있는 그룹 서명 기반 익명인증 기술에 대한 표준화를 추진하고 있음. 이를 위해 "익명인증 서비스 프레임워크"와 "그룹서명 기반 익명인가 프레임워크"에 대한 표준화를 2010년까지 완료할 예정이며, 익명디지털 전자서명 알고리즘에 대한 표준화도 2011년까지 진행할 예정임
- ISO는 JTC1 SC27 WG2(Anonymous Authentication)에서 그룹서명 기반의 익명인증 표준화를 추진하기로 의결하고(2009년 10월), TCG는 익명으로 TPM기기를 인증하는 기술 표준화가 진행 중임

• 바이오정보를 이용한 전자서명 기술

- 국내의 경우, ITU-T X.1088 표준을 국내 환경에 맞게 정의한 TTAK.IT-X108(TTA, 2008, 바이오 인식 정보에 기반한 전자서명 키생성 프레임워크)을 제정함. 본 표준은 바이오 인식 정보를 기반으로 전자서명에서 사용한 디지털 전자서명 키를 생성하기 위한 절차와 방법 등 제반 프레임워크에 대한 규격을 정의하는 것을 목적으로 함

〈인증 및 바이오 정보 관련 TTA 표준현황〉

분 야	표준번호	제목	제정년도	비 고
PKI	ISTF-001	전자서명 인증서 프로파일 표준	2000	TTAS.KO-12.0012
	ISTF-002	전자서명 인증서 효력정지 및 폐지목록 프로파일 표준	2000	TTAS.KO-12.0013
	ISTF-002/R	전자서명 인증서 효력정지 및 폐지 목록 프로파일 표준	2006	개정
	ISTF-012	무선 전자서명 인증서 프로파일 표준	2002	TTAS.KO-12.0016
	ISTF-013	무선 전자서명 인증서 효력정지 및 폐지목록 프로파일 표준	2002	TTAS.KO-12.0017
	ISTF-014	무선 WTLS 인증서 프로파일 표준	2002	TTAS.KO-12.0019
	ISTF-017/R	무선 인증서 요청형식 프로토콜 표준	2003	TTAS.KO-12.0018/R1
	ISTF-018	공인인증기관간 상호연동을 위한 PKI 표준	2002	
	ISTF-021	무선 인증서 관리 프로토콜 표준	2003	TTAS.OT-12.0001
	ISTF-023	암호 토큰을 위한 PKCS#11 프로파일 표준	2003	TTAS.OT-12.0002
	ISTF-030	인증서 경로검증 알고리즘 표준	2004	TTAS.KO-12.0028
	ISTF-031	식별번호를 이용한 본인확인 기술 표준	2004	TTAS.KO-12.0029
	ISTF-036	공인인증기관간 상호연동을 위한 사용자 인터페이스 표준	2005	
	ISTF-037	인증서 정책 및 인증업무준칙 프레임워크 표준	2005	TTAS.IF-RFC3267
	ISTF-038	전자서명인증체계 공인인증서 갱신 표준	2005	
	ISTF-039	공개키 인증서를 이용한 개체인증 프로토콜 표준	2005	
	ISTF-040	인증기관간 상호연동을 위한 CTL 기술 표준	2005	
	ISTF-043	웹서버보안, 코드서명, 보안메일용 인증서 프로파일 표준	2006	
	ISTF-045	XML 전자서명 X.509 인증서 토큰 프로파일	2006	
인증	ISTF-046	익명성을 갖는 전자서명 인증 기술 표준	2006	
	TTAS.KO-12.0012/R1	전자서명 인증서 프로파일	2006	
	TTAS.KO-12.0018/R1	무선 인증서 요청형식 프로토콜	2004	

분 야	표준번호	제목	제정년도	비 고
인증	TTAS.IF-RFC3267	인증서정책 및 인증업무준칙 프레임워크	2004	
	TTAS.KO-12.0027	암호키분배용 인증서 및 키 관리 지침	2004	
	TTAS.OT-12.0002	암호 토큰을 위한 PKCS#11 프로파일	2004	
	TTAS.OT-12.0001	무선 인증서 관리 프로토콜	2004	
	TTAS.KO-12.0018/R1	무선 인증서 요청형식 프로토콜	2004	
	TTAS.KO-12.0028	전자서명 인증서 경로처리 알고리즘	2005	
	TTAS.KO-12.0029	식별번호를 이용한 본인확인 기술	2005	
	TTAS.KO-09.0003/R1	부가형 디지털 전자서명방식 - 제 1 부 : 기본 구조 및 모델	2005	
	TTAE.IF-RFC2716	EAP-TLS 인증 프로토콜	2005	
	TTAE.IF-RFC3748	EAP 프로토콜	2005	
	TTAE.IF-RFC3588	인증과 권한제어 및 과금용 다이아메터(Diameter) 베이스 프로토콜	2005	
	TTAS.KO-12.0030	홈서버 중심의 홈네트워크 사용자 인증 메커니즘	2005	
	TTAS.KO-12.0030	홈서버 중심의 홈네트워크 사용자 인증 메커니즘	2005	
	TTAS.KO-12.0038	본인확인서비스 중복가입 확인정보	2006	
	TTAS.KO-12.0012/R1	전자서명 인증서 프로파일	2006	
	TTAI.KO-12.0035	홈네트워크를 위한 보안기술 프레임워크	2006	
	TTAS.IT-X800	개방시스템 상호접속-개방시스템에서의 보안골격-제4부 부인방지	2006	
	TTAS.KO-12.0047	온라인 인증 시스템을 위한 지문 센서 인터페이스	2006	
	TTAS.KO-12.0052	홈네트워크 등에 적용 가능한 디바이스 인증서 프로파일	2007	
	TTAS.KO-12.0013/R1	전자서명 인증서 효력정지 및 폐지목록 프로파일	2007	
	TTAS.IT-X509/R4	디렉토리 : 공개키와 속성 인증서에 대한 프레임워크 표준	2007	
	TTAS.KO-12.0054	i-PIN 서비스 프레임워크	2007	
	TTAS.KO-12.0055	i-PIN 서비스 전달 메시지 형식	2007	
	TTAS.IT-X509/R4	디렉토리 : 공개키와 속성 인증서에 대한 프레임워크 표준	2007	
	TTAS.KO-12.0013/R1	전자서명 인증서 효력정지 및 폐지 목록 프로파일	2007	
	TTAS.KO-12.0052	홈네트워크 등에 적용 가능한 디바이스 인증서 프로파일	2007	
	TTAK.OT-12.0009	XML 전자서명 X.509 인증서 토큰 프로파일	2008	
	TTAK.KO-12.0071	웹서버보안, 코드서명, 보안메일용 인증서 프로파일	2008	
	TTAK.KO-12.0068	추적 가능한 익명 인증서 이용 기술	2008	
	2006-478	사용자 익명성을 갖는 전자서명 인증 기술	2008	제정 예정
	2008-1127	통신상에서의 바이오기반 시스템 인증 메커니즘	2008	제정 예정

〈 인증 기술 관련 KS 표준 〉

분 야	표준번호	제목	등록일
인증	KSXISOIEC15945	정보기술-보안기법-전자서명의 응용을 지원하기 위한 TTP서비스 규격	2002-11-26
	KSXISOIEC9594-8	정보기술-개방형시스템간 상호접속-디렉토리: 공개키와 속성인증 프레임워크	2002-11-27
	KSXISOIEC9798-3	정보기술-보안기술-실체인증-제3부: 디지털 서명기법을 이용한 메커니즘	2003-11-26
	KSXISOIEC9798-1	정보기술-보안기술-실체인증-제1부:일반	2003-11-26
	KSXISOIEC15946-2	정보기술-보안기술-타원형 곡선에 기반한 암호기술-제2부: 전자서명	2003-12-29
	KSXISOIEC15946-3	정보기술-보안기술-타원형 곡선에 기반한 암호기술-제3부: 키 설정	2003-12-29
	KSX1207	정보기술-보안기술-메세지 복원형 디지털 서명 방식	2003-12-31
	KSX1204-3	정보보호기법-실체 인증-제3부: 디지털 서명 기법을 이용한 메커니즘	2004-06-23
	KSX1204-1	보안기술의 실체인증 기법-제1부: 일반모델	2004-06-23
	KSX6033	확장가능한 마크업 언어 전자서명 구문과 처리	2005-07-01
	KSXISOIEC9796-2	정보기술-보안기술-메시지 복원형 디지털 서명 기법-제2부: 정수 인수분해(Integer factorization) 기반 메커니즘	2005-12-21
	KSXISOIEC15946-4	정보기술-보안기법-타원 곡선 암호화 기법-제4부: 메시지 복원을 실현하는 전자 서명	2005-12-21
	KSXISOIEC9796-2	정보기술-보안기술-메시지복원형디지털서명기법-제2부: 정수 인수분해(Integer factorization) 기반 메커니즘	2005-12-21
	KSXISOIEC14888-1:2001	정보기술-보안기술-부가형 디지털 서명-제1부: 일반	2006-12-11
	KSXISOIEC9796-3	메시지 복원형 디지털 서명 기법-제3부: 이산대수 기반 메커니즘	2006-12-11
	KSXISOIEC14888-3:2001	정보기술-보안기술-부가형 디지털 서명 - 제3부: 인증서 기반 매커니즘	2006-12-11
	KSXISOIEC14888-2:2001	정보기술-보안기술-부가형 디지털 서명 - 제2부: 신분 기반 매커니즘	2006-12-11
	KSXISOIEC9798-4	정보기술-보안기술-실체인증-제4부: 암호학적 확인 함수를 이용한 메커니즘	2006-12-26
	KSXISOIEC9798-5	정보기술-보안기술-실체인증-제5부: 영지식 기법을 이용한 메커니즘	2006-12-26
	KSXISOIEC9798-2	정보기술-보안기술-실체인증-제2부: 대칭형 암호 알고리즘을 이용한 메커니즘	2006-12-26

다) 권한관리 기술

• 기기 관리자 및 소유자간의 권한관리 기술

- TTA 정보보호기반 프로젝트 그룹(PK501)을 통해 기기인증서와 관련한 기술 표준화가 추진되고 있음. 현재, 기기관리자 및 기기소유자에 대한 권한관리와 관련한 표준화는 추진되고 있지 않으나, 기기와 기기관리자 및 기기소유자와의 관계, 권한관리 등에 대한 표준화 수요가 증가할 것으로 판단됨

• 통합 권한관리 프레임워크 및 응용 서비스

- 2009년부터 통합인증 및 권한관리 기술이 전자정부에 시범적으로 적용되는 등 기술개발은 활발히 진행되고 있으나, 국내 표준화를 위한 노력은 상대적으로 미흡한 실정임. 전자정부 등에 구축 · 운영된 결과를 바탕으로 표준화를 적극적으로 추진하여, 민간분야 등 다양한 도메인에 도입될 수 있는 기반 조성이 요구되고 있음

• 사용자 권한관리를 위한 인증 기술 및 응용

- 국내의 경우 TTA에서 PMI에 대한 표준이 제정되었음(TTA, TTAS.IT-X509/R4, 2007, 디렉토리 : 공개키와 속성 인증서에 대한 프레임워크 표준)

2.3.2. 국외 표준화 현황 및 전망

가) 암호기술

• 유비쿼터스 환경에 적합한 경량 암호알고리즘

- 국제 표준화 기구인 ISO/IEC JTC1/SC27에서는 블록 암호 알고리즘, 전자서명 알고리즘, 공개키 암호 알고리즘, 해쉬 함수 등 다양한 암호 알고리즘을 표준화하고 있으며, 암호분야에서는 미국, 유럽, 일본이 주도적으로 표준화를 진행하고 있음
  - 미국의 경우, NIST는 DES보다 안전한 암호 알고리즘 공모를 통해 새로운 차세대 암호를 공모하여 2000년 11월 AES를 선정 발표하고 AES에 적합한 새로운 모드를 개발할 목적으로 운영 모드를 공모하였고, SP 800-38 시리즈를 통해 권고 모드들을 제안함. SP 800-38A에는 기밀성을 제공하는 5가지 모드 ECB, CBC, OFB, CFB, CTR를, SP 800-38B에는 무결성을 제공하는 CMAC을, SP 800-38C에는 기밀성과 무결성을 동시에 제공하는 CCM 모드를, SP 800-38D에는 병렬처리가 가능한 인증-암호화 모드 GCM을 표준으로 권고함. 그 중에서 CCM은 IEEE 802.11 WLAN 표준으로도 채택된 알고리즘임
  - NIST는 지속적으로 SP 800-38 시리즈를 업데이트 할 것으로 보이며, 현재 계획으로는 1개 이상의 인증-암호화 모드를 추가적으로 선정할 것으로 예상되며 그 대상은 키와 같은 특정 대상을 인증-암호화하기 위한 AES KEY Wrap(AESKW) 알고리즘임. 또한, 미국 주도의 IEEE P1363에서는 공개키 기반의 키 교환, 암호화, 서명 등에 대한 알고리즘의 DB 작업을 시작하여 완성하고 있으며, lattice 기반, 패스워드 기반 인증 등을 위하여 p1363.1, p1363.2 등을 새롭게 작성하여 정리하고 있음. 또한, NIST에서는 FIPS 180-2로 제정된 SHA-1 해쉬 함수를 대체하기 위하여 2007년부터 2012년까지 차세대 해쉬함수 SHA-3 공모사업을 진행 중에 있음
  - 유럽에서는 전자상거래, 전자정부 및 전자서명 등을 구현하기 위해 필수적 요소인 암호 원천 기술에 대한 공모 사업 NESSIE를 통해 2003년 블록 암호, MAC 알고리즘 등 다수를 선정함. 현재, ECRYPT 프로젝트의 일부인 스트림 암호 공모사업 eSTREAM이 추진 중에 있으며 30여개 알고리즘이 제안되어 공개 검증이 수행되고 있음. 이 공모사업은 고속 소프트웨어 환경용과 제한적인 하드웨어 환경용의 두 가지 분야로 진행되고 있으며, 특히 제한적인 하드웨어 분야에 제안된 알고리즘들은 RFID 태그에 탑재가 가능할 것으로 예상되고 있음
  - 일본에서는 ISO/IEC JTC/SC27의 ISO/IEC 18033-3(블록 암호알고리즘) 표준에 MISTY1, Camellia 등에 대한 국제 표준화를 추진하였으며, 지속적으로 국제 표준화를 추진하고 있음
  - 국내의 경우는 ISO/IEC JTC1/SC27의 국내 암호 알고리즘 SEED가 포함된 ISO/IEC 18033-3(블록 암호 알고리즘)에 64비트 블록 암호 알고리즘 HIGHT에 대한 표준화 활동이 활발히 이루어지고 있음

• 블록암호 운영모드

- IETF에서는 AES를 기반으로 하여 NIST에서 정의한 운영모드를 다양한 보안프로토콜에서 활용하는 방안에 대한 표준화를 추진 중에 있으며, ITU-T에서는 IPTV 서비스 보안을 위해 블록암호 알고리즘 사용 가이드라인에 대한 표준화를 추진 중임

• 응용서비스에서의 암호 알고리즘 활용 방법

- 국제 표준화 기구 IETF, IEEE 등에서 네트워크 시스템, 시스템 장비, VoIP, IPTV 등의 시스템 및 서비스를 위한 암호 알고리즘에 대한 표준화가 추진되고 있으며, 국내의 경우 VoIP의 음성데이터 암호화에 사용되는 SRTP(Secure Real-time Transport Protocol)내 SEED 암호 알고리즘 적용 방법에 대한 IETF 표준화를 추진하여 제정단계임. 하지만, 클라우드컴

퓨팅과 스마트그리드의 경우, 2009년부터 표준화가 추진되어 아직 초기상태임. 그 이외의 국내에서 추진 중인 암호 알고리즘 및 암호 알고리즘 사용 표준화 현황은 아래와 같음

〈암호기술 표준화 현황〉

구 분	표준번호	제목	표준상태	제정년도
ISO/IEC	18033-3	Information technology --Security techniques -- Encryption algorithms - Part 3: Block ciphers - SEED	표준채택	2005
ISO/IEC	-	Information technology --Security techniques -- Encryption algorithms - Part 3: Block ciphers - HIGHT	표준채택 예정	2011
IETF	RFC4269	The SEED Encryption Algorithm	표준채택	2005
IETF	RFC 4010	Use of the SEED Encryption Algorithm in Cryptographic Message Syntax(CMS)	표준채택	2005
IETF	RFC 4162	Addition of SEED Cipher Suites to Transport Layer Security(TLS)	표준채택	2005
IETF	RFC 4196	The SEED Cipher Algorithm and Its Use with IPsec	표준채택	2005
IETF	-	The SEED Cipher Algorithm and Its Use with the Secure Real-time Transport Protocol(SRTP-SEED)	표준채택 예정	2010
IETF	-	IANA Registry Update for Support of the SEED Cipher Algorithm in the Multimedia Internet KEYing (MIKEY)	표준채택 예정	2010
IETF	-	Modes of Operation for SEED for Use with IPsec	표준채택 예정	2011
IETF	-	Use of the Advanced Encryption Standard (AES) Encryption Algorithm in Cryptographic Message Syntax (CMS)	표준채택	2003
IETF	-	Using Advanced Encryption Standard (AES) Counter Mode With IPsec Encapsulating Security Payload (ESP)	표준채택	2004
IETF	-	Using AES-CCM and AES-GCM Authenticated Encryption in the Cryptographic Message Syntax (CMS)	표준채택	2007
IETF	-	TLS Elliptic Curve Cipher Suites with SHA-256/384 and AES Galois Counter Mode (GCM)	표준채택	2008
IETF	-	Using Advanced Encryption Standard Counter Mode (AES-CTR) with the Internet Key Exchange version 02 (IKEv2) Protocol	표준채택	2010
ITU-T	-	Key managements framework for secure IPTV communication	표준채택 예정	2010
ITU-T	-	Guidelines on criteria for selecting cryptographic algorithms for the IPTV SCP	표준채택 예정	2011

나) 인증기술

• 다양한 인증수단에 대한 보안성 검증 프레임워크

- 사이버 상에서의 다양한 인증수단별 표준화는 활발히 진행되고 있으나, 이들간 보안성을 정의 및 검증하기 위한 부분은 아직까지 시도되지 않고 있음. 다양한 거래유형별로 적합한 인증수단의 선택 및 적용을 위해 이들간 보안수준을 정의 및 검증하기 위한 프레임워크에 대한 표준화 수요가 증가할 것으로 전망됨

• 디바이스 인증 기술 및 응용

- 케이블모뎀과 케이블모델 터미네이션 시스템 간의 기기인증의 경우, 기기인증서 프로파일 및 관련된 규격은 케이블모뎀 업계표준인 Data Over Cable Service Interfase Specification(DOCSIS)에서 정의
- 저작권 발급자로부터 모바일기기까지 안전한 방법으로 콘텐츠를 배포하기 위한 규격으로 OMA(Open Mobile Alliance) 2.0 규격이 존재함. OMA 규격은 CMLA(Content Management Licensing Administrator)는 Intel, Nokia, MEI/Panasonic, Samsung 4개의 회사가 모여서 만든 무한책임회사(LLC). OMA DRM 2.0에서는 PKI기반으로 Right Issuer와 Device간에 Content 보호를 위한 end-to-end protocol을 정의하고 있으며, CMLA는 이를 지원하기 위해 인증(Certification)체계 기기인증서 및 CRL 발급에 대한 규격을 정의

- 2005년에 ISO에서 홈네트워크 보안요구사항과 댁내 및 댁외 보안에 대한 표준을 제정함. ITU-T SG17에서는 2004년부터 홈네트워크 디바이스 인증서 프로파일, 홈네트워크 서비스에서의 사용자인증 프레임워크 등에 대해 표준화를 추진하고 있음
- VoIP의 통신트래픽은 시그널링 트래픽과 미디어트래픽으로 구분되며 시그널링 트래픽에 대한 암호화는 IETF 표준프로토콜인 SIP(Session Initiation Protocol)에서 정의하고 있는 TLS(Transport Layer Security)와 S/MIME(Secure/Multipurpose Internet Mail) 보안프로토콜을 준용하고, 미디어 트래픽은 IETF 표준 프로토콜인 SRTP(Secure Real-time Transport Protocol)을 준용함
- VoIP 통신 트래픽에 대한 암호화를 수행하기 위해서 암호 키의 생성, 전달 및 폐기 등의 키 관리 기능이 필요함. 미디어 트래픽 암호화를 위한 프로토콜인 SRTP에는 키 관리 기능을 정의하고 있지 않으므로, IETF 표준 키 관리 프로토콜인 MIKEY(Multimedia Internet KEYing)을 준용함
- 인가된 사용자에게 VoIP 데이터 접근을 허가하기 위한 주체 확인 및 식별에 의한 접근 제어를 수행해야 함. IETF 표준 프로토콜인 SIP에서는 사용자 인증을 위해 HTTP Digest 인증 프로토콜을 준용함
- 사용자간에 VoIP 메시지를 주고받을 때 메시지 변경을 예방하기 위한 메시지 인증 기능을 수행해야 함. 미디어 암호 프로토콜인 SRTP와 키 관리 프로토콜인 MIKEY에서는 메시지 무결성을 보장하기 위해 HMAC-SHA1 메커니즘을 준용함

구 분	문서명	문서이름	상 태	발표월일
VoIP	RFC 3261	SIP: Session Initiation Protocol	표준	2002.7
	RFC 3711	The Secure Real-time Transport Protocol (SRTP)	표준	2004.4
	RFC 3830	MIKEY: Multimedia Internet KEYing	표준	2004.8
기기인증	RFC 5916	Device Owner Attribute	표준	2010.6

• 일회용패스워드(OTP) 인증 기술 및 응용
- 1995년에 IETF에 일회용패스워드 인증 워킹그룹이 설립되어 S/Key 기술을 일회용패스워드 시스템 표준(RFC 2289)으로 제정한 이래로, OTP 인증기술에 관련한 표준화 활동은 VeriSign사, IBM사, VASCO사 등 60여개의 업체가 참여하고 있는 인증기술 컨소시엄인 OATH(Open AuTHentication)와 RSA사를 중심으로 이루어지고 있음
- 2005년에 OATH에서 제안한 HMAC 기반의 일회용패스워드 알고리즘 표준(RFC 4226)이 제정되었고, 2007년에는 RSA사가 제안한 EAP와 일회용패스워드 프로토콜을 결합한 표준(RFC4793)이 제정되었으며, OATH(Open AuTHentication)에서 제안한 시도-응답방식의 일회용패스워드 알고리즘과 시간 동기화방식의 일회용패스워드 알고리즘에 관한 스펙, RSA사에서 제안한 Kerberos에 일회용패스워드를 적용한 프로토콜과 TLS에 일회용패스워드를 적용한 프로토콜 등이 현재 IETF 인터넷드래프트 버전으로 있음

구 분		문서이름	상 태	발표일
OTP	IETF RFC2289	A One-Time Password System	표준	1998
	IETF RFC4226	HOTP: An HMAC-Based One-Time Password Algorithm	표준	2005
	PKCS #11 v.2.20	PKCS #11 Mechanisms for One-Time Password Tokens	표준	2005
	IETF RFC4758	Cryptographic Token Key Initialization Protocol (CT-KIP) Version 1.0 Revision 1	표준	2006

구 분		문서이름	상 태	발표일
OTP	IETF Internet Draft	XKMS Provisioning of OATH Shared Secret Keys, 2006	표준 초안	2006
	IETF Internet Draft	OTP Methods for TLS, 2006	표준 초안	2006
	IETF RFC4793	The EAP Protected One-Time Password Protocol (EAP-POTP)	표준	2007
	IETF Internet Draft	OTP-Kerberos: Using OTPs in Kerberos pre-authentication	표준 초안	2008
	IETF Internet Draft	OCRA: OATH Challenge-Response Algorithms	표준 초안	2009
	IETF Internet Draft	TOTP: Time-based One-time Password Algorithm	표준 초안	2009
	IETF Internet Draft	Dynamic Symmetric Key Provisioning Protocol (DSKPP)	표준 초안	2009
	IETF Internet Draft	Portable Symmetric Key Container (PSKC)	표준 초안	2009
	ITU-T X.sap-3	The management framework of OTP-based authentication services	표준 초안	2009

• 일회용패스워드(OTP) 인증 시스템 보안 요구사항

- ITU-T 개방형통신기술 보안연구그룹(SG17)의 안전한 응용 프로토콜(Q7) 표준 프로젝트에서 일회용패스워드를 위한 관리 프레임워크(X.sap-3) 표준이 추진중이며, 2010년 최종 표준승인을 목표로 하고 있음

구 분	표준번호	문서이름	상 태	발표일
OTP	ITU-T X.sap-3	The management framework of OTP-based authentication services	표준 초안	2010

• 익명성을 보장하는 인증 기술

- 익명 인증기술과 관련하여 추적 가능한 익명인증서가 2009년 8월 IETF 표준 "Traceable Anonymous Certificate"(RFC 5636)으로 제정됨. 본 표준은 인증서와 실제 사용자간의 연결을 유지하면서, 익명 인증서를 이용하는 이용자에 대해 프라이버시를 제공하기 위한 실질적인 아키텍처와 프로토콜을 정의함
- ISO/IEC는 JTC1 SC27 WG2(Anonymous Authentication)에서 그룹서명 기반의 익명인증 표준화를 추진하고 있음
- 익명 인증기술과 관련하여 가명 기반의 추적 가능한 익명인증서가 2009년 8월 IETF 표준 "Traceable Anonymous Certificate"(RFC 5636)으로 제정됨. 본 표준은 인증서와 실제 사용자간의 연결을 유지하면서, 익명 인증서를 이용하는 이용자에 대해 프라이버시를 제공하기 위한 실질적인 아키텍처와 프로토콜을 정의함
- ITU-T SG17 WP2 Q.7에서는 전자상거래에서 고객들의 프라이버시를 보호하기 위한 요구사항 및 익명인증 모델을 정의하는 "전자상거래를 위한 익명인증 가이드라인" 표준(X.sap-5, 에디터:ETRI 이석준 선임)이 추진되고 있으며, 2011년까지 최종 드래프트를 완성하고자 함
- ISO/IEC JTC1 SC27 WG2에서는 익명 전자서명(Anonymous Digital Signature)과 익명 개체 인증(Anonymous Entity Authentication)에 대해 동시에 표준화가 추진되고 있음. 이 표준들은 각각 세부 Part 2개로 문서가 나뉘어 총 4개의 문서로 진행이 되고 있으며, 익명 개체 인증 표준의 Part 2인 "Mechanisms based on anonymous digital signature(익명 전자 서명 기술 기반 방식)"의 공동 에디터를 한국(포항공대 이필중 교수)에서 담당하고 있음

• 바이오정보를 이용한 전자서명 기술

- ITU-T/SG17 WP2/Q.8은 바이오인식 기술을 유무선 통신 환경에서 활용할 때 발생할 수 있는 다양한 형태의 위협에 대

한 보안 기술을 표준으로 제정하고 있음. 2005-2008 회기를 통해 전자서명과 관련한 바이오인식 관련 표준인 X.1088, X.1089가 국제표준으로 승인됨

- X.1088(Telebiometrics digital key - A framework for biometric digital key generation and protection)은 한국(한신대 이형우 교수)이 제안한 표준으로 X.1084, X.1089가 정의하는 "텔레바이오인식 시스템 메커니즘"과 "텔레바이오인식 인증 인프라스트럭처"를 기반으로 하여 이들과 일관성을 유지하는 동시에 바이오정보 템플릿으로부터 디지털 키를 생성하고 보호하는 프레임워크와 보안 요구사항을 정의하고 있으며, 텔레바이오인식 서비스에서 바이오 데이터의 암호화 및 디지털 서명에 활용할 수 있을 것으로 기대됨
- X.1089(Telebiometrics authentication infrastructure)는 중국의 우와웨이(주)가 제안한 국제표준으로서, PKI와 PMI 환경을 동시에 고려한 바이오정보 인증모델 및 보안 프로토콜을 정의함

〈인증기술 표준화 동향〉

구 분	문서명	문서이름	상 태	발표월일
암호	RFC 3874	A 224-bit One-way Hash Function: SHA-224	표준	2004. 9
	RFC 3279	Additional Algorithms and Identifiers for RSA Cryptography for use in the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile	표준	2005. 6
	RFC4491/3279	Using the GOST R 34.10-94, GOST R 34.10-2001, and GOST R 34.11-94 Algorithms with the Internet X.509 Public Key Infrastructure Certificate and CRL Profile	표준	2006. 5
	RFC4055	Additional Algorithms and Identifiers for RSA Cryptography for use in the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile	표준	2005. 6
인증서	RFC 2459/3280/5280	Internet X.509 Public Key Infrastructure Certificate and CRL Profile	표준	1999.1/20 02.4/2008.5
	RFC 2528	Internet X.509 Public Key Infrastructure Representation of Key Exchange Algorithm (KEA) Keys in Internet X.509 Public Key Infrastructure Certificates	정보	1999. 3
	RFC 3039	Internet X.509 Public Key Infrastructure Qualified Certificates Profile	표준	2001. 1
	RFC 3281	An Internet Attribute Certificate Profile for Authorization	표준	2002. 4
	RFC 3647	Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework	표준	2003. 11
	RFC 3709	Internet X.509 Public Key Infrastructure: Logotypes in X.509 certificates	표준	2004. 2
	RFC 3739	Internet X.509 Public Key Infrastructure: Qualified Certificates Profile	표준	2004. 5
	RFC 3770	Certificate Extensions and Attributes Supporting Authentication in PPP and Wireless LAN	표준	2004. 5
	RFC 3779	X.509 Extensions for IP Addresses and AS Identifiers	표준	2004. 6
	RFC 3820	Internet X.509 Public Key Infrastructure Proxy Certificate Profile	표준	2004. 6
	RFC 4059	Internet X.509 Public Key Infrastructure Warranty Certificate Extension	표준	2005. 5
	RFC 4043	Internet X.509 Public Key Infrastructure Permanent Identifier	표준	2005. 5
	RFC 4325/3280	Internet X.509 Public Key Infrastructure Authority Information Access Certificate Revocation List (CRL) Extension	표준	2005. 12
	RFC 4334/3770	Certificate Extensions and Attributes Supporting Authentication in Point-to-Point Protocol (PPP) and Wireless Local Area Networks (WLAN)	표준	2006. 2
	RFC 4476	Attribute Certificate (AC) Policies Extension	표준	2006. 5
	RFC 4985	Internet X.509 Public Key Infrastructure Subject Alternative Name for expression of service name	표준	2007. 8
	RFC 5280	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile	표준	2008. 5
	RFC5636	Traceable Anonymous Certificate	표준	2009. 8

구 분	문서명	문서이름	상 태	발표월일
인증서 정책	RFC 2527	Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework	정보	1999. 3
	RFC 3628	Policy Requirements for Time-Stamping Authorities	정보	2003. 11
	RFC 3647	Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework	표준	2003. 11
운영/관리	RFC 2510	Internet X.509 Public Key Infrastructure Certificate Management Protocols	표준	1999. 3
	RFC 2511	Internet X.509 Certificate Request Message Format	표준	1999. 3
	RFC 2559	Internet X.509 Public Key Infrastructure Operational Protocols - LDAPv2	표준	1999. 4
	RFC 2585	Internet X.509 Public Key Infrastructure Operational Protocols: FTP and HTTP	표준	1999. 5
	RFC 2587	Internet X.509 Public Key Infrastructure LDAPv2 Schema	표준	1999. 6
	RFC 2875	Diffie-Hellman Proof-of-possession algorithm	표준	2000. 7
	RFC 2797	Certificate Management Messages over CMP	표준	2000. 4
	RFC 4158	Internet X.509 Public Key Infrastructure: Certification Path Building	정보	2005. 9
	RFC 4210/2510	Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP)	표준	2005. 9
	RFC 4211/2511	Internet X.509 Public Key Infrastructure Certificate Request Message Format (CRMF)	표준	2005. 9
	RFC 4387	Internet X.509 Public Key Infrastructure Operational Protocols: Certificate Store Access via HTTP	표준	2006. 2
	RFC 4630	Update to DirectoryString Processing in the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile	표준	2006. 8
	RFC 5274	Certificate Management Messages over CMS (CMC): Compliance Requirements	표준	2008. 6
	RFC 5273	Certificate Management over CMS (CMC): Transport Protocols	표준	2008. 6
	RFC 5272	Certificate Management Messages over CMS	표준	2008. 6
응용 프로 토콜	RFC 2560	Internet X.509 Public Key Infrastructure Online Certificate Status Protocol-OCSP	표준	1999. 6
	RFC 3029	Internet X.509 Public Key Infrastructure Data Validation and Certification Server Protocols	실험	2001. 2
	RFC 3161	Internet X.509 Public Key Infrastructure Time Stamp Protocols (TSP)	표준	2001. 8
	RFC 3379	Delegated Path Validation and Delegated Path Discovery Requirements	정보	2002. 9
	RFC 4386	Internet X.509 Public Key Infrastructure Repository Locator Service	표준	2006. 2
	RFC 4683	Internet X.509 Public Key Infrastructure Subject Identification Method (SIM)	표준	2006. 10
	RFC 5019	The Lightweight Online Certificate Status Protocol (OCSP) Profile for High-Volume Environments	표준	2007. 9
	RFC 5055	Server-based Certificate Validation Protocol	표준	2007. 12
	RFC 5274	Certificate Management Messages over CMS(CMC) : Compliance Requirements	표준	2008. 6
	RFC 5273	Certificate Management over CMS (CMC): Transport Protocols	표준	2008. 6
바이오 인식 관련 인증기술	X.1088	Telebiometrics digital key - A framework for biometric digital key generation and protection	표준	2008. 9
	X.1089	Telebiometrics authentication infrastructure	표준	2008. 9

다) 권한관리 기술

• 기기 관리자 및 소유자간의 권한관리 기술

- IETF에서는 기기의 소유자 속성을 정의하는 RFC 5916(Device Owner Attribute) 표준을 제정함. 기기를 소유하고 있는 개체, 즉 회사 및 기관 등을 지칭하며 이러한 속성은 공개키 인증서 또는 속성인증서에 사용될 수 있음

• 사용자 권한관리를 위한 인증 기술 및 응용

- ITU-T에서 2005년에 ISO와 공동으로 기존 공개키 인증 프레임워크를 확장하여 속성 인증서 프레임워크를 추가하여 표준을 제정하였으며, IETF에서는 인터넷 환경에 적합한 속성 인증 프로파일과 정책 확장에 대한 표준을 제정

2.4. 표준화 대상항목별 현황분석

구 분		암호		
표준화대상항목		유비쿼터스 환경에 적합한 경량 암호 알고리즘	블록암호 알고리즘 운영모드	응용서비스에서의 암호 알고리즘 활용 방법
시장 현황 및 전망	국 내	- 암호 알고리즘 기반 정보보호 제품 시장이 전체적으로 경제 상황이 열악한 가운데 비교적 높은 성장률을 보임 - 신규 IT 서비스의 등장으로 암호 알고리즘의 적용 및 활용방안에 대한 표준화가 필요함		
	국 외	- 전세계 지식정보보안 산업은 미국과 EU 등 2개 지역이 세계시장의 88%를 점유하는 전형적인 글로벌 독과점 산업이며, 일본과 이스라엘이 나머지 시장을 분할하고 있음		
기술 개발 현황 및 전망	국 외	- SEED, HIGHT 등 국내에서 자체 개발한 블록암호 알고리즘을 다양한 보안프로토콜에서 활용할 수 있도록 NIST에서 정의한 운영모드 기반으로 활용하는 방안을 마련하고 있음 - VoIP 환경에서 안전한 통신을 위해 SRTP(Secure Real-time Transport Protocol)에서의 SEED 암호 알고리즘을 활용할 수 있는 방법을 개발함 - IP망에서 데이터가 안전하게 전송될 수 있는 보안기술의 개발이 필요하므로, 이러한 응용 서비스를 고려한 SEED 암호 알고리즘 활용 방법을 개발중에 있음		
	국 내	- NIST에서는 다양한 IT환경에서 블록암호를 활용할 수 있는 운영모드를 개발 중이며, AES 암호 알고리즘을 기반으로 다양한 보안프로토콜에서 운영모드를 활용하는 방안을 마련하고 있음 - 미국, 일본, 유럽의 일부 선진국들은 NIST, NTT, ECRYPT 등을 기반으로 AES, Camellia, Blowfish 등의 암호 알고리즘을 개발하였으며, 네트워크 장비, 시스템 운영체제, IPsec 등의 어플리케이션에 적용할 수 있도록 암호 알고리즘 탑재 제품 및 시스템 개발을 추진하고 있음		
기술 개발 수준	국 내	구현	시제품	구현
	국 외	시제품	상용화	시제품
	기술격차	-1.0년	-2.0년	-1.0년
IPR 보유현황	국 내	경량암호 구현 설계 및 경량 암호알고리즘 관련 특허 보유	블록암호 알고리즘 관련 특허 보유	응용서비스 관련 다수의 IPR 보유
	국 외	-	-	-
IPR확보 가능분야		저전력 사용 등 경량 디바이스에 적합한 알고리즘 개발 및 적용분야 등	다양한 응용에서의 블록암호 알고리즘 적용 및 활용분야 등	다양한 응용서비스에서의 암호 알고리즘 적용 및 활용분야 등
IPR확보 가능성		보통	낮음	높음
표준화 현황 및 전망	국 내	- 국내에서도 자체 기술로 개발한 SEED, HIGHT 등 블록 암호 알고리즘이 다양한 보안프로토콜에서 활용할 수 있도록 NIST에서 정의한 운영모드를 기반으로 국내 표준화를 추진 중임		
	국 제	- IETF에서는 AES를 기반으로 NIST에서 정의한 운영모드를 다양한 보안프로토콜에서 활용하는 방안에 대한 표준화를 추진 중에 있으며, ITU-T에서는 IPTV 서비스 보안을 위해 블록암호 알고리즘 사용 가이드라인에 대한 표준화를 추진 중임 - 미국의 경우, NIST를 기반으로 암호 알고리즘이 활용될 수 있도록, AES, 3TDES(Triple DES) 등이 탑재된 제품을 개발. TLS, S/MINE, IPsec, IEEE 802.11i 등에 적용될 수 있도록 기술을 개발하여 IETF, ISO/IEC, IEEE, ESTI 등에서 국제 표준화를 추진 중임 - 일본의 경우, 3GPP의 UMTS(Universal Mobile Telecommunication System), SSL/TLS, S/MINE 등에서 Camellia, KASUMI, MISTY1 등의 알고리즘이 활용될 수 있도록 하였으며, 국외에서 활용될 수 있도록 ISO/IEC, IETF 등의 국제 표준화를 추진 중임		
	표준화격차	+0.5년	-2.0년	-2.0년
표준화 수준	국 내	제/개정	최종검토	기획
	국 제	제/개정	제/개정	제/개정
표준화 기구/ 단체	국 내	TTA	TTA	TTA
	국 제	IETF, ISO/IEC	IETF, ISO/IEC	IETF, ISO/IEC, ITU-T
	국내참여 업체 및 기관 현황	KISA, ETRI, KIISC, TTA	KISA, ETRI, KIISC, TTA	KISA, ETRI, KIISC, TTA
	국내기여도	보통	보통	보통
국내표준화의 인프라수준		보통	보통	보통
개발 주체	표준개발	TTA	TTA	TTA
	기술개발	연구소, 학계	연구소, 학계	연구소, 학계

구 분		인증					
표준화대상항목		다양한 인증수단에 대한 보안성 검증 프레임워크	디바이스 인증 기술 및 응용	일회용패스워드(OTP) 인증 기술 및 응용	일회용패스워드(OTP) 인증 시스템 보안 요구사항	익명성을 보장하는 인증 기술	바이오정보를 이용한 전자서명 기술
시장 현황 및 전망	국 내	- 현재 국내에 디바이스 인증서가 적용된 사례는 인터넷전화 등 소수에 불과하나, 기기에서의 정보보호 필요성이 지속적으로 부각되어 기기에서의 디바이스 인증수요가 계속적으로 증가할 것으로 전망됨 - 케이블 및 디지털TV 등에서 기기인증서를 이용한 상용서비스 진행 중임 - 인터넷전화, CCTV 등에 대한 기기인증 시범사업과 상용서비스를 준비 중임 - 1990년대 말부터 기업뱅킹을 위해 금융권에서는 OTP 기기를 도입하여 사용하였으며, 2007년도 OTP 통합인증센터 설립 이후 전자금융거래를 위한 1등급 보안 매체 중 하나로 OTP 기기가 선정됨에 따라, 일반 전자금융 사용자에게 OTP 기기 보급이 확대되어 400만 명 이상이 OTP를 사용하고 있으며 이용량이 계속적으로 증가될 전망임 - 온라인 게임 사이트 및 웹포탈 서비스의 사용자 인증 수단으로 모바일 OTP가 사용되고 있으며 100만명이 사용중이며 확대될 전망임 - 익명인증에 대한 시장의 수요는 없으나, 향후 익명인증 분야, 의료정보보안, 클라우드 컴퓨팅 인증, 미래인터넷 보안, 차량통신보안, 익명 핑거프린트 등 폭넓고 다양하게 활용이 예상됨 - 제한적 본인확인제도 등 익명성이 요구되는 제도적인 증가에 따라 기술적으로 안전한 익명성 기술 요구가 증대하고 있는 상황임 - X.509 인증서를 이용한 전자서명 기술과 바이오정보를 결합하는 인증기술에 대해 아직 구체적인 시장수요는 없으나, 인증서 개인키에 대한 보호기술 측면에서 수요가 증가할 것으로 전망됨					
	국 외	- 기존의 케이블모뎀, WiMAX, CCTV, 휴대폰 등의 기기 이외에 스마트그리드에 이용되는 기기 등 다양한 기기에 디바이스 인증서가 적용될 것으로 전망됨 - 2002년 FFIEC(미국 연방금융기관 검사협의회)에서 인터넷뱅킹 사용자 인증을 위해 2-factor 인증 및 OTP 사용을 권고함에 따라 미국의 주요 은행들은 OTP를 전자금융거래에 활용하고 있으며, 미국방성에서도 사용자 인증 및 접근통제 권한 부여를 위해 사용중임 - 싱가폴, 일본, 호주, 유럽 등지에서 주요은행을 중심으로 전자금융거래에 2-factor 인증 도구로 OTP를 이용하고 있으며, 전자상거래, 온라인 교육 등에서도 사용이 확대될 전망임 - 해외 금융권의 인증 매체나 각국 전자정부에서 OTP 인증 수단 정의 - 익명인증에 대한 시장의 수요는 없으나, 향후 수요가 발생할 것으로 예상됨 - 바이오정보를 이용하여 전자서명 기술에 대한 수요는 구체적으로 없으나, 향후 증가할 것으로 전망됨					
기술 개발 현황 및 전망	국 내	- 정부를 중심으로 유비쿼터스 환경에 적합한 인증기술 및 제도 연구 등 향후 다양한 디바이스에서 인증서비스 제공을 위한 신뢰된 인증체계 구축을 위한 사업을 추진 중에 있음 - 디바이스 인증서 관련하여 디바이스 인증서의 발급, 재동 갱신 및 재발급, 경량화된 검증방법 등 다양한 기술개발이 이루어질 예정 - 인터넷 전화, CCTV 등의 제조회사에서는 기기인증서를 수용하여 기기간의 인증을 적용한 제품 개발이 서비스 중임 - 하드웨어 OTP 기기는 토큰형, 카드형, USB 등 다양하게 개발되어 판매중이며, 휴대폰에 탑재되는 형태인 모바일 OTP는 온라인 게임 및 웹포탈 사이트 등에서 사용중임 - 시각장애인을 위한 보이스 OTP 기술, 바코드와 모바일 OTP를 결합한 결제 솔루션 등 OTP 응용기술들이 개발되어 있으며 향후에도 다양한 응용환경에 OTP 인증 기술을 접목한 서비스 개발이 활발할 예정임 - OTP 통합인증 프레임워크의 구축과 함께 여기에 적용된 프레임워크에 대한 개발이 진행되고 있음 - 하나의 OTP 토큰을 가지고 어느 은행에서도 전자금융거래를 수행하는 것이 가능하도록 제공해주는 서비스 제공 구조에 해당함 - 현재 익명 인증은 ETRI와 산학공동으로 그룹서명 기반의 익명ID 기술이 연구개발 중이며 익명ID 발급을 위해 공개키 기반 구조가 사용되고 있으며 익명 인증 기술 및 서비스 등이 학술적인 단계에서 연구가 이루어지고 있으나, 상용 서비스는 이루어지고 있지 않음 - 익명게시판, 익명거래인증 등의 다양한 응용서비스에 대한 적용에 대한 연구가 진행 중임 - ETRI는 익명성 제어가 가능한 그룹서명 기반의 익명인증 기술을 연구개발 중이며 기존에 연구차원으로 진행되어온 그룹서명 기술들에 비해 다양한 실제 서비스에 적용 가능한 연구 진행 중. 또한, 관련 공동연구기관과 함께 실제 서비스에 적용할 수 있는 수준의 요구 사항 도출을 통하여 익명 인증 기술의 실용화 및 국내외 표준화 추진 - 바이오정보를 이용한 전자서명 키 생성기술은 초기 연구단계로, 기술적인 측면에서의 안정적인 구현 및 평가방안 등의 개발이 필요					
	국 외	- 케이블모델, CCTV, WiMAX 등의 기기에 디바이스 인증서를 적용하여 서비스를 하고 있으나, 각 기기별 독자적인 디바이스 인증서 규격을 만들어 사용되고 있음 - 카드형 및 토큰형 OTP 기기들이 개발되어 판매되고 있으며, PC상에서 이용가능한 소프트웨어 OTP, 휴대폰등에 탑재되는 모바일 OTP들이 이용되고 있음 - 전자투표 구현에 익명성을 보장하는 인증기술이 이용되고 있으며, 익명성을 보장하는 응용기술에 대한 연구가 지속적으로 이루어질 것으로 전망됨 - 익명성을 보장하는 인증 기술은 조건부 추적성을 제공하는 그룹 서명 중심으로 연구되어 옴. 특히 2004년 Stanford대학에서 VSC(Vehicle Secure Communication)에서 요구하는 통신량을 만족할 수 있는 수준의 짧은 그룹 서명 기법 등을 연구한 바 있으며, IBM에서 제안한 익명 인증 기법은 TPM Group의 DAA(Direct Anonymous Attestation)에 적용됨 - 바이오정보, 특히 지문정보를 이용한 전자서명 키 생성 기법 등이 연구되고 있으며, 지문 외에도 망막, 홍채 등 다중 바이오정보를 활용한 기술로 발전되고 있음					
기술 개발 수준	국 내	기획	시제품	시제품	상용화	구현	구현
	국 외	설계	구현	설계	상용화	구현	구현
	기술격차	-	+0.5년	+1년	-	+1~1년	+1.0년
IPR 보유현황	국 내	-	홈네트워크 및 디바이스에서의 인증방법 관련 특허 출원	기술 특허(약 50여건)	특허 출원상태(일회용 패스워드 인증 프레임워크)	인터넷 유통환경에 적용가능한 수준의 익명 인증인가 암호 프리미티브 및 핵심모듈 개발을 통한 국내특허 5건 출원	바이오정보를 이용한 인증기술 다수 특허 존재

IPR 보유현황	국 외	-	-	OTP 생성알고리즘 등 다수 기술 특허 출원	-	ETRI에서 Short roup Signature를 기반으로 지역연결성을 제공하는 익명인증 및 회원관리(미국) 등 국제특허 7건 보유	-
IPR확보 가능분야		다양한 인증수단의 보안성 검증을 위한 기준 및 검증절차 등	신규로 등장하게 될 IT 기기에 대한 인증기술 디바이스 인증서 발급/검증 기술 및 활용 서비스 등	유비쿼터스 환경에 접목한 OTP 응용 기술 등	일회용패스워드 통합인증 프레임워크 등	익명인증서 발급 및 익명 권한관리 플랫폼기술 익명인증, 선택적 익명성 제어, 실명추적성, 익명으로 차별화된 개인화 서비스가 가능한 차세대 암호프리미트브 및 익명 PKI 시스템 요소기술	그룹서명 기반의 익명인증 기술 등 바이오정보를 이용한 전자서명 기술
IPR확보 가능성		보통	보통	높음	높음	보통	보통
표준화 현황 및 전망	국 내	- 홈네트워크 등에 적용되는 디바이스 인증서 프로파일에 대한 표준은 제정 - 디바이스 인증서 발급/관리를 위한 절차 및 인증기관 지정 가이드 등에 대한 표준화 추진 예정 - 2009년 TTA의 정보보호기반 프로젝트그룹(PG501)에서 표준화 추진하고 있으며 올해 제정 예정임 - X.509 인증서를 이용한 익명인증 기술 등 익명인증 기술의 표준화가 추진되어 국내 제정 및 국외 표준 추진 중 - 프라이버시 강화형 익명인증기술에 대한 표준화 추진 중 - 가명 기반의 추적 가능한 익명인증서 이용 기술에 대한 국내 및 국외 표준 제정 - 그룹 서명 및 이를 기반으로 하는 프라이버시 강화형 익명인증인가기술에 대한 표준화 추진 중 - ITU-T X.1088 표준을 국내 환경에 맞게 정의한 TTAK.IT-X108(TTA, 2008, 바이오 인식 정보에 기반한 전자서명 키생성 프레임워크)을 제정하였으며, 관련한 표준이 추가적으로 개발될 것으로 전망					
	국 제	- 다양한 인증수단에 대한 보안성 검증을 위한 기준 및 절차 등 프레임워크 관련 표준화 수요가 증가하고 있으나 표준화 수준은 미흡 - 단일 도메인에서 통용되는 디바이스 인증기술에 대한 표준화는 응용서비스별로 추진된 사례가 있으나, 서로 다른 이기종의 기기간 인증 및 호환성 제공을 위한 표준화 수준은 미흡한 실정임 - 최근 유비쿼터스 환경의 도래와 함께 다양한 정보통신기기에 대한 인증 및 권한관리 기술에 대한 국제적인 표준화 수요가 증가할 것으로 예상됨 - OTP 인증기술에 관련한 표준화 활동은 Verisign, IBM, VASCO등 60여개의 업체가 참여하고 있는 인증기술 컨소시엄인 OATH(Open AuTHentication)와 RSA를 중심으로 이루어지고 있음- 최근 OTP를 활용한 부인방지 및 거래연동 기술 등에 대한 표준화가 추진되고 있음 - 국내에서 개발된 추적 가능한 익명인증서가 IETF 표준으로 추진중에 있으며, ISO/IEC SC27에서 그룹서명 기반의 익명인증 기술을 비롯하여 익명 전자서명 기술 및 익명 개체인증 기술에 대한 표준화가 동시에 진행중에 있음 - ITU-T SG17에서는 전자상거래를 위한 익명인증 가이드라인에 대한 표준화가 진행되고 있는 등 국내 기술이 비교적 활발히 제안되고 있음 - 통합인증 및 권한관리 분야의 경우, 단일 도메인에 한정된 접근에서 벗어나 다양한 정보시스템 및 서비스의 보안수준별로 통합관리가 가능한 모델에 대한 표준화 수요가 증가할 것으로 예상됨					
	표준화격차	-1.0년	-	+0.5년	+1.0년	-	-
표준화 수준	국 내	기획	최종검토	최종검토	제/개정	최종검토	개발
	국 제	기획	최종검토	최종검토	최종검토	최종검토	개발
표준화 기구/단체	국 내	TTA	TTA	TTA	TTA	TTA	TTA
	국 제	ITU-T, IETF, ISO/IEC	ITU-T, IETF	ITU-T, IETF	ITU-T, IETF	ITU-T, IETF, ISO/IEC	ITU-T, IETF
	국내참여 업체 및 기관 현황	KISA, TTA	KISA, TTA, 한국정보인증, 한국전자인증	금융보안연구원, TTA	금융보안연구원, TTA	KISA, ETRI, TTA	KISA, ETRI, TTA
	국내기여도	높음	보통	낮음	보통	보통	보통
국내표준화의 인프라수준		높음	높음	높음	높음	보통	보통
개발 주체	표준개발	TTA	TTA	TTA	TTA	TTA	TTA
	기술개발	연구소	연구소, 산업체	연구소, 산업체	연구소, 산업체	연구소	연구소, 산업체

구 분		권한관리		
표준화대상항목		기기 관리자 및 소유자간의 권한관리 기술	통합 권한관리 프레임워크 및 응용 서비스	사용자 권한관리를 위한 인증기술 및 응용
시장 현황 및 전망	국 내	- 최근 많은 기기들이 폐쇄망에서 벗어나 IP 기반으로 연계되고 있어 이에 대한 보안이 크게 대두되고 있는 상황임. 특히 IT강국이라는 이미지에 걸맞게 CCTV나 스마트 그리드 등은 선도적으로 진행하고 있기 때문에 이 분야에 대한 시장은 나날이 성장할 것으로 예상됨 - PMI 등 권한관리 기술은 독자적인 제품으로 구성되지 않고 기존 PKI 제품의 기능 확장 요소로 추가되거나 EAM 제품에 확장 기술로 제품화되고 있음		
	국 외	- 해외에서는 현재 IBS, ITS, SCADA 중심으로 하여 보안 관련 필요성이 대두되고 있으며 불황타개를 위한 방안의 일환으로 관련 분야에 대한 정부 지원에 힘입어 시장이 나날이 성장할 것으로 예상됨. 미국의 경우도 스마트 그리드에 대하여 막대한 투자가 예상되고 있음 - PMI 관련 제품으로서는 Baltimore Technologies사의 SelectAccess, Entrust Technologies사의 Entrust GetAccess, RSA Security사의 ClearTrust, Netegrity사의 SiteMinder 등이 있음		
기술 개발 현황 및 전망	국 외	- 국내는 원천 기술보다는 주로 응용 기술이 발달한 관계로 필요성이나 인프라는 앞서가고 있지만 기본 가이드라인이나 표준 보다는 서비스의 필요에 의해 개별적으로 기술 개발이 이루어지고 있는 상황임 - PMI 기능들은 접근제어 제품, EAM, 포털 관리 및 e-비즈니스 시스템 등에 끼어 들어가는 형태로 동작하고 있지만, 앞으로는 XML 기반으로 발전할 것으로 전망됨		
	국 내	- IBS와 같이 오래 전부터 원천 기술과 많은 기술적 KNOW-HOW를 보유하고 있어 이런 인프라를 기반으로 다양한 시도를 하고 있으며 별도 기술 개발보다는 다른 분야에서 이미 검증된 기술 적용 중심으로 진행되고 있음 - 선도적인 다국적 정보보호업체의 경우에는 PMI관련 표준을 준수하는 제품들을 개발하여 여러 업계에 공급하고 있으며 현재 이러한 권한 관리 제품을 다른 보안 솔루션과 통합한 제품을 집중적으로 연구 및 개발		
기술 개발 수준	국 내	구현	시제품	설계
	국 외	설계	구현	구현
	기술격차	-1.0년	+1.0년	-1.0년
IPR 보유현황	국 내	-	-	속성인증서를 이용한 인증방법 등 특허 출원 중
	국 외	-	-	Method for issuing attribute certificate from an LDAP entry 등 특허 출원 중
IPR확보 가능분야		다양한 응용서비스 환경에서의 다중 사업자에 의한 기기 접근제어 분야 등	다양한 응용서비스 환경에서의 통합 권한관리 및 관련 응용기술 분야 등	다양한 응용에 적용하기 위한 인증기술 및 응용서비스 분야 등
IPR확보 가능성		보통	보통	낮음
표준화 현황 및 전망	국 내	- 국내뿐만 아니라 국외에서도 최근 초고속통신망 확산으로 인해 기존 폐쇄망에 있던 기기들이 인터넷 망에 연결 되면서 기기 인증 및 접근 권한 관리에 대한 이슈가 커지고 있으며 단일 사업자나 관리자일 경우 인증만 필요하겠지만 복수 사업자나 다양한 비즈니스 모델들이 등장함에 따라 이를 뒷받침하기 위한 표준이 필요한 상황임. 기기별로 서비스 별로 각각 진행되고 있지만 기본적인 가이드라인 안에서 진행될 필요가 있음 - 국내의 경우 2008년도에 PMI 관련 표준이 제정되었음		
	국 제	- 국외의 경우 ITU-T에서 2005년에 ISO와 공동으로 기존 공개키 인증 프레임워크를 확장하여 속성 인증서 프레임워크를 추가하여 표준을 제정하였으며, IETF에서는 인터넷 환경에 적합한 속성 인증 프로파일과 정책 확장에 대한 표준을 제정		
	표준화격차	-1.0년	-1.5년	-1.0년
표준화 수준	국 내	개발/검토	기획	기획
	국 제	개발/검토	기획	개발/검토
표준화 기구/ 단체	국 내	TTA	TTA	TTA
	국 제	OMA, ITU-TS, CableLabs, ISO, IET	IETF, ITU-T, IEEE	IETF, ITU-T
	국내참여 업체 및 기관 현황	KISA, ETRI, 한국정보인증, TTA	KISA, TTA	KISA, TTA
	국내기여도	보통	보통	보통
국내표준화의 인프라수준		높음	높음	높음
개발 주체	표준개발	TTA	TTA	TTA
	기술개발	연구소, 산업체	산업체	연구소, 산업체

3. 표준화 추진전략

3.1. 중점기술의 표준화 환경분석

3.1.1. 표준화 추진상의 문제점 및 현안사항

- 암호 · 인증 · 권한관리 기술은 정보보호 기반 기술이지만, 사회적인 관심 부족으로 정부 차원의 지속적인 투자를 이끌어내기가 쉽지 않음. 또한 암호 · 인증 · 권한관리는 보안서비스 제공을 위한 인프라로 인식되고 있음에도 당장 이익을 창출하기 어렵다는 이유로 업체의 신기술 개발 및 표준화 활동이 미미한 실정임
- 무엇보다 암호 · 인증 · 권한관리는 인터넷의 다양한 서비스가 활성화되고 홈네트워크, u-health 등과 같이 새로운 서비스가 정착하기 위하여 꼭 필요한 기반 기술임을 정부기관 이외에 관련 업체들도 인지하는 것이 필수적임. 따라서, 유비쿼터스 환경에 적합한 정보보호 기반기술의 확보를 위한 경량암호 및 양자암호, 암호평가 기술 등 차세대 암호기술에 대한 정부차원의 지속적인 지원이 필요함
- 해킹 등의 공격으로부터 안전하게 데이터를 송수신하기 위한 원천기술인 암호 알고리즘이 개발되고 있으며, 이를 국내 및 국제 표준화 기구에서 표준화 추진을 활발히 수행하고 있음. 반면, VoIP, IPTV, 스마트그리드, 클라우드컴퓨팅, RFID/USN 등의 신규 IT 응용서비스에서 알고리즘 적용에 대한 표준화 추진이 미흡한 실정이므로 관련 기술에 대한 표준화 요구 증가 및 시장 파급효과가 높음
- 또한, 새로운 암호기술이나 새로운 인증기술 개발 이외에도 센서 네트워크와 같이 새로운 네트워크 환경과 초소형 기기들이 등장함에 따라, 기존 기술을 이들 새로운 환경에 적응시키기 위한 기술개발도 선행되어야 함. 소형 기기에서 연산가능한 TinyECC 등의 개발이 이미 국외에서는 진행되고 있으며, 앞서 표준화 동향에서 기존의 다양한 알고리즘들을 새로운 환경의 프로토콜에 적용하기 위한 노력이 진행되고 있음
- 최근 전자금융거래의 인증방법에 대한 규제완화에 따라 거래 유형 및 규모, 위험수준 등에 대응하는 다양한 인증기술이 도입 및 활성화될 수 있는 제도적 기반이 조성됨. 금융기관 등이 안전한 인증방법을 자율적으로 선택할 수 있도록 안전성 검증기준 및 기술 등이 필요하지만, 관련 표준의 부재 등 기반이 미흡한 상황이므로 기준 및 절차에 대한 조기 표준화가 요구됨
- 산업전반에 OTP 인증 기술을 확대하기 위해서는 OTP 기기를 비롯한 관련 인프라 기술 개발이 계속되어야 하는데, 국내 OTP 제조 업체들의 규모가 작고 저가 납품으로 인한 출혈 경쟁으로 전반적인 어려움이 가중되고 있어 신기술 개발의 어려움이 예상됨. 현재 개발 중인 국내 OTP 관련 표준 기술과 기존에 운영되고 있는 OTP 인증 시스템과의 호환성 제공방안의 수립이 필요함
- 다양한 특성과 처리능력을 가진 하드웨어 기반 접근통제 수단이 제시되고 있으나, 이에 기반한 인증방법 및 기술들에 대한 명시적 접근이 미비하여 관련 기술 표준화가 개발되지 못하고 있는 실정임. 접근통제 수단으로서 사용되는 하드웨어의 고유 특성과 활용성을 고려한 인증기술 개발 및 해당 기술에 대한 국내외 표준화 추진이 필요한 상황임
- 요컨대, 유비쿼터스 환경의 보급 및 발전과 함께 정보제공의 주체로 등장한 다양한 정보통신기기 등 디바이스에 대한 식별 · 인증 및 권한관리의 중요성이 대두되고 있으며, 경량화된 소형 디바이스를 포함하는 암호 · 인증 · 권한관리 기술개발 및 표준화 수요가 증가하고 있음

3.1.2. SWOT 분석 및 표준화 추진방향

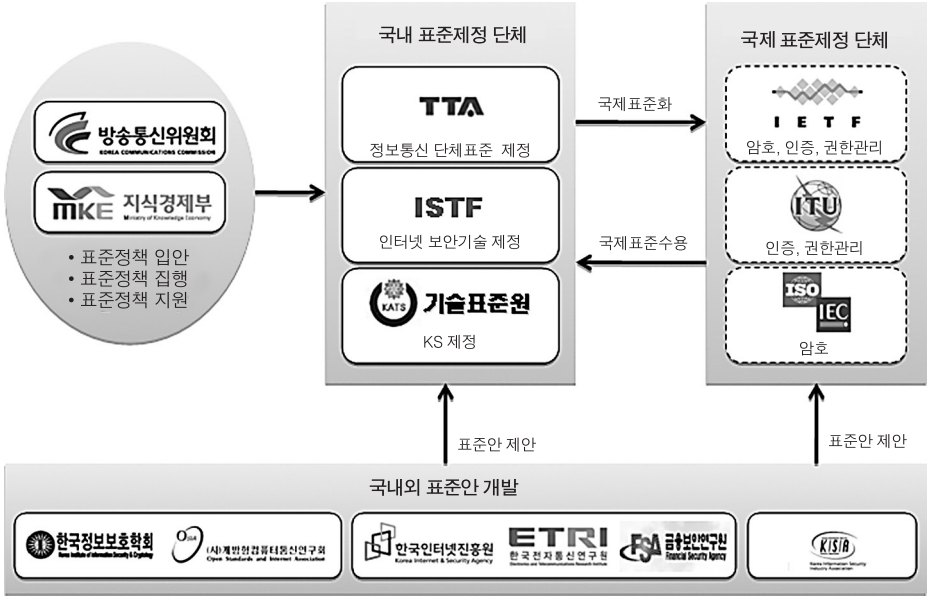
국외환경요인 \ 국내역량요인			강점 요인 (S)		약점 요인 (W)	
			시장	- 다양한 신규 IT서비스 증가에 의한 정보보호 시장도 확대	시장	- 암호, 인증, 권한관리 등은 기반기술로서 시장과 직접적인 연관성 적음
			기술	- 암호,해쉬, PKI 등의 다양한 암호 기반 및 응용기술 확보	기술	- 경량암호 및 차세대 암호에 대한 지속적인 투자 및 연구가 부족
			표준	- 암호 알고리등에 대한 원천 및 구현기술의 국내외 표준 보유	표준	- KISA, ETRI 등 정부기관 중심으로 표준화가 진행되고 있고 학계 및 업체의 참여가 부족
기회요인 (O)	시장	- IT 서비스의 발전으로 국제적으로도 정보보호 제품에 대한 요구증가	• 현황분석에 의한 우선순위 : 1 - u-환경에서의 암호 · 인증기술에 대한 요구 및 응용서비스 경험을 바탕으로 적시에 표준 개발 - IETF, ITU-T 등에서의 국제표준화 역량을 바탕으로 응용기술 분야에 국제 표준 활동 강화 - 익명 인증, 디바이스 인증 등 신규 기술을 바탕으로 국내 독자 IPR 개발하고 이를 바탕으로 국제 표준화 추진		• 현황분석에 의한 우선순위 : 2 - u-IT 서비스를 중심으로 국내 보안기술을 적용하여 국내 시장경쟁력 확보 - 지속적인 기반 기술 개발을 통해 국내 정보보호 수준 선진화 및 제품 경쟁력 향상	
	기술	- 정보통신 기술의 발달, 컴퓨터 성능 향상, 해킹 기술의 고도화 등으로 안전한 정보보호 기반 기술 요구 증가				
	표준	- IETF 및 ITU-T에서 정보보호기반 기술의 표준화 증가				
위협요인 (T)	시장	- FTA 등 시장개방으로 인해 자국 암호만을 사용하도록 의무화하기 어려움				
	기술	- 지속적인 원천기술 개발에 대한 투자 미흡으로 IPR 확보가 미흡	• 현황분석에 의한 우선순위 : 3 - 신규 IT 서비스를 중심으로 정보보호 응용 기술 및 응용서비스 관점에서의 표준 개발을 통한 국제 경쟁력 확보 - CC 평가 및 암호 모듈 평가를 통한 정보보호 제품의 수준 제고 및 국내 정보보호 산업체의 전략적 육성		• 현황분석에 의한 우선순위 : 4 - 지속적인 전문 인력 양성을 통한 자체 기술 기반 확보	
	표준	- 시장개방에 따라 국제적 호환성 보장을 위해 국내 표준보다는 국제표준을 준용함으로써 국외 제품에 의한 국내 시장경쟁력 저하				

SO전략 : 공격적 전략(강점사용-기회활용) / WO전략 : 만회전략(약점극복-기회활용) / ST전략 : 다각화 전략(강점사용-위협회피) / WT전략 : 방어적 전략(약점최소화-위협회피)

• 표준화 추진방향 : WT전략의 중점추진을 통한 SO전략의 보완

- 암호 · 인증 · 권한관리 기술분야의 경우, 정보보호 기반 기술로서 정부차원의 지속적인 선도 기반 기술 개발 및 지속적인 인력양성을 통해 암호 응용 기술, 디바이스 인증 및 익명인증 기술, HW 기반 접근제어 기술 등 세계적으로 경쟁력이 있는 기술들을 선도 개발하여 관련 기술에 대한 IPR 확보 및 국제 표준화 추진
- 국내 표준화 추진을 위해서 기 개발된 기술이나 국제 표준들에 대해 TTA, 기술표준원 등의 표준화 단체를 통해 적극적인 표준 제안이 필요. 특히, 암호응용기술 등과 같은 분야는 국내 다양한 암호응용 서비스와 연계하여 새로운 표준안 도출 및 표준화 추진
- 또한, 최근 국내 표준전문가들이 국제 표준화 기관에 상당수 참석하고 있기 때문에 국외 표준화 전문가와의 지속적인 교류 확대를 통해 국내 기술에 대한 국제 표준화 추진 시 시간 및 노력을 절감하고 다양한 표준들이 채택될 수 있도록 추진
- 정부차원에서 표준화를 추진하는 기업 및 기관에 대해 인센티브 줄 수 있는 제도를 도입하는 등 기술개발 최전방에 있는 기업체들의 적극적인 표준화 추진 동기를 부여하여 제2차 부가산업으로 표준화를 활용할 수 있는 기반 마련. 일반적으로 표준화가 선행적으로 추진될 경우, 국내 기술의 홍보효과는 물론, 국산 보안제품에 대한 국제시장 진출의 활성화에 기여할 수 있음

3.1.3. 표준화 추진체계



• 학계 및 산업계의 경우, 개인 또는 학교/업체 자격으로 표준안을 개발하여 TTA PG에 단체표준으로 제안
- 선행적으로 국제 표준을 제안하는 분야도 있지만, 일반적으로 국내 TTA 등에서 표준안을 추진 후 해당 표준안을 기반으로 국제 표준화 추진

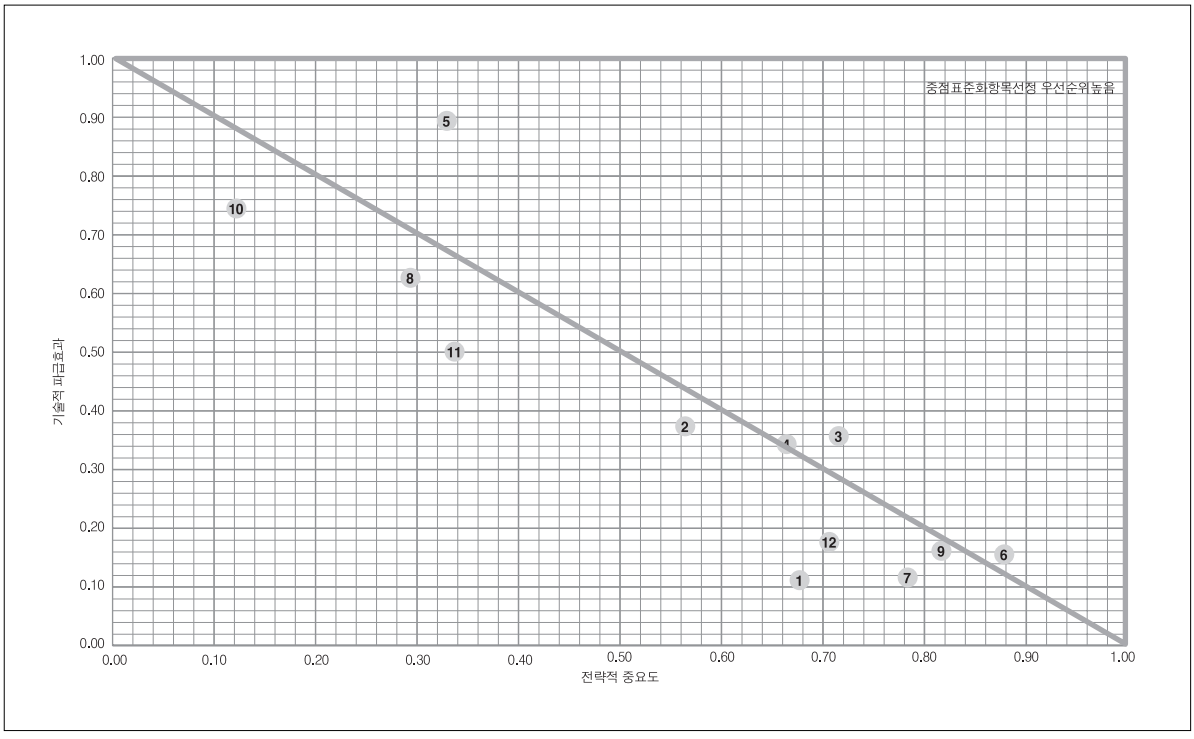
• KISA, ETRI 등에서는 자체 개발한 표준안을 국내 및 국제 표준화 단체에 제안하여 표준화 추진
- 자체적으로 개발한 원내 기술규격 또는 기준 등을 TTA PG에 단체표준으로 제안하거나, 국제 표준화를 추진하면서 완성도가 검증된 버전을 기반으로 국내 표준화를 병행 추진

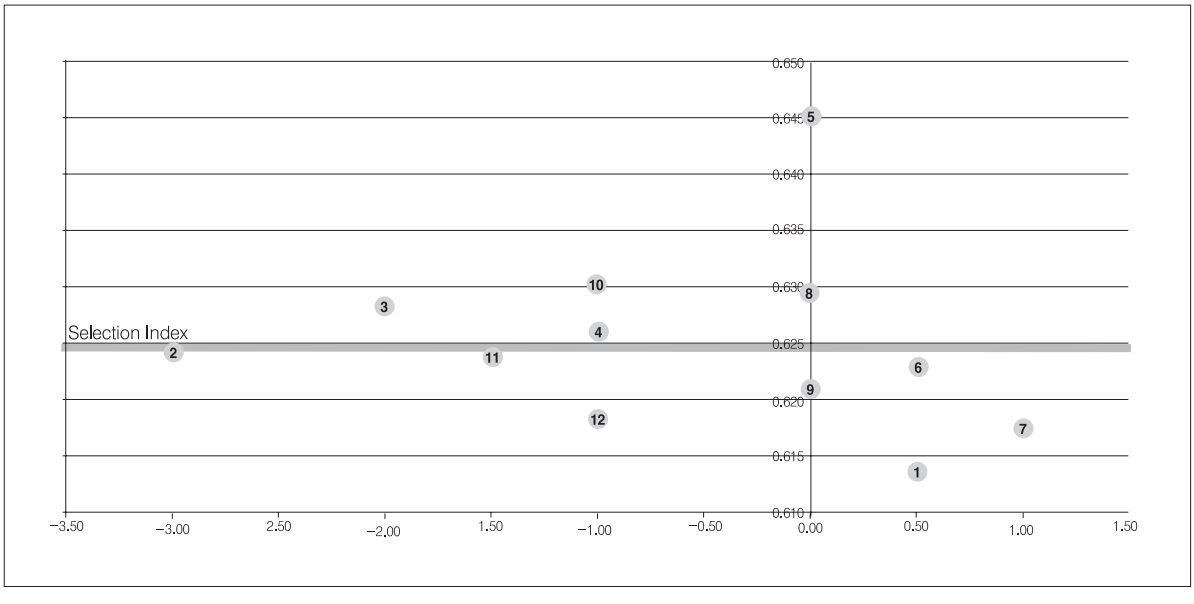
3.2. 중점 표준화항목 선정

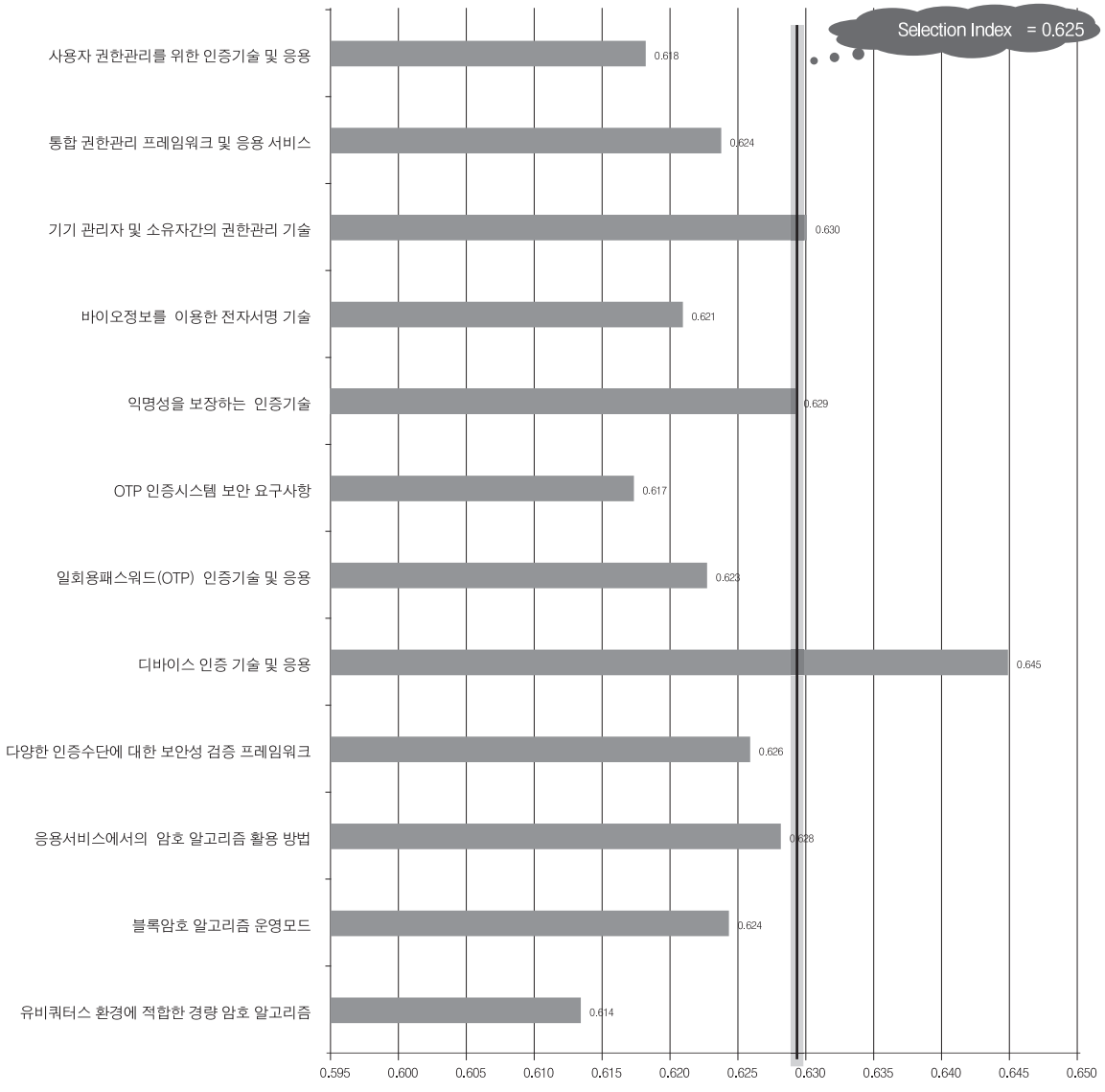
3.2.1. 중점 표준화항목 선정방법

중점기술 후보별 전략적 중요도 및 기술적 파급효과 분석

평가지표	표준화 격차	전략적 중요도(Priority)						기술적 파급효과(Effect)					
		P1 정부 및 산업체 의지(국가 산업전략과의 연관성, 국내 기업의 표준화 참여 및 관심도 등)	P2 공공성(사용자 편리성, 중복 투자 방지 등)	P3 적시성 (현재 표준 수요자의 요구정도 등)	P4 기술적 선도 가능성 (국제표준경쟁력, IPR확보 등)	P5 국제표준화 이슈정도 (국제표준화기구의 표준항목 채택 등)	PI (Priority Index)	E1 기술적 중요도 (원천성 등)	E2 타 기술에 파급효과 (연관성, 활용성 등)	E3 시장파급성 및 상용화 가능성 (구현가능성 등)	E4 산업적 파급효과 (산업화로 인한 이득, 국내 관련산업 규모 및 성숙도 등)	E5 미래 영향력 (미래 표준항목에의 적용/응용성)	EI (Effect Index)
표준화 대상항목 \ 평가지표의 중요도		0.18	0.21	0.25	0.22	0.14	0.40	0.17	0.16	0.24	0.27	0.16	0.60
1 유비쿼터스 환경에 적합한 경량 암호 알고리즘	0.5	2.43	1.86	3.86	3.43	2.71	0.58	3.14	3.43	3.00	4.00	1.71	0.63
2 블록암호 알고리즘 운영모드	-3.0	1.86	2.57	3.57	3.43	2.57	0.58	3.29	3.86	3.86	3.43	1.57	0.66
3 응용서비스에서의 암호 알고리즘 활용 방법	-2.0	2.86	2.57	4.00	3.14	1.43	0.59	3.29	3.43	3.57	3.57	2.14	0.66
4 다양한 인증수단에 대한 보안성 검증 프레임워크	-1.0	3.57	4.43	3.14	1.57	1.57	0.58	2.14	3.29	4.14	3.57	2.57	0.65
5 디바이스 인증 기술 및 응용	0	3.00	3.14	2.86	3.14	1.29	0.56	3.29	2.86	3.86	4.71	1.86	0.70
6 일회용패스워드(OTP) 인증기술 및 응용	0.5	3.57	4.00	3.14	2.29	1.71	0.60	3.29	2.71	3.86	3.57	1.86	0.64
7 OTP 인증시스템 보안 요구사항	1.0	3.14	4.14	3.14	2.14	2.00	0.59	3.00	3.14	3.57	3.43	2.29	0.63
8 익명성을 보장하는 인증기술	0	2.71	3.43	2.86	2.86	1.57	0.55	3.86	2.71	4.14	3.43	2.43	0.68
9 바이오정보를 이용한 전자서명 기술	0	2.71	3.57	3.14	3.29	1.71	0.60	3.86	2.71	3.29	3.57	2.14	0.64
10 기기 관리자 및 소유자간의 권한관리 기술	-1.0	2.29	3.14	2.71	2.86	2.29	0.54	2.43	3.86	3.43	4.29	2.71	0.69
11 통합 권한관리 프레임워크 및 응용 서비스	-1.5	3.43	3.86	2.86	1.57	2.14	0.56	2.71	3.14	4.14	3.57	2.57	0.67
12 사용자 권한관리를 위한 인증기술 및 응용	-1.0	3.14	3.43	2.86	3.00	2.00	0.59	3.29	2.43	3.43	3.57	2.86	0.64


중점표준화항목선정 우선순위높음
기술적 파급효과
전략적 중요도
1.00
0.90
0.80
0.70
0.60
0.50
0.40
0.30
0.20
0.10
0.00
0.00
0.10
0.20
0.30
0.40
0.50
0.60
0.70
0.80
0.90
1.00
5
10
8
11
2
3
12
9
6
1
7


Selection Index
0.650
0.645
0.640
0.635
0.630
0.625
0.620
0.615
0.610
−3.50
−3.00
2.50
−2.00
1.50
−1.00
−0.50
0.00
0.50
1.00
1.50
5
10
3
8
4
2
11
6
9
12
7
1


Selection Index = 0.625
사용자 권한관리를 위한 인증기술 및 응용
0.618
통합 권한관리 프레임워크 및 응용 서비스
0.624
기기 관리자 및 소유자간의 권한관리 기술
0.630
바이오정보를 이용한 전자서명 기술
0.621
익명성을 보장하는 인증기술
0.629
OTP 인증시스템 보안 요구사항
0.617
일회용패스워드(OTP) 인증기술 및 응용
0.623
디바이스 인증 기술 및 응용
0.645
다양한 인증수단에 대한 보안성 검증 프레임워크
0.626
응용서비스에서의 암호 알고리즘 활용 방법
0.628
블록암호 알고리즘 운영모드
0.624
유비쿼터스 환경에 적합한 경량 암호 알고리즘
0.614
0.595
0.600
0.605
0.610
0.615
0.620
0.625
0.630
0.635
0.640
0.645
0.650

3.2.2. 중점 표준화항목 선정사유

• 전략적 중요도 및 기술적 파급효과 평가 결과

- 암호 · 인증 · 권한관리 분야의 중점 표준화 항목으로 선정된 7건의 표준화 항목은 기술적 선도 가능성, 적시성, 정부 및 산업체 의지 등 전략적 중요도와 타기술의 파급효과, 시장파급성 및 상용화 가능성, 산업적 파급효과 등 기술적 파급효과에서 높은 점수를 획득한 표준화 항목을 대상으로 선정함

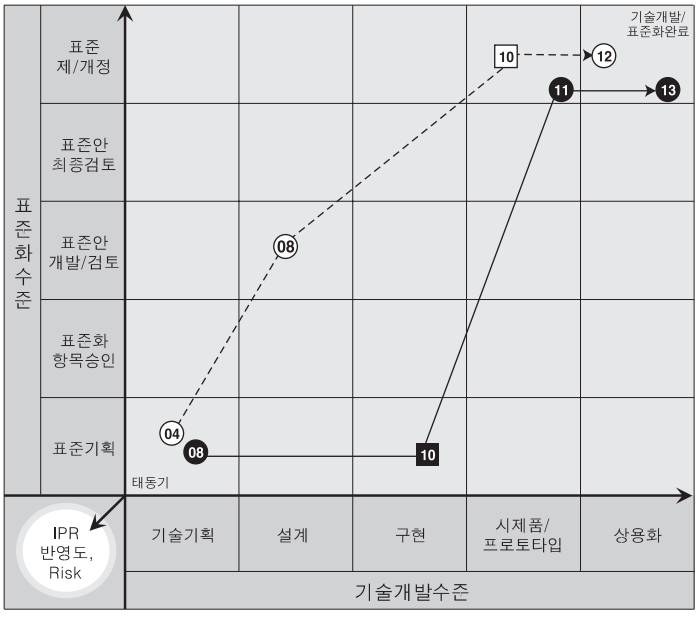
• 중점 표준화항목별 선정사유

- 〔응용서비스에서의 암호 알고리즘 활용 방법〕 해킹 등의 공격으로부터 안전하게 데이터를 송수신하기 위한 원천기술인 암호 알고리즘이 개발되고 있으며, 이를 국내 및 국제 표준화 기구에서 표준화 추진을 활발히 수행하고 있음. 반면, 스마트그리드, 클라우드컴퓨팅, RFID/USN 등의 신규 IT 응용서비스에서 알고리즘이 적용에 대한 표준화 추진이 미흡한 실정이므로 관련 기술에 대한 표준화 요구 증가 및 시장 파급효과가 높은 기술임
- 〔다양한 인증수단에 대한 보안성 검증 프레임워크〕 최근 전자금융거래 제도의 개선에 따라, 다양한 인증수단을 금융기관 등이 도입할 수 있게 됨. 이에 보안수준이 다양한 인증수단 중에서 운영환경에 적합한 것을 선택할 수 있는 기반을 조성함으로써 신뢰성 및 안전성의 제고는 물론, 공정한 기술경쟁 및 시장환경 조성이 요구되고 있으므로 보안성 검증을 위한 프레임워크를 중점 표준화 항목으로 선정함
- 〔디바이스 인증 기술 및 응용〕 유비쿼터스환경의 도래에 따라 인증의 범위가 사람뿐만 아니라 인터넷전화기, CCTV, IPTV 등의 다양한 기기로 확산되고 있으며, 기기인증 기술은 u-City, u-Health 등의 산업전반에서 활발히 적용 가능한 기술이기 때문에 전략적 중요도 측면에서 영향력이 높은 항목으로 중점 표준화 항목으로 선정함
- 〔일회용패스워드(OTP) 인증 기술 및 응용〕 강한 인증을 제공하면서 상대적으로 편리하게 사용할 수 있는 OTP 인증 기술은 10여 년간 유 · 무선 네트워크 접근 제어, 기업 내부망 접속, 전자상거래 및 전자금융거래에서의 사용자 인증 등 다양한 분야에서 활용되어 왔으며 다수의 기술 특허들이 출원되어 있음. 그동안 OTP 인증기술은 해외에서 표준화가 활발하게 진행되고 있는 반면, 국내에서는 이에 관한 표준화 활동이 미비하였음. 그러나 2007년 6월 OTP 통합인증센터 설립이후에 국내 OTP기기 사용자수는 400만명 이상이 되었고, 온라인 게임 등에서 모바일 OTP를 사용하는 사용자 수 역시 100만명을 돌파하고 있는 상황이기에 향후 국내에서 OTP 인증기술에 대한 수요는 더욱 늘어날 전망이기 때문에, OTP 인증 서비스의 안정성을 제공하기 위해서 이에 관한 표준화가 필요함
- 〔익명성을 보장하는 인증기술〕 최근의 불법 게시물 및 악성 댓글 등 사회적으로 문제가 되고 있는 온라인 게시문화를 개선하기 위한 정보보호 기술에 대한 관심이 높아짐에 따라, 평상시에는 익명성을 보장하다가 불법 또는 악의적인 댓글 게시 등 필요시 게시자의 신원을 파악할 수 있는 익명인증 기술의 중요성 부각 및 사회적 수요에 대응하기 위해 중점 표준화 대상으로 선정함
- 〔기기관리자 및 소유자간의 권한관리 기술〕 기기인증 기술의 발달, 다양한 기기인증 응용서비스의 등장과 함께 유비쿼터스 환경의 서비스 제공주체로 등장한 다양한 기기와 기기를 관리하는 기기관리자 및 기기를 소유하는 기기소유자에 대한 권한관리 기술이 요구됨. 이에 따라 해당 항목은 기술적 파급효과 측면에서 산업적 파급효과와 타기술에 파급효과가 높아 선정함
- 〔통합 보안관리 프레임워크 및 응용 서비스〕 전자정부 등 대규모 조직에서 다양한 인증 및 권한관리 체계를 표준화 없이 도입 · 운영하다 보니 보안수준에 따른 차별적인 관리의 어려움 및 기관별 보안 솔루션의 중복 도입 등의 문제가 발생하고 있음. 이에 다양한 정보시스템 및 서비스의 보안수준에 따른 신뢰수준 관리, 통합인증 및 정보자원에 대한 접근권한 제어, 사용이력 기록 등을 지원하기 위한 통합 권한관리 프레임워크 표준화의 중요성을 고려해 중점 표준화 대상으로 선정함

3.3. 중점 표준화항목별 세부전략(안)

3.3.1. 응용서비스에서의 암호알고리즘 활용 방법

• 표준화-기술개발-IPR 연계분석



표준화 중요도	국내 개발주체		활용도	관련 국제 표준화 기구
고(★★★) 중(★★☆) 저(★☆☆)	표준개발	기술개발		
★★★	KISA, ETRI, KIISC, TTA-PG501	KISA, ETRI 등	VoIP, IPsec 등	ISO/IEC IETF, ITU-T 등

범 례

10 : 중점 표준화항목의 국내상태

10 : 중점 표준화항목의 국제상태

→ : 중점 표준화항목의 국내 표준상태전이

-→ : 중점 표준화항목의 국제 표준상태전이

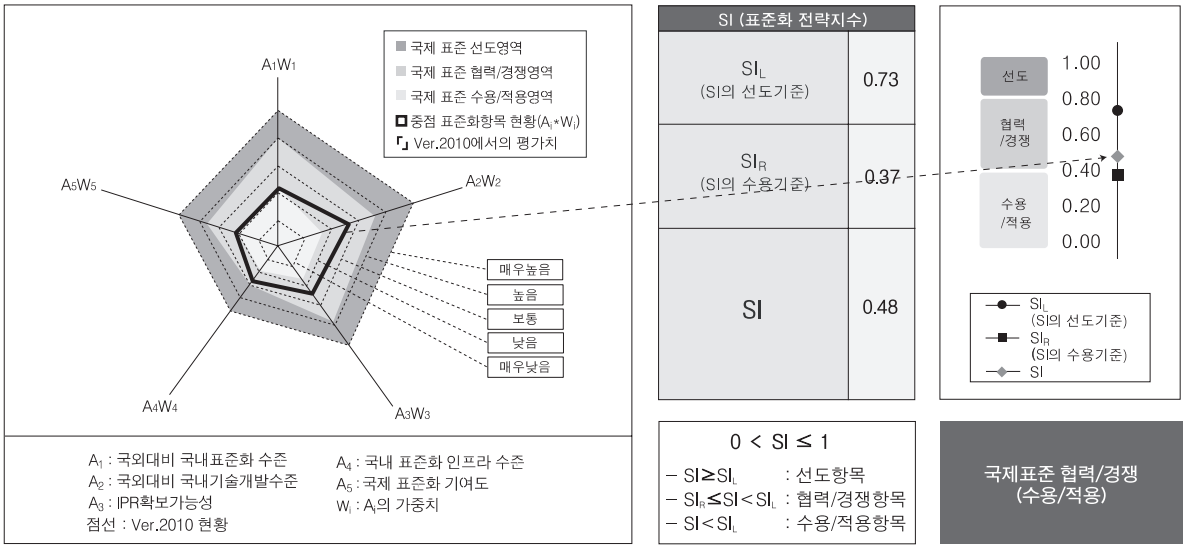
↑ : 선행표준(선 표준화 후 기술개발)

↗ : 동시표준(표준화&기술개발 동시추진)

↓ : 후행표준(선 기술개발 후 표준화)

표준화 특성	선행표준
표준화-기술개발- IPR 연계방안	IT 강국으로서 선도 기술 및 서비스에 국산 암호 알고리즘을 활용하는 표준개발 및 IPR 확보. 이를 기반으로 관련 기술 및 서비스 경쟁력 선점 도모

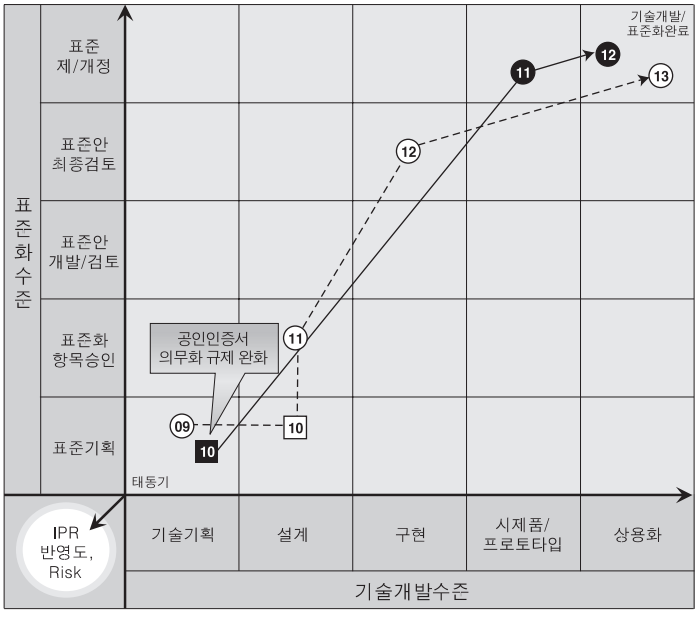
• 국제표준화 전략목표 및 세부전략(안)



국제표준화 전략목표	국제표준 협력/경쟁(수용/적용)
Trace Tracking (Ver.2010 ⟼ 2011)	- 본 중점 표준화 항목의 경우 Ver.2010 신규 항목임. 최근 국외 표준화단체에서 VoIP, IPTV, 스마트그리드, 클라우드컴퓨팅, RFID/USN 등 신규 IT 기술에 암호알고리즘을 활용하는 방법에 대한 표준화를 활발히 진행하는 등 표준화 수준은 점차적으로 상향되는 경향임
세부전략	- 블록암호 알고리즘과 같은 고전적 암호기술은 이미 국내외에서 표준화가 완료되었으므로, 이들 보다는 다양한 ICT 응용 및 융합서비스에 대한 안전성 강화를 위해 이들 암호기술을 적용 및 활용하는 방안에 집중하는 것이 효과적임. 즉, 신규 암호 알고리즘의 개발보다는 이를 다양한 응용에 활용하는 방안의 개발 · 보급을 통한 서비스 안전성 및 신뢰성 제고를 도모 - 2000년 초기부터 다양한 암호 응용기술 개발이 추진되어 왔으며, 최근에는 클라우드컴퓨팅, 스마트그리드, 텔레매틱스 등 신규 서비스에 대한 안전성 보장을 위해 암호기술 적용 및 활용을 위한 연구가 활발히 진행되고 있는 등 국내외 표준화의 필요성 및 중요성이 증가하고 있음 - 블록암호 등 알고리즘 관련 기술 및 서비스에 대한 특허는 이미 많이 출원된 관계로 IPR 확보가 어려울 것으로 판단되지만, 최근의 다양한 신규 서비스들에 적용하기 위한 암호 응용기술 분야는 신규 IPR을 확보할 여지가 많을 것으로 기대 - 암호 알고리즘 및 응용기술 관련 표준화 활동이 KISA 및 TTA 등을 중심으로 지속적으로 추진되고 있는 등 국내 표준화 인프라는 좋은 편이므로, 이를 활용한 실효성 있는 표준화 추진을 통해 경쟁력을 강화 - ISO/IEC, IETF 등에서 다양한 응용 서비스에서 적용 가능한 암호 알고리즘에 대한 표준화 추진이 활발히 진행되고 있으므로, 국내 전문가들의 적극적인 참여 및 이를 수용한 국내 표준화를 통해 적용을 확산
IPR 확보방안	- 국내 암호 알고리즘을 다양한 IT 서비스들에 적용하여 응용 서비스 분야 도출, 응용 환경에 적용 가능한 방법 개발하여 국내외 IPR 확보

3.3.2. 다양한 인증수단에 대한 보안성 검증 프레임워크

• 표준화-기술개발-IPR 연계분석



표준화 중요도	국내 개발주체		활용도	관련 국제 표준화 기구
고(★★★) 중(★★☆) 저(★☆☆)	표준개발	기술개발		
★★★	KISA, 금강원, TTA-PG501	KISA, 금보연 등	금융사, 쇼핑몰, 공공/행정 등	ISO/IEC ITU-T, IETF 등

범 례

10 : 중점 표준화항목의 국내상태

10 : 중점 표준화항목의 국제상태

→ : 중점 표준화항목의 국내 표준상태전이

⇢ : 중점 표준화항목의 국제 표준상태전이

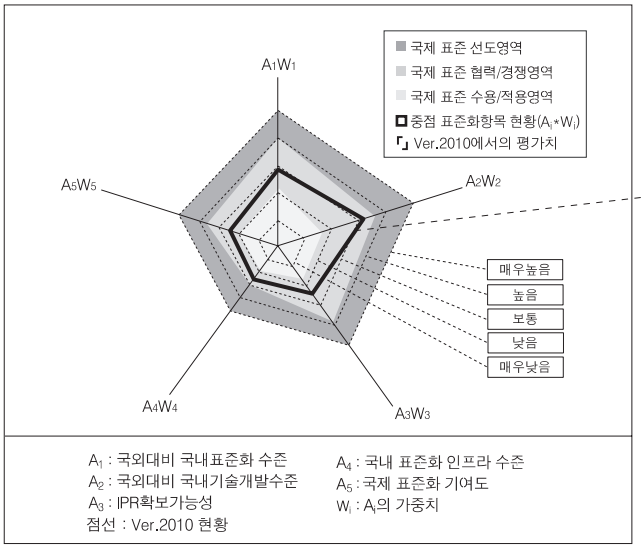
↑ : 선행표준(선 표준화 후 기술개발)

↗ : 동시표준(표준화&기술개발 동시추진)

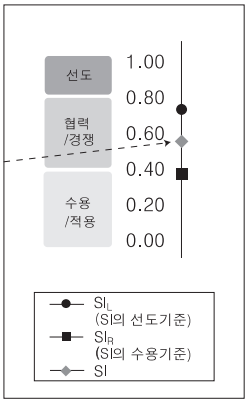
↓ : 후행표준(선 기술개발 후 표준화)

표준화 특성	동시표준
표준화-기술개발- IPR 연계방안	표준화 및 기술개발을 병행하는 한편, 보안성 검증 기준 및 절차, 방법론에 대한 IPR 확보 추진

• 국제표준화 전략목표 및 세부전략(안)



SI (표준화 전략지수)	
SI_L (SI의 선도기준)	0.73
SI_R (SI의 수용기준)	0.37
SI	0.55



$0 < SI \leq 1$

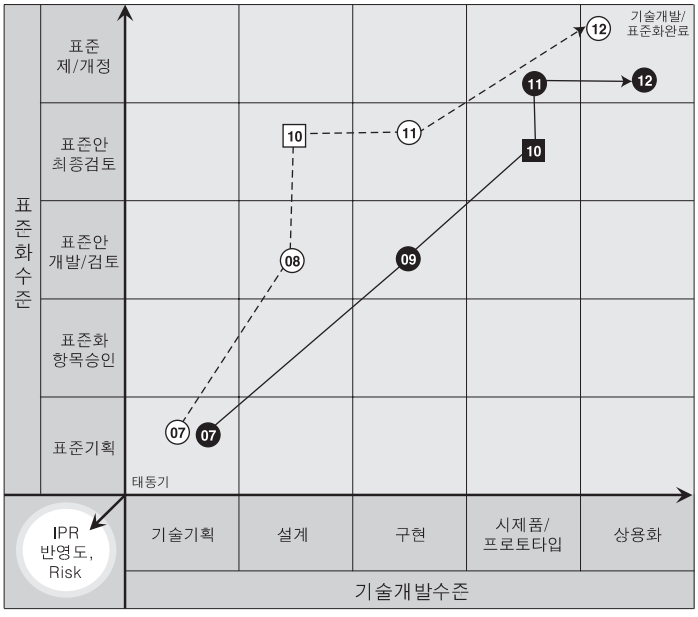
- $SI \geq SI_L$: 선도항목
- $SI_R \leq SI < SI_L$: 협력/경쟁항목
- $SI < SI_L$: 수용/적용항목

국제표준 협력/경쟁

국제표준화 전략목표	국제표준협력/경쟁
Trace Tracking (Ver.2010 ⟼ 2011)	- 본 중점 표준화 항목의 경우 Ver.2010 신규 항목임
세부전략	- 다양한 인증수단별 기술 · 운영 규격 등 개별적인 표준화 수준은 준수한 편이나, 이들간의 보안수준 산정 및 검증 등 특정 서비스 및 플랫폼에 적합한 인증수단을 개발 · 도입 및 검증하기 위한 지침 역할을 할 표준은 부재한 실정임. 국외의 경우엔 사이버 환경에서의 인증수단이 갖추어야할 보안 요구사항을 중심으로 표준화가 진행된 사례가 있으나 아직 초기단계이므로 전략적으로 접근하면 조기에 선도할 수 있음 - 국내 인터넷뱅킹 및 전자상거래, 전자정부 등에서의 전자결제는 양과 질에서 세계 최고수준에 이르는 등 관련 기술개발 및 상용화는 매우 활성화되어 있음. 반면에 이러한 국내 기술이 국외에 수출 및 적용된 사례는 드문데, 글로벌 환경에 적합한 전자결제 인증수단의 개발 및 도입을 촉진할 수 있는 기반 조성을 위해 보안성 검증 프레임워크의 국제 표준화가 요구됨 - 다양한 응용서비스 및 플랫폼에서의 안전한 전자결제를 지원하는 인증수단에 대한 요구사항 도출 및 검증 등을 지원함으로써 인증기술 개발 및 검증분야의 IPR을 확보할 수 있음 - 2010년 6월, 다양한 인증수단의 도입을 허용한 전자금융감독규정 및 시행세칙의 개정에 따라 관련 기술개발 및 경쟁이 활발할 것으로 예상되지만, 보안 적합성을 평가 · 검증하기 위한 기준 및 절차 등에 관한 표준화는 미흡한 실정임. 인증수단이 갖추어야할 보안 요구사항 및 이를 평가 · 검증하기 위한 기준 및 절차에 대한 표준화 추진 및 제도 도입이 시급함 - 스마트폰의 등장 등으로 모바일 환경에서의 전자결제가 활성화되는 추세에 따라 ISO, ITU-T 등 다양한 표준화 기구에서 관심을 가질 것으로 기대됨. 상대적으로 강화된 인증수단의 도입이 활성화된 국내 시장에서 검증된 기술 및 기준 등을 중심으로 국제 표준화 선도가 요구됨
IPR 확보방안	- 다양한 인증수단에 대한 표준 보안강도 산출을 위한 보안성 검증 기준 및 절차, 방법론 등에 대한 국내외 IPR 확보를 추진

3.3.3. 디바이스 인증 기술 및 응용

• 표준화-기술개발-IPR 연계분석



표준화 중요도	국내 개발주체		활용도	관련 국제 표준화 기구
고(★★★) 중(★★☆) 저(★☆☆)	표준개발	기술개발		
★★★	KISA, ETRI, TTA-PG501	ETRI, 보안업체	VoIP, CCTV, RFID 등	IETF, ITU-T

범 례

10 : 중점 표준화항목의 국내상태

10 : 중점 표준화항목의 국제상태

→ : 중점 표준화항목의 국내 표준상태전이

-→ : 중점 표준화항목의 국제 표준상태전이

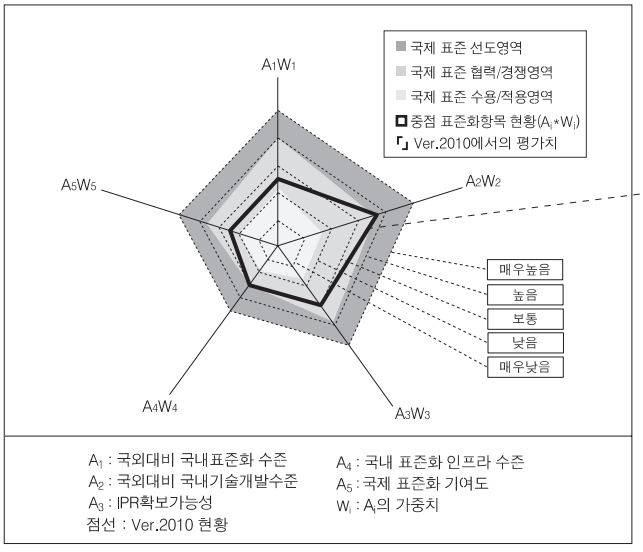
↑ : 선행표준(선 표준화 후 기술개발)

↗ : 동시표준(표준화&기술개발 동시추진)

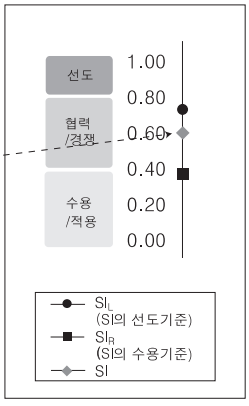
↓ : 후행표준(선 기술개발 후 표준화)

표준화 특성	동시표준
표준화-기술개발- IPR 연계방안	국내의 기기인증체계를 통한 기술개발을 추진하고 이를 바탕으로 한 국제표준을 선도하여 IPR 확보 필요

• 국제표준화 전략목표 및 세부전략(안)



SI (표준화 전략지수)	
SI_L (SI의 선도기준)	0.73
SI_R (SI의 수용기준)	0.37
SI	0.60



$0 < SI \leq 1$

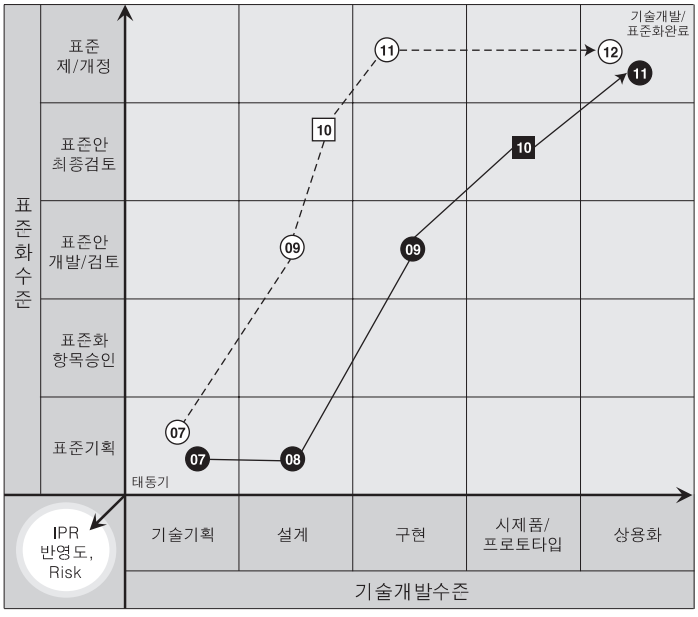
- $SI \geq SI_L$: 선도항목
- $SI_R \leq SI < SI_L$: 협력/경쟁항목
- $SI < SI_L$: 수용/적용항목

국제표준 협력/경쟁 (선도)

국제표준화 전략목표	국제표준 협력/경쟁(선도)
Trace Tracking (Ver.2010 ⟼ 2011)	- 본 중점 표준화 항목의 경우 Ver.2010 신규 항목임
세부전략	- ITU-T, TTA 등 국내외 표준화 단체에서 홈 네트워크용 디바이스 인증서 프로파일 표준이 국내 전문가 주도로 개발되는 등 디바이스 인증분야의 선도적인 역량을 지속적으로 유지함으로써 국제 표준화 선도 - 국내에서는 유비쿼터스 사회의 도래에 따라 u-시티 구축사업 등 정부 · 지자체 및 산업체 주도로 다양한 디바이스를 활용한 서비스 도입이 추진되고 있으며, 비인가된 디바이스를 통한 정보유출 및 위변조 등을 방지하기 위한 디바이스 식별 · 인증 분야에서 기술개발 및 표준화를 병행하여 추진 - 홈 네트워크용 디바이스에 대한 인증방법은 이미 국내 특허가 출원된 상태지지만, 최근의 스마트폰 및 스마트미터기 등 신규 디바이스를 위한 인증 및 응용 부분은 새로운 IPR 확보의 여지가 있음. 이에 표준화 추진 및 기술 개발을 병행하는 한편, 응용서비스별 인증 및 응용기술 관련 IPR 확보를 추진 - 디바이스 인증 관련 국내 기술 개발은 KISA, ETRI, LG CNS 등 연구소 및 산업계에서 활발히 진행되고 있으며, TTA를 통해 국내 표준화를 추진중 - 국제적으로도 ITU-T, ISO, IETF 등 다양한 표준화 기구에서 디바이스 인증에 많은 관심을 가지고 있고, 국내 디바이스 인증기술이 경쟁력을 확보하고 있으므로, 디바이스 인증 분야에 국내 전문가가 지속적으로 참가한다면 표준화 선도도 가능할 것으로 기대
IPR 확보방안	- 현재, KISA 중심으로 한국정보인증과 한국전자인증을 통한 기기인증서 발급 체계가 구축되어 있고 이를 통한 인터넷전화, CCTV등의 기기에 대한 인증서 발급이 진행중에 있음. 또한 인증서가 필요한 스마트 그리드 등 다양한 기기에 대한 발급이 요구되고 있어, 이를 국내시장의 성공적인 사례를 바탕으로 국외의 IPR 확보에 대한 노력이 필요하다고 판단됨

3.3.4. 일회용 패스워드(OTP) 인증기술 및 응용

• 표준화-기술개발-IPR 연계분석



표준화 중요도	국내 개발주체		활용도	관련 국제 표준화 기구
고(★★★) 중(★★☆) 저(★☆☆)	표준개발	기술개발		
★★★	금보연, TTA –PG501	보안업체 등	제조업, 서비스, 공공/행정 등	IETF, ITU–T

범 례

10 : 중점 표준화항목의 국내상태

10 : 중점 표준화항목의 국제상태

→ : 중점 표준화항목의 국내 표준상태전이

-→ : 중점 표준화항목의 국제 표준상태전이

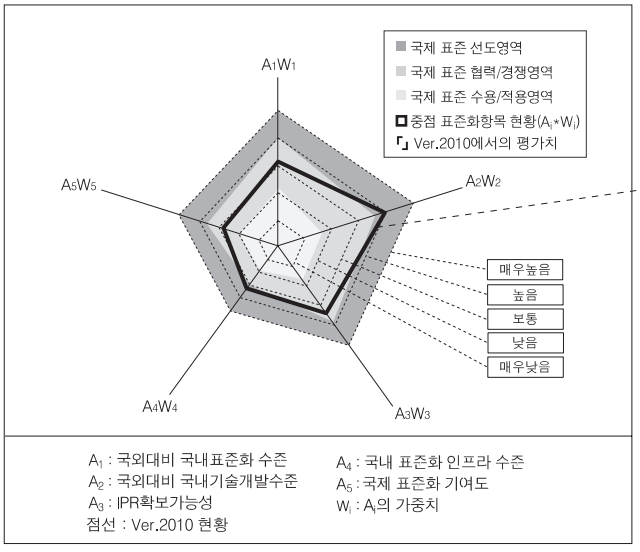
↑ : 선행표준(선 표준화 후 기술개발)

↗ : 동시표준(표준화&기술개발 동시추진)

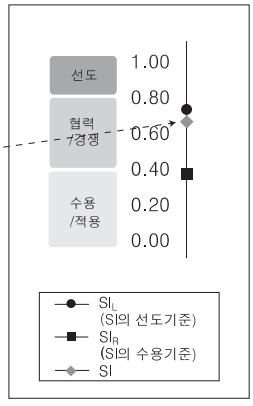
↓ : 후행표준(선 기술개발 후 표준화)

표준화 특성	동시표준
표준화-기술개발- IPR 연계방안	OTP 관련 인증기술 개발은 최근 금융권에서의 활발한 이용에 따라 점차적으로 확대되고 있는 실정이기 때문에 국내에 적용된 우수한 OTP 인증기술에 대한 국내 및 국제표준화 추진을 통해 IPR 확보기반 마련 필요

• 국제표준화 전략목표 및 세부전략(안)



SI (표준화 전략지수)	
SI_L (SI의 선도기준)	0.73
SI_R (SI의 수용기준)	0.37
SI	0.67



$0 < SI \leq 1$

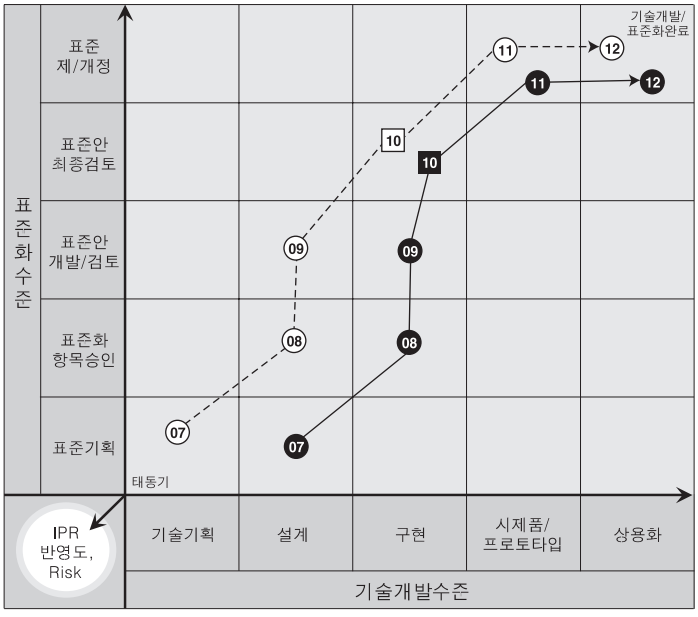
- $SI \geq SI_L$: 선도항목
- $SI_R \leq SI < SI_L$: 협력/경쟁항목
- $SI < SI_L$: 수용/적용항목

국제표준 협력/경쟁 (선도)

국제표준화 전략목표	국제표준 협력/경쟁(선도)
Trace Tracking (Ver.2010 ⟼ 2011)	- 본 중점 표준화 항목의 경우 Ver.2010 신규 항목임
세부전략	- OTP 인증 기술 및 응용과 관련한 분야의 표준화는 IETF를 통해 OTP 기본 인증기술이 표준화되어 있으며, 기존의 TLS, Kerberos 등의 인증 프로토콜과 연동하는 방안도 이미 표준화가 추진됨. 국내 TTA에서는 2008년부터 OTP와 관련한 암호키 관리, 키 배포 파일, 인증 프레임워크 등이 표준화 추진 중에 있음. OTP 인증기술의 상호연동 및 보안성 강화를 위한 표준 기술들은 여전히 개발 중이며, 특히 OTP 응용과 관련한 표준기술에 대한 표준안의 개발 노력이 활발히 요구됨 - OTP 기기 및 인증 기술의 개발은 국내외적으로 상당한 완성도를 가지고 있으며, 많은 분야에서 이미 사용 중임. 해외의 제품은 대부분 상호연동을 고려하지 않고 해당 도메인에서만 사용되는 방식으로 구현되어 있으나, 국내의 경우 금융분야에서 OTP 통합인증센터를 통해 OTP 상호인증이 제공되고 있음. 국내의 OTP 상호인증 기술의 우월성을 기반으로 한 표준안 개발 및 모바일 OTP 등의 최신 응용기술에 대한 표준기술 개발 필요 - 금융분야의 활발한 이용으로 인해 국내 IPR 현황은 약 50여건의 관련된 특허가 출원되어 있으며, 현재도 꾸준하게 관련 특허 출원이 진행되고 있음. 표준기술을 기반으로 하는 국내 특허의 개발 및 확보도 가능할 것으로 전망되며, 표준화를 통해 실효성 있는 IPR의 추진을 가능하도록 함 - OTP와 관련한 국내 금융분야의 인프라는 전 세계적으로 매우 우수한 상황이며, 2010년 7월에 발급자 수가 400만명을 돌파하였음. 국내의 선진 기술 및 인프라를 활용한 표준 개발을 통해 국제 경쟁력 확보가 용이함 - OTP 기반기술에 대한 국제 표준화는 미국의 산업분야에서 시작되었지만, 응용기술 및 상호연동성과 관련한 기술은 국내의 선진 인프라를 기반으로 국제 표준화를 선도할 수 있을 것으로 기대. 국내 OTP 업체 및 관련 기관의 협조 및 지원을 통해 국제 표준화를 추진하여 중장기적으로 OTP 표준기술의 주도권을 확보
IPR 확보방안	- 현재 OTP 기반 기술에 대한 특허가 국내외적으로 많이 출원되어져 있기 때문에 고전적인 OTP 기술에 대한 IPR 확보보다는 다양한 응용에 적용가능한 OTP 인증기술을 개발하고 이에 대한 IPR 확보 노력 필요

3.3.5. 익명성을 보장하는 인증기술

• 표준화-기술개발-IPR 연계분석



표준화 중요도	국내 개발주체		활용도	관련 국제 표준화 기구
고(★★★) 중(★★☆) 저(★☆☆)	표준개발	기술개발		
★★★	KISA, ETRI, TTA-PG501	ETRI, 보안업체 등	게시판, 지불 거래인증, 회원가입	ITU-T, IETF ISO/IEC

범 례

10 : 중점 표준화항목의 국내상태

10 : 중점 표준화항목의 국제상태

→ : 중점 표준화항목의 국내 표준상태전이

⇢ : 중점 표준화항목의 국제 표준상태전이

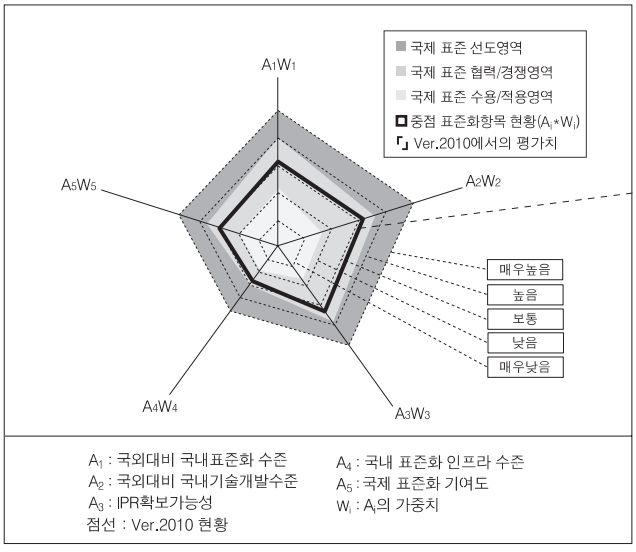
↑ : 선행표준(선 표준화 후 기술개발)

↗ : 동시표준(표준화&기술개발 동시추진)

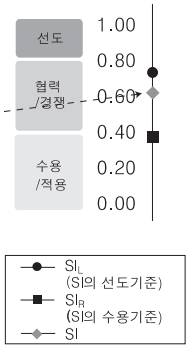
↓ : 후행표준(선 기술개발 후 표준화)

표준화 특성	선행표준
표준화-기술개발- IPR 연계방안	국내의 기술개발을 바탕으로 기술검증을 통한 국제표준을 선도하여 다양한 IPR 확보 추진

• 국제표준화 전략목표 및 세부전략(안)



SI (표준화 전략지수)	
SI_L (SI의 선도기준)	0.73
SI_R (SI의 수용기준)	0.37
SI	0.62



$0 < SI \leq 1$

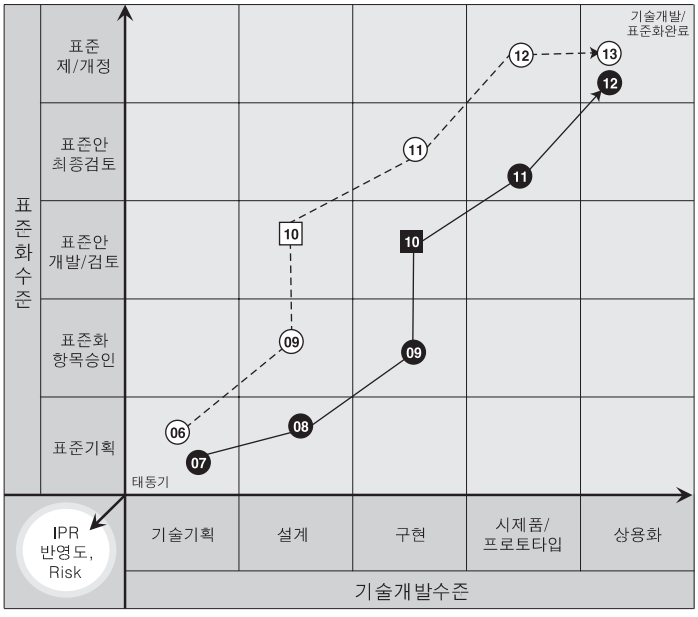
- $SI \geq SI_L$: 선도항목
- $SI_R \leq SI < SI_L$: 협력/경쟁항목
- $SI < SI_L$: 수용/적용항목

국제표준 협력/경쟁 (선도)

국제표준화 전략목표	국제표준 협력/경쟁(선도)
Trace Tracking (Ver.2010 ⟼ 2011)	- 본 중점 표준화 항목의 경우 Ver.2010 신규 항목임
세부전략	- 익명인증기술 분야는 국내에서 독자적으로 개발한 기술이 IETF에서 국제 표준으로 채택되었고, 동시에 국내 TTA에서도 해당 표준화가 추진되는 등 이에 기반한 상용서비스가 가능한 제품을 개발하기 위한 상세 표준화 노력 필요 - 익명인증에 대한 기술 표준화는 국내외적으로 추진되는 반면, 아직 기술개발은 아직까지 시제품 수준을 벗어나지 못하고 있음. 최근 인터넷상에서 악성 댓글 등의 피해를 줄이기 위해 익명인증에 관심을 가지고 있기 때문에 국내 익명인증 기술개발도 조만간 활성화될 것으로 전망되는 등 해당 익명인증 서비스와 관련된 표준안 개발 필요 - 익명인증기술 관련 국내 특허출원은 시작단계로 해당 기술에 대한 IPR 확보는 타 기술보다는 가능성이 높은 것으로 판단됨. 따라서, 국내 IPR은 물론, 국제 IPR까지 고려한 표준화 추진이 필요 - 익명인증기술 등 국내에서 개발된 기술에 대한 표준화는 ETRI, TTA를 중심으로 활발하게 진행되고 있으며, 관련 기술 전문가들의 적극적인 관심과 참여를 통해 국제 경쟁력을 갖춘 표준화 개발 필요 - 익명인증기술의 경우 국내에서 먼저 적극적으로 국제 표준화를 제안 및 추진한 것으로 그간 IETF, ISO 등에서 지속적인 국제 표준화 참여 및 기여를 통해 얻어낸 성과라 할 수 있음. 차기 표준채택을 위해서 보다 적극적이고 영향력 있는 표준화 활동이 필요
IPR 확보방안	- 익명인증기술은 국내에서 주도로 익명인증기반의 상용서비스를 가능할 수 있도록 기술개발이 진행 중이고 이를 바탕으로 국외표준을 선도하고자 중임. 즉 국외표준화를 선도하고 이를 바탕으로 한 익명기술 및 서비스를 제공하여 이를 적용함으로써 IPR 확보를 선도할 필요가 있음

3.3.6. 기기 관리자 및 소유자간의 권한관리 기술

• 표준화-기술개발-IPR 연계분석



표준화 중요도	국내 개발주체		활용도	관련 국제 표준화 기구
고(★★★) 중(★★☆) 저(★☆☆)	표준개발	기술개발		
★★★	KISA, ETRI, TTA-PG501	공인 인증기관, 보안업체 등	제조업, 서비스, 공공/행정 등	OMA, IETF, ITU-TS, CableLabs ISO/IEC

범 례

10 : 중점 표준화항목의 국내상태

10 : 중점 표준화항목의 국제상태

→ : 중점 표준화항목의 국내 표준상태전이

⇢ : 중점 표준화항목의 국제 표준상태전이

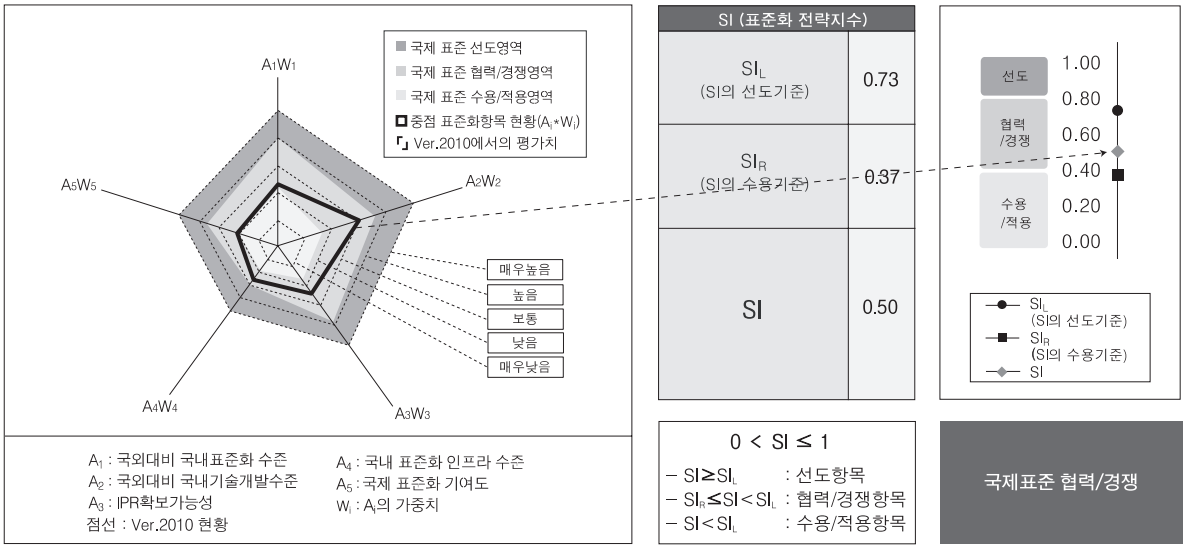
↑ : 선행표준(선 표준화 후 기술개발)

↗ : 동시표준(표준화&기술개발 동시추진)

↓ : 후행표준(선 기술개발 후 표준화)

표준화 특성	동시표준
표준화-기술개발- IPR 연계방안	국내의 기기인증서 관련한 기술개발을 바탕으로 국내표준 및 국제표준을 선도하여 다양한 IPR 확보 추진

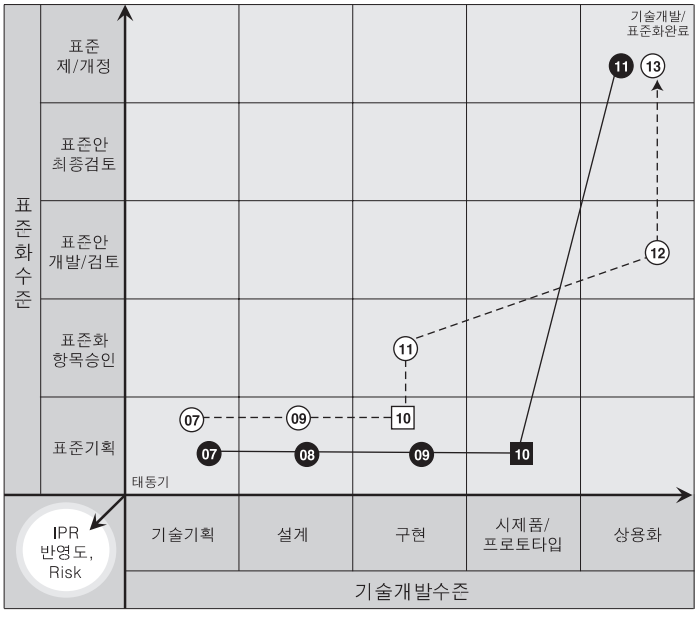
• 국제표준화 전략목표 및 세부전략(안)



국제표준화 전략목표	국제표준 협력/경쟁
Trace Tracking (Ver.2010 ⟼ 2011)	- 본 중점 표준화 항목의 경우 Ver.2010 신규 항목임
세부전략	- ITU-T, TTA 등 국내외 표준화 단체에서 홈 네트워크용 디바이스 인증서 프로파일 표준이 국내 전문가 주도로 개발되는 등 디바이스 인증분야의 선도적인 역량을 지속적으로 유지함으로써 국제 표준화 선도 - 국내에서는 유비쿼터스 사회의 도래에 따라 u-시티 구축사업 등 정부 · 지자체 및 산업체 주도로 다양한 디바이스를 활용한 서비스 도입이 추진되고 있음. 특히, 유비쿼터스 환경을 위한 기기인증체계가 국내의 공인인증체계 기반으로 구축됨에 따라 사람에게 발급되는 공인인증서와 달리, 기기 관리자 및 소유자에 대한 권한관리가 필요하며, 이를 위한 기술개발 및 표준화를 병행하여 추진 - 홈 네트워크용 디바이스에 대한 인증방법 등이 이미 국내 특허가 출원된 상태지지만, 기기 관리자 및 소유자에 대한 권한관리 분야는 신규 특허출원 등 IPR 확보의 여지가 있음. 이에 표준화 추진 및 기술 개발을 병행을 통해 관련 IPR을 적극적으로 확보 - 디바이스(기기) 인증 관련 국내 기술 개발은 KISA, ETRI, LG CNS 등 연구소 및 산업계에서 활발히 진행되고 있으며, TTA를 통해 국내 표준화를 추진중 - 국제적으로도 ITU-T, ISO, IETF 등 다양한 표준화 기구에서 기기 인증에 많은 관심을 가지고 있고, 국내의 기술력 및 표준화 인프라가 경쟁력을 확보하고 있음. 이에 관련 전문가의 지속적인 참여를 통해 국제 표준화 선도도 가능할 것으로 기대
IPR 확보방안	- 현재, KISA를 중심으로 한국정보인증과 한국전자인증을 통한 기기인증서 발급 체계가 구축되어 있고 이를 통한 인터넷전화, CCTV등의 기기에 대한 인증서 발급이 진행 중임. 또한 인증서가 필요한 스마트 그리드 등 다양한 기기에 대한 발급이 요구되고 있어, 이를 국내시장의 성공적인 사례를 바탕으로 국외의 IPR 확보에 대한 노력이 필요하다고 판단됨

3.3.7. 통합 권한관리 프레임워크 및 응용 서비스

• 표준화-기술개발-IPR 연계분석



표준화 중요도	국내 개발주체		활용도	관련 국제 표준화 기구
고(★★★) 중(★★☆) 저(★☆☆)	표준개발	기술개발		
★★★	KISA, TTA-PG501	KISA, 보안업체 등	제조업, 서비스, 공공/행정 등	IETF, ITU-T

범 례

10 : 중점 표준화항목의 국내상태

10 : 중점 표준화항목의 국제상태

→ : 중점 표준화항목의 국내 표준상태전이

⇢ : 중점 표준화항목의 국제 표준상태전이

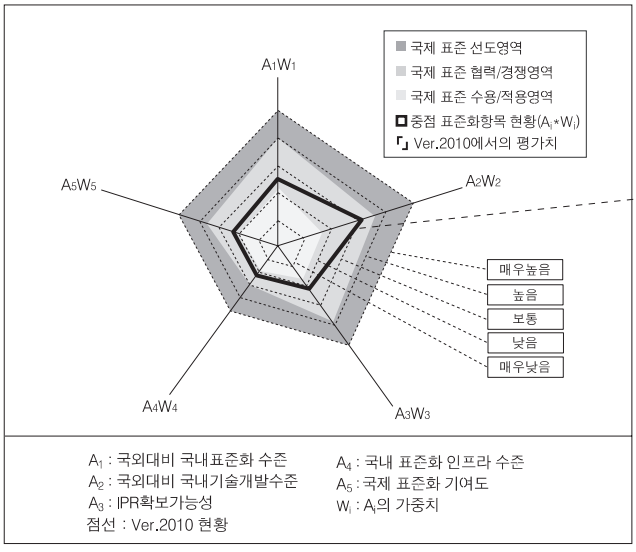
↑ : 선행표준(선 표준화 후 기술개발)

↗ : 동시표준(표준화&기술개발 동시추진)

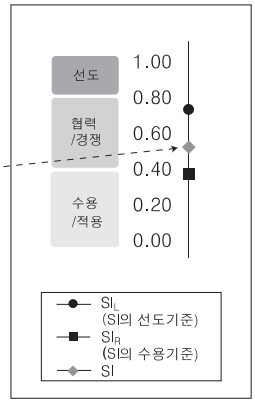
↓ : 후행표준(선 기술개발 후 표준화)

표준화 특성	후행표준
표준화-기술개발- IPR 연계방안	행안부 추진 '차세대 통합인증체계 구축' 사업 결과물 활용 등 기술개발 선행 후, 표준화 추진 및 IPR 확보

• 국제표준화 전략목표 및 세부전략(안)



SI (표준화 전략지수)	
SI_L (SI의 선도기준)	0.73
SI_R (SI의 수용기준)	0.37
SI	0.51



$0 < SI \leq 1$

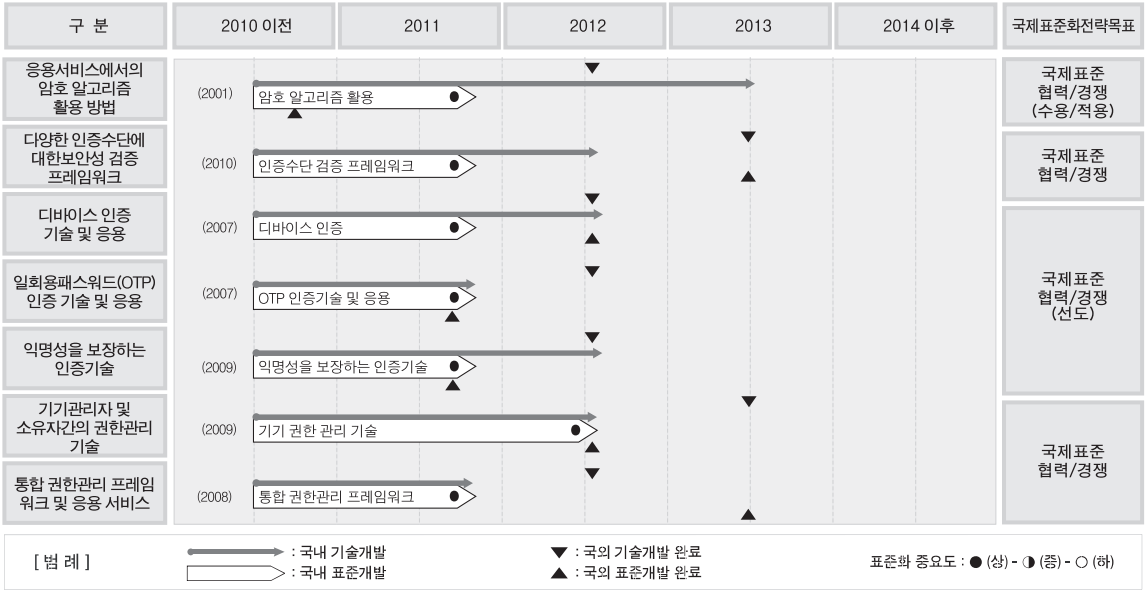
- $SI \geq SI_L$: 선도항목
- $SI_R \leq SI < SI_L$: 협력/경쟁항목
- $SI < SI_L$: 수용/적용항목

국제표준 협력/경쟁

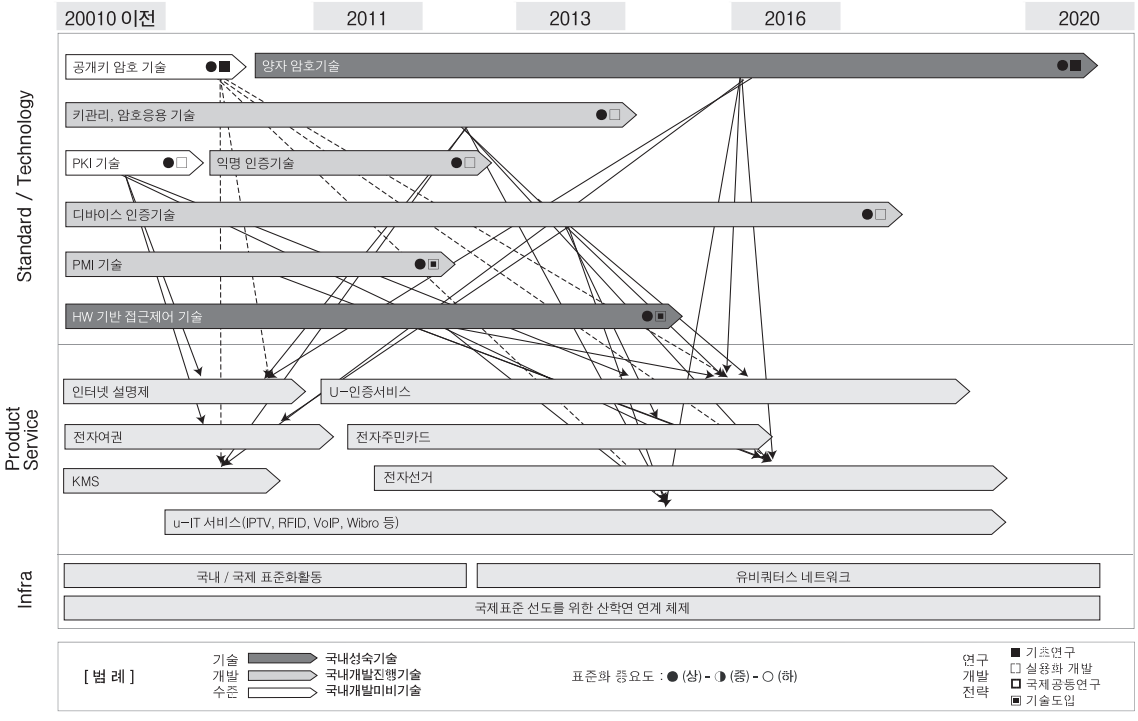
국제표준화 전략목표	국제표준 협력/경쟁
Trace Tracking (Ver.2010 ⟼ 2011)	- 본 중점 표준화 항목의 경우 Ver.2010 신규 항목임
세부전략	- 개별 권한관리 기술의 경우 국내외 수준격차가 미미하며, 현장에서의 도입 및 구현은 국내 환경이 보다 활성화된 상황임. 통합 권한관리 프레임워크 및 응용 서비스 분야의 경우엔 국내외 모두 성숙되지 않은 단계이므로 국내외 표준화를 병행해서 추진할 필요가 있음 - 개별 권한관리 기술의 개발 및 적용은 국외에 뒤지지 않는 수준이며, 통합 보안관리 부분도 최근 전자정부에 도입되어 시범 구축 · 운영되는 등 기술개발 수준은 높음 - 다양한 응용서비스에 적용된 권한관리 기술간 연동을 위한 통합 프레임워크 개발이 전자정부를 중심으로 개발 및 적용되고 있으므로 통합 권한관리 및 관련 응용기술 분야에서 IPR 확보가 용이할 것으로 기대 - 전자정부에 도입하기 위한 통합 권한관리 프레임워크 개발이 가시적인 성과를 보이고 있는 반면, 이에 대한 표준화 추진은 미흡한 실정임. 이에 전자정부에서 선도적으로 개발 · 적용된 결과 정리 및 보완을 통한 후행 표준화 추진이 요구됨 - 국제적으로도 ITU-T, ISO, IETF 등 다양한 표준화 기구에서 통합 권한관리 프레임워크에 관심을 가지고 있고, 현장에서 검증된 기술을 기반으로 국내 전문가의 지속적인 참여를 통해 표준화 선도가 가능할 것으로 기대
IPR 확보방안	- 기술개발을 선행 후, 다양한 응용서비스 환경에서의 통합 권한관리 및 관련 응용기술 분야 등에서 IPR 확보를 추진

3.4. 중장기 표준화 계획

3.4.1. 중점 표준화항목별 중기('11~'13) 표준화 계획



3.4.2. 장기 표준화 계획(10년 기술예측)



[국내외 관련표준 대응리스트]

구 분	표준명	기구 (업체)	제정 연도	제개정 현황	국내 관련표준	국내 추진기구
암호기술	FIPS 46-3 Data Encryption Standard	NIST	1999	재제개정	KS X 1201	TTA/ISTF
	FIPS 81 DES Modes of Operation	NIST	1980	초안	KS X 1202	TTA/ISTF
	FIPS 180-2 Secure Hash Standard (SHS)	NIST	2002	제개정	-	TTA/ISTF
	FIPS 185 Escrowed Encryption Standard(EES)	NIST	1994	초안	-	TTA/ISTF
	FIPS 186-2 Digital Signature Standard (DSS)	NIST	2001	제개정	-	TTA/ISTF
	FIPS 197 Advanced Encryption Standard	NIST	2001	초안	-	TTA/ISTF
	FIPS 198 The Keyed-Hash Message Authentication Code (HMAC)	NIST	2002	초안	-	TTA/ISTF
	ISO/IEC 18031 Random number generation	JTC1/SC27/WG2	2000	초안	-	TTA/ISTF
	ISO/IEC 18032 Prime number generation	JTC1/SC27/WG2	2000	초안	-	TTA/ISTF
	ISO/IEC 18033-1 Encryption algorithms - Part 1 : General	JTC1/SC27/WG2	2002	초안	-	TTA/ISTF
	ISO/IEC 18033-2 Encryption algorithms - Part 2 : Asymmetric Ciphers	JTC1/SC27/WG2	2002	초안	-	TTA/ISTF
	ISO/IEC 18033-3 Encryption algorithms - Part 3 : Block Cyphers	JTC1/SC27/WG2	2002	초안	-	TTA/ISTF
	ISO/IEC18033-4 Encryption algorithms - Part 4 : Stream Ciphers	JTC1/SC27/WG2	2002	초안	-	TTA/ISTF
	ISO/IEC 15946-1 Cryptographic techniques based on elliptic curves-Part1: General	JTC1/SC27/WG2	2002	초안	-	TTA/ISTF
	ISO/IEC 15946-2 Cryptographic techniques based on elliptic curves-Part 2: Digital Signatures	JTC1/SC27/WG2	2002	초안	TTAS.KO-12.0015	TTA/ISTF
	ISO/IEC 15946-3 Cryptographic techniques based on elliptic curves-Part 3: Key establishment	JTC1/SC27/WG2	2002	초안	-	TTA/ISTF
	ISO/IEC 14888-1 Information processing - Security techniques - Digital signatures with appendix - Part 1: General	JTC1/SC27/WG2	1999	초안	-	TTA/ISTF
	ISO/IEC 14888-2 Information technology - Security techniques - Digital signatures with appendix - Part 2: Identity-based mechanisms	JTC1/SC27/WG2	1999	초안	-	TTA/ISTF
	ISO/IEC 14888-3 Information technology - Security techniques - Digital signatures with appendix - Part 3: Certificate-based mechanisms	JTC1/SC27/WG2	1998	초안	-	TTA/ISTF
	ISO/IEC 10118-1 Information technology-Security techniques-Hash-functions-Part 1: General	JTC1/SC27/WG2	2000	초안	KS X 1208-2	TTA/ISTF
	ISO/IEC 10118-2 Information technology-Security techniques-Hash-functions-Part 2: Hash-functions using an n-bit block cipher algorithm	JTC1/SC27/WG2	2000	초안	KS X 1208-2	TTA/ISTF
	ISO/IEC 10118-3 Information technology-Security techniques-Hash-functions-Part 3: Dedicated hash-functions	JTC1/SC27/WG2	1998	초안	-	TTA/ISTF
	ISO/IEC 10118-4 Information technology - Security techniques - Hash-functions - Part 4: Hash-functions using modular arithmetic	JTC1/SC27/WG2	1998	초안	-	TTA/ISTF
	ISO/IEC 10116 Information technology-Security techniques-Modes of operation for an n-bit block cipher	JTC1/SC27/WG2	1997	초안	KS X 1205	TTA/ISTF
	ISO/IEC 9796-1 Information technology-Security techniques-Digital signature scheme giving message recovery	JTC1/SC27/WG2	1999		KS X 1207	TTA/ISTF
	ISO/IEC 9798-2 Information technology-Security techniques-Entity authentication-Part 2:Mechanisms using symmetric encipherment algorithms	JTC1/SC27/WG2	1999	초안	TTA.KO-12.0006	TTA/ISTF
	ISO/IEC 9796-3 Digital signatures schemes giving message recovery - Part 3: Mechanisms using a check function	JTC1/SC27/WG2	2000	초안	-	TTA/ISTF
	ISO/IEC 9796-4 Digital signatures schemes giving message recovery - Part 4: Discrete logarithm based mechanisms	JTC1/SC27/WG2	2000	초안	-	TTA/ISTF

구 분	표준명	기구 (업체)	제정 연도	제개정 현황	국내 관련표준	국내 추진기구
암호기술	ISO/IEC 9798-4 Information technology-Security techniques-Entity authentication-Part 4:Mechanisms using a cryptographic check function	JTC1/SC27/WG2	1999	초안	TTA.KO-12.0005	TTA/ISTF
	ISO/IEC 9798-5 Information technology-Security techniques-Entity authentication-Part 5:Mechanisms using zero knowledge techniques	JTC1/SC27/WG2	1999	초안	-	TTA/ISTF
	ISO/IEC 9797-1 Information technology - Security techniques-Message Authentication Code(MAC) - Part 1: Mechanisms using a block cipher	JTC1/SC27/WG2	1999	초안	KS X 1206	TTA/ISTF
	ISO/IEC9797-2 Information technology - Security techniques - Message authentication codes (MACs) - Part 2: Mechanisms using a hash-function	JTC1/SC27/WG2	1999	초안	-	TTA/ISTF
	ISO 8372 Information processing-Modes of operation for a 64-bit block cipher algorithm	JTC 1/SC27/WG2	1997	초안	-	TTA/ISTF
인증기술	RFC 3820 Internet X.509 Public Key Infrastructure Proxy Certificate Profile	IETF	2004	초안	-	TTA/ISTF
	RFC 3779 X.509 Extensions for IP Addresses and AS Identifiers	IETF	2004	초안	-	TTA/ISTF
	RFC 3770 Certificate Extensions and Attributes Supporting Authentication in PPP and Wireless LAN	IETF	2004	초안	-	TTA/ISTF
	RFC 3739 Internet X.509 Public Key Infrastructure: Qualified Certificates Profile	IETF	2004	초안	-	TTA/ISTF
	RFC 3709 Internet X.509 Public Key Infrastructure: Logotypes in X.509 certificates	IETF	2004	초안	-	TTA/ISTF
	RFC 3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework	IETF	2003	초안	-	TTA/ISTF
	RFC 3628 Policy Requirements for Time-Stamping Authorities	IETF	2003	초안	-	TTA/ISTF
	RFC3379 Delegated Path Validation and Delegated Path Discovery Protocol Requirements	IETF	2003	초안	-	TTA/ISTF
	RFC 3379 Delegated Path Validation and Delegated Path Discovery Requirements	IETF	2002	초안	-	TTA/ISTF
	RFC 3281 An Internet Attribute Certificate Profile for Authorization	IETF	2002	초안	-	TTA/ISTF
	RFC 3280 Internet X.509 Public Key Infrastructure Certificate and CRL Profile	IETF	2002	개정	ISTF-002, TTAS.KO-12.0012, TTAS.KO-12.0013	TTA/ISTF
	RFC 3279 Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and CRI Profile	IETF	2002	초안	ISTF-001, TTAS.KO-12.0013	TTA/ISTF
	RFC 3161 Internet X.509 Public Key Infrastructure Time Stamp Protocols (TSP)	IETF	2001	초안	-	TTA/ISTF
	RFC 3039 Internet X.509 Public Key Infrastructure Qualified Certificates Profile	IETF	2001	초안	-	TTA/ISTF
	RFC 3029 Internet X.509 Public Key Infrastructure Data Validation and Certification Server Protocols	IETF	2001	초안	-	TTA/ISTF
	RFC 2875 Diffie-Hellman Proof-of-Possession Algorithms	IETF	2000	초안	-	TTA/ISTF
	RFC 2797 Certificate Management Messages over CMS	IETF	2000	초안	-	TTA/ISTF
	RFC 2587 Internet X.509 Public Key Infrastructure LDAPv2 Schema	IETF	1999	초안	-	TTA/ISTF
	RFC 2585 Internet X.509 Public Key Infrastructure Operational Protocols: FTP and HTTP	IETF	1999	초안	-	TTA/ISTF
	RFC 2560 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP	IETF	1999	초안	-	TTA/ISTF
	RFC 2559 Internet X.509 Public Key Infrastructure Operational Protocols - LDAPv2	IETF	1999	초안	-	TTA/ISTF
	RFC 2511 Internet X.509 Certificate Request Message Format	IETF	1999	초안	-	TTA/ISTF

구 분	표준명	기구 (업체)	제정 연도	제개정 현황	국내 관련표준	국내 추진기구
인증기술	RFC 2510 Internet X.509 Public Key Infrastructure Certificate Management Protocol	IETF	1999	초안	-	TTA/ISTF
	RFC 2459 Internet X.509 Public Key Infrastructure Certificate and CRL Profile	IETF	1999	개정되어 폐기됨	ISTF-001, ISTF-002	TTA/ISTF
	RFC 2692 SPKI Requirements	IETF	1999	초안	-	TTA/ISTF
	RFC 2693 SPKI Certificate Theory	IETF	1999	초안	-	TTA/ISTF
	ISO/IEC 18014-1 Time stamping services and protocols- Part 1 : Framework	ISO/IEC JTC1/SC27/WG1	2002	초안	-	TTA/ISTF
	ISO/IEC 18014-2 Time stamping services and protocols - Part 2 : Mechanisms producing independent tokens	ISO/IEC JTC1/SC27/WG2	2002	초안	-	TTA/ISTF
	ISO/IEC 18014-3 Time stamping services and protocols - Part 3 : Mechnisms producing linked tokens	ISO/IEC JTC1/SC27/WG2	2000	초안	-	TTA/ISTF
	ISO/IEC 15945 Specification of TTP services to support the application of digital signatures	ISO/IEC JTC1/SC27/WG1	2002	초안	-	TTA/ISTF
	ISO/IEC9979 Information technology-Security techniques-Procedures for the registration of cryptographic algorithms(Revision of ISO/IEC 9979:1991)	JTC1/SC27/WG1	1999	초안	KS X 1209	TTA/ISTF
	ISO/IEC 9594-8 Information technology-OSI-The Directory-Public-key and Attribute Certificate framework TTA/ISTF	ISO/IEC JTC1/SC6	2000	초안	TTAS.IT	-X.509/R2
	X.509 Information Technology - OSI - The Directory: Public-key and Attribute Certificate framework TTA/ISTF	ITU SG7	2000	-	TTAS.IT	-X509/R2
일반 응용중 전자 우편보안	Transporting S/MIME Objects in X.400 (RFC 3855)	IETF	2004	초안	-	TTA/ISTF
	Securing X.400 Content with S/MIME (RFC 3854)	IETF	2004	초안	-	TTA/ISTF
	Cryptographic Message Syntax (CMS) (RFC 3852)	IETF	2004	초안	-	TTA/ISTF
	S/MIME Version 3.1 Message Specification (RFC 3851)	IETF	2004	초안	-	TTA/ISTF
	S/MIME Version 3.1 Certificate Handling (RFC 3850)	IETF	2004	초안	-	TTA/ISTF
	Use of the Camellia Encryption Algorithm in CMS (RFC 3657)	IETF	2004	초안	-	TTA/ISTF
	Use of the Advanced Encryption Standard (AES)Encryption Algorithm in Cryptographic Message Syntax (CMS) (RFC 3565)	IETF	2003	초안	-	TTA/ISTF
	Use of the RSAES-OAEP Key Transport Algorithm in Cryptographic Message Syntax (CMS) (RFC 3560)	IETF	2003	초안	-	TTA/ISTF
	Wrapping a Hashed Message Authentication Code (HMAC) key with a Triple-Data Encryption Standard (DES) Key or an Advanced Encryption Standard (AES)Key (RFC 3537)	IETF	2003	초안	-	TTA/ISTF
	Implementing Company Classification Policy with the S/MIME Security Label (RFC 3114)	IETF	2002	초안	-	TTA/ISTF
	Advanced Encryption Standard (AES) Key Wrap Algorithm (RFC 3394)	IETF	2002	초안	-	TTA/ISTF
	Cryptographic Message Syntax (CMS) Algorithms (RFC 3370)	IETF	2002	초안	-	TTA/ISTF
	Cryptographic Message Syntax (RFC 3369)	IETF	2002	초안	-	TTA/ISTF
	Compressed Data Content Type for Cryptographic Message Syntax (CMS) (RFC 3274)	IETF	2002	초안	-	TTA/ISTF
	RFC 3278 Use of ECC Algorithms in CMS	IETF	2002	초안	-	TTA/ISTF
	RFC 3274 Compressed Data Content Type for Cryptographic Message Syntax (CMS)	IETF	2002	초안	-	TTA/ISTF

구 분	표준명	기구 (업체)	제정 연도	제개정 현황	국내 관련표준	국내 추진기구
일반 응용중 전자 우편보안	RFC 3211 Password-based Encryption for SMS	IETF	2001	초안	-	TTA/ISTF
	RFC 3185 Reuse of CMS Content Encryption Keys	IETF	2001	초안	-	TTA/ISTF
	RFC 3156 MIME Security with OpenPGP	IETF	2001	초안	-	TTA/ISTF
	RFC 2984 Use of the CAST-128 Encryption Algorithm in CMS	IETF	2000	초안	ISTF-011	TTA/ISTF
	RFC 2634 Enhanced Security Services for S/MIME	IETF	1999	초안	ISTF-010	TTA/ISTF
	RFC 2633 S/MIME Version 3 Message Specification	IETF	1999	초안	ISTF-009	TTA/ISTF
	RFC 2632 S/MIME Version 3 Certificate Handling	IETF	1999	초안	ISTF-008	TTA/ISTF
	RFC 2631 Diffie-Hellman Key Agreement Method	IETF	1999	초안	ISTF-007	TTA/ISTF
	RFC 2630 Cryptographic Message Syntax	IETF	1999	초안	ISTF-006	TTA/ISTF
	RFC 3125 Electronic Signature Policies	IETF	2001	초안	-	TTA/ISTF
	RFC 3183 Domain Security Services using S/MIME	IETF	2001	초안	-	TTA/ISTF
	RFC 2857 The Use of HMAC-RIPEMD-160-96 within ESP and AH	IETF	2000	초안	-	TTA/ISTF
	RFC 2440 OpenPGP Message Format	IETF	1998	-	-	TTA/ISTF

[참고문헌]

〔1〕 TTA, 정보통신표준활용맵2009, 2009.4
〔2〕 KISA, 건전한 암호이용 활성화 방안 마련을 위한 보고서, 2002.12
〔3〕 KIISC, 국내외 암호관련 법제도 현황, 2005.4
〔4〕 KISA, 다양한 보안프로토콜에서의 SEED 이용 가이드라인, 2008.6
〔5〕 KIISC, 선진국 민간분야 암호사용실태 및 사용정책동향연구, 1998.11
〔6〕 KISA, 암호 알고리즘 및 키 길이 이용 안내서, 2010.1
〔7〕 KISA, 암호이용 가이드라인, 2007.12
〔8〕 KISA, 암호이용기반구축 보고서, 2004.12
〔9〕 KISA, 암호정책 수립 기준 설명서, 2008.10
〔10〕 전자통신동향분석, NIST의 키 관리 표준, 17권 제5호, 2002.10
〔11〕 KISA, SEED 소스코드 매뉴얼 v1.0, 2008.06
〔12〕 TTA, IT 839전략 표준화 로드맵 Ver.2007, 2006.12
〔13〕 IITA, 2006년도 정보통신 기술수준 조사 보고서, 2006.07
〔14〕 KIPA, 국내 정보보호 시장 동향과 전망, 2008.01
〔15〕 IDC, Worldwide and U.S Security Services 2006-2011 Forecast and Analysis, 2008.1
〔16〕 KISA, 2009 국내 정보보호 산업 시장 및 동향 조사, 2010.3
〔17〕 씨큐어넷, 인터넷정보보호 동향, 2010
〔18〕 텔레매틱스 표준화 포럼, www.kotba.or.kr
〔19〕 정보통신용어사전, www.tta.or.kr
〔20〕 VeriSign, www.verisign.com
〔21〕 CMLA, Content Management License Administrator, www.cm-la.com
〔22〕 IETF, The Internet Engineering Task Force, www.ietf.org
〔23〕 WiMAX Forum, www.wimaxforum.org
〔24〕 Trusted Computing Group, http://www.trustedcomputinggroup.org/

[약어]

AM	After Market
BM	Before Market
OBD	On-Board Diagnosis
CAGR	Compound Annual Growth Rate
VICS	Vehicle Information and Communication System
RWIS	Road Weather Information System
DVR	Digital Video Recorder
VII	Vehicle Infrastructure Integration
ERTICO	Europe Road Transport Telematics Information Coordination Organization
VSL	Variable Speed Limit

ETC	Electronic Toll Collection
CVIS	Cooperative Vehicle-Infrastructure System
CMS	Cryptographic Message Syntax
CALM	Communication, Air-interface, Long and Medium range
NOW	Network On Wheel
SEVECOM	Secure Vehicular Communication
BMBF	Federal Ministry of Education and Research
UWB	Ultra Wide Band Radio
ECU	Electronic Control Unit
XTPM	eXtensible Telematics Protocol from Mobile to Server
DSRC	Dedicated Short Range Communication
SAE	Society Automotive Engineers
AMI-C	Automobile Multimedia Interface Collaboration
WAVE	Wireless Access for Vehicular Environment
UMTS	Universal Mobile Telecommunication System
GeoPriv	Geographic Location/Privacy
PDA	Personal Digital Assistant
IAM	Identity and Access Management
TM	Threat Management
SVM	Security and Vulnerablity Management
IPSec	IP Security
SSL	Security Socket Layer
TLS	Transport Layer Security
IKE	Internet Key Exchange
DES	Data Encryption Standard
SIM	Subscriber Identity Module
USIM	Universal Subscriber Identity Module
FPGA	Field-Programmable Gate Array
TPM	Trusted Platform Module
SSO	Single Sign-On
WiMAX	Worldwide Interoperability for Microwave Access
TinyECC	Tiny Elliptic Curve Cryptography
CMLA	Content Management License Administrator
TCG	Trusted Computing Group
MPWG	Mobile Phone Working Group