암호 / 인증 / 권한관리

1. 개요

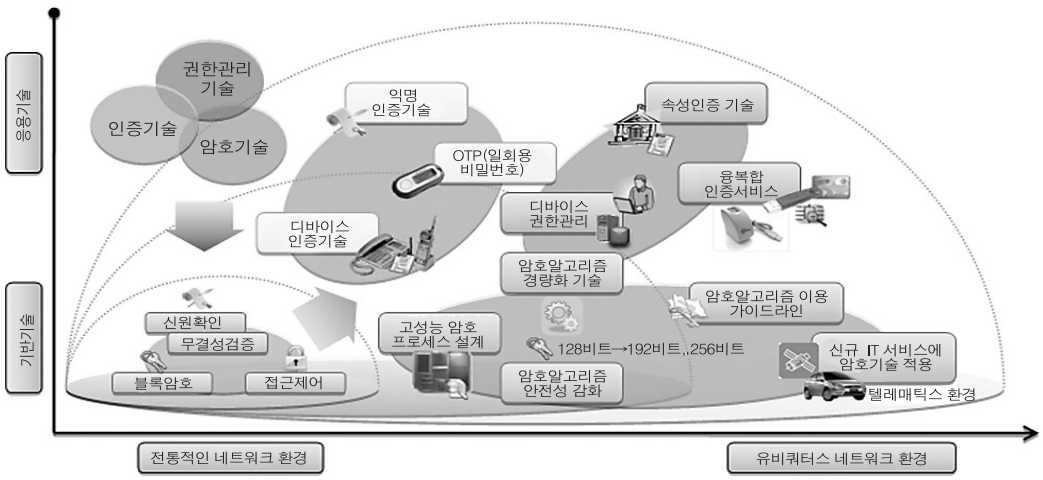
1.1. 기술개요

1.1.1. 중점기술 및 표준화 대상항목의 정의

• 중점기술의 정의

인터넷상에서 유통되고 있는 다양한 정보에 대해 안전하고 신뢰성 있게 전송 및 이용하기 위한 기반 기술로, 안전한 정보의 송수신을 위한 프리미티브 기술인 암호 기술, 인터넷상에서 사용자의 신원확인 및 전송되는 정보에 대한 무결성 보장을 제공하는 인증기술, 인터넷상에서의 불법적인 정보 접근을 통제하기 위한 권한관리 기술로 구분될 수 있다. 또한, 최근 급속한 인터넷 해킹 기술의 발전과 유비쿼터스 환경이 도래됨에 따라 사회적으로 요구되고 있는 안전성이 강화되고 경량화된 암호 · 인증 · 권한관리 기술을 포함

- 암호기술은 인터넷상에서 안전한 정보의 송수신을 위한 프리미티브 기술로서 기존의 128비트 이외에 안전성이 강화된 192비트 및 256비트 블록 암호 알고리즘 기술, VoIP 등 최근 보급 확산되고 있는 다양한 신규 IT서비스에 암호기술 적용을 위한 암호 응용 기술, 유비쿼터스 환경에 적합한 경량화된 암호 알고리즘 기술 등 다양한 분야의 암호기술을 포괄. 또한, 텔레매틱스 환경에서의 키관리 기술, 암호알고리즘 이용 가이드라인, 고성능 암호프로세서 설계 기술 등 최근 이슈가 되고 있는 암호 기술을 포함하고 있음
- 인증기술은 인터넷상에서 적법한 사용자를 식별하기 위한 신원확인 기능 뿐 아니라 전송되는 정보에 대한 무결성을 보장하는 기능을 포함하는 기술로써, 기존 사람에 대한 신원확인 뿐 아니라 최근 유비쿼터스 사회로의 전환에 따라 보급 확산되고 있는 다양한 방송 · 통신 단말기에 대한 진위성 여부를 보장하는 디바이스 인증 기술까지 포함하고 있음. 또한, 온라인 게시판에서 기본적으로 익명으로 글을 게시하고 추후 사고 발생 시 이를 추적할 수 있는 익명 인증기술, 매번 비밀번호가 변경되는 OTP(One Time Password) 인증 기술 등을 포함하고 있음
- 권한관리기술은 인터넷상에서 유통되고 있는 정보에 대한 접근 시 적합한 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

구 분	정 의	표준화 대상항목	표준화 내용
암 호	유무선 환경에서의 데이터 기밀성 및 무결성 보장을 위한 암호기술, 미래 유비쿼터스 환경에서 요구되는 경량화된 암호기술 등을 정의	유비쿼터스 환경에 적합한 경량 암호알고리즘	유비쿼터스 환경 등에서 이용되는 다양한 디바이스에서 안전한 데이터 전송을 위해서는 해당 디바이스에 적합한 경량화된 암호알고리즘이 필요, 경량화 된 블록 암호알고리즘에 대한 키 생성 및 암 · 복호화 과정 정의 ※ 경량 블록 암호알고리즘 HIGHT 등이 국제 표준화 추진 중
		블록 암호알고리즘 기술	전자상거래, 금융, 무선 통신 등에서 전송되는 정보의 안전성 강화를 위해 개발된 암호 알고리즘에 대한 키 확장, 암복호화 과정, S-box 생성방법 및 테이블, 라운드 키 생성 과정 등을 정의 ※ 최적화된 범용 알고리즘인 ARIA, 192/256비트 블록 암호알고리즘 SEED 등의 블록암호알고리즘 포함
		응용서비스에서의 암호 알고리즘 활용 방법	VoIP, IPTV 및 IPSec 등에서 음성 데이터의 암호화, 키 관리 및 네트워크 프로토콜 등에서의 암호 알고리즘의 활용 및 적용 방안 ※ SRTP 및 MIKEY 키관리 기술에서 SEED 알고리즘 활용 방법, IPTV 내의 멀티캐스트 기법에서 SEED 알고리즘 활용 방법, IPsec 프로토콜에서의 SEED 운영모드 사용 규격 등 연구 진행 중
		텔레메틱스 환경에서의 암호 키 관리 기술	텔레메틱스 기술은 자동차와 정보통신 등 이종산업간 융합적 특성을 지닌 기술로, 차량 내부와 외부 통신, 차량간 통신시스템에서 정보를 실시간으로 주고받는 기술로써, 원격정보 서비스 및 차량안전, 보안, 개인화된 정보 서비스에서의 안전한 통신을 위한 키 관리 기술을 정의
		암호알고리즘 이용 가이드라인	전자서명, 암 · 복호화, 메시지 인증 코드 등 다양한 암호학적 응용분야를 세분화하고 각 응용분야에서 암호 알고리즘을 안전하게 사용하기 위한 요구사항들을 정의
		고성능 암호프로세서 설계 기술	암호알고리즘은 다량의 연산처리 등으로 인해 SW적인 수행의 경우 속도문제가 발생하므로 고속으로 다량의 데이터를 처리하는 차세대 네트워크 서비스에서 고속 암호처리를 지원하고 안전한 보안 서비스를 제공하기 위한 암호프로세서의 구현 요구사항을 정의
인 증	사람에 대한 신원확인을 위해 이용되는 인증기술 및 유비쿼터스 환경에서 인증주체로 등장하는 디바이스에 대한 인증 기술 등을 정의	USIM 등 모바일 환경에서의 인증서비스 모델 및 인증기술	USIM 칩이 탑재된 스마트폰, 3G폰 등의 보급 확대에 따라, 모바일 환경에서 인증서 기반의 다양한 인터넷 서비스 이용을 위한 USIM 기반의 인증서비스 이용 모델 및 관련 기술에 대해 정의
		인터넷 전화 등에 이용 가능한 디바이스 인증 기술 및 응용	인터넷 전화기, CCTV, 휴대단말기, 지능형 가전 등 네트워크에 참여하는 디바이스에 대한 신뢰된 인증서비스를 제공하기 위한 기술로써, 디바이스 인증모델, 디바이스 인증서 프로파일, 인증서 관리 및 검증 기술, 전자서명키 보호기술 등 정의
		일회용패스워드(OTP) 인증 기술 및 응용	일회용 패스워드(OTP) 보안 서비스 제공을 위한 암호키 관리 및 정책 요구사항, 배포 절차 및 요구사항, 인증 보증레벨 등 OTP 인증기술과 응용에 대해 정의 ※ 일회용 패스워드(OTP) 암호키 관리보안 요구사항, 일회용 패스워드(OTP)키 컨테이너, 일회용패스워드(OTP)인증서비스를 위한 보증레벨과 응용 가이드라인 등에 대해 연구 진행 중
		일회용패스워드(OTP) 인증 프레임워크	OTP 인증 기본 모델, 통합인증 모델, 대체인증서버가 있는 통합인증 모델, 센터간 통합인증 모델 등 총 4개의 인증 서비스 모델을 포함하는 OTP 인증 서비스 프레임워크를 정의하고, 서비스 요구사항, 기본 업무, 보안 고려 사항 및 참고사항을 정의
		익명성을 보장하는 인증 기술	웹사이트 가입, 성인인증 등 개인의 실명이 필요 없는 곳에서 프라이버시 보장을 위해 가명 또는 익명을 사용할 수 있도록 보장하면서 익명성 남용을 방지하기 위한 기술로서 익명인증체계, 익명인증서 프로파일, 익명인증 프로토콜, 익명인증서 검증기술, 익명에 대한 추적기술 등으로 분류
		바이오정보를 이용한 전자서명 기술	기존 공개키 기반의 전자서명 기술에서의 단점을 보완하기 위해 지문, 홍채 등 바이오정보를 포함한 전자서명 인증 기술 및 이용 효율성 제고를 위한 융합 기술 등 정의
권한관리	기업 및 기관 단위에서 사용자들에게 특정 시스템 및 애플리케이션에 접근할 수 있는 권한을 차등 부여해주는 기술	기기 관리자 간의 권한 관리 응용 기술	센서, 무선 네트워크 장치, 기능형 가전, CCTV 등 다양한 디바이스에 대한 인증 서비스의 필요성이 대두. 따라서 디바이스를 관리하는 기기 관리자나 기기 소유자의 디바이스에 대한 권한관리 모델 및 시나리오, 기기 식별체계 등을 개발
		융복합 인증 서비스 모델	다양한 IC카드의 사용, USIM 카드, 신용카드 등이 복합적으로 활용되므로 이에 대한 융복합 인증 서비스 모델 및 시나리오 개발이 필요
		사용자 권한관리를 위한 인증 기술 및 응용	속성인증서 프로파일, 속성인증서 관리프로토콜, 속성인증서 운용 프로토콜, 속성인증서 검증프로토콜, 사용자 인터페이스 기술 등 속성인증서를 이용하여 사용자에 대한 권한을 관리하기 위한 기술

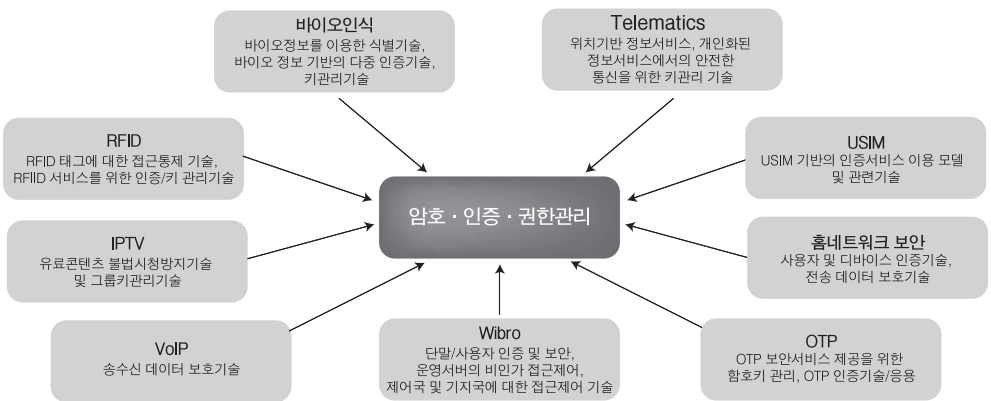
• 표준화 대상항목의 그린ICT 관련성

표준화 대상항목 (음영:중점표준화항목)	물건의 소비감소	전력 · 에너지 소비감소	인간의 이동 감소	물류의 이동 감소	공간 효율화	폐기물 감소	고 효율화 (업무 효율화)	비 고
유비쿼터스 환경에 적합한 경량 암호알고리즘	-	●	-	-	-	-	○	- CPU 연산량 감소를 통해 컴퓨터 전력소모를 줄임으로써 컴퓨터에서 발생하는 CO2 배출 감소
블록 암호알고리즘 기술	-	-	-	-	-	-	-	-
응용서비스에서의 암호 알고리즘 활용 방법	-	-	◐	○	-	-	○	-
텔레메틱스 환경에서의 암호 키 관리 기술	-	○	○	-	-	-	-	-
암호알고리즘 이용 가이드라인	-	-	-	-	-	-	◐	-
고성능 암호프로세서 설계 기술	-	○	-	-	-	-	◐	-
USIM 등 모바일 환경에서의 인증서비스 모델 및 인증기술	-	-	●	-	-	-	○	- 모바일 뱅킹/증권, 모바일 쇼핑 활성화를 통해 금융기관, 백화점, 상점(마트 등) 방문 횟수를 줄임으로써 차량 이동 감소에 따른 CO2 배출 감소
인터넷 전화 등에 이용 가능한 디바이스 인증 기술 및 응용	-	○	○	○	-	-	○	-
일회용패스워드(OTP) · 인증 기술 및 응용	-	-	○	-	-	-	-	- 안전한 인터넷 금융업무 보장을 통해 국민의 오프라인 금융업무 횟수를 줄임으로써 금융업무 등을 위한 차량 이동 감소에 따른 CO2 배출 감소
일회용패스워드(OTP) 인증 프레임워크	-	-	-	-	-	-	◐	- 안전한 인터넷 금융업무 보장을 통해 국민의 오프라인 금융업무 횟수를 줄임으로써 금융업무 등을 위한 차량 이동 감소에 따른 CO2 배출 감소
익명성을 보장하는 인증 기술	-	-	●	-	-	-	-	- 익명기술을 이용한 인터넷 투표 서비스 제공 시 투표장 이동을 위한 차량 이용 감소 등으로 CO2 배출 감소
바이오정보를 이용한 전자서명 기술	-	-	◐	-	-	-	-	- 안전한 인터넷 금융업무 보장을 통해 국민의 오프라인 금융업무 횟수를 줄임으로써 금융업무 등을 위한 차량 이동 감소에 따른 CO2 배출 감소
기기 관리자 간의 권한 관리 응용 기술	-	-	-	-	-	-	-	-
융복합 인증 서비스 모델	-	-	○	-	-	-	◐	-
사용자 권한관리를 위한 인증 기술 및 응용	-	-	-	-	-	-	-	-

〈범례〉 -(관련없음) ○(소) ◐(중) ●(대)

1.1.2. 연관기술 분석

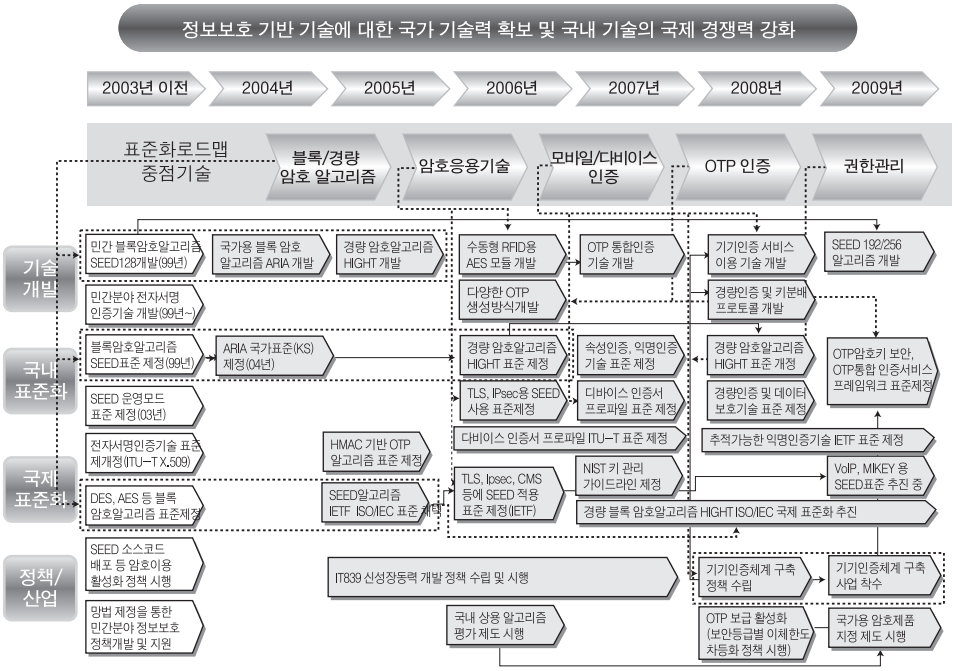
• 연관기술 관계도



• 연관기술 분석표

연관기술	내 용	표준화기구/단체		표준화수준		기술개발수준	
		국내	국외	국내	국외	국내	국외
RFID	RFID태그의 접근을 제어할 수 있는 인증 및 키 관리 기술	TTA/USN 포럼	ETF, 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 네트워 서비스를 제공하기 위해 홈 내부 및 원격 사용자에게 보안서비스를 제공하기 위한 기술	TTA/홈네트워크 보안포럼	ITU-T	표준안 개발/검토	표준안 개발/검토	구현	구현
VoIP	VoIP 단말기간의 송 · 수신 데이터에 대한 보호기술	TTA	ITU-T	표준안 개발/검토	표준안 개발/검토	구현	구현
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

1.2. 중점기술의 연도별 주요현황 및 이슈



• 기술 개발
- 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 RFID 용 AES 모듈 개발
- 2006년 ~ 2008년 스마트 카드, 바코드, 음성신호 및 그래픽 등을 이용한 OTP 생성 방식 개발
- 2007년 금융보안연구원에서 OTP 통합인증 기술 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(2010년 기술 개발 완료 예정)

• 국내 표준화
- 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, IPsec 용 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 등 TTA 표준 제정 추진 중

• 국제 표준화
- 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, IKE 용 SEED 사용 표준 제정(RFC 41623, 4916, 4615)
- 2005년 IETF에서 HMAC 기반의 일회용패스워드 알고리즘 표준 제정(RFC4226)
- 2007년 IETF에서 EAP와 일회용패스워드 프로토콜을 결합한 표준 제정(RFC4793)
- 2007년 ITU-T에서 홈네트워크에 적용 가능한 디바이스 인증서 프로파일 표준 제정(X.1112)
- 2007년~ ISO/IEC에서 경량 암호블록 암호 알고리즘(HIGHT) 표준 추진
- 2007년 NIST 키관리 가이드라인(NIST Publication 800-57) 개발
- 2008년~ IETF에서 추적가능한 익명인증 기술 표준 추진('09년 11월 제정 예정)
- 2009년 IETF에서 VoIP용 SEED 사용 표준 제정 예정
- 2009년 IETF에서 MIKEY에서의 SEED OID 추가 표준 추진

• 정책/산업
- 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 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 사업 착수(12월 완료 예정)

1.3. 추진경과 및 중점 추진방향

• 추진경과
- Ver.2007에서는 정부의 추진의지가 강한 VoIP 분야를 포함한 응용서비스 정보보호분야와 최근 ITU-T와 IETF 등의 국제표준화기구에서 활발하게 국제표준화가 추진 중인 네트워크 정보보호분야를 중점적으로 정리함

- 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 트랜드 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 정부 정책 추진 방향 및 신규 IT 서비스 분야에 적용 가능한 세부 아이템 위주로 표준화 대상항목을 추가 선정. 이에 따라, 안전성이 강화된 블록암호알고리즘 및 경량 암호알고리즘 기술, 암호알고리즘 이용 가이드라인, 모바일 등 디바이스 인증기술, OTP 인증 기술 등 총 15개의 표준화 대상항목을 선정함

• 버전별 중점 표준화항목의 변천

구 분	Ver.2007	Ver.2008	Ver.2009	Ver.2010
암호	- 응용서비스 정보보호 - 네트워크 정보보호	- 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
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 - 일회용패스워드(OTP) 인증 프레임워크 - 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

• 중점 추진방향

- 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

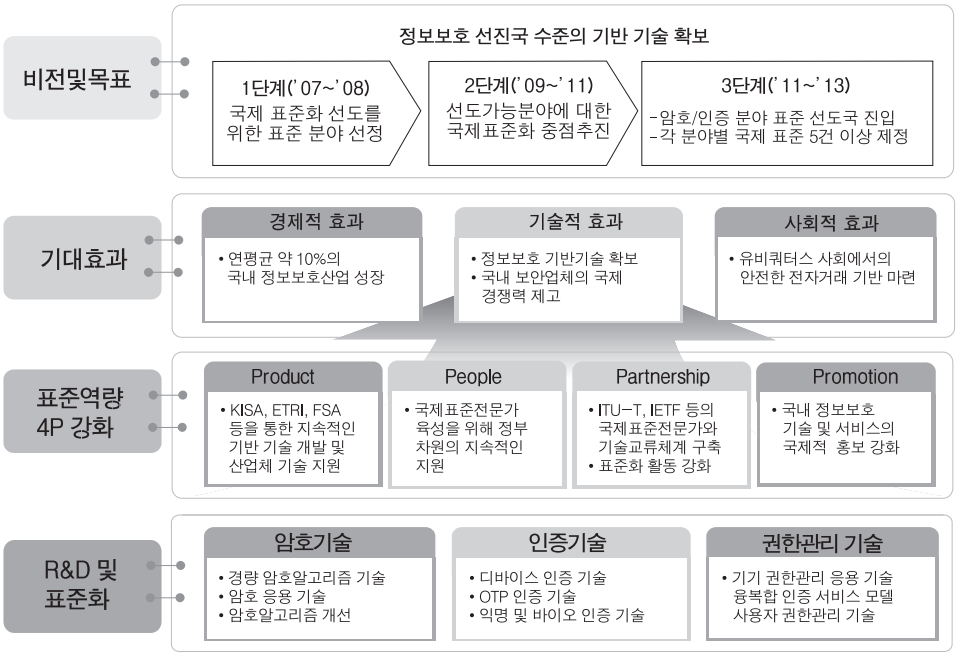
- 최근 발생한 행정분야 인터넷 전화(VoIP) 보급 관련 국제 통상 마찰과 같이 국가차원의 IT 제품 조달 문제를 근본적으로 해결하기 위해서는 WTO 조달 협정에 명시된 것과 같이 각 응용 서비스별로 국산 암호알고리즘을 적용할 수 있는 국제 표준화 추진이 반드시 필요. 이에 따라, 우선적으로 융합서비스, 그린 IT 관련 서비스, IPv6 등 향후 활용도가 높은 분야의 표준에 국산 암호알고리즘을 탑재하기 위한 표준화를 중점적으로 추진

- 불법 게시물, 불법 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 파악할 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 사용되기 때문에 해당 기술들에 대한 표준화를 지속적으로 추진

- 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

21.4. 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 표준화 개발이 필요
- 또한, 국제 표준화는 정보보호 제품에 대한 국제 통상 문제를 해결하는 역할을 수행할 수 있기 때문에 국내 정보보호기술의 국제적 위상 제고 및 국내 정보보호 제품의 국내외 경쟁우위 확보를 위해 암호/인증/권한관리 기술에 대한 국제 표준화 개발 필요

- 암호/인증/권한관리는 정보보호에서 기반이 되는 기술이기 때문에 기반기술에 대한 상호호환성, 안전성 및 신뢰성은 매우 중요한 요소이다. 즉, 실생활에 사용되는 네트워크 및 시스템 정보보호기술, 응용서비스 보안기술 등 다양한 정보보호제품이 상호 유기적으로 안전하게 연동할 수 있기 위해서는 기반기술에 대한 표준화가 절실히 필요
- 국내에서는 암호, 인증, 권한관리 기술과 관련하여 지금까지 다양한 표준화가 이루어져 왔다. 특히 암호알고리듬의 경우, SEED, KCDSA, HAS-160 등을 포함하여 차세대 암호로서 HIGHT, FORK256 등 컴퓨팅 및 정보보호 기술의 변화에 따라 기술개발 및 표준화를 추진하여 왔다. 또한, 최근 유비쿼터스 사회가 도래됨에 따라 다양한 디바이스간의 안전한 정보전송을 위한 경량화된 암호응용기술의 요구가 지속적으로 증가하고 있어 해당 기술에 대한 표준화가 요구된다.
- 인증기술의 경우는 국내뿐만 아니라 세계적으로 활용도가 높은 PKI 기술을 기반으로 지속적인 국제 표준화 추진이 필요하다. 특히, 세계적으로 유례를 찾아보기 어려울정도로 확산된 공인인증서 분야를 중심으로 관련 응용기술에 대한 국제 표준화 추진 노력이 필요하다. 최근, 인터넷 이용확산과 맞물려 인터넷 역기능에 대한 우려가 제기되고 있어 이를 개선하기 위한 인

증기술 표준화 역시 요구된다.

- 양자암호의 경우 향후 10년 내 10대 이머징(emerging)으로 선정(MIT 미디어랩, Technology Review, 2003.2) 되었고, 선진국을 중심으로 많은 연구가 이루어지고 있으나 아직은 일부만 상용화되어 있을 뿐이어서 원천기술 및 주요 요소기술을 중심으로 연구 개발 및 표준화가 필요
- 유비쿼터스 환경에서는 다양한 오프라인 서비스가 온라인으로 변환될 것으로 예상되기 때문에 현재 독자적으로 추진하고 있는 u-시티 또는 u-헬스 사업에 암호, 인증, 권한관리 등이 적용될 수 있도록 관련 기술 표준화 추진 및 기술 적용 노력이 필요
- 텔레매틱스 환경에서는 다른 네트워크와 달리 잘못된 메시지로 인하여 국가의 기반시설인 도로, 교통 등에 심각한 문제를 일으켜 국가적인 손실 및 인명 피해를 초래할 수 있으며, 개인의 프라이버시가 침해될 수 있음. 따라서 텔레매틱스 환경에서 안전한 서비스를 제공하기 위해서는 암호 키 관리 기술에 대한 표준화가 필수적임
- 암호기술은 현재 인터넷뱅킹, 사이버증권, 신용카드결제, 전자입찰, 전자화폐, 저작권이나 산업정보, 개인정보보호, 전자선거 등 다양한 분야에서 정보의 기밀성 및 무결성, 사용자 인증 등을 위해 광범위하게 이용되고 있으나, 암호 솔루션 도입 필요성에 대한 인식 부족 및 암호적용 범위 수준에 대한 구현 가이드라인 부재로 암호 솔루션 도입이 늦어지고 있으므로, 이에 대한 표준화가 필수적임

1.4.2. 표준화의 목표

- 암호 기술과 관련해서는 유비쿼터스 사회에 적합한 대칭키 · 공개키 · 스트림 암호 알고리즘에 대한 원천기술을 확보하여 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)

- 인터넷전화의 암호모듈연동을 위하여 2009년부터 단말/신호 인증, 신호메시지 보호, 음성트래픽 보호 부분에 유비쿼터스 환경에 적합한 인증기술에 대한 국내 및 국제 표준화를 순차적으로 추진
- 암호 기술의 경우 국내에서 개발한 경량 암호 알고리듬, 256비트 해쉬 알고리듬, 스트림 암호 알고리듬 등에 대해 2008년도에 순차적으로 국내 표준을 개발하고 있으며, 2009년부터 경량 암호 알고리듬부터 단계적으로 국제 표준화를 추진하여 2012에는 분야별 1개 이상의 국제 표준을 보유할 수 있도록 추진
- 인증 기술의 경우 2008년까지 익명인증 기술, 속성인증 기술 등에 대한 국내 표준화를 추진. 또한 2008년부터 익명인증 프로토콜에 대한 국제 표준을 개발하고 있으며 2009년 말까지 익명인증 기술에 대한 국제 표준화 완료 예정. 또한 디바이스 인증 기술의 경우 디바이스 인증서 프로파일에 대한 국내 및 국제표준이 2008년 완료되었으며, 2009년 부터는 유비쿼터스 환경에 적합한 인증기술에 대한 국내 표준을 선행적으로 추진하고 2010년 이후에는 국제 표준화 추진
- 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

1.4.3. Vision 및 기대효과

- 국내 암호/인증/권한관리 등 정보보호 기반기술에 대한 국제 표준화 추진을 통해 국내 정보보호 기술 및 제품의 국제 경쟁력 강화
- 암호/인증/권한관리 기술에 대한 보급 확대 및 산업 적용을 통해 안전하고 신뢰할 수 있는 u-사회 구축에 기여

- 암호 · 인증 · 권한관리 기술의 경우 모든 정보보호 제품의 기반 기술이므로 지속적인 관련 원천기술 확보를 통해 국내 제품의 국제 경쟁력 강화 및 국내 정보보호기술에 대한 국제 위상 제고에 기여
- 암호 · 인증 · 권한관리 관련 기반 기술의 경우 국제적으로 표준화가 이미 활발히 진행된 상태이긴 하지만 유비쿼터스 사회에 적용 가능한 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

2. 국내외 현황분석

2.1. 시장 현황 및 전망

2.1.1. 국내 시장 현황 및 전망

가) 암호기술

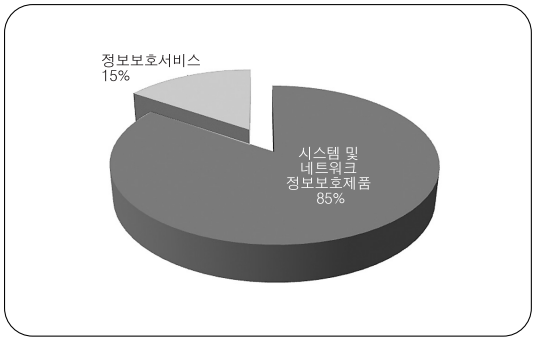
- 국내 정보보호 산업의 경우 매년 증가하는 추세이며 특히 정보보호서비스 산업의 매출 증가가 두드러지게 나타나는 경향을 보이고 있다. 한국인터넷진흥원(KISA)(구, 한국정보보호진흥원)이 발표한 2008년도 국내 정보보호 매출은 2007년 보다 8% 증가한 약 7,724억 원으로 나타났으며, 분야별로는 시스템 및 네트워크 정보보호제품이 6.8% 성장한 약 6,441억 원에 이르렀으며, 정보보호서비스는 상대적으로 성장률이 높은 14.5%로 약 1,282억 원의 시장을 형성함

- 하지만, '08년도 정보보호산업 전체 매출에서 시스템 및 네트워크 정보보호제품은 약 83.4%, 정보보호서비스는 약 16.6%를 차지하고 있어 전년도에 비해 정보보호서비스 매출이 1.2% 증가하기는 하였으나 전체적으로 양자간의 매출비중은 여전히 큰 차이를 보이고 있음

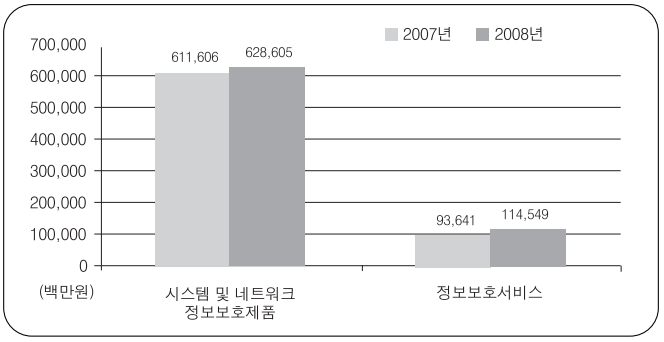
〈정보보호산업의 매출현황 (단위 : 백만원)〉

구 분	2007년	2008년	증감률(%)	매출비중(%)
시스템 및 네트워크 정보보호 제품	602,949	644,174	6.8	83.4
정보보호 서비스	111,995	128,238	14.5	16.6
합 계	714,944	772,412	8.0	100.0

※ 출처 : KISA, 2008 국내 정보보호산업 시장 및 동향조사, 2008



〈정보보호산업의 분류별 매출 비중 현황〉



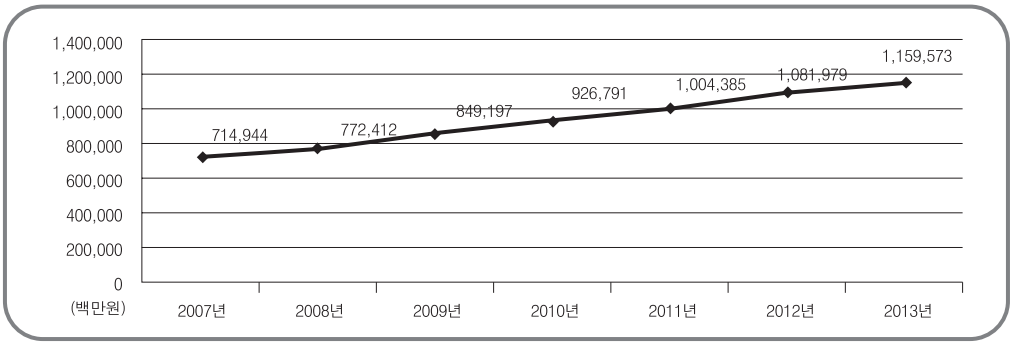
〈정보보호산업의 분류별 매출액 현황〉

- 2008년 국내 정보보호산업 시장 및 동향조사(한국인터넷진흥원) 결과에 따르면 전체적으로 국내 정보보호 산업의 시장규모는 완만한 성장을 보이고 있는 가운데 2008년도 7,724억 원대인 매출규모는 2013년도에는 1조 2595억 원대 규모에 이를 것으로 전망되며, 이 기간 연평균성장률(CAGR: Compound Annual growth Rate)은 전체 8.4%로 예상되며 정보보호서비스 분야가 조금 높은 성장률을 보일 것으로 전망

〈정보보호산업의 분류별 매출 전망 (단위 : 백만원)〉

구 분	07년	08년	09년	10년	11년	12년	13년	CAGR(%)
시스템 및 네트워크 정보보호제품	602,949	644,174	704,677	765,180	825,683	886,186	946,689	7.8
정보보호 서비스	111,995	128,238	144,520	161,611	178,702	195,793	212,884	11.3
합 계	714,944	772,412	849,197	926,791	1,004,385	1,081,979	1,159,573	8.4

※출처 : KISA, 2008 국내 정보보호산업 시장 및 동향조사, 2008



〈정보보호산업 시장 및 동향조사〉

- 신성장 동력으로서 RFID/USN 산업은 급격한 성장이 예측되었으나, 현재 RFID 산업의 경우, 인식률 및 가격등의 문제로 성장속도가 느린 상황임. 그러나, RFID 적용에 프라이버시 문제로 인해 보안기술에 적용에 대한 요구가 지속적으로 증가하고 있음. RFID 전체 시장에서 보안성이 요구되는 부분은 약 42% 정도로 보임

- 국내 RFID/USN 보안 시장은 2008년 8,366억원에서 2014년 130,155억원으로 예측됨. 그러나, 유비쿼더스 환경에 적합한 경량 암호알고리즘에 대한 시장 수요는 현재까지는 극히 미미한 상태임
  ※ RFID/USN 확산 추진계획, 2008년 자료를 토대로 보안 및 프라이버시 보호 기술의 기여도를 17%로 추정함 결과임

- 정보보호제품 및 시스템에 암호 알고리즘을 탑재 · 적용하는 경우, 알고리즘의 종류나 키 길이 등은 해당 시스템의 안전성 수준을 만족할 수 있도록 선택되어야 함. 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 정보보호제품의 국가 · 공공기관 도입기준을 구체화하여 암호기반 제품의 경우 국가암호정책과 직결됨을 감안하여, 국가용 암호제품 지정제도를 신설하였음. 국가용 암호제품 지정제도의 대상 제품군은 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 포함됨

  - 이에, 국가 암호기반 제품에 대한 정책에 따라 정보보호제품 및 시스템에 암호알고리즘을 활용하는 가이드라인이 제시되어야 한다는 필요성이 강조되고 있으며, 해당 정보보호제품에 대한 수요는 정보보호의 중요성이 강조되는 현 시점에서 더욱 증가될 것으로 판단됨

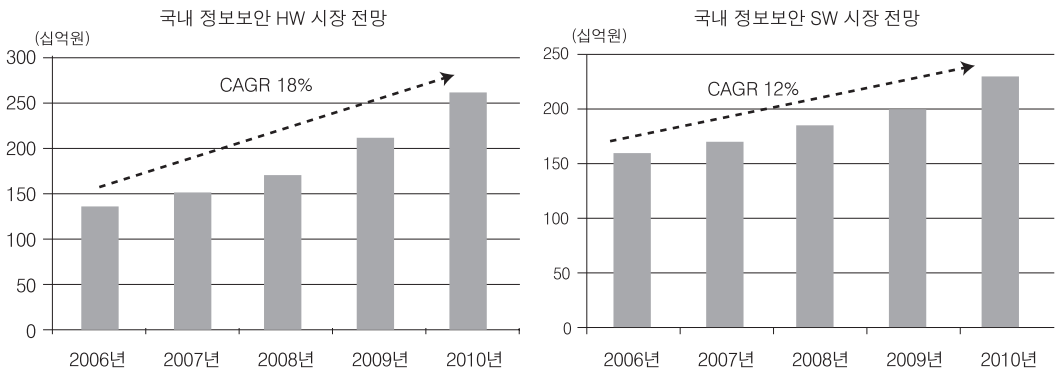
- 또한, 고성능 암호프로세서의 경우, 이동성이 가능한 모든 소형/저용량 전자기기에서의 보안모듈의 성능을 높이기 위해 사용될 수 있으몰, 모바일, 센서 기기, 노트북 등의 다양한 영역에서 활용될 수 있음

  - 삼성전자의 경우 이미 3G 이동통신용 단말기 등에 필수적인 사용자 인증 수단용으로 강력한 암호기능을 가진 비메모리칩을 개발되었음

  - ETRI에서도 사용자 인증, 기기 인증, 데이터 보호 등의 기능을 제공하는 모바일 컴퓨팅용 칩을 개발하였으며 이 기술을 적용한 단말 수 및 서비스 시장 규모는 2010년 1억 1천만대 및 1억 1천만 달러에 이를 것으로 전망됨

- 다음 그림과 같이 국내 정보보안 시장은 SW부분은 연평균 12% 성장세를 보이는 반면, HW 부문이 연평균 18%의 성장세를 보일것으로 전망됨. 이에 하드웨어 기반의 고성능의 암호프로세스 기술 개발에 대한 연구가 진행될 것으로 사료됨

〈국내 정보보안 HW 시장 전망〉



※출처 : KIPA, 국내 정보보호 시장 동향과 전망, 2008

• 특히, 텔레매틱스 시장은 무선인터넷의 급속한 성장과 높은 자동차 보급률로 인하여 높은 성장 잠재력을 가지고 있음. 또한, 국내 1인당 연 평균 차량 주행 시간이 약 750시간으로 선진국과 비교해볼 때 현저히 높기 때문에 이에 따른 시장 선점을 위한 기업간 경쟁이 치열하게 전개될 것으로 예상됨

〈텔레매틱스 서비스 생산액 현황(단위 : 억원)〉

구 분		생산액			
텔레매틱스 서비스		'05연간	'06연간	전년대비(증액)	비 고
		576	822	42.7%	
이통사	KTF	63	100	58.7%	직접조사
	LGT	-	-	-	
	SKT	498	686	37.8%	추정
	소계	561	786	40.1%	
자동차업체	모젠	15	36	133.3%	직접조사
	쌍용	-	1	0.0%	
	소계	15	36	139.5%	

※출처 : KAIT, 2007

- 국내의 경우, 2001년 대우자동차가 KTF 통신망을 이용하여 안전보안, 차량 원격제어, 교통정보 및 네비게이션 등의 기능을 제공하는 "드림넷" 서비스가 제공되기도 하였음

- 현대기아자동차는 휴대폰 기반의 차량 원격 진단 제어 서비스 "SHOW 현대차 모바일 서비스"를 상용화할 예정이며 르노삼성자동차는 2003년 9월 SK텔레콤과 공동으로 텔레매틱스 시스템인 INS를 개발하여 SM5와 SM3에 서비스를 제공하고 있음, 이 처럼 이동통신사와 자동차 제조사들의 사업화와 구매자들의 필요에 부합되어 적극적으로 진행될 것으로 전망됨

• 따라서 향후 텔레매틱스를 통하여 다양한 서비스를 제공하기 위해서는 적절한 수준의 보안을 제공하기 위한 암호 키 관리 기술에 대한 수요가 증가할 것으로 전망됨

나) 인증 기술

• 시스템 및 네트워크 정보보호 제품의 소분류별 매출현황 중 공개키기반구조는 2007년도 매출액 26,474백만원에서 2008년도 26,954백만원으로 1.8%의 증가를 보이고, 인증제품의 경우 2007년도 매출 14,450백만원에서 20087년도 17,360백만원

으로 20.1%의 증가를 보인다. 하지만 전체 시스템 및 네트워크 정보보호 제품의 매출에서 인증제품 및 공개키기반구조가 차지하는 비중은 6.9%에 불과함

〈정보보호 제품의 매출 현황(단위: 백만원)〉

구 분	2007년	2008년	증감율(%)	매출비중(%)
공개키기반구조	26,474	26,954	1.8	4.2
인증제품	14,450	17,360	20.1	2.7

※ 출처 : 한국인터넷진흥원, 2008 국내 정보보호산업 시장 및 동향조사, 2008

• 정보보호 서비스의 소분류별 매출 현황 중 인증서비스는 2007년 20,645백만원에서 2008년 24,463백만원으로 13.6% 증가

〈정보보호 서비스의 매출 현황(단위: 백만원)〉

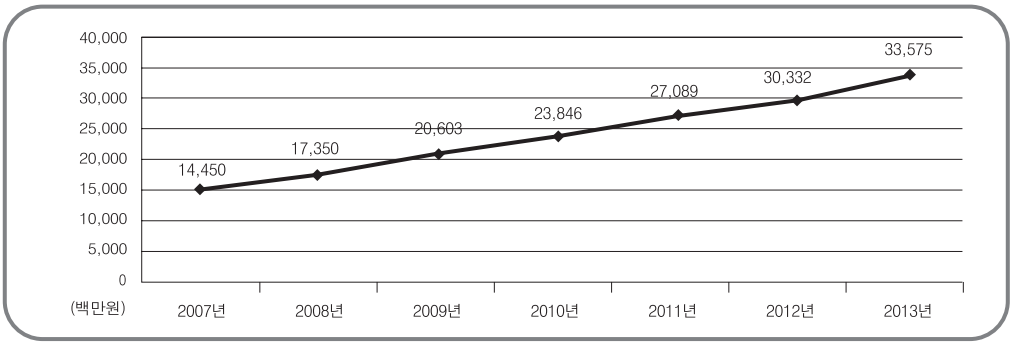
구 분	2007년	2008년	증감율(%)	매출비중(%)
인증서비스	20,645	24,463	18.5	19.1
인증제품	14,450	17,360	20.1	2.7

※ 출처 : 한국인터넷진흥원, 2008 국내 정보보호산업 시장 및 동향조사, 2008

• 인증제품의 매출액은 2008년 17,360백만원으로 2,910백만원(20.1%) 증가하였으며, 연평균성장률(CAGR) 15.1%로 지속적으로 증가하여 2013년에는 총 매출액이 33,575백만원에 이를 것으로 예상된다. 특히 1회 입금 규모에 따라 정해진 기준이 좀 더 맞아진 2008년 이후부터 인증제품에 대한 수요가 더 늘어난 것으로 추정된다. 금융권을 중심으로 새롭게 부각되고 있는 사용자인증 수단인 일회용비밀번호(OTP)와 더불어 보안토큰(HSM) 시장이 지속적으로 성장할 것으로 전망

〈인증제품의 매출 전망(단위: 백만원)〉

구 분	2007년	2008년	2009년	2010년	2011년	2012년	2013년	GAGR(%)
스마트카드	7,590	9,638	11,917	14,196	16,475	18,754	21,033	18.5
보안토큰	2,940	3,418	3,902	4,386	4,870	5,354	5,838	12.1
OTP	3,920	4,304	4,784	5,264	6,224	6,224	6,704	9.4
합 계	14,450	17,360	20,603	23,846	27,089	30,332	33,575	15.1



※ 출처 : 한국인터넷진흥원, 2008 국내 정보보호산업 시장 및 동향조사, 2008

- 보안 스마트카드는 일반카드와는 달리 반도체 칩을 내장하여 방대한 양의 데이터를 저장할 수 있으며, 보안성이 뛰어나 향후 다양한 분야에서 지속적으로 활용될 것으로 전망된다. 보안토큰 및 OTP의 경우 금융기관에서 보급단계에 들어설 것으로 보여 꾸준한 성장이 전망

- 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 있음

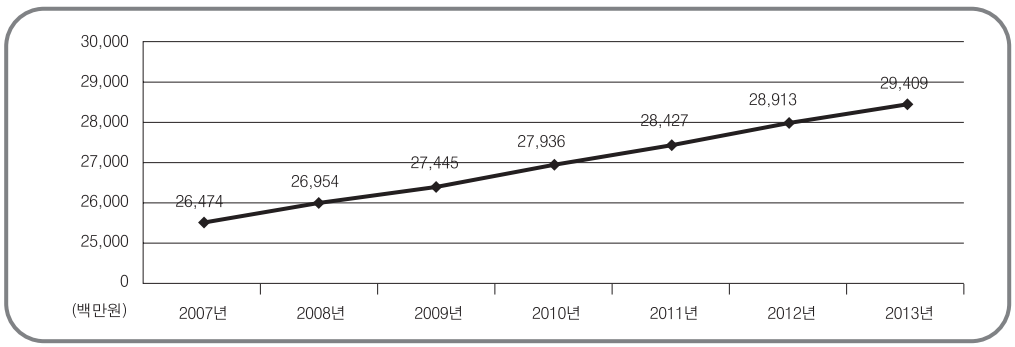
- 2008년 4월 "보안등급별 이체한도 차등화 정책" 시행에 따라 보안 1등급 매체인 OTP 발급자수는 꾸준히 증가하여 2009년 7월 OTP 기기의 발급자수가 280만 명을 돌파하였으며 전자금융거래에서 OTP 인증은 계속 늘어날 전망이다. 모바일 OTP의 경우 웹 포탈 및 온라인 게임 서비스 등에서 사용자 인증 수단으로 서비스되고 있으며 현재 약 70만 명 정도가 사용 중에 있고 계속 늘어나는 추세임

- 현재 국내 금융권에서는 OTP 통합인증센터를 구축하여 전자금융거래에 통합인증서비스를 이용하고 있다. 향후 전자정부 등에서 OTP를 활용할 경우, 전자정부용 OTP 인증센터가 구축될 수 있으며 이 경우 OTP 센터간의 연동을 위해 표준 인증 프레임워크가 확대될 수 있을 것으로 예상됨

• 공개키기반구조의 2008년도 매출액은 26,954백만원으로 2007년도 매출액 26,474백만원보다 480백만원(1.8) 증가하였다. 연평균성장률(GAGR) 1.8%의 성장추세를 꾸준히 유지하여 2013년도는 29,409백만원으로 예상된다. 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	2007년	2008년	2009년	2010년	2011년	2012년	2013년	GAGR(%)
공개키기반구조(PKI)	26,474	26,954	27,445	27,936	28,427	28,918	29,409	1.8



※ 출처 : 한국인터넷진흥원, 2008 국내 정보보호산업 시장 및 동향조사, 2008

• 무선/모바일 보안의 2008년도 매출액은 8,200백만원으로 전년도 매출액 6,649백만원에 비해 1,551백만원(18.9%) 증가하였으며, 연평균성장률(CAGR) 15.2%로 매년 상승하여 2013년에는 15,540백만원의 매출에 이를 것으로 전망된다. 무선/모바일 보안은 비즈니스 프로세스를 지원하는 형태로 점차 발전하고 있어 수요 증대가 확대될 것으로 예상됨

〈무선/모바일 보안의 매출 전망(단위: 백만원)〉

구 분	2007년	2008년	2009년	2010년	2011년	2012년	2013년	GAGR(%)
무선/모바일 보안	6,649	8,200	9,668	11,136	12,604	14,072	15,540	15.2

※ 출처 : 한국인터넷진흥원, 2008 국내 정보보호산업 시장 및 동향조사, 2008

- 현재 핸드폰 환경에서 지원되고 있는 인증서비스는 크게 3가지가 있다. 하나는 인증서를 활용한 뱅킹, 증권, 신용 확인, 입찰 등이며 2009년 현재 관련 서비스 이용자는 150만명이 넘어서고 있음. 두번째는 게임사이트 및 기업 등에서 사용되고 있는 모바일 OTP로 가입자가 100만명을 넘어서고 있다. 마지막으로 각종 사이트의 회원가입시 신원확인과 중복 가입 방지, 과금 등을 목적으로 사용되고 있는 SMS 인증이 있다.

- 3G폰의 보급이 확산 되면서 USIM에 금융 솔루션 탑재가 되고 있으며 2009년 말경부터 대용량 USIM이 출시될 예정이어서 다양한 솔루션 탑재가 가능하게 될 것이며 인증서 및 모바일 OTP관련 솔루션도 USIM을 활용하여 탑재 할 예정이다. 그러나 아직까지 USIM의 개방이 완전히 이루어지지 않았거나 이루어졌어도 활용하는 사례가 많지 않아 통신사들이 자체 규격 및 기술을 반영하는 일들이 진행되고 있기 때문에 이는 또 다른 폐쇄 정책이 될 수 있다. 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 구현될 것으로 예상된다. 특히 해외에서 NFC USIM기술이 확보되어 있기는 하나 접촉 위주의 서비스인 반면, 국내에서는 교통카드처럼 비접촉으로 사용되는 경우가 많아서 이를 기반으로 한 기기 간 인증까지도 향후 도입/확산될 가능성이 높음

• 2009년 바이오인식 시장은 지난해 대비 27.3% 성장한 1,528억원 규모를 형성할 것으로 전망되며, 2012년까지 17.0%의 연평균성장률(CAGR)을 기록하며 2,264억원에 달할 것으로 전망됨

〈바이오인식의 매출 전망(단위: 백만원)〉

구 분	2007년	2008년	2009년	2010년	2011년	2012년	GAGR(%)
지문인식	94,521	112,108	135,201	154,864	177,215	199,566	16.1
안면인식	6,073	5,565	14,900	15,756	18,894	22,033	29.4
정맥인식	1,500	2,088	2,400	3,134	3,741	4,349	23.7
홍채인식	1,340	200	250	333	408	483	24.7
합 계	103,434	119,961	152,751	174,087	200,259	226,432	17.0

※ 홍체인식의 경우, 2008년부터는 응답업체 수의 감소로 인해 시장규모가 줄어듬. 그러므로 2008년부터 연 평균 성장률을 산출함

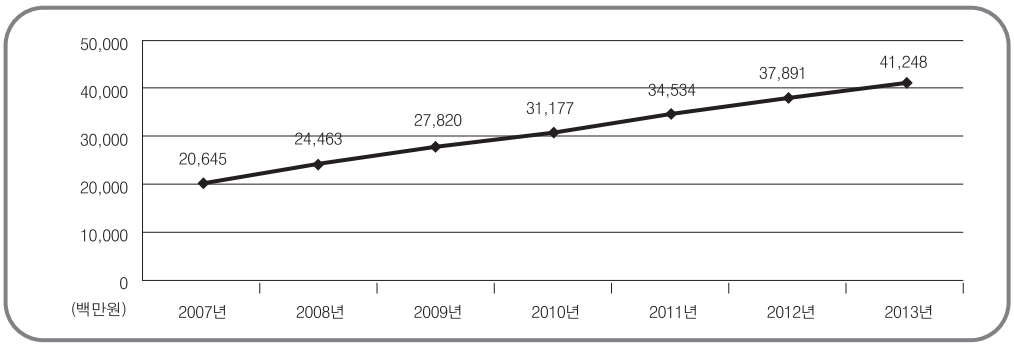
출처 : 국내 바이오인식 산업 현황 조사 보고서(한국바이오인식포럼)

• 인증서비스의 2008년도 매출액은 24,463백만원으로 2007년 매출액 20,645백만원보다 3,818백만원(15.6%) 증가한 것으로 분석된다. 연평균성장률(CAGR) 12.2%로 매년 성장하여 2013년도에는 41,248백만원에 이를 것으로 전망됨

- 유비쿼터스 환경에 참여하는 다양한 기기 및 정보에 대한 신뢰된 인증서비스 제공이 필요함에 따라 향후 거래인증서비스, 기기인증서비스, 공인전자문서서비스의 시장 수요가 크게 증가할 전망임

〈인증서비스의 매출 전망(단위: 백만원)〉

구 분	2007년	2008년	2009년	2010년	2011년	2012년	2013년	GAGR(%)
인증서비스	20,645	24,463	27,820	31,177	34,534	37,891	41,248	12.2



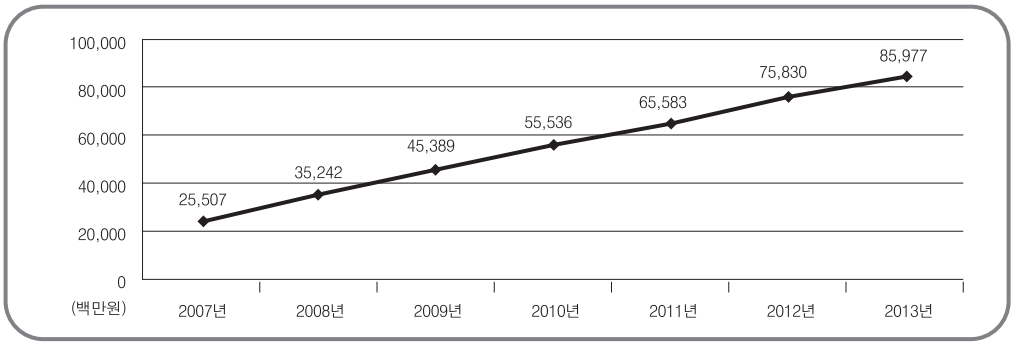
※ 출처 : 한국인터넷진흥원, 2008 국내 정보보호산업 시장 및 동향조사, 2008

다) 권한관리 기술

- 권한관리는 개인정보보호와 기업정보보호 등이 주요시되는 보안추세에 힘입어 2008년도 매출액은 35,242백만원으로 2007년도 매출액 25,507백만원에 비해 9,735백만원(27.6%)이나 상승하였으며, 연평균성장률(CAGR) 22.4%로 지속적으로 성장하여 2013년에는 총 매출액 85,977백만원에 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	2007년	2008년	2009년	2010년	2011년	2012년	2013년	GAGR(%)
네트워크 접근제어(NAC)	14,084	16,578	19,899	23,220	26,541	29,862	33,183	15.4
통합접근관리(EAM)	2,236	3,584	4,892	6,199	7,506	8,813	10,120	28.6
싱글사인온(SSO)	5,393	7,960	10,814	13,668	16,522	19,376	22,230	26.6
통합계정관리(IM/IAM)	3,794	7,119	9,784	12,449	15,114	17,779	20,444	32.4
합 계	25,507	35,242	45,389	55,536	65,683	75,830	85,977	22.4



※ 출처 : 한국인터넷진흥원, 2008 국내 정보보호산업 시장 및 동향조사, 2008

- 최근 들어 많은 원격 기기들이 IP망 및 내부 네트워크로 연결되기 시작하면서 기기 인증 및 접근자 인증에 대한 이슈가 생겨나고 있다. 2005년에는 홈네트워크 인증 프레임워크를 ETRI에서 개발 하였고 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 되어 이를 위한 표준화가 필요한 상태이다. 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 보안이 필요한 상황임
- 그러나 현재 적용된 설비에는 권한관리가 포함되어 있지 않으며 암호화도 적용되어 있지 않다. 보안이 아예 적용 불가한 경우도 있어 개방에 있어 새로운 적용 방법 검토 및 재고가 필요한 상황임

• 융복합 인증 서비스 시장의 경우 단순히 정보보호 서비스와 관련되기 보다는 인터넷 뱅킹과 모바일뱅킹, 인터넷 쇼핑 등 최근 각종 전자거래의 증가와 휴대폰, PDA 다양한 단말기의 사용, 센서네트워크와 무선 메쉬 네트워크, 홈네트워크 서비스 등 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

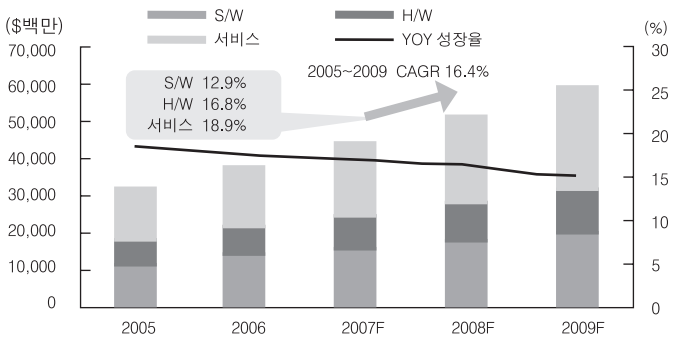
• 시장조사기관 IDC에서 따르면, 전 세계 정보보호시장은 2005년부터 연평균 13.5%의 고속 성장을 지속하면서 2007년에는 417억 달러 규모로 성장한 것으로 나타내고 있으며, 이에 따라 전체 정보통신시장에서 정보보호 시장이 차지하는 비중이 2005년 1.44%, 2006년 1.48%, 2007년 1.64%로 꾸준히 증가하고 있음

〈전 세계 정보보호 산업 및 정보통신 시장 규모 추이 (단위: 백만달러)〉

구 분	2005년	2006년	2007년	CAGR
세계 정보보호시장	32,331	35,686	41,668	13.5%
세계 정보통신시장	2,248,395	2,405,222	2,546,449	6.4%
세계 정보통신시장 대비 정보보호시장 비중	1.44%	1.48%	1.64%	

※출처 :IDC, KISA 2008 정보보호시장 트렌드 및 해외 정보보호시장 분석, 2008

• 해외 정보보안 시장의 경우 보안 서비스 부문이 2005년부터 2009년까지 연평균 16.4%로 가장 높은 성장세를 보일 것으로 전망되고 있음. 보안 HW 및 SW 시장은 각각 16.8%와 12.9%의 성장세가 나타날 것으로 전망되고 있음. 이는 IT인프라 구축 이후 발생하는 다양한 정보화 역기능의 문제를 해결하기 위해 정보보호에 대한 투자가 지속적으로 발생하였고, 미국을 중심으로 금융, 보건, 국방 등 사회 각 분야에 있어서 정보보호에 대한 규제가 강화되고 있으며 이는 민간의 수요를 촉발하는 원인이 된 것으로 파악됨



〈글로벌 정보보안 시장의 전망〉

※ 출처 : KIPA, 국내 정보보호 시장동향과 전망, 2008

• 국내 정보보호기술은 정보보호 선진국의 80% 수준으로 지속적인 기술개발이 필요하며, 국내 연구기관 및 기업의 경우 기술의 성능향상, R&D에 주력하고 있으나 이런 Catch-up기술 개발전략은 세계 시장 경쟁에 있어 한계가 있으므로 신규 IT서비스 등에 있어서 새로운 혁신적 정보보호기술 및 상품을 개발하기 위한 전략이 필요

〈u-정보보호 관련 현 정보보호 요소기술 경쟁력 분석〉

구 분	기술 분류	인프라 보호기술	국내외 기술격차(년)	상대수준(%)
사용자 측면	암호/인증/권한관리 기술	암호	1.5	82.5
		인증(SSO, PKI, WPKI 포함)	0.3	98.8
		접근제어	1.2	90.0
	개인정보보호 및 바이오 보안	개인정보관리	0.8	90.0
		바이오 정보 관리(지문, 홍채 인식 등)	3.0	75.0
서비스 및 디바이스 측면	해킹/바이러스/범죄대응기술	해킹 및 웜/바이러스 방지	0.7	83.8
		디지털 포렌직	2.8	67.5
	디바이스 및 서비스 보호기술	이동통신서비스/기기 보안(WiBro 포함)	1.0	86.7
		지능형 로봇 서비스/기기 보안	2.3	79.0
		U-Home 서비스/기기 보안	0.5	90.0
		텔레매틱스 서비스/기기 보안	0.5	90.0
		광대역융합서비스/기기 보안(IPTV 등)	1.5	80.0
		바이오보안 응용(의료 정보보호 포함)	3.5	65.0
		디지털 콘텐츠 서비스 보안	3.3	70.0
		IT Soc 보안	1.7	80.0
		VoIP/MoIP 보안	0.5	95.0
		임베이드 SW 보안	2.2	80.0
		웹서비스 보안	0	100
국내외 평균 기술격차 및 상대수준			1.4	84.8

※ 출처 : ETRI 정보보호연구단, 정보보호기술 및 제품 경쟁력 분석서, 2006. 9.

• 시장 경쟁에서 네트워크 보안제품, 취약성 및 로그분석 SW의 경우 미국이 비교우위를 차지하고 있고, 바이오 인증 및 DB 보안제품군에 있어서는 국내 제품이 상대적으로 경쟁력을 지닌 것으로 조사되었으며, PKI 기반 제품군의 경우 미국과 국내 제도가 상이하여 관련 제품의 상대국가 시장에서 경쟁은 발생하기 힘들 것으로 전망

〈미국과의 정보보호 제품 경쟁력〉

구 분	미국과의 제품 경쟁력 조사		수출비중	수입시장
	격 차	상대수준		
정보보호 HW	1.87년	75.0%	66.79%	50.95%
정보보호 SW	1.25년	80.5%	31.65%	33.98%
정보보호 서비스	1.03년	95.7%	1.56%	15.07%
합 계	1.40년	84%	100%	100%

※ 출처 2005년 국내 정보보호산업 통계조사, KISA

• 전체 정보통신시장 중에 정보보호산업이 차지하는 비중을 살펴보면, 아래 〔표 9〕에서 보는 바와 같이 세계 정보통신시장은 2004년부터 2006년까지 3년간 연평균성장률(CAGR: Compound Annual growth Rate)이 6.69% 성장한 반면, 세계 정보보호시장은 동기간에 17.78%의 성장률을 보여, 세계 정보통신시장 성장 속도에 비하여 세계 정보보호시장 성장 속도는 약 2.7배 정도 빠른 것으로 분석됨

〈국내외 정보보호산업과 정보통신산업의 성장률 비교 (단위: 억원(국내), 백만달러(세계))〉

구 분		2004년	2005년	2006년	3년간 CAGR(%)
정보보호시장	세계(A)	274,770	323,310	381,140	17.78
	국내(B)	6,261	6,807	7,052	6.13
	점유비율 (B/A)(%)	2.28	2.11	1.85	-
정보통신시장	세계(C)	2,084,633	2,248,395	2,372,708	6.69
	국내(D)	2,285,251	2,332,089	2,481,011	4.20
	점유비율(C/D)(%)	10.96	10.37	10.46	-
세계 정보통신시장 대비 정보보호시장 비중(A/C)		13.18	14.38	16.06	-
국내 정보통신시장 대비 정보보호시장 비중(B/D)		0.27	0.29	0.28	-

자료: 국내정보통신시장(KAIT), 국내정보보호시장(KISA), 세계정보통신시장 및 정보보호시장(IDC)의 자료
※ 출처 : KISA, 2007 국내 정보보호산업 시장 및 동향조사, 2007

• 최근, 유비쿼터스 및 컨버전스라는 시대적 패러다임의 변화에 따라 경량 암호 알고리즘, 텔레매틱스 기술에 대한 관심이 고조되고 있음. 경량 암호 알고리즘은 무선 통신, 주위 정보 센싱 등과 같은 RFID/USN 기술에 대한 연구가 활발히 이루어지고 있으며, 텔레매틱스가 크게 주목받는 것은 텔레매틱스 산업이 오프라임 산업의 IT화를 추진하는 대표적인 산업이며, 세계 5위권인 자동차 산업을 기반으로 세계적으로 앞서있는 IT산업과의 결합을 통해 새로운 시너지 효과의 극대화가 가능할 것으로 예삼됨

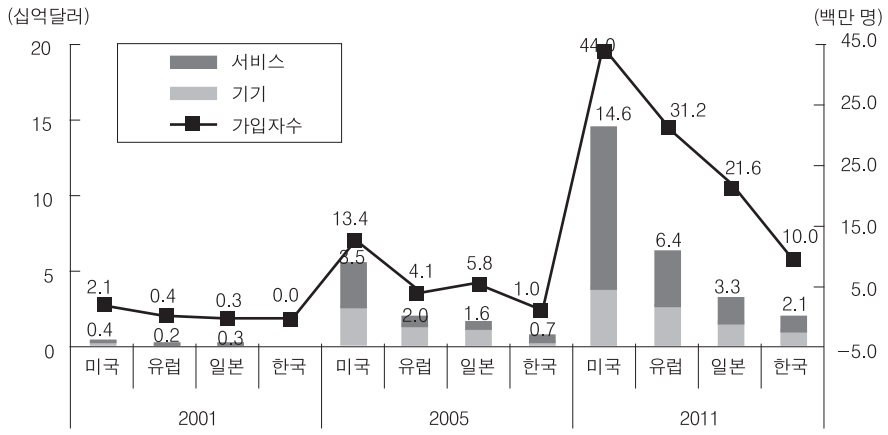
- 국외 RFID/USN보안 시장은 2008년 15억달러에서 2014년 160억 달러로 예측됨
  ※ RFID/USN 확산 추진계획, 2008년 자료를 토대로 보안 및 프라이버시 보호 기술의 기여도를 17%로 추정함 결과임
- 그러나, 보안 기술 적용이 필수인 미국 u-health 시장이 매년 52.1%의 높은 성장세를 보임에 따라, 경량 암호알리즘에 대한 시장 수요가 점점 증가할 것으로 예측됨(Forrester의 2004년 발표에 따르면, 미국 u-health 시장은 2010년 57억 달러가 되며, 2015년 336억 달러 규모로 급성장할 것으로 전망)
- 전세계 텔레매틱스 시장규모가 2003년 130억 달러에서 2008년 410억 달러로 증가할 것이며, 전세계 텔레매틱스 서비스 가입자 수가 2003년 1,100만에서 2008년 6,200만으로 증가할 것으로 전망됨

〈세계 텔레매틱스 시장 규모 (단위: 백만달러)〉

구 분	2003년	2004년	2005년	2006년	2007년	2008년	CAGR('03-' 08)	2010년	2015년
서비스	3,252	4,010	5,135	6,635	8,940	12,192	30.3%	20,338	51,565
시스템	3,204	3,681	4,243	4,887	5,664	6,686	15.8%	9,349	22,180
단말(node)	6,633	8,054	10,150	12,758	16,756	22,214	27.3%	34,094	91,112
합 계	13,089	15,745	19,528	24,280	31,359	41,092	25.7%	63,781	164,857

※ 출처 : KISDI, 2005 ETRI 정책지원자료, 2005

- 향후 2010년에는 미국 · 유럽 · 일본 등에서 판매되는 자동차에 내장되는 GPS와 위성라디오 · 이동통신서비스 등의 IT관련 시장규모가 상당히 큰 규모로 발전할 것으로 예상되며, 탤레매틱스 서비스 및 기기 매출액 규모는 미국 2001년 4억 달러 규모에서 2010년 146억 달러로 평균 49% 이상의 높은 성장률을 보일 것으로 전망되며, 유럽은 47%, 일본은 31%의 증가세를 보일 것으로 전망



〈세계 텔레매틱스 매출액 및 가입자 규모 예측〉

※ 출처 : IITA 정보조사분석, 2009

나) 인증 기술

• IT 시장 조사 기관인 IDC는 세계정보보호시장 규모 및 전망 보고서인 "Worldwide and U.S. Security Services 2006~2011 Forecast and Analysis" 발표하였다(2008.1). 이 보고서에 따르면 2006년부터 2011년까지 세계정보보호시장은 약 15% 성장 할 것으로 전망된다. OTP, 보안토큰 등 개인용 휴대보안기기에 탑재되는 사용자 인증 및 접근 관리(IAM) 소프트웨어는 로그온 및 패스워드 관리를 단순화하여 컴플라이언스와 거버넌스 환경에서 필요로 하는 신뢰성을 제공할 것으로 전망하고 있음

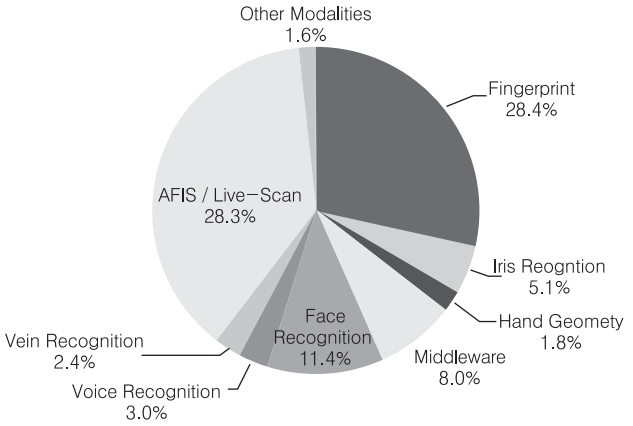
• 해외에서는 국내와 같이 공인인증서 인프라가 잘 갖추어져 있거나 활용도가 높은 국가를 찾아보기 어렵다. 그로 인하여 모바일 환경에서 인증서를 활용한 서비스가 지금까지 알려져 있지 않다. 그러나 RIM사의 블랙베리에서 메시지 보안을 ID기반 암호화를 적용하면서 새로운 트랜드가 생겨나기 시작했다. 공개키를 비롯한 보안 프로토콜을 연구하는 분야에서는 주요 연구과제로 자리 잡기 시작 했다. 국내에서도 이에 대한 연구가 활발한 상황임

- 국내처럼 활발하지는 않지만 SMS 인증도 역시 널리 사용이 되고 있다. 그러나 해외의 경우 USIM의 이동성이 보장되고 있기 때문에 USIM을 활용한 특정 통신사에 의한 기능 추가나 기술 선도가 거의 이루어지기 어려운 현실이다. 결국 글로벌한 표준 반영이 있기 전에는 새로운 기술 반영이 있기 어려우며 동시에 필요성이 인정되면 오히려 더욱 빨리 표준화가 진행될 가능성도 높다고 할 수 있음

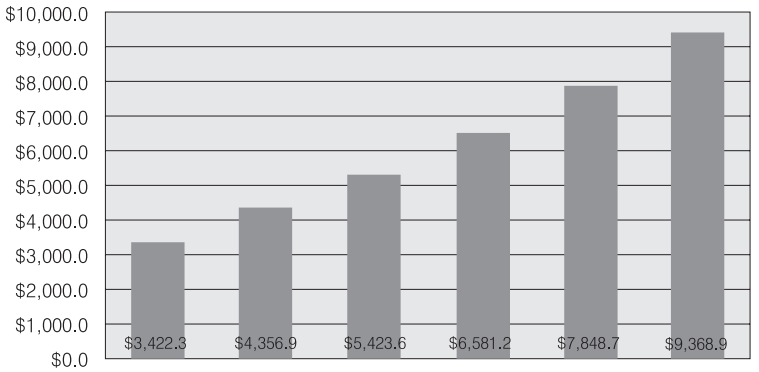
• 2002년 FFIEC(미국 연방금융기관 검사협의회)에서 발표한 인터넷뱅킹 사용자 인증 가이드라인에서 2-factor 인증 및 OTP 사용을 권고함에 따라, 미국의 BoA(Bank of America), Citibank를 비롯하여 싱가폴 HSBC, 일본, 호주, 유럽의 주요은행들이 전자금융거래에 2-factor 인증 도구로 모바일 OTP 및 하드웨어 OTP 기기를 활용하고 있다. 또한 미 국방성에서도 사용자 인증 및 접근통제 권한 부여를 위해 OTP를 활용하고 있다. 인터넷 전자상거래 및 온라인 교육, 의료 서비스에서도 사용자 인증을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

- 싱가폴 등에서는 전자금융거래를 위한 OTP서비스를 구축중이며, 국내에서 개발하고 있는 OTP 인증 프레임워크와 유사한 모델을 구현 중에 있다. 해외 OTP 인증 프레임워크 사례들은 일반적으로 특정 벤더에 의한 단일 OTP 인증 프레임워크가 제공되고 있는 현황이다. 향후 개발도상국의 전자정부나 해외 금융권에서의 강한 인증 수단으로서 OTP 인증프레임워크 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 나타났다. 2009년 3,422.3 백만달러 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

• 2006년부터 2011년까지 세계정보보호시장은 약 15% 성장 할 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 Vulnerablity 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 있다. 이것은 국내 정보보호 부분에서도 마찬가지이며 최근에 정보보호 소프트웨어 보다는 보안관제 등과 같은 서비스 부분이 많이 강화되고 있는 것이 그 예

〈각 국가별 GDP 대비하여 정보보호 시장 규모〉

구 분	Hardware	Software	Service	합 계	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 두가지 방향으로 진행 중에 있음

• 블록 암호알고리즘 기술

- 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

- 그 이외에도 퓨쳐시스템, 포럼 등 보안제품 개발 업체에서 암호 알고리즘을 개발하기도 함. 국내에서 안전하게 개인정보 등이 포함된 중요한 데이터를 안전하게 전송하기 위한 시스템을 구축하기 위해 연구를 진행하고 있으나, 일부 원천기술의 미흡으로 인하여 선진국에 비하여 1.3년 정도 뒤져있다고 판단
  - SEED 암호 알고리즘은 1998년 민간 표준으로 사용하기 위해 개발한 128비트의 블록암호를 개발한 이후, MS 윈도우 비스타, 서버 2008, Openssl 용 SEED 패치를 개발하는 등 다양한 환경에서 활용될 수 있는 관련 도구를 개발하고 있음
  - 국내의 SEED 블록 암호 알고리즘은 2000년도 초기에 128비트 키를 사용하도록 개발되었으나, 컴퓨터 기술의 발달 등으로 128비트 이상의 안전성을 제공하는 암호 알고리즘이 개발 및 활용되고 있어, SEED 암호 알고리즘의 안전성 강화를 위해 2009년도 192/256비트의 키를 지원하는 암호 알고리즘을 개발하였음

▫ ARIA 암호 알고리즘은 2004년에는 경량 환경 및 하드웨어의 최적화된 구현을 위해 128/192/256비트의 키 길이를 지원하는 암호 알고리즘을 개발하였으며, 정부 및 공공기관의 보안통신 등에 활용됨

▫ HIGHT 암호 알고리즘은 저전력 · 경량화를 요구하는 컴퓨팅 환경에서 기밀성을 제공하기 위한 목적으로 2005년 KISA, ETRI 부설연구소 및 고려대가 공동으로 개발한 64비트 블록암호 알고리즘으로 RFID, USN 등과 같은 환경에서 적용 가능함

▫ 퓨쳐시스템 암호체계센터에서 자체 개발한 128비트 알고리즘 CRYPTON은 NIST의 AES 공모에서 1차 평가대상 알고리즘으로 선정되어 자사 보안제품에 탑재하고 있음. 소프트포럼에서 개발한 128비트 암호 알고리즘으로 Xenon, Zodiac이 개발되어 ISO/IEC의 표준화 추진 알고리즘으로 국내에서 선정되기도 하였으나, 안전성의 문제로 표준으로 제정되지 못함

- 최근에는 RFID/USN과 같은 초경량 구현 환경에 적합한 블록 암호 알고리즘 개발에 관심이 높아지고 있으며, 이를 고려하여 초경량 환경에서도 구현 가능한 HIGHT 암호 알고리즘을 개발하여 ISO/IEC 국제 표준화를 추진 중임, 대부분 KISA, ETRI, NSRI, 고려대학교 등과 같은 소수 그룹에 한정되어 연구되고 있는 실정임

• 응용서비스에서의 암호 알고리즘 활용 방법

- 원천기술인 암호 알고리즘을 개발하는 한 후에 개발한 블록 암호 알고리즘의 활성화 제고를 위해 VoIP, IPTV 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

• 텔레매틱스 환경에서의 암호 키 관리 기술

- (구) 정보통신부는 지난 2004년 IT839 전략의 일환으로 텔레매틱스 서비스 및 산업 활성화 전략을 수립하여 추진한 바 있음. 텔레매틱스 9대 핵심사업 중 하나로 텔레매틱스 기반 및 응용기술 개발을 2004년부터 2006년까지 약 3개년에 걸쳐 추진한 바 있으며, 텔레매틱스 테스트베드 구축, 시범도시 구축, 텔레매틱스 정보센터 구축 등의 사업에 적용하였음

- 국내에서 텔레매틱스 환경에서의 보안 기술 및 키 관리 기술 연구는 ETRI에서 주도하고 있으며, 그 외에 고려대학교, 성균관대학교, 숭실대학교 등이 학계에서 보안 기술을 연구 · 개발하고 있음

▫ ETRI에서는 텔레매틱스 단말기 상에서 다양한 정보 기기와 연동되고 텔레매틱스의 활용성 및 제품성을 높이기 위한 단말 S/W 플랫폼 및 정보 관리 기술을 개발하였으며, 유무선 네트워크, 유무선 네트워크, 휴대 단말기, 콘텐츠 응용 시스템 간 상호운용성을 지원하는 개방형 LBS 미들웨어 플랫폼 기술 및 LBS 핵심공통 기술, 단말-센터 간 서비스 응용 프로토콜 확장 개발 및 최적화와 센터-외부 콘텐츠 서버 간 통합 프레임워크를 개발하였음

▫ 또한, 2007년부터 2011년까지 실내외에서 연속적이고 안정적이며 정확도가 높은 측위정보 및 위치기반서비스 제공을 위한 무선통신 인프라 기반 실내측위 기술, 실내외연속 복합 측위용 단말 등을 개발하는 "실내외 연속 측위 기술 개발", 고속으로 이동하는 차량에 차량 안전 및 ITS 서비스를 제공하기 위한 차량간 V2V 통신 및 V2I 통신 핵심 기반 기술을 개발하는 "차량 멀티홉 통신(VMC) 기술 개발" 과제를 ETRI에서 추진중에 있음

- 정부 차원에서는 건설교통부는 과천시를 시범사업대상지로 결정하여 종합적 ITS 시범운영사업에 착수하였으며, 서울시는 도시고속도로의 원활한 교통소통 및 안전성 향상을 목적으로 올림픽대로 전 구간에 걸쳐 교통관리 시스템을 도입 · 운영 중임

- HK e-CAR의 블랙박스는 차량운행기록, 사고 전/후 일정시간의 조향각도 차량속도 등의 정보와 운전자 조작상황 및 차량 거동 상황 저장, 분석 가능한 모델을 개발한 바 있음

- 아이디스는 DVR(Digital Video Recorder) 기술을 이용한 차량용 블랙박스와 관련하여 충격과 진동에 관한 해외규격을 통과한 차량용 DVR 2 모델을 개발한 데 이어 스쿨버스를 운영 중인 교육단체와 차량용 DVR 납품에 관한 협상을 전개하고 있는데, 유럽 철도회사에 차량용 DVR을 납품함

- 차량간 무선통신을 위한 Mobile Ad-hoc Network에 대한 연구는 대부분 시뮬레이션이나 간단한 테스트베드 상에서의 기능 및 성능 확인 정도가 주를 이루고 있고 실험실 수준의 연구개발을 추진하고 있으며 상용화의 추진은 아직 이루어 지지 않고 있음. 최근, 텔레매틱스는 컴퓨팅, 통신, 콘텐츠, 측위 및 자동차 산업의 융합 기술로서 개별적으로 존재하는 각 기술을 통합하는 핵심 기술로 부상하고 있으며, 이에 대한 연구가 활발히 이루어질 것으로 보임

• 암호알고리즘 이용 가이드라인

- '06년 한국정보보호진흥원에서 조사한 국내 IT 서비스 제공업체의 암호 솔루션 사용현황에 따르면, 금유기관을 제외한 교육, 의료, 전자거래 업체 등의 암호 솔루션 사용현황이 40%이하로 낮게 나타남. 또한 동일한 조사에서 암호솔루션 도입 필요성에 대한 CEO의 인식 부족 및 비용 부담, 관련 전문가 및 분야별 암호적용 범위 수준 등에 대한 구체적인 구현 가이드라인 부재 등이 암호 솔루션의 도입을 미루는 이유로 분석됨

- 이에 따라 '07년 12월, KISA는 기업 및 기관의 시스템관리자 및 보안 관리자에게 해당 기업이 보유하고 있는 정보의 보안등급 및 이용단계에 따른 암호기술의 적용수준과 범위, 교육, 의료 등 분야별 암호기술 활용방안을 제시하고자 암호 이용 가이드라인을 제작하여 배포함.

- '08년 KISA는 기업 및 기관의 IT 정보자산 보호를 위한 "암호정책 수립 기준 설명서"를 제작하여 배포함. 암호정책 수립 기준 설명서에서는 정보보호관리 체계 관련하여 국내 ISMS(정보보호관리체계 인증제도)에서 명시하고 있는 암호통제 정책의 수립 기준, 방법 및 암호기술 도입기준 등을 제공함

- '08년 KISA는 국산 암호 알고리즘을 포함한 암호 알고리즘 및 키 길이 선택에 대한 기준을 제공하고자, "암호 알고리즘 및 키 길이 이용 안내서"를 제작하였음. "암호 알고리즘 및 키 길이 이용 안내서"는 SEED, HAS-160, KCDSA 등의 국산 알고리즘을 포함하여 보안강도에 따른 암호 알고리즘의 종류, 키 길이, 유효기간을 제공하고 있음

- 국내에서도 암호 기술 관련 산 · 한 · 연 전문가들을 기반으로 국산 암호알고리즘 및 국내 IT환경을 고려하여 안전한 정보보호 제품 및 시스템을 개발할 수 있도록 암호알고리즘 이용 가이드를 개발할 필요가 있음

• 고성능 암호프로세서 설계 기술

- 최근 정부에서는 Green IT를 "뉴 IT 전략"의 12개 세부 과제 중의 하나로 선정하고 에너지 효율성을 제공하는 IT 기술 개발되고 있음.

- 국내 암호 알고리즘 기술 현황은 2000년 공개키 암호 기술을 개발하는 등 다양한 암호 알고리즘을 개발하였고, 해쉬 알고리즘을 개발하는 증 선진국 수준과 기술 격차를 줄이고 있음. 최근 네트워크의 성향이 소형화, 무선/이동 네트워크, 저전력/저용량 등의 기술로 개발되고 있으므로 저전력의 경량 암호 알고리즘의 개발이 시급함

- 또한, 저전력, 소형화의 센서 노드나 무선 네트워크용 노드와 같은 소형 단말기 위주의 서비스가 개발되고 있으므로 이런 단말에서는 다량의 연산을 필요로 하는 암호 알고리즘을 수행하기가 어려우므로 암호 프로세서의 개발도 적용되고 있음
- 고속 암호 프로세서의 경우 시스템의 성능향상, 과도한 부하의 경감으로 시스템의 수명 연장, 안정성 증가와 중요한 암호 정보의 물리적 보호 등의 장점을 제공하므로 ETRI 등의 연구소와 보안 기술 업체, 메모리 칩 업체 등에서 개발을 진행하고 있음
  - 산업체에서는 비밀키 암호 알고리즘, 공개키 암호 알고리즘, 무결성 및 인증 알고리즘 등 네트워크 상에서의 Security Algorithm 동작을 하드웨어로 구현한 고성능 암호 전용 프로세서를 개발하고 있음
  - 삼성전자는 2008년 3세대 이동통신용 단말기나 유료 방송 서비스 등에 필수적인 사용자 인증 수단으로 활용되는 90나노 공정을 적용한 비메모리칩을 개발하였음
  - ETRI에서는 서비스 사업자에게 사용자 인증, 플랫폼 인증, 기기 인증, 데이터 보호 및 무결성 보장 등의 기능을 제공하는 모바일 컴퓨팅의 보안칩으로 모바일용 SoC인 mTPM칩을 개발함. 이 기술은 운용체제와 프로세서에 독립적이며 기존 플랫폼의 수정을 최소화하고 저렴한 초소형 칩으로 제공가능하며, 다양한 복합 단말 및 기지국 등에도 보안 모듈로 고정 장착이 가능한 하드웨어 기반의 기술임
  - 대학과 연구소 등에서는 Rijndael 암호 알고리즘 등 다양한 암호 알고리즘의 FPGA 설계에 대한 기술 개발을 진행 중임

- 국외의 경우 소형 센서 노드에 적합한 경량 암호 알고리즘의 개발 외에 가속화 기술이나, 고속 암호 프로세서의 적용 등의 기술 개발이 활발히 진행되고 있으나, 국내의 경우 아직까지 경량 암호 알고리즘 개발에 치중하고 있는 상황임

나) 인증 기술

• USIM 등 모바일 환경에서의 인증서비스 모델 및 인증기술

- USIM은 자체 암호 연산이 가능하기 때문에 사용자 인증을 위한 각종 키 값을 외부 유출 없이 내부에 보관하며 그 연산 결과 값만을 외부에서 이용하게 함으로써 사용자 인증을 보다 안전하게 할 수 있음. 그러나 USIM(UICC)는 이러한 다양한 키와 이 키를 사용하는 applet을 설치할 수는 있지만 이를 위해서는 내부에서 동작하는 프로그램에 관계없이 외부에서 바라보는 USIM의 모습은 동일하여야 함. 그래야 USIM의 이동이 가능하기 때문이며, 즉 통신사와 휴대단말의 종류에 관계없이 사용 가능할 수 있도록 개발 되어야 한다는 것임. 이는 PC에서 기존의 보안토큰이 API 수준에서 호환(PKCS#11)을 이루었지만 이제는 USIM과 통신하는 부분까지 호환이 이루어져야 한다는 것을 의미함 이를 위해서 검토해 볼 수 있는 기술은 HSM분야에서 오래 전부터 언급되어 오고 있는 PKCS#15을 적용하는 방법과 SCWS(Smart Card Web Server)를 도입하는 방법을 고려해 볼 수 있음. PKCS#15은 전체 applet을 변경 해야 하기 때문에 어플리케이션 추가 변경이 어려움. 그러나 SCWS는 기본적으로 웹서버이기 때문에 다양한 페이지를 만들어 넣을 수가 있으며 심지어 내부 리소스를 URI 형태로 접근 가능하기 때문에 웹의 장점을 그대로 가질 수 있음. 최근 국내에서도 SCWS 기술 개발을 완료한 상태이기 때문에 이를 기반으로 한 처리 페이지 입력, 파라미터 전달, 페이지 실행 결과 획득이 가능하게 되어 손쉬운 확장이 가능해지며 통신사별 재량권도 가져갈 뿐만 아니라 공간이 허락하는 한 무한대의 확장이 가능하게 됨
- 현재 국내에서는 카드 내부는 금융결제원의 금융 IC 스펙을 준수하고 외부 인터페이스는 KISA의 PKCS#11을 준수하는 것으로 되어 있음. 현재 금융 IC 스펙에는 인증서 관련 스펙은 있지만 OTP를 비롯한 다양한 사용자 인증을 위한 스펙은 고려되어 있지 않음. 그리고 그것을 금융 IC에 반영을 해야 되는지 여부도 타당성이 없는 상황

• 인터넷 전화 등에 이용 가능한 디바이스 인증 기술 및 응용

- 최근 유비쿼터스 환경 가속화로 사람뿐만 아니라 홈디바이스, 지능형 로봇, RFID 등 다양한 기기가 네트워크를 통해 연결됨에 따라 기기가 서비스 주체로 등장하고 있으나 이들 기기에 대한 신뢰된 인증체계 구축이 미흡한 실정임. 이에 따라, 행정안

전부 및 한국정보보호진흥원에서는 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**

- 국내에서 (주)미래테크놀로지사 및 (주)인터넷시큐리티사가 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
- 시각장애인을 위한 보이스 OTP 기술, 바코드와 모바일 OTP를 결합한 결제 솔루션 등 OTP를 응용한 기술 및 서비스 개발이 활발히 이뤄지고 있음

• **일회용패스워드(OTP) 인증 프레임워크**

- 일회용패스워드 인증 프레임워크란 하나의 OTP 토큰을 가지고 어느 은행에서도 전자금융거래를 수행하는 것이 가능하도록 제공해주는 서비스 제공 구조를 말하며, 국내 금융권의 금융보안연구원이 개발하여 구축한 OTP 통합인증 프레임워크가 이에 해당함. 현재 OTP 통합인증 프레임워크에 대한 표준개발이 진행되고 있음.

• **익명성을 보장하는 인증 기술**

- 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 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.
- 최근 인터넷상에서 악성 댓글, 불법 게시물 등에 따른 피해가 확산됨에 따라 인터넷 역기능 예방 및 대응을 위해 다양한 기술개발의 필요성이 대두되고 있음. 이를 위해, 기본적으로 인터넷 게시판 등에서 익명성을 보장하면서 범죄 등의 수사목적으로 해당 게시자의 신원을 확인할 수 있는 익명인증기술에 대한 요구가 증가되고 있으며 2008년부터 한국정보보호진흥원에서 익명인증서 프로파일에 대한 국제 표준화를 IETF PKIX WG에서 추진 중에 있으며, 2009년 하반기에는 IETF 표준화로 채택될 예정.

• **바이오정보를 이용한 전자서명 기술**

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

다) 권한관리 기술

• **기기 관리자 간의 권한 관리 응용 기술**

- 기기 관리자는 기기에 대한 키 생성, 키 분배, 각 기기들의 상태를 모니터하는 등의 보안 관련 활동을 수행하는 사용자임. 통신에 참여하는 개체(예, 사람, 기기, 서비스, 응용 등)에 대한 인증은 ID 인증서 및 디바이스 인증서를 통해 가능하며, 네트워크 자원에 대한 인가되지 않은 사용에 대한 접근제어는 ACL(Access Control List)을 이용한 인가, 인증서버를 이용한 인가,

권한 인증서 또는 인증서와 ID 인증서 속성을 이용한 인가가 있음.

- 일반적으로 기기 관리자 간의 접근제어 또는 인가는 권한인증서와 접근제어리스트를 사용함으로써 성취될 수 있음. 기기 관리자 인가를 위한 또 다른 방법은 권한인증서의 권한 위임을 허락하는 것으로 권한인증서는 서명된 ACL 입력이 디지털화된 것임.

• 융복합 인증 서비스 모델

- 지금까지 인증 서비스는 인증서 기반과 ID/PW 기반 등 기술과 서비스에 따라 별도로 제공되고 있으며 최근 관련 서비스끼리 통합하여 인증 서비스를 제공하는 SSO 서비스가 증가되고 있음.
- 최근 인증서 외에 생체정보, OTP, USIM 등 다양한 인증 수단이 제공되고, 모바일 환경이나 인터넷 전화, 기기 인증과 같은 새로운 인증 서비스 환경이 나타남에 따라 다양한 인증 서비스 모델이 등장하고 있어서 서비스 환경이 복잡하게 형성됨
- 따라서 인증 수단별, 서비스 환경별, 단말기 별로 적용되는 다양한 인증 서비스 모델을 통합하여 서비스 간의 이동이 편리하고 관리가 용이한 환경을 제공하는 것에 대한 관심 증가. 이러한 기술은 아직까지 연구 단계이지만, 최근 은행이나, 이동통신 서비스 업체 별로 자신의 서비스 영역에서 통합 인증 시스템을 구축하여 제공하는 예가 늘고 있음.
- 한국정보보호진흥원에서는 2008년 2월 이와 관련하여 u-인증 서비스 도입 및 이용 기준(안)을 마련하여 발표
- 2008년 KTF는 통합 인증 시스템 구축 프로젝트를 통해 실시간 인증 서비스와 무정지 시스템을 구현하여 내부 인프라와의 실시간 정보 동기화를 통해 데이터를 통합하고 유무선 서비스를 위한 가입자와 서비스 인증 기능을 제공
- 따라서 융복합 인증 서비스에 대한 서비스 분야의 부분적인 시행과 준비가 먼저 실행되고 있으며 관련 표준과 연구가 뒤따라야 하는 상황으로 판단됨

• 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 안저하게 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 대학등에서 이에 대한 취약성을 보고하였음
- USN 환경에서는 TinyOS기반의 TinySec 및 TinyECC에 대한 연구가 진행 중이며, 주로 ECC 암호 알로리즘은 저가의 USN 센서 노드에서 구현 가능하도록 경량 구현설계를 하였음

• 블록 암호알고리즘 기술

- 국외 암호 기술은 미국, 일본, 유럽의 일부 선진국들이 주도하고 있음. 미국은 NIST를 중심으로 AES 프로젝트를 통해 차세대 블록 암호를 선정하였고, 현재 AES에 적합한 블록 암호 운영 모드 선정과 SHA-1을 대체하기 위한 차세대 해쉬 함수 공모 사업을 진행하고 있음. 유럽은 전자서명, 무결성 및 암호화 기능을 제공하는 암호 원천기술에 대한 유럽 표준 암호 공모인 NESSIE 프로젝트를 통해 다양한 플랫폼에 적용 가능한 강력한 암호 원천기술을 개발하여 다양한 권고 알고리즘들을 제안함. 일본은 전자 정부의 구현을 목표로 이에 필요한 보안 기술을 확보하기 위하여 CRYPTREC 프로젝트 진행하였고 지속적인 암호 기술에 대한 평가와 조사를 실시하여 전자정부 실현을 위한 가능 기술에 대한 안전성, 구현성 등의 특징을 도출함
  - 초기에 블록 암호 알고리즘 DES가 표준으로 채택된 이후, DES와 유사한 구조를 갖는 다양한 블록 암호들 (FEAL, GOST, LOKI 등)이 개발됨. DES의 키 전수 조사가 가능해지고 대부분의 블록 암호들이 차분 공격과 선형 공격에 의해 취약점이 발견되면서 DES를 대체하기 위한 차세대 블록 암호 공모 사업이 진행되었고 AES가 차세대 불록 암호 표준으로 선정됨
  - 현재는 AES의 실용화에 대비한 다양한 블록 암호의 운영 모드 등을 비롯한 블록 암호 응용 기술에 대한 활발한 연구가 진행되고 있고 MISTY1, SHACAL-2, IDEA 표준 권고 알고리즘들에 대한 안전성 분석 연구가 지속되고 있음

• 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 중
  - 일본의 경우, 3GPP의 UMTS(Universal Mobile Telecommunication System), SSL/TLS, S/MINE 등에서 Camellia, KASUMI, MISTY1 등의 알고리즘이 활용 될 수 있도록 하였으며, 국외에서 활용될 수 있도록 ISO/IEC, ITEF 등의 국제 표준화를 추진 중

• 텔레매틱스 환경에서의 암호 키 관리 기술

- 미국 · 유럽 · 일본의 선진국에서는 자동차산업과 IT산업의 기술융합을 통해 자동차산업의 부가가치가 높아질 것을 인식하고, 이와 관련된 차량간, 차량과 도로변간 통신 시스템과 관련된 기술 개발을 추진하고 있음
  - 미국의 경우, 전국적인 차량 간, 차량과 도로변간 통신 시스템을 구축하여 안전성, 이동성, 시장이익 극대화를 위한 새로운 서비스의 실현을 목적으로 추진 중임
  - 유럽의 경우, 유럽위원회(EC) 주도아래 유럽의 ITS 기구인 ERTICO(Europe Road Transport Telematics Information Coordination Organization)가 주도적으로 참여하여 ITS를 추진하고 있음
  - 일본의 경우, 1995년 VICS(Vehicle Information & Communication System) 센터를 설립하고, 일본 전역(고속도로 및 국도, 주요도로)에서 실시간 교통정보를 수집 · 가공해 VICS 전용단말기를 통해 교통정보를 제공하고 있음(07년 3월 기

준 약 1,817만대 보급)

- 텔레매틱스 환경을 구축하기 위한 기반 기술에 대한 개발이 추진되고 있으나, 차량과 기기간의 무선통신 상에서 발생할 수 있는 도청, 정보 위·변조 등의 위협에 안전한 보안기술을 개발할 필요가 있음, 텔레매틱스와 관련된 실질적으로 암호 알고리즘 및 프로토콜을 연구하는 프로젝트에는 NOW(Network On Wheels)과 SEVECOM(SEcure VEhicular COMmunication)이 있음
  - ▫ NOW(Network On Wheels) : 2004년 6월부터 2008년 5월까지 진행된 프로젝트로 독일의 BMBF(Federal Ministry of Education and Research)에서 진행됨. 차량 간 통신 프로토콜, 보안이슈 등을 다룸
  - ▫ SEVECOM(SEcure VEhicular COMmunication) : 2006년 2월부터 진행 중인 프로젝트로 프랑스의 EPFL에서 진행 중임. 차량 간 통신을 이용한 서비스들의 보안을 향상시키는데 목적을 두고 있음. 다양한 공격을 방지하기 위한 인증 연구 및 아키텍처, 보안 메커니즘의 명세를 위한 연구를 진행 중임

• 암호알고리즘 이용 가이드라인

- 정보보호제품 및 시스템에 암호 알고리즘을 탑재 및 적용하는 경우, 알고리즘의 종류나 키 길이 등은 해당 시스템의 안전성 수준을 만족할 수 있도록 선택되어야 함. 이를 위해 현재 미국, 일본, 유럽 등에서는 암호 알고리즘 및 키 길이에 대한 가이드라인을 제시하고 있음.

〈국내외 권고 암호 알고리즘(2008년 기준)〉

분 류		NIST(미국)	CRYPTREC(일본)	ECRYPT(유럽)
대칭키 암호 알고리즘		AES 2TDEA 3TDEA	AES, 3TDEA Camellia,Cipherunicorn-A Cipherunicorn-E Hierocrypt-3 Hierocrypt-L1 MISTY1 SC2000	AES 2TDEA 3TDEA KASUMI Blowfish
해쉬함수		SHA-1 SHA-224/256 SHA-384/512	SHA-1 SHA-256 SHA-384/512 RIPEMD-160	SHA-1 SHA-224/256 SHA-384/512 RIPEMD-128/160 Whirlpool
공개키 암호 알고리즘	키 공유용	DH ECDH MQV ECMQV	DH ECDH PSEC-KEM	ACE-KEM PSEC-KEM RSA-KEM
	암 · 복호화용	RSA	RSAES-OAEP RSAES-PKCS1(v1.5)	RSAES-OAEP
	전자서명용	RSA DSA ECDSA	RSASSA-PSS RSASSA-PKCS1(v1.5) DSA ECDSA	RSASSA-PSS RSASSA-PKCS1(v1.5) DSA ECDSA

※ 출처 : KISA, 2008 암호 알고리즘 및 키길이 이용 안내서,2008

- NIST는 2007년 키관리 가이드라인(NIST Publication 800-57, Recommendation for Key Management-Part 1 : General)을 통해 암호 제품의 사용자 및 관리자가 설정해야 하는 적절한 암호 알고리즘과 알고리즘에 따라 선택할 수 있는 적절한 키 크기를 제공함.
- NIST는 정보를 보호하기 위한 보안 강도를 5가지(80, 112, 128, 192, 256 비트)로 나누고, NIST가 권고하는 알고리즘별

보안 강도, 키관리 가이드라인을 통해 제공하는 키 유형별 권장 유효기간을 제시하고 있으며, 알고리즘의 안전성 및 키 크기의 조절 등에 대해 주기적인 검토를 실시하고 있음

〈NIST가 제공하는 알고리즘별 보안 강도(2007년)〉

보안 비트	대칭 키 알고리즘	FFC (예, DSA, D-H)	IFC (예, RSA)	ECC (예, ECDSA)
80	2TDEA	공개키 크기: 1024, 개인키 크기 : 160	키 크기 : 1024	키 크기 : 160-223
112	3TDEA	공개키 크기: 2048, 개인키 크기 : 224	키 크기 : 2048	키 크기 : 224-255
128	AES-128	공개키 크기: 3072, 개인키 크기 : 256	키 크기 : 3072	키 크기 : 256-383
192	AES-192	공개키 크기: 7680, 개인키 크기 : 384	키 크기 : 7680	키 크기 : 384-511
256	AES-256	공개키 크기: 15360, 개인키 크기 : 512	키 크기 : 15360	키 크기 : 512+

※ 출처 : KISA, 2007 암호이용가이드라인, 2007

〈NIST의 키 유형별 권장 유효기간(2007년)〉

키유형	키 유효기간	
	발신자 암호 사용 기간 (OUP)	수신자 암호 사용기간
암호키	≤2년	≤2년
키 암호키	≤2년	≤2년
마스터 키	약1년	
암호키분배개인키(전송 방식)	≤2년	
암호키분배공개키(전송 방식)	1-2년	
암호키분배개인키(동의 방식)	1-2년	
암호키분배공개키(동의 방식)	1-2년	

※ 출처 : KISA, 2007 암호이용가이드라인, 2007

• 고성능 암호프로세서 설계 기술

- 국외의 경우, Wavesat사가 Elliptic Semiconductor사의 라이선스를 받아서, Shark 칩셋에 사용하기 위해 Elliptic사의 휴대형(802.16e-2005)과 고정(802.16-2004) WiMAX 제품을 목표로 하는 암호 프로세서 엔진을 선택함. 이외에도 wireless mesh node 등 데이터의 신속한 처리가 주요 이슈인 장치들의 개발에 암호 알고리즘의 연산 속도를 높이기 위해 암호 프로세서를 적용하는 예가 늘고 있음

- 브로드컴에서는 2005년 IPSec, SSL 프로토콜 프로세싱, 암호화 가속, 하드웨어 기반의 ID 관리, Single Chip solution 인증 기능 등을 통합한 보안 프로세서를 개발하였음, 또한, 소형의 센서 노드에 적합한 경량 알고리즘 개발의 일환으로 미국에서는 TinyECC 프로세서를 개발하여 센서 노드에 적용됨

- 컴퓨터 기술이 발달함에 따라, 사용자 단말기나 이동 기기들이 소형화되는 것이 추세이므로 소형 기기에서의 암호 알고리즘의 연산이 가능하도록 하기 위해 고성능 암호프로세서의 개발이 다양하게 진행되고 있음

나) 인증 기술

• USIM 등 모바일 환경에서의 인증서비스 모델 및 인증기술

- 지금까지 USIM의 최대 저장 메모리는 144KB로 다양한 어플리케이션을 올려 사용하기 어려운 상황임. 그러나 유럼의 이동통신사에서는 대용량 USIM이 1GB까지 개발이 되었으며 지속적으로 커지고 있는 상황임. 또한 SUN사에서는 USIM에서 사용되는 JavaCard 3.0을 2007년 9월에 공개하면서 동시에 여러 어플리케이션 사용이 가능하게 되었음.

- USIM은 보안 특성을 강조한 스마트카드를 기반으로 했기 때문에 접근, 개발, 사용이 상당히 제한적이었으나 EPSCP,

OMA를 중심으로 SCWS 표준화를 진행하여 2007년 10월에 v1.0을 배포하였음.

- 즉 해외에서는 이미 대용량 USIM을 기반으로 개인정보의 안전한 보관은 물론 다양한 서비스를 손쉽게 개발 확장할 수 있는 인프라를 이미 확보한 상황.

• **인터넷 전화 등에 이용 가능한 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 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

• **일회용패스워드(OTP) 인증 프레임워크**

- OTP 관련된 인증프레임워크의 개발은 주로 표준화 단체에서 개발 되고 있으며, VeriSign등이 참여하고 있는 OATH(Open AuTHentication) 단체에서 OTP를 포함한 PKI 공인인증서, 바이오 인증에 관련된 서비스를 통합하는 구조인 OATH 레퍼런스 아키텍처라는 범용인증 프레임워크를 개발하고 있음

- 또한 OTP에 대한 인증 프레임워크에 대한 개발이 국내 금융보안연구원에 의해 2008년부터 ITU-T의 안전한 응용서비스(Q7/SG17)분야에서 추진되고 있으며, 2009년 X.sap-3 최종 초안이 완료 예정임. 2010년 말에 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 dLT는 전자투표시스템을 구축하여 누가 누구를 선택했는지 알 수 없도록 설계하여야 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)으로 구분됨. 전세계적으로 30여개 국가가 전자투표를 실시하고 있으며, 투표소 전자투표(PSEV), 원격

인터넷 전자투표(REV) 방식을 적용하여 사용함

• 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 있다. Bioscrypt 기술인 경우 지문정보에 대한 입력 후 키를 생성. 하지만 Bioscrypt 기술은 사용자 인증 및 메시지 인증부분이 취약하기 때문에 이를 개선한 새로운 전자서명 키 생성 기법이 필요

- 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 방법. 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 방법

- 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 방식. 따라서 다양한 입력장치를 요구하게 됨

다) 권한관리 기술

• 기기 관리자 간의 권한 관리 응용 기술

- 해외에서도 현재 기기에 대한 보안에 있어서는 기존의 VPN과 SSL기반으로 기밀성(Confidentiality)을 확보한 후 전달되는 내용을 기반으로 한 인증을 고려하고 있어 암호와 인증이 분리된 상태. 즉 기존에 인터넷에 사용되던 것을 그대로 사용하려고 하고 있는데 현재 진행대로라면 인증을 강화한다고 하더라도 기존의 VPN과 SSL에서 제공하는 인증 기능을 채용할 가능성이 높아 보임. 결국 권한 관리의 필요성이 대두 되었을 때 암호/인증된 채널 위로 별개의 권한 정보를 전달하게 될 것인지 아니면 인증정보와 결부된 권한 정보를 사용하게 될 지에 대해서는 아직 두드러진 움직임은 없는 상황.

• 융복합 인증 서비스 모델

- 외국에서는 PKI 기반의 인증 서비스가 활발해짐에 따라, WiMAX나 Cable 셋톱박스 등의 기기 인증이나, WiFi 서비스 등에 인증서를 사용하는 인증 모델을 적용하고 있음. Verisign이나 CMLA 등은 이미 이와 관련한 서비스를 제공하고 있음.

• 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 기술

- 국내 블록 암호 알고리즘 관련 특허 출원은 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 데이터 및 민간한 개인 정보를 안전하게 보호하기 위한 정보보호 기술에 대한 관심 높아질 뿐만아니라 지능화된 첨단 기술 및 서비스들이 개발되어 있으므로, 이에 적합한 암호 알고리즘의 응용에 관려된 IPR 발굴 노력이 필요함

• 텔레메틱스 환경에서의 암호 키 관리 기술

- 텔레매틱스 환경에서의 2005년 말 차량용 블랙박스 관련 국내에서의 특허출원 건수는 135건이 특허 출원됨. 그 중 내국인이 93%로 대부분을 차지하고 있으며 설치 의무화로 필요성이 높아져 특허출원 증가 추세임
  - 특허청에 따르면 자동차와 휴대폰이 결합된 텔레매틱스 관련 기술의 특허출원이 2000년 이전 8건에 불과했었으나 2003년 31건으로 연평균 111%의 급격한 증가세를 보이며, 원격 차량진단 서비스 기술 41%, 항법 서비스 기술 11%, 휴대폰의 리모콘 기능 기술 16%, 도난 사고 예방 기술이 32%로 나타남

- RFID/USN, UWB 및 ZigBee 등의 센서 네트워크 기술을 이용하는 텔레매틱스 정보수집 및 제공 기술에 대한 특허 맵을 작성하고, 기존 텔레매틱스 서비스와 센서네트워크를 연계할 수 있는 비즈니스 모델 및 기술 개발 필요함, 또한, 개발 기술에 대한 시장 경쟁력 강화를 위한 특허추진이 이루어져야함

- 국외의 경우, 일본은 미쓰비시전기,FUJITSU, MITSUBISHI, HITACHI, TOSHIBA 등이 텔레매틱스 기반 기술에 대한 특허들을 추진하고 있으며, 미국에서는 소수의 기업보다는 산 · 학 · 연에서 특허를 추진하고 있음, 현재 보안에 대한 기술 특허 추진은 미흡한 실정임

• 암호알고리즘 이용 가이드라인

- 암호알고리즘 이용에 대한 가이드라인은 각 국가 기관별로 제시되고 있으며, 국가 정책의 일환으로 연구가 진행되고 있으나, 전체적인 암호알고리즘 이용 가이드라인에 대한 특허는 전무한 상황임

• 고성능 암호프로세서 설계 기술

- 고성능 암호프로세서 설계 기술의 경우 국내에서는 아직까지 대학에서 FPGA를 이용한 암호프로세서 개발 연구를 진행 중

이므로 IPR현황이 미흡한 실정이다. ETRI의 경우 보안기능을 갖춘 모바일용 SoC인 mTPM칩과 관련하여 60여건의 국내 및 국제특허를 출원 중임

▫ 우선적으로 알고리즘 별로 산재한 고성능 암호프로세서 설계 기술에 대하여 고성능 암호프로세서의 기준과 설계 가이드라인 분야에 대한 IPR확보가 가능할 것으로 판단됨. 또한, 고성능 암호프로세서의 검증 방안 분야에 대한 IPR 확보도 가능하며, 다양한 사용자 단말에 대한 고성능 암호프로세서의 적용 모델 및 인터페이스 분야에 대한 IPR 확보도 필요함

〈암호 기술 관련 주요 특허〉

출원번호	출원일자	등록번호	공고일자	출원인	발명의 명칭	진행상태
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
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 파일의 죠호 시스템	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 처리시스템 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	-	-	한국전자통신연구원	프라이버시를 보장하는 암호화와 복호화를 이용한 파일 공유 방법 및 시스템	공개
10-2007-0114402	2007.11.09	-	-	한국전자통신연구원	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	-	-	한국전자통신연구원	베타 전개를 이용한 순서 보존 수치 데이터 암호화 시스템 및 방법	공개
10-2007-0125472	2007.12.05	-	-	한국전자통신연구원	보안모듈 프로그램을 보호하기 위한 디지털 케이블 시스템 및 그 방법	공개

출원번호	출원일자	등록번호	공고일자	출원인	발명의 명칭	진행상태
10-2007-0127977	2007.12.11	-	-	한국전자통신연구원	RFID시스템에서 대칭키 암호화 기반 통신 데이터 보호 방법과 이를 수행하기 위한 리더 및 태그	공개
10-2007-0131205	2007.12.14	-	-	한국전자통신연구원	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

• USIM 등 모바일 환경에서의 인증서비스 모델 및 인증기술

- USIM과 관련해서는 통화 및 USIM 이용과 관련한 특허는 존재하나, USIM을 이용한 인증서비스 모델 및 인증기술과 관련한 특허는 현재 없으며, USIM 내에 인증서 탑재, 인증서 처리 SW의 탑재 등의 연구가 진행되고 있어 향후 특허가 등장할 것으로 예상됨

• 인터넷 전화 등에 이용 가능한 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 않으며 신규 IT서비스에 적용되는 디바이스별로 서비스 모델이 확정될 경우 각 디바이스별 또는 디바이스 인증 관련 기반 기술에 대한 특허 출원은 가능할 것으로 판단됨.

• 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 예상함

〈OTP 인증기술 관련 주요 특허〉

출원번호	출원일자	등록번호	공고일자	출원인	발명의 명칭	진행상태
OTP 인증 기술 및 응용						
10-2004-0044628	2004.06.16	10-0668387-0000	2007.01.12	(주)에스케이텔레콤	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 스마트 카드	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	OTP 를 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 동기방식 오티피 생성 및 인증시스템과 그 방법	등록
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			뱅크오브아메리카	일회용 비밀번호 신용/직불 카드	공개
10-2007-0112532	2007.11.06	10-0835260-0000	2008.06.10	(주)미래테크놀로지	메모리해킹 방지를 위한 인터넷뱅킹 제어방법과 이에 사용되는 오티피토큰장치	등록

• **일회용패스워드(OTP) 인증 프레임워크**

– 2008년 일회용 패스워드 인증 프레임워크에 대한 특허 출원상태이며 국제 특허 분야에 대한 가능성 확인 후 추진 필요

• **익명성을 보장하는 인증 기술**

– 프라이버시 침해 및 개인정보 유출 등의 사회문제가 발생하고 있어 이를 해결하기 위한 익명성 기반의 정보보호기술에 대한 핵심기술개발이 필요. 익명인증 및 익명권한관리 플랫폼 기술 등의 개발을 통해 익명인증 원천 IPR 확보가 가능할 것으로 보이며, 이를 통해 상용화 원천기술을 개발 가능

• **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 기대

〈인증 및 권한 기술 관련 특허〉

출원번호	출원일자	등록번호	공고일자	출원인	발명의 명칭	진행상태
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(SIM) 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

출원번호	출원일자	등록번호	공고일자	출원인	발명의 명칭	진행상태
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 간의 권한 관리 응용 기술

- 기기 관리자 간의 권한 관리 기술은 한가지 기술도 정의될 수 없기 때문에, 기기인증 등 각 분야에 별도의 특허가 출원 중에 있기 때문에 해당 원천기술에 대한 IPR확보는 어려울 것으로 판담됨.

• 융복합 인증 서비스 모델

- 융복합 인증 서비스 모델 분야는 기존의 기술을 이용하는 융복합 서비스이므로 원천 기술에 대한 IPR 확보는 어려운 실정임. 그러나 다양한 인증 서비스를 융합하는 응용 모델이나 융복합 기술에 대한 IPR 확보는 가능할 것으로 판단

• 사용자 권한관리를 위한 인증 기술 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/블록 암호알고리즘 기술

- 1999년 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 제정되었으며, 최근 ISO/IEC의 국제 표준화 기구에서 블록 암호 알고리즘으로 표준화를 추진 중임

- 2005년 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

• 응용서비스에서의 암호알고리즘 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 개발 될 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

• 텔레매틱스 환경에서의 암호 키 관리 기술

- 텔레매틱스 개발 기술 관련해서는 ETRI, 한국전산원 등이 텔레매틱스와 기술적 연관성이 높은 ITS, GIS, LBS 분야와 유기적인 연계하에 활용성이 높은 표준을 개발하고 표준화를 추진하고 있으나 대부분 텔레매틱스 시스템을 구축하기 위한 기반 기술에 대한 표준화가 이루어지고 있음

- 텔레매틱스 국내 표준화는 TTA, 텔레매틱스 표준화 포럼, 국내 LBS 표준화 포럼을 중신으로, 텔레매틱스 관련 표준안의 개발 및 심의에 전문성을 기하기 위한 기술 표준화 추진 중임

• 암호알고리즘 이용 가이드라인

- 방송통신위원회와 KISA에서 암호알고리즘의 이용활성화를 위해 "암호 이용 가이드라인", "암호 알고리즘 및 키 길이 이용 안내서"를 개발하여 발간하고 있으나 이에 대한 표준화는 진행되고 있지 않음

- 정보보호관리체계 인증제도에서는 관련 제도와 표준, 지침에서 명시하고 있는 암호통제 항목들은 암호정책 수립을 위한 기본 요구사항을 정의하고 있으나, 구체적인 암호정책 수립 기준이나, 방법, 암호기술 도입기준 등은 명시하고 있지 않음. 이와 관련하여 국내 보안 정책에 의거하여 암호알고리즘 이용 가이드라인에 표준화는 반드시 필요한 것으로 판단됨

• 고성능 암호프로세서 설계 기술

- 고성능 암호프로세서 설계 기술 관려해서는 아직까지 국내에서는 이에 대한 표준화 진행이 없는 상황이므로 최근 무선/이동 네트워크의 발달과 센서 노드 등의 소형 단말의 등장으로 다량의 암호연산을 처리하는 고성능 암호 프로세서 개발이 가속되고 있고 다양한 단말이 등장하고 있으므로 이에 대한 국내 표준 제정이 필요한 실정임

〈 암호 기술 관련 TTA 표준 현황 〉

분 야	표준번호	표준 제목	제정 년도
암호	TTA.KO-12.0001	부가형 전자서명 방식 표준 - 제2부 : 확인서 이용 전자서명 알고리즘	1998
	TTAS.KO-12.0011/R2	해쉬함수표준 - 제2부 : 해쉬함수알고리즘표준(HAS-160)	2005
	TTAS.KO-12.0004	128비트 블록암호알고리즘 표준	1999
	TTAS.IS-10181.4	개방시스템 상호접속-개방시스템에서의 보안 골격-제4부:부인방지	1999
	TTAS.KO-12.0001/R1	부가형 전자서명 방식 표준 - 제 2 부 : 인증서 기반 전자서명 알고리즘	2000
	TTAS.KO-12.0011/R2	해쉬함수표준-제2부 : 해쉬함수알고리즘표준(HAS-160)	2005
	TTAS.KO-12.0015	부가형 전자서명 방식 표준-제3부 : 타원곡선을 이용한 인증서 기반 전자서명 알고리즘	2001
	TTAS.IF-RFC2631	Diffie-Hellman 키합의 방식	2003
	TTAS.KO-12.0025	블록암호알고리즘 SEED의 운영모드	2003
	TTAS.IF-RFC3217	3-DES와 RC-2 키 싸기	2005
	TTAS.IF-RFC3394	AES 키 싸기 알고리즘	2005
	TTAS.KO-12.0004/R1	128비트 블록암호알고리즘 SEED	2005
	TTAS.KO-12.0011/R2	해쉬함수표준-제2부 : 해쉬함수알고리즘표준(HAS-160)	2005

분 야	표준번호	표준 제목	제정 년도
암호	TTAS.IF-RFC3370	암호 메시지 규격에서 사용되는 알고리즘	2005
	TTAS.KO-06.0102	텔레매틱스 단말-TSP 서버간 서비스 프로토콜 Stage 1: 요구기능	2005
	TTAS.KO-06.0117	텔레매틱스 단말 소프트웨어 플랫폼Stage2 : 요구기능	2006
	TTAS.KO-12.0039	해쉬함수 알고리즘 FORK-256	2006
	TTAS.KO-12.0040	64비트 블록암호알고리즘 HIGHT	2006
	TTAS.IF-RFC3369	암호 메시지 규격	2006
	TTAS.KO-12.0041	스트림암호알고리즘 TSC-4	2006
	TTAR-12.0001	MD5 메시지-다이제스트 알고리즘	2006
	TTAS.IF-RFC4196	IPsec을 위한 SEED 암호알고리즘	2006
	TTAS.IF-RFC4162	TLS를 위한 SEED 암호알고리즘	2006
	TTAS.IF-RFC4010	CMS를 위한 추가암호 알고리즘 : Part1 SEED	2006
	TTAS.IF-RFC3565	CMS를 위한 추가암호 알고리즘 : Part2 AES	2006
	TTAS.KO-12.0040/R1	64비트 블록암호알고리즘 HIGHT	2009 (예정)
	2009-073	한국형 암호정책 수립 기준	2009 (예정)
	2009-074	안전한 해쉬함수 이용 가이드라인	2009 (예정)

〈암호 기술 관련 KS 표준 현황〉

분 야	표준번호	표준 제목	제정 년도
암호	KSX6513-5	금융 거래 카드- 집적 회로 카드를 사용하는 금융 거래 시스템의 보안 - 제5부 : 알고리즘의 사용	2002
	KSX6315-1	금융-메시지 인증을 위한 승인된 알고리즘 - 제1부 : DEA 알고리즘	2002
	KSXISOIEC9979	정보기술-보안기술-암호 알고리즘 등록절차	2003
	KSXISOIEC13888-1	정보기술-보안기술-부인 봉쇄-제1부:일반	2003
	KSXISOIEC11770-1	정보기술- 보안기술-키 관리-제1부:기본 틀	2003
	KSXISOIEC13888-2	정보기술-보안기술-부인봉쇄-제2부: 대칭 암호기법을 이용한 메커니즘	2003
	KSXISOIEC15946-3	정보기술 - 보안기술 - 타원형 곡선에 기반한 암호기술 -제3부 : 키 설정	2003
	KSXISOIEC9797-2	정보기술-보안기술-메시지 인증 코드 -제2부 : 전용 해쉬 함수를 이용한 메커니즘	2003
	KSXISOIEC15946-1	정보기술-보안기술-타원형 곡선에 기반한 암호기술-제1부:일반	2003
	KSX6922-2	지불 시스템을 위한 IC 카드 규격 - 제2부 : 보안 및 키 관리	2003
	KSX1208-2	정보기술-보안기술-N비트 블록암호 알고리즘을 이용하는 해쉬함수	2003
	KSX1205	정보기술-보안기술- n비트 블럭암호 알고리즘의 운영모드	2003
	KSX1211-2	정보 보안의 부인 봉쇄 - 제2부 : 대칭 암호 기법을 이용한 메커니즘	2004
	KSX1209	정보 보안의 암호 알고리즘 등록 절차	2004
	KSX1210-1	정보 보안의 키 관리 - 제1부 : 기본 틀	2004
	KSX1206	블럭 암호 알고리즘을 사용한 데이터 무결성 기법	2004
	KSX1204-3	정보 보호 기법-실체 인증-제3부:디지털 서명 기법을 이용한 메커니즘	2004
	KSX1204-1	보안기술의 실체인증 기법 - 제1부 일반모델	2004
	KSX1213	128비트 블록 암호 알고리즘 ARIA	2004
	KSXISOIEC10118-2	정보기술-보안기술-해시함수-제2부 : n-bit block cipher를 사용한 해시 함수	2005
	KSX6923-3	비접촉식 전자화폐 단말기용 지불SAM 규격 제3부 : 지불SAM의 암호 알고리즘	2006
	KSX6924-3	선불IC카드 - KS X 6923 대응 사용자 카드 - 제3부 : 암호 알고리즘	2006
	KSXISOIEC9797-1	메시지 인증 코드- 제1부 : 블록암호를 이용한 메커니즘	2006
	KSXISOIEC9797-1	메시지인증코드-제1부:블록암호를이용한메커니즘	2006
	KSXISOIEC10118-4:2001	정보기술-보안기술-해쉬함수 - 제4부 : 법 연산을 이용하는 해쉬함수	2006
	KSXISO8731-2_2001	금융- 메시지 인증을 위한 알고리즘-제2부 : 메시지인증 알고리즘	2006
	KSXISOIEC11770-2	정보기술 - 보안기술 - 키 관리 - 제2부: 대칭 기법을 이용한 메커니즘	2006

분 야	표준번호	표준 제목	제정 년도
암호	KSXISOIEC9798-4	정보기술 - 보안기술 - 실체인증 - 제4부: 암호학적 확인 함수를 이용한 메커니즘	2006
	KSXISOIEC9798-2	정보기술 - 보안기술 - 실체인증 - 제2부: 대칭형 암호 알고리즘을 이용한 메커니즘	2006
	KSXISOIEC18033-4	정보 기술 - 보안 기술 - 암호 알고리즘 - 제4부 : 스트림 암호	2006
	KSXISOIEC18033-3	정보 기술 - 보안 기술 - 암호 알고리즘 - 제3부 : 블록 암호	2006
	KSXISOIEC18033-1	정보 기술 - 보안 기술 - 암호 알고리즘 - 제1부 : 일반	2006
	KSXISOIEC10118-3:2001	정보기술-보안기술-해쉬함수-제3부: 전용 해쉬 함수	2006
	KSX1208-1	정보기술 - 보안기술 - 해시함수 - 제1부 : 일반	2006

나) 인증 기술

• USIM 등 모바일 환경에서의 인증서비스 모델 및 인증기술

- 모바일 기기가 개인의 필수 휴대품으로 자리잡게 되면서 개인의 신분증, 개인정보 등과 함께 사용자 인증수단으로써 함께 사용됨. 하지만 모바일 기기 자체가 인증이 되지 못하고 사용자가 입력한 정보가 사용자의 신원을 인증하고 있는 상황.

- 모바일 기기에서의 인증기술로 모바일 기기에 공인인증서를 탑재하여 사용 또는 모바일 OTP를 사용하고 있는 상황. 공인인증서의 경우 모바일 기기의 일반 파일시스템에 저장되어 이중 암호화 등 별도의 보안을 고려하여야 하며, 모바일 OTP의 경우도 SEED 값이 파일시스템에 암호화 저장되어 있어 마찬가지로 별도의 보안을 고려하여야 하는 상황.

- 모바일 기기의 USIM에 공인인증서를 저장하는 방식으로 PKCS#11, PKCS#15, 금융IC카드, SCWS(Smartcard Webserver) 등이 고려되고 있으며, 아직 이에 대한 표준화는 진행 중. 대용량 USIM의 개발과 함께 SCWS의 출현으로 USIM의 SCWS의 HTTP 통신에 기반을 둔 인증기술에 대한 표준 또한 고려되어야 함.

• 인터넷 전화 등에 이용 가능한 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 활성화될 것으로 전망

• 일회용패스워드(OTP) 인증 기술 및 응용

- 현재 TTA PG 501에서 OTP 키 컨테이너, OTP 암호키 관리 보안요구사항, OTP 인증 서비스를 위한 보증 레벨과 응용 가이드라인에 관한 표준을 추진하고 있으며 올해 제정 예정임

구 분	과제번호	문서이름	상 태	과제 제안일
OTP	2008-1044	일회용패스워드(OTP) 암호키 관리 보안요구사항	표준초안	2008.9.
	2009-826	일회용패스워드(OTP) 키컨테이너표준초안	2009.6.	
	2009-845	일회용패스워드(OTP) 인증 서비스를 위한 보증레벨과 응용 가이드라인	표준초안	2009.6.
	2009-827	일회용패스워드(OTP) 인증 서비스 프레임워크	표준초안	2009.6

• 일회용패스워드(OTP) 인증 프레임워크

- 2009년 TTA의 정보보호기반 프로젝트그룹(PG501)에서 표준화를 추진하고 있으며 올해 제정 예정임

• 익명성을 보장하는 인증 기술

- 2008년 TTA의 정보보호기반 프로젝트그룹(PG501)에서 표준화를 추진하여 2009년 말 "추적 가능한 익명 인증서 이용 기술"이 표준으로 채택됨. 해당 표준은 추적 가능한 익명인증서 이용기술을 다루고 있으며, 추적 가능성을 위해 등록대행기관과 인증기관의 역할을 분리하여 익명성을 보장하면서 추적 가능한 익명인증서 이용기술을 정의함.

• 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 기술 관련 TTA 표준 현황 〉

분 야	표준번호	표준 제목	제정 년도
암호	TTAS.KO-12.0012	전자서명 인증서 프로파일	2000
	TTAS.KO-12.0018	무선 인증서 요청형식 프로토콜	2002
	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(개정)	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-12.0012/R1	전자서명 인증서 프로파일(개정)	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-12.0013/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
	TTAK.IT-X1088	바이오 인식 정보에 기반한 전자서명 키생성 프레임워크	2008

〈 인증 기술 관련 KS 표준 현황 〉

분 야	표준번호	표준 제목	제정 년도
암호	KSXISOIEC15945	정보기술-보안기법-전자서명의 응용을 지원하기 위한 TTP서비스 규격	2002
	KSXISOIEC9594-8	정보 기술 - 개방형시스템간 상호접속-디렉토리: 공개키와 속성인증 프레임워크	2002
	KSXISOIEC9798-3	정보기술-보안기술-실체인증-제3부:디지털 서명기법을 이용한 메커니즘	2003
	KSXISOIEC9798-1	정보기술-보안기술-실체인증-제1부:일반	2003
	KSXISOIEC15946-2	정보기술 - 보안기술 - 타원형 곡선에 기반한 암호기술 -제2부:전자서명	2003
	KSXISOIEC15946-3	정보기술 - 보안기술 - 타원형 곡선에 기반한 암호기술 -제3부 : 키 설정	2003
	KSX1207	정보기술-보안기술-메세지 복원형 디지털 서명 방식	2003
	KSX1204-3	정보 보호 기법-실체 인증-제3부:디지털 서명 기법을 이용한 메커니즘	2004
	KSX1204-1	보안기술의 실체인증 기법 - 제1부 일반모델	2004

분 야	표준번호	표준 제목	제정 년도
암호	KSX6033	확장가능한 마크업 언어 전자서명 구문과 처리	2005
	KSXISOIEC9796-2	정보기술-보안기술-메시지 복원형 디지털 서명 기법- 제2부 : 정수 인수분해(Integer factorization) 기반 메커니즘	2005
	KSXISOIEC15946-4	정보기술-보안기법-타원 곡선 암호화 기법-제4부: 메시지 복원을 실현하는 전자 서명	2005
	KSXISOIEC9796-2	정보기술-보안기술-메시지복원형디지털서명기법- 제2부:정수인수분해(Integerfactorization)기반메커니즘	2005
	KSXISOIEC14888-1:2001	정보기술-보안기술-부가형 디지털 서명 - 제1부 : 일반	2006
	KSXISOIEC9796-3	메시지 복원형 디지털 서명 기법-제3부:이산대수기반 메커니즘	2006
	KSXISOIEC14888-3:2001	정보기술-보안기술-부가형 디지털 서명 - 제3부 : 인증서 기반 매커니즘	2006
	KSXISOIEC14888-2:2001	정보기술-보안기술-부가형 디지털 서명 - 제2부 : 신분 기반 매커니즘	2006
	KSXISOIEC9798-4	정보기술 - 보안기술 - 실체인증 - 제4부: 암호학적 확인 함수를 이용한 메커니즘	2006
	KSXISOIEC9798-5	정보기술-보안기술-실체인증-제5부:영지식 기법을 이용한 메커니즘	2006
	KSXISOIEC9798-2	정보기술 - 보안기술 - 실체인증 - 제2부: 대칭형 암호 알고리즘을 이용한 메커니즘	2006

다) 권한관리 기술

• 기기 관리자 간의 권한 관리 응용 기술

- 현재까지 기기 관리자간의 권한 관리 응용 관련 기술 및 표준화 개발은 극히 일부에서 진행되고 있으며, 기기인증 관련한 표준화는 최근 기기인증 기술개발과 더불어 제안될 예정임.

- 또한, 향후 유비쿼터스 환경 도래와 더불어 기기 관리자간 권한관리 응용 기술에 대한 기술 및 표준화 개발은 점차 활성화 될 것으로 기대됨

• 융복합 인증 서비스 모델

- 현재까지 국내 표준화는 융복합 인증 서비스 모델 보다는 각 인증 서비스 모델 별로 진행되어 왔다. 하지만, 최근 융복합 서비스의 등장과 함께 개별적 인증에서 다양한 인증 수단들이 융합되는 인증 서비스 요구가 증가되고 있음

- 현재 관련 분야 국내 표준화는 아직 전무한 상태이며 금년도를 시발점으로 하여 각 인증서비스가 좀 더 숙성된 시점부터 본격적으로 표준화 작업이 활성화 될 것으로 예상됨

• 사용자 권한관리를 위한 인증 기술 및 응용

- 국내의 경우 TTA에서 PMI에 대한 표준이 2007년 제정되었으며(TTA, TTAS.IT-X509/R4, 2007, 디렉토리 : 공개키와 속성 인증서에 대한 프레임워크 표준) 2008년에는 속성인증 응용서비스 모델 관련 TTA 표준이 제정(TTA, TTAK.KO-12.0069, 2008, 속성인증을 이용한 응용 서비스 모델)

분 야	표준번호	표준 제목	제정 년도	비고
권한관리	TTAS.IT-X509/R4	디렉토리 : 공개키와 속성 인증서에 대한 프레임워크 표준	2007	
	TTAK.KO-12.0069	속성인증을 이용한 응용서비스 모델	2008	

2.3.2. 국외 표준화 현황 및 전망

가) 암호기술

• 유비쿼터스 환경에 적합한 경량 암호알고리즘/블록 암호알고리즘 기술

- 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

• 응용서비스에서의 암호알고리즘 활용 방법

- 국제 표준화 기구 IETF, IEEE 등 에서 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. 그 이외의 국내에서 추진중인 암호 알고리즘 및 암호 알고리즘 사용 표준화 현황은 아래와 같음

〈암호기술 표준화 현황〉

구 분	표준번호	문서이름	표준상태	제정년도
ISO/IEC	18033-3	Information technology- Security-techniques-Encryption algorithms-Part3:Block Cipher	표준채택	2005
IETF	RFC 4009(RFC 4269)	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
ISO/IEC	-	Relayed MultiCast Protocol-Part2: Amedment 1, Security Extensions (RMCP-2/Draft Amd,1)	표준채택 예정	2006
IETF	RFC 4615	The Advanced Encryption Standard-Cipher-based Message Authentication Code-Pseudo-Random Function-128 (AES-CMAC-PRF-128) Algorithm for the Internet Key Exchange Protocol (IKE)	표준채택	2006
IETF	-	Low Power Encryption	과제채택	2007
ITU-T	-	Security framework for Ubiquitous Sensor Network(X.usnsec-1)	과제채택	2007

구 분	표준번호	문서이름	표준상태	제정년도
ITU-T	-	Proposal for new work item on a framework for countering cyber attacks in VoIP service	과제채택	2008.
IETF	-	The SEED Cipher Algorithm and Its Use with the Secure Real-time Transport Protocol(SRTP-SEED)	표준채택 예정	2009
ITU-T	-	Founctional requirements and architecutre for IPTV security aspects	표준채택 예정	2009
ITU-T	-	Requirements and mechanism for secure transcodable scheme of IPTV	표준채택 예정	2010
ITU-T	-	Key managements framework for secure IPTV communication	표준채택 예정	2010
ITU-T	-	Security requirements and framework in multicast communication	표준채택 예정	2010
ITU-T	X.1112	Device certificate profile for the home network	표준제정	2007
ITU-T	-	Authorization framework for home network(X.homesec-4)	표준제정검토중	2008

• 텔레매틱스 환경에서의 암호 키 관리 기술

- 텔레매틱스 기술 표준화 관련하여, 미국, 영국, 일본, 호주 등 선진국에서는 이미 오래 전부터 국가 차원의 공간 정보 유통 활성화 기반기술 및 표준 개발을 꾸준히 추진하고 있으며, 국제 표준화기구에도 적극적인 참여를 하고 있으므로 텔레매틱스를 위한 기반 마련과 활용 체계가 수립되고 있음
  - ▫ ISO TC204의 경우 현재 12개 WG에서 기술 분야별로 표준화 활동을 진행하고 있으며, 일본의 자동차기술회, 미국의 SAE(Society Automotive Engineers), 유럽의 CEN(유럽표준화위원회) 등의 국제기구 이외의 국가, 지역별, 민간단체및 업체 표준화 기구에서 표준화 추진하고 있음
  - ▫ 텔레매틱스의 차내망 표준으로는 CAN, LIN, FlexRay, MOST, 1394 등 ISO, SAE에서 개발된 다양한 프로토콜이 존재함. 물리적 포트로는 미국 배출가스 규제 표준인 OBD-II 포트(ISO9141)가 일반적임. 진단 프로토콜로는 ISO에서 KWP2000(ISO14230)이라는 표준을 개발하였으며 UDS등 기능을 확장 보강한 표준을 추가로 개발 중임. 데이터 포맷으로는 ISO에서 ODX라는 표준을 개발 중임
  - ▫ ISO TC204에서는 통신영역 확대(최대 1000m), 통신영역간 핸드오버 및 차량 고속 이동성, 차량간 Ad-hoc 네트워크 지원 기술 및 프로토콜을 포함하는 근거리 통신영역 내에서 차량과 기지국간 무선접속을 통해 다양한 서비스를 제공할 수 있는 응용 서비스 계층 프로토콜 표준화를 추진하고 있음
  - ▫ 통신영역간 핸드오버, 차량 고속 이동성 및 차량간 Ad-hoc 네트워크 기능 지원을 위하여 기존의 802.11 PHY/MAC 개선 기술 표준화 작업은 WAVE라는 명칭아래 IEEE802.11p가 주도
  - ▫ 인터넷 표준기관인 IETF의 GeoPriv(Geographic Location/Privacy) WG에서는 에이전트를 통해 위치 정보들의 표현 또는 Release하기 위한 권한을 제한하거나, 위치정보를 전송하기 위해 필요한 권한, 무결성, Privacy 요구사항들을 평가하기 위한 표준을 제정하고 있음

• 암호알고리즘 이용 가이드라인

- 국제 표준화 기구인 ISO/IEC JTC 1/SC27에서는 블록 암호 알고리즘, 전자서명 알고리즘, 공개키 암호 알고리즘, 해쉬 함수 등 수십 종의 암호 알고리즘을 표준화하고 있음. 국외의 경우, 미국의 NIST, 일본의 CRYPTREC, 유럽의 ECRYPT 등의 암호연구기관에서는 권고하는 암호알고리즘에 대한 지침을 배포하고 있음
- 향후 정보보호제품의 수요 증가와 각 국가별로 시행하는 정보보호제품 도입 기준 및 암호 알고리즘 이용 정책에 의해 암호 알고리즘 이용 가이드라인의 표준화가 필요할 것으로 판단됨

• 고성능 암호프로세서 설계 기술

- 차세대 모바일 단말 자체의 보안성 강화를 위해 TCG(Trusted Computing Group)에서 국제 표준화 진행을 하고 있으며,

MPWG(Mobile Phone Working Group)에서 2007년 6월 최초 표준 스펙 개발 및 공개하였음

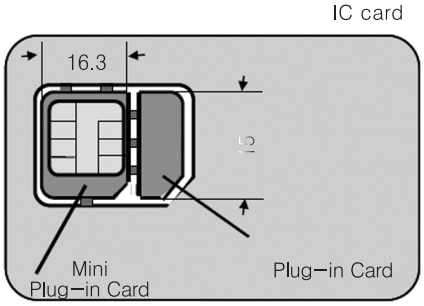
▫ Trusted Platform Module(TPM) Working Group은 산업체 표준으로서 TPM 표준을 제정하는 것을 목표로 하여 TPM 구조의 구현을 정의하고 공개키 암호, 암호 알고리즘과 프로토콜을 포함한 암호 기술 뿐 아니라 암호 모듈의 설계 및 사용과 관련하여 보안에 대한 전반적인 내용을 포함함

- ETRI에서는 보안기능을 갖춘 모바일용 SoC인 mTPM칩 기술과 관련하여 현재 국내 표준 2건을 기고하여 채택되었고, 국제 표준을 4건 기고하였으며 이를 통한 국제표준화 작업이 진행 중임

나) 인증기술

• USIM 등 모바일 환경에서의 인증서비스 모델 및 인증기술

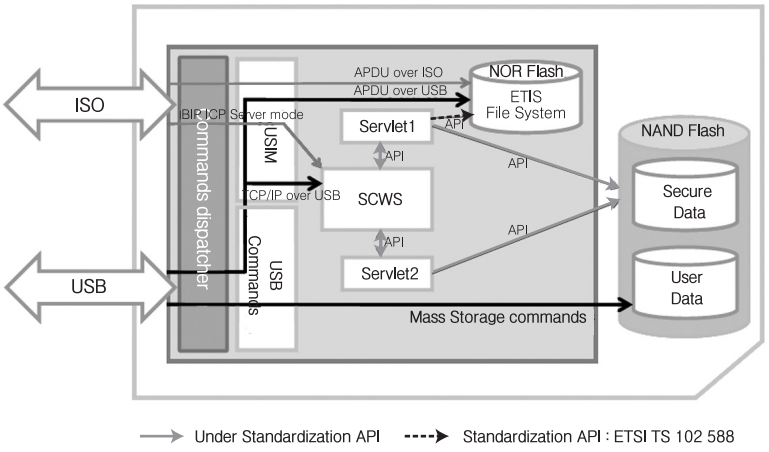
- 휴대 단말이 다양한 크기와 두께로 출시되면서 이를 효과적으로 지원하기 위해 USIM의 물리적 형상을 소형화 하는 작업이 이루어 졌으며 이는 ETSI SCP에서 제정됨. 이를 통하여 ISO 7816-1에 정의된 ID-1타입과 Plug-in타입에 모두 호환되며 52%가량 사이즈를 줄임.



〈Mini UICC 형상〉

- USIM의 고속통신 기술은 ETSI SCP에서 2006년 11월 IC-USB를 표준으로 선택하였고 2007년 5월 최종 승인되어, 2주후 3GPP에서도 IC-USB 프로토콜을 승인함.

- SCWS 표준화는 OMA와 ETSI SCP에서 나누어 진행하고 있는데 OMA에서는 SCWS와 단말, 관리 서버 등 외부 기기와의 통신 프로토콜 및 HTTP 프로파일링 등을 제정하여 2007년 10월 v1.0을 배포함. ETSI SCP에서는 USIM 내부에 SCWS 기능을 구현하기 위한 API 표준을 제정함.



〈SCWS API 구조〉

- 또한 USIM은 내부 COS로서 자바 카드를 선택하고 있는데 SUN사는 다양한 서비스를 원활하게 지원하기 위하여 자바 카드 3.0 플랫폼을 2007년 9월 공개함. 이와 별도로 폰에서 사용할 수 있는 인터페이스인 PKCS#11은 RSA Laboratories에서 현재 v2.20이 진행되고 있음. USIM 내부를 접근하는 방식을 SCWS이 아닌 PKCS#15으로 할 경우에는 RSA Laboratories에서 현재 v1.1까지 나와 있는 상황이며 ISO/IEC 7816-15로 표준화 되어 있음.

• 인터넷 전화 등에 이용 가능한 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 존재. 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 기기 인증서 및 CRL 발급에 대한 규격을 정의.

- 2005년 ISO에서 홈네트워크 보안요구사항과 댁내 및 댁외 보안에 대한 표준 제정. ITU-T SG17에서는 2004년부터 홈네트워크 디바이스 인증서 프로파일, 홈네트워크 서비스에서의 사용자인증 프레임워크 등에 대해 표준화 제정 추진.

- 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 필요하다. 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 한다. 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 한다. 미디어 암호 프로토콜인 SRTP와 키 관리 프로토콜인 MIKEY에서는 메시지 무결성을 보장하기 위해 HMAC-SHA1 메커니즘을 준용함

구 분	문서명	문서이름	상태	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.

• 일회용패스워드(OTP) 인증 기술 및 응용

- 1995년에 IETF에 일회용패스워드 인증 워킹그룹이 설립되어 S/Key 기술을 일회용패스워드 시스템 표준(RFC2289)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(RFC4226)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, RSA

사에서 제안한 Kerberos에 일회용패스워드를 적용한 프로토콜과 TLS에 일회용패스워드를 적용한 프로토콜 등이 현재 IETF 인터넷드래프트 버전으로 있음

구 분	문서명	문서이름	상태	발표월일
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
	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	표준초안	2009

• 일회용패스워드(OTP) 인증 프레임워크

- ITU-T 개방형통신기술 보안 (SG17)연구 그룹의 안전한 응용 프로토콜(Q7) 표준 프로젝트에서 일회용패스워드를 위한 관리 프레임워크(X.sap-3) 표준이 추진중이며 올해 최종 초안 완성을 목표로 하고 있음

• 익명성을 보장하는 인증 기술

- 익명 인증기술과 관련하여 추적 가능한 익명인증서가 2009년 8월 IETF 표준 "Traceable Anonymous Certificate" (RFC5636)으로 제정됨. 본 표준은 인증서와 실제 사용자간의 연결을 유지하면서, 익명 인증서를 이용하는 이용자에 대해 프라이버시를 제공하기 위한 실질적인 아키텍처와 프로토콜을 정의함.

• 바이오정보를 이용한 전자서명 기술

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

〈인증기술에 대한 국제표준화 동향〉

구 분	문서명	문서이름	상태	발표월일
암호 기술	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
인증 기술	RFC 2459/3280/5280	Internet X.509 Public Key Infrastructure Certificate and CRL Profile	표준	1999.1./ 2002.4/2008.5
	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
	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.
	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.

구 분	문서명	문서이름	상태	발표월일
인증 기술	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.
바이오인식 관련 인증 기술	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 간의 권한 관리 응용 기술

- 대부분 기기별, 서비스별로 관련 표준화가 진행되고 있으며, OpenCable, EPCGlobal, WiMax, CMLA 등 각자 필요한 보안 스펙을 정의하고 있음. OpenCable의 경우 공개키 기반 인증서를 이용하여 정당한 기기에 대한 인증 및 과금 등을 처리하고 있음.

- VeriSign에서는 케이블 모뎀이나 셋톱박스, 디지털 케이블이 장착된 TV, WiMAX 규격의 가입자 단말기 같은 종류의 하드웨어 디바이스내에 X.509 인증서를 탑재하는 서비스를 제공하여 기기 인증에 PKI를 적용하는 서비스를 제공 중

- CMLA(Content Management Licensing Administrator)에서는 새로운 디바이스와 서비스 사이의 상호연동성을 제공하기 위하여 암호화된 키와 인증서를 제공하는 방법을 제시.

- 국제표준화기구 IEEE는 2009년 6월부터 스마트 전력망의 표준을 정의하는 노력을 본격화 할 것으로 전망. 미국 Santa Clara에서 열리는 인텔 주최 모임에서 IEEE는 스마트 그리드 표준화를 주도할 예정임. IEEE 2030 그룹은 컴퓨터, 통신 전력 공학자를 모아 스마트 그리드 상호운용성을 보장할 표준 초안을 만들 계획임.

- NAESB (North American Energy Standards Board: 북미에너지표준화기구)는 FERC(Federal Energy Regulatory Commission: 연방에너지규제위원회)와 함께 도매 전력시장에서 수요반응 표준화를 정립하고자 함. 반면 로렌스 버클리 국립연구소의 수요반응 연구센터는 건물의 수요반응 표준을 개발 중임.

• 융복합 인증 서비스 모델

- 인증 서비스에 대한 표준화는 대체로 IETF와 ITU 등에서 이루어져왔으며 이와 별도로, IEEE, WiMax Forum 등에서 EAP를 개선하거나 수정하여 무선 네트워크 특성에 맞는 인증 모델을 개발하여 적용하고 있음. IETF의 pana나 oauth에서는 네트워크의 접속에 대한 인증과 사용자 권한에 대한 인증과 관련하여 표준화를 진행 중임. 향후 다양한 무선 네트워크 서비스가 사용자에게 제공되어 사용이 활발해지게 되면 통합 인증 서비스 모델이 개발될 것으로 판단됨.

작업반	관련내용
oauth	Open Authentication Protocol
pana	Protocol for carrying Authentication for Network Access

• 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 제정함.

번 호	표준명	제정년도
ISO 9594-8/ITU-T Rec. X.509	The Directory: Public-key and attribute certificate frameworks	2005
IETF, RFC 3281	An Internet Attribute Certificate Profile for Authorization	2002
IETF, RFC 4476	Attribute Certificate (AC) Policies Extension	2006

2.4. 표준화 대상항목별 현황 요약

구 분		암호기술		
표준화 대상항목		유비쿼터스 환경에 적합한 경량 암호알고리즘	블록 암호알고리즘 기술	응용서비스에서의 암호 알고리즘 활용 방법
시장현황 및 전망	국 내	- 국내외 SEED, 3DES, AES 등 정보보호 제품에 탑재된 정보보호 제품이 출시 - 민간 분야의 전자거래, 금융, 무선통신 보안 제품에 SEED 탑재 - 정부 및 공공기관의 보안 통신 제품에 ARIA 탑재		
	국 외	- 인증 기술, 시스템, 네트워크 정보보호 기술, 응용 정보보호 기술은 모두 기반 기술인 암호 기술에 의존하고 있음 - 독자적인 암호 모듈 제품이 상용화되고 있고, 시장을 형성하고 있음		
기술개발 현황 및 전망	국 내	- 대칭키 암호 분야는 민간 표준으로 사용하기 위한 블록 암호 SEED 개발하였고, 2004년 ARIA 알고리즘이 개발되었음 - 2005년 64비트 블록 암호알고리즘으로 HIGHT 개발 - 미국, 영국, 프랑스, 캐나다, 호주 등에서 암호키관리 장비(HSM) 및 스마트카드 등에 SEED가 탑재되어 상용화됨 - ETRI, 삼성전자 등에서 900MHz RFID 태그/리더칩 개발하였으나 보안기술이 탑재되어있지 않음 - AES가 탑재된 수동형 RFID 태그칩을 ETRI에서 설계/구현 완료		
	국 외	- 대칭키 암호 알고리즘은 1970년대 중반 미 연방 표준 암호 알고리즘으로 DES가 채택된 이후로 IDEA, MISTY 등을 비롯한 다양한 블록 암호가 개발되었음. 현재 대칭키 암호 분야의 연구는 AES의 실용화에 대비한 다양한 안전성 분석, 운영 모드, MAC 등을 비롯한 블록 암호 응용 기술 분야에서 연구가 진행됨 - IETF의 경우 ECC 알고리즘을 포함한 다양한 암호 알고리즘에 대한 확인자를 개발하고 있고, 관련 보안 프로토콜의 기반 알고리즘으로 활용하고 있음 - ITU-T의 경우, 접근제어 프레임워크, 부인방지 프레임워크, 키관리 프레임워크 등의 다양한 프레임워크를 개발완료하였음 - AES, 가변 길이 해쉬 알고리즘이 개발되는 등 핵심 암호 알고리즘 설계 및 암호 분석 분야에 대한 연구가 활발히 추진되고 있음 - Crypto2004에서 MD5 와 SHA1 에 대한 암호 해독 가능성을 제시함으로써, 이 분야에 대한 해독과 이를 회피할 수 있는 새로운 해쉬 알고리즘의 개발이 활발히 수행될 예정이고, 2005년과 2006년 두 차례에 걸쳐 NIST 주관 해쉬 워크샵이 개최되어 2011년까지 해쉬 알고리즘을 개발할 목적으로 공개 공모과정을 2007년부터 시작하는 것을 골자로 하는 로드맵이 확정되어 있음 - 미국의 Savi, 퀄컴 등에서 능동형 RFID 태그 보안 기술이 개발되어 컨테이너 보안 시스템을 주도하고 있으나, 실질적인 유비쿼터스 환경을 고려한 경량 암호를 개발하여 적용한 것은 아님 - USN 환경에서는 TinyOS기반의 TinySec 및 TinyECC에 대한 연구를 진행하고 있으며, 저가의 USN 센서 노드에서 구현 가능하도록 경량 구현 설계를 추진하고 있음		
기술 개발 수준	국 내	시제품/프로토타입	구현	시제품/프로토타입
	국 외	구현	구현	시제품/프로토타입
	기술격차	1.3년		
	관련제품	- 암호 모듈, 암호 칩, 암호 알고리즘을 구현한 각종 암호 API		
IPR 보유현황	국 내	- SEED, ARIA, HIGHT 등의 블록 암호 알고리즘		
	국 외	- 공개키, 대칭키, 전자서명, 키분배 알고리즘, ECC 알고리즘		
IPR확보 가능분야		- 방송, 통신, 등 융복합 환경, 유비쿼터스 환경 등을 고려하여 신규 IT 서비스 및 시스템을 고려한 암호 알고리즘의 개발이 필요하므로 이에 적합한 암호기술에 대한 IPR 확보는 매우 중요한 과제임 - 안전한 시스템 구축을 위한 각종 상용화를 위한 요소기술에서 IPR 확보가 가능함		
IPR확보 가능성		- 보통		
표준화 현황 및 전망		- 현재 일본은 Cryptrec 사업을 통하여 전자정부에 필요한 암호 알고리즘을 표준화 하였고, 유럽의 경우도 NISSIE 사업을 통하여 암호알고리즘 표준화 사업을 수행하고 있는 바, 각 나라는 개별적으로 암호 알고리즘에 대한 표준을 제정할 것으로 예측됨 - 우리나라의 경우도 암호 모듈 평가에 대비한 안전성이 검증된 암호 알고리즘을 선정하고, 이를 탑재한 암호 모듈 평가를 2005년부터 시행하고, 이를 위한 프레임워크 및 관련 기준이 마련됨 - 국외 표준화 단체의 경우, 여러 알고리즘을 시스템 특성에 따라서 선택적으로 협상을 통하여 사용할 수 있도록 하는 암호 알고리즘 에 대한 표준화를 진행 중 에 있음 - 우리나라가 제안한 SEED가 2005년에 ISO/IEC JTC1 및 IETF에서 표준으로 선정되었음 - 저전력 암호 알고리즘 HIGHT이 TTA 표준으로 제정되었고 HIGHT는 ISO 표준으로 추진예정임 - NIST는 SP 800-A,B,C,D 시리즈를 통해 블록암호 기반 운영모드를 권고하고 있으며 1개 이상의 인증-암호화 모드를 추가할 예정임 - 유럽의 스트림 암호 프로젝트 ECRYPT-eSTREAM이 지속적으로 진행될 것으로 예측됨 - ISO/IEC, IETF 등 에서 신규 IT 서비스 및 시스템에 적용을 위한 표준화 추진이 예측됨		
표준화 기구/ 단체	국 내	TTA, 기술표준원		
	국 외	IETF, ISO/IEC JTC1		
	국내참여 업 체 및 기관현황	KISA, ETRI, KIISC, TTA		
	국내기여도	- 국내 암호 알고리즘(SEED)이 ISO/IEC JTC1(18033-3), IETF(RFC 4269) 에서 국제 표준화되었음		
표준화 수준	국 내	표준안 최종검토	표준안 개발/검토	표준안 개발/검토
	국 외	표준안 최종검토	표준 제/개정	표준안 최종검토
국내표준화의 인프라수준 (시장요구정도및참여도)		높음		

구 분		암호기술		
표준화 대상항목		텔레매틱스 환경에서의 암호 키 관리 기술	암호알고리즘 이용 가이드라인	고성능 암호프로세서 설계 기술
시장현황 및 전망	국 내	2006년 12월 국내 텔레매틱스 서비스 가입자 75만 명 이상, BM 단말기 15,000대 텔레매틱스 서비스 매출은 2007년 1,146억원, 2008년 1,572억원, 2009년 2,214억원, 2010년 3,287억원으로 전망됨	2006년부터 국내에서도 상용 암호모듈평가프로그램이 시작됨 2009년 국가/공공기관에 납품되는 정보보호 제품/시스템에 암호 알고리즘이 주기능으로 탑재되는 경우, 국가용 암호제품 지정제도에 포함(제도 신설)	고성능 암호프로세서의 경우 휴대폰, 센서 기기, 노트북 등의 다양한 응용 영역을 가짐. 모바일 컴퓨팅용 칩을 적용한 단말 수 및 서비스 시장 규모가 급속히 증가하고 있음
	국 외	2005년 세계 텔레매틱스 시장은 711.8만대 판매량 기록, 2011년 연 4132만대의 판매량을 기록할 전망 2005년 연간 62억 달러의 판매액 달성, 2011년 200.5억 달러의 판매액을 보일 것으로 전망	인증 기술, 시스템, 네트워크 정보보호 기술, 응용 정보보호 기술 등을 활용한 정보보호 제품은 기반 기술인 암호알고리즘에 의존하고 있음 미국, 일본, 유럽을 중심으로 전자상거래, 금융부문, 인터넷, 전자서명 등 거의 모든 분야에서 암호기술을 사용하고 있음	무선 센서 네트워크 및 무선 메쉬 네트워크 등의 활용이 증가함에 따라 소형노드에 적합한 고성능 암호프로세서의 필요성이 증가하고 있음
기술개발 현황 및 전망	국 내	국내 텔레매틱스 환경에서의 보안 기술 및 키 관리 기술 연구는 ETRI에서 주도하고 있으며, 고려대학교, 성균관대학교, 숭실대학교 등이 학계에서 보안 기술을 연구 및 개발하고 있음 기존에 제안된 암호 키 관리 기술을 텔레매틱스 환경에 적합하도록 하는 연구가 진행 중임	대칭키 암호분야는 민간 표준으로 사용하기 위한 블록 암호SEED, 국가용 블록 암호 ARIA 알고리즘이 개발됨 KISA는 2007년 "암호이용 가이드라인"과 2008년 "암호정책 수립 기준 설명서"와 "암호 알고리즘 및 키 길이 이용안내서"를 개발함	대칭키알고리즘, 공개키 알고리즘, 인증 알고리즘 등이 구현된 암호 프로세서가 개발됨. IPSec, SSL 등 보안 프로토콜이 구현된 암호 프로세서가 개발됨. 사용자 인증 수단의 스마트카드 칩과 보안기능을 갖춘 모바일용 SoC인 mTPM칩이 개발됨. Rijndael 암호 알고리즘 등 다양한 암호 알고리즘의 FPGA 설계가 진행 중임
	국 외	미국은 VII 프로젝트인 ITS를 통해 관련 연구를 진행 중임. 독일 BMBF 프로젝트를 통해 차량간 통신 프로토콜, 보안 이슈 등을 연구함. 프랑스 EPFL에서는 SEVECOM에서는 차량간 통신을 이용한 서비스들의 보안을 향상시키기 위한 인증 기술, 보안 메커니즘 명세에 대하여 연구 중임	미국의 NIST, 일본의 CRYPTREC, 유럽의 ECRYPT에서는 암호 알고리즘 및 키 길이에 대한 가이드라인을 제시하고 있음. NIST는 2007년 키관리 가이드라인을 통해 암호 제품의 사용자 및 관리자가 설정해야 하는 적절한 암호알고리즘 및 알고리즘별 적절한 키 크기를 제공함 WiMAX 제품을 목표로 하는 ECC 암호 프로세서 엔진을 개발중임	미국에서는 TinyECC 프로세서를 개발하여 센서 노드에 적용함 IPSec, SSL 프로토콜 프로세싱, 암호화 가속, 하드웨어 기반의 ID 관리, Single Chip solution 인증 기능 등을 통합한 보안 프로세서를 개발함
기술 개발 수준	국 내	설계	일부 구현	연구
	국 외	구현	일부 구현	구현
	기술격차	1년	-	1년
	관련제품		인증 기술, 시스템, 네트워크 정보보호 기술, 응용 정보보호 기술 등을 활용한 정보보호 제품	HSM, 암호 프로세서, 암호칩
IPR 보유현황	국 내		- KCDSA 전자서명 알고리즘, SEED, ARIA 등의 대칭키 암호 알고리즘 명세	
	국 외		- 공개키, 대칭키, 전자서명, 키분배, ECC 알고리즘 명세	
IPR확보 가능분야		텔레매틱스 환경에서 익명성과 위치 추적성을 동시에 제공할 수 있는 인증 기술에서 필요로 하는 암호 키 관리 기술, 패스워드 기반 키 교환, 공개키 암호 등을 이용한 서비스에서 필요로 하는 암호 키 관리 기술 등	전자서명, 암 · 복호화, 메시지 인증 코드 등 각 응용 분야에서 암호 알고리즘을 안전하게 사용하기 위한 가이드라인 제시	고성능 암호프로세서의 기준과 설계 가이드라인 분야에 대한 IPR확보 가능 고성능 암호프로세서의 검증 방안 분야에 대한 IPR 확보 가능. 다양한 사용자 단말에 대한 고성능 암호 프로세서의 적용 모델 및 인터페이스 분야
IPR확보 가능성		보통	보통	보통
표준화 현황 및 전망		텔레매틱스 개발 기술 표준화 사업은 2004년부터 2006년까지 "ITS, GIS, LBS, 텔레매틱스 표준화 연구"라는 과제명으로 텔레매틱스와 기술적 연관성이 높은 ITS, 한, LBS 분야와 유기적인 연계 하에 활용성이 높은 표준을 개발한 바 있음 TTA 텔레매틱스/ITS PG(PG310)는 텔레매틱스 관련 표준안의 개발 및 심의에 전문성을 기하기 위하여 2007년 실무반을 확대함	일본은 CRYPTREC 사업을 통하여 전자정부에 필요한 암호 알고리즘을 표준화하고 있으며, 암호 알고리즘 및 키 길이에 대한 가이드라인을 제시하고 있음 NIST는 암호 제품의 사용자/관리자가 설정해야 하는 적절한 암호알고리즘 및 알고리즘별 적절한 키 크기를 제공함 유럽에서는 스트림 암호 프로젝트 ECRYOT-eSTREAM이 지속적으로 진행 국내에서 SEED는 2005년 ISO/IEC JTC1 및 IETF에서 표준으로 선정되었으며, 블록 암호 HIGHT와 해쉬 함수 FORK-256이 TTA 표준으로 제정됨 현재 TCG에서 관련 표준 제정 중	
표준화 기구/ 단체	국 내	TTA, 기술표준원	TTA, 기술표준원	TTA
	국 외	IETF, ISO/IEC JTC1, ITU-T, 3GPP	IETF, ISO/IEC, ITU-T	TCG, ITU-T
	국내참여업체 및 기관현황	KISA, ETRI, KIISC, 현대기아자동차, KT, LG텔레콤, SK텔레콤	KISA, ETRI, KIISC, TTA, 방송통신위원회	ETRI, 삼성전자, 보안업체 등
	국내기여도	보통		
표준화 수준	국 내	표준안기획	표준안 개발/검토	-
	국 외	표준안기획	표준안 개발/검토	기획
국내표준화의 인프라수준 (시장요구정도및참여도)		보통	높음	보통

구 분		암호기술		
표준화 대상항목		USIM 등 모바일 환경에서의 인증서비스 모델 및 인증기술	인터넷 전화 등에 이용 가능한 디바이스 인증 기술 및 응용	일회용패스워드 (OTP) 인증 기술 및 응용
시장현황 및 전망	국 내	올 하반기부터 대용량 USIM이 출시될 예정. 본격적인 USIM활용 시장은 2010년 중반에 형성 될 것으로 전망	국내에 디바이스 인증서가 적용된 기기의 경우 소수에 불과하나, 기기에서의 정보보호 필요성이 지속적으로 부각되어 기기에서의 디바이스 인증수요가 계속적으로 증가할 것으로 전망됨	1990년대 말부터 기업뱅킹을 위해 금융권에서는 OTP 기기를 도입하여 사용하였으며, 2007년도 OTP 통합인증센터 설립이후 300만명이 사용중이고 계속적으로 증가할 전망임
	국 외	Gemalto가 시장의 대부분을 독식하고 있으며 대용량 USIM에 대한 시범서비스도 미리 진행을 하고 있기 때문에 이를 활용한 다양한 서비스도 조만간 출시될 것으로 전망.	기존의 케이블모뎀, WiMAX, CCTV, 휴대폰 등의 기기 이외에 스마트그리드에 이용되는 기기 등 다양한 기기에 디바이스 인증서가 적용될 것으로 전망됨	싱가폴, 일본, 호주, 유럽 등지에서 주요은행을 중심으로 전자금융거래에 2-factor 인증 도구로 OTP를 이용하고 있으며, 전자상거래, 온라인 교육 등에서도 사용이 확대될 전망임
기술개발 현황 및 전망	국 내	IPTV 장치인증서는 상용서비스 CCTV 장치인증관련 시범 구축 인터넷 전화에 대한 장치인증서에 대한 기술규격	디바이스 인증서의 발급, 재동 갱신 및 재발급, 경량화된 검증방법 등 예정 인터넷 전화, CCTV 등의 제조회사에서는 기기인증서를 수용하여 기기간의 인증을 적용한 제품 개발이 진행 중	하드웨어 OTP 기기는 토큰형, 카드형, USB 등 다양하게 개발되어 판매중이며, 휴대폰에 탑재되는 형태인 모바일 OTP는 온라인 게임 및 웹포탈 사이트 등에서 사용중임
	국 외	SUN사에서는 다양한 어플리케이션을 동시에 실행할 수 있는 자바 카드 3.0을 이미 공개 했으며 대용량 USIM개발, SCWS개발 등이 Gemalto에서 이미 마친 상태.	케이블모뎀, 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
기술 개발 수준	국 내	국내	구현	시제품/프로토타입
	국 외	구현	설계	설계
	기술격차	1년	-	-
	관련제품	대용량 USIM	PKI 툴킷	하드웨어 OTP 토큰, OTP 카드, USB형 OTP, 모바일 OTP, 소프트웨어 OTP 등 다수
IPR 보유현황	국 내		홈네트워크 디바이스 인증서 프로파일 등	OTP 기술 특허(약 50여건)
	국 외		케이블모뎀 디바이스 인증서 프로파일, 인증 프로토콜 및 인증체계 등	OTP 생성알고리즘 등 다수 기술 특허 출원
IPR확보 가능분야		USIM을 활용한 인증 서비스	- 신규로 등장하게 될 다양한 IT기기에 대한 인증 - 디바이스 인증서 발급/검증 기술 및 기술 및 관련 프로토콜 활용 서비스 등	유비쿼터스 환경에 접목한 OTP 응용 기술 등
IPR확보 가능성		보통	보통	높음
표준화 현황 및 전망		USIM은 그 특성상 대부분의 기능과 스펙이 표준에 의하여 진행되며 현재 대용량 USIM, USIM 외형, SCWS등에 대한 표준화가 이루어진 상황이다. 향후 이를 기반으로 한 서비스를 위한 표준화가 추가적으로 진행될 예정이다.	- 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
표준화 기구/ 단체	국 내	TTA	TTA	TTA
	국 외	ETSI SCP, 3GPP, OMA	ITU-T, IETF	ITU-T, IETF
	국내참여업체 및 기관현황	SKT, KT, KISA, TTA	KISA, TTA, 한국정보인증, 한국전자인증	금융보안연구원
	국내기여도			낮음
표준화 수준	국 내	기획	표준안 개발/검토	표준안 개발/검토
	국 외	기획	표준안 개발/검토	표준안 개발/검토
국내표준화의 인프라수준 (시장요구정도및참여도)		보통	높음	높음

구 분		인증기술		
표준화 대상항목		일회용패스워드(OTP) 인증 프레임워크	익명성을 보장하는 인증 기술	바이오정보를 이용한 전자서명 기술
시장현황 및 전망	국 내	2007년 금융권 도입을 위해 OTP 통합인증센터 구축	익명인증에 대한 시장의 수요는 없으나, 향후 익명게시판, 전자투표 등 관련 인증서비스의 등장이 예상됨 제한적 본인확인제도 등 익명성이 요구되는 제도적인 증가에 따라 익명성 기술 요구 증대	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	- 싱가폴 통화청에서 OTP 인증 프래임워크 구축 중 - 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
기술개발 현황 및 전망	국 내	OTP 통합인증 프레임워크의 구축과 함께 여기에 적용된 프레임워크에 대한 개발이 진행되고 있음	익명 인증 관련 ETRI와 산학공동으로 그룹서명 기반의 익명ID 기술이 연구개발 중	바이오정보를 이용한 전자서명 키 생성기술은 초기 연구단계로, 기술적인 측면에서의 안정적인 구현 및 평가방안 등의 개발이 필요
	국 외	OTP에 대한 인증 프레임워크에 대한 개발이 국내 금융보안연구원으로부터 2008년부터 ITU-T의 Q7/SG17분야에서 추진 중임	전자투표 구현에 익명성을 보장하는 인증기술이 이용되고 있으며, 익명성을 보장하는 응용기술에 대한 연구가 지속적으로 이루어질 것으로 전망됨	바이오정보, 특히 지문정보를 이용한 전자서명 키 생성 기법 등이 연구되고 있으며, 지문뿐만아니라 망막, 홍채 등 다중 바이오정보를 활용한 기술로 발전되고 있음.
기술 개발 수준	국 내	구현	부분적 구현	연구
	국 외	설계	부분적 구현	연구
	기술격차	-	-	-
	관련제품		전자투표 장치, 익명게시판 등	지문인식장치, 홍채인식장치 등 바이오인식 장치
IPR 보유현황	국 내	특허 출원상태(OTP인증 프레임워크)		
	국 외	-		
IPR확보 가능분야		일회용패스워드 통합 인증 프레임워크 등	- 익명인증 및 익명 권한관리 플랫폼 기술 - 그룹서명 기반의 익명인증 기술 등	바이오정보를 이용한 전자서명 기술
IPR확보 가능성		높음	보통	보통
표준화 현황 및 전망		- 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 중ITU-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
표준화 기구/ 단체	국 내	TTA	TTA	TTA
	국 외	ITU-T	ITU-T, IETF	ITU-T, IETF
	국내참여업체 및 기관현황	금융보안연구원	KISA, TTA, 한국정보인증	KISA, ETRI
	국내기여도			
표준화 수준	국 내	표준안 개발/검토	표준 제/개정	기획
	국 외	표준안 개발/검토	표준 제/개정	기획
국내표준화의 인프라수준 (시장요구정도및참여도)		높음	보통	보통

구 분		권한관리기술		
표준화 대상항목		기기 관리자 간의 권한 관리 응용 기술	융복합 인증 서비스 모델	사용자 권한관리를 위한 인증 기술 및 응용
시장현황 및 전망	국 내	최근 많은 기기들이 폐쇄망에서 벗어나 IP 기반으로 연계되고 있어 이에 대한 보안이 크게 대두되고 있는 상황이다. 특히 IT강국이라는 이미지에 걸맞게 CCTV나 스마트 그리드 등은 선도적으로 진행하고 있기 때문에 이 분야에 대한 시장은 나날이 커질 예상이다.	융복합 인증 서비스의 경우 단순히 정보보호 서비스와 관련되기 보다는 각종 전자거래의 증가와 다양한 단말기의 사용, 새로운 서비스의 등장으로 다양화되고 복잡화된 정보 시스템에 적응하기 위하여 융복합 인증 서비스가 적용되므로 그 시장 규모를 정보보호 서비스로 제한할 수는 없음	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 커질 예정이다. 미국의 경우도 스마트 그리드에 대하여 막대한 투자가 예상되고 있다.	세계정보보호시장은 서비스부문 매출이 전체 시장 성장 견인역할을 할 것으로 예측되며 IAM시장과 SVM S/W는 2011년 까지 지속적으로 성장할 전망임.	PMI 관련 제품으로서는 Baltimore Technologies사의 SelectAccess, Entrust Technologies사의 Entrust GetAccess, RSA Security사의 ClearTrust, Netegrity사의 SiteMinder 등이 있음
기술개발 현황 및 전망	국 내	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.	최근 인증서 외에 생체정보, OTP, USIM 등 다양한 인증 수단이 제공되고, 모바일 환경이나 인터넷 전화, 기기 인증과 같은 새로운 인증 서비스 환경이 나타남에 따라 다양한 인증 서비스 모델이 등장하여 복잡한 서비스 환경을 만들고 있음(아직까지 연구 단계이지만, 최근 은행이나, 이동통신 서비스 업체별로 자신의 서비스 영역에서 통합 인증 시스템을 구축하여 제공하는 예가 늘고 있음) 한국정보보호진흥원에서는 2008년 2월 이와 관련하여 u-인증 서비스 도입 및 이용 기준(안)을 마련하여 발표함	- PMI 기능들은 접근제어 제품, EAM, 포털 관리 및 e-비즈니스 시스템 등에 끼어 들어가는 형태로 동작하고 있지만, 앞으로는 XML 기반으로 발전할 것으로 전망됨
	국 외	IBS와 같이 오래 전부터 원천 기술과 많은 기술적 KNOW-HOW를 보유하고 있어 이런 인프라를 기반으로 다양한 시도를 하고 있으며 별도 기술 개발 보다는 다른 분야에서 이미 검증된 기술 적용 중심으로 진행되고 있음	- WiMAX나 Cable 셋톱박스 등의 기기 인증이나, WiFi 서비스 등에 인증서를 사용하는 인증 모델을 적용하고 있음 - Verisign이나 CLMA 등은 이미 이와 관련한 서비스를 제공하고 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	연구	부분적 구현/시작단계	구현/상용화
	국 외	연구	부분적 구현/시작단계	구현/상용화
	기술격차	2년	-	-
	관련제품	DOCSIS	SSO	PMI, EAM
IPR 보유현황	국 내			
	국 외			
IPR확보 가능분야		스마트 그리드에서의 다중 사업자에 의한 기기 접근 제어	융복합 인증 서비스 모델, 응용 모델	
IPR확보 가능성		보통	보통	낮음
표준화 현황 및 전망		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 상황이다. 기기별로 서비스 별로 각각 진행되고 있지만 기본적인 가이드라인 안에서 진행될 필요가 있다.	- 아직까지 별도 인증 서비스, 인증 모델 분야의 표준화가 진행중	- 국내의 경우 2008년도에 PMI 관련 표준이 제정되었음 - 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
표준화 기구/ 단체	국 내	TTA	TTA	TTA
	국 외	OMA, ITU-TS, CableLabs, ISO, IET	IETF, ITU, IEEE	IETF, ITU-T
	국내참여업체 및 기관현황	KISA, ETRI, Samsung	KISA, TTA	KISA, TTA
	국내기여도			
표준화 수준	국 내	기획	기획	표준안 개발/검토
	국 외	기획	기획	표준안 개발/검토
국내표준화의 인프라수준 (시장요구정도및참여도)		보통	보통	보통

3. 표준화 추진전략

3.1. 중점기술의 표준화 환경분석

3.1.1. 표준화 추진상의 문제점 및 현안사항

- 암호, 인증, 권한관리 기술은 IT 서비스에 직접적으로 요구되는 요소기술이기 보다는 정보보호 기능 적용 시 필요한 기반 기술이기 때문에 사회적으로 이슈화 시키는 것이 어려우며 이에 따라 정부차원의 지속적인 투자를 이끌어내기가 어렵다. 또한 업체에서도 이러한 현실을 감안하여 인프라 차원의 기술인 암호/인증/권한관리 분야에 투자를 꺼려하고 있음
- 하지만, 암호/인증/권한 관리는 최근 인터넷상에서 발생하는 다양한 보안 위협으로 부터 국민을 안전하게 보호하기 위해 반드시 필요한 요소기술이며 u-City, u-health 등 정부에서 관심을 가지고 추진하는 신규 IT 산업에도 없어서는 안되는 중요한 기반 기술이기 때문에 정부, 학계, 산업체 등에 암호/인증/권한관리 기술의 국내외 표준화 필요성에 대한 인식을 제고시키는 노력이 필요
- 최근 유비쿼터스 환경의 도래에 따라 해당 환경에 적합한 정보보호 기반기술 확보를 위해 경량 암호/인증 기술, 바이오 인식 기술, u-IT 서비스 보호 기술, 암호 평가 기술 등 차세대 정보보호 기반기술에 대한 개발을 위한 정부차원의 지속적인 지원 요청 필요
- 또한, 센서 네트워크와 같이 새로운 네트워크 환경과 초소형 기기 들이 등장함에 따라 기존 기술을 이들 새로운 환경에 적응시키기 위한 기술개발도 선행되어야 함. 소형 기기에서 연산가능한 TinyECC등의 개발이 이미 국외에서는 진행되고 있음. 기존의 다양한 알고리즘을 새로운 환경의 프로토콜에 적용하기 위한 노력이 진행 중인 것도 같은 맥락으로 생각됨
- 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 신규 기술 개발의 어려움이 예상되며 현재 개발 중인 국내 OTP 관련 표준 기술과 기존에 운영되고 있는 OTP 인증 시스템과의 호환성 제공방안의 수립이 필요
- 다양한 특성과 처리능력을 가진 하드웨어 기반 접근통제 수단이 제시되고 있으나, 이에 기반한 인증 방법 및 기술들에 대한 명시적 접근이 미비하여 관련 기술 표준화가 개발되지 못하고 있는 실정임. 접근 통제 수단으로서 사용되는 하드웨어의 고유 특성과 활용성을 고려한 인증 기술 개발 및 해당 기술에 대한 국내외 표준화 추진 필요

3.1.2. SWOT 분석 및 표준화 추진방향

국내역량요인 / 국외환경요인			강점 요인 (S)	약점 요인 (W)
		시장	- 다양한 신규 IT서비스 증가에 의한 정보보호시장도 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 알고리즘에 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 : 2** - 국가적으로 확산되고 있는 신규 u-IT 서비스 보안 기술 개발 요구에 맞게 정보보호 기반 기술에 대한 국제 표준화 우선 추진 - IETF, ITU-T 등에서의 국제표준화 역량을 바탕으로 디바이스 인증, OTP 인증 등 신규 기술의 국제표준 및 독자 IPR 개발 확대 - 국제표준화 기구 의장단(국내 전문가) 활용을 통해 선도 가능 분야 표준화 활동 강화	**- 현황분석에 의한 우선순위 : 3** - u-IT 서비스 보안 등 최근 이슈가 되는 분야를 중심으로 정부 및 산업계의 투자 지원 유도 및 표준화 활동 지원 강화 요청 - 지속적인 자체 정보보호 기반 기술 개발 및 표준화 활성화를 통해 국내 정보보호 수준 선진화 및 제품 경쟁력 향상 - 국제 표준화 전문가 활용을 통해 국내 산업에 직접적으로 적용될 수 있는 표준 개발 확대
	기술	해킹기술의 고도화 등에 대처하기 위한 안전한 정보보호 기반기술 요구 증가		
	표준	IETF 및 ITU-T에서 정보보호기반 기술의 표준화 요구 증가 및 표준화 기구 의장단 진출 확대		
			SO전략 : 공격적 전략(강점사용-기회활용) / WO전략 : 만회전략(약점극복-기회활용) ST전략 : 다각화 전략(강점사용-위협회피) / WT전략 : 방어적 전략(약점최소화-위협회피) SO WO 전략 ST WT	
위협요인 (T)	시장	FTA 등 시장개방으로 인해 호환성 보장이 되지 않는 국내 보안 제품의 시장경쟁력 저하	**- 현황분석에 의한 우선순위 : 1** - 다양한 응용서비스에 국산 암호알고리즘 활용을 위한 국제 표준 개발을 통해 국내 제품의 국제 경쟁력 확보 기반 마련 - 신규 u-IT서비스에 국내 원천기술 적용 표준 개발 등을 통해 국내 IPR 확보 노력 강화 - 암호 모듈 평가를 통한 정보보호 제품의 수준 제고 및 국내 정보보호 산업체의 전략적 육성	**- 현황분석에 의한 우선순위 : 4** - 디바이스 인증 등 신규 IT서비스에 필요한 기술 개발 확대를 통해 장기적으로 산업 친화적인 정보보호 인프라 구축 추진 - 정보보호 분야 전문 인력의 지속적인 양성 노력을 통한 국내 원천 기술 개발 및 국제 표준화 추진 확대
	기술	지속적인 원천기술 개발에 대한 투자 미흡으로 IPR 확보가 미흡		
	표준	암호알고리즘 응용에 대한 표준 개발 미흡 등으로 국산 보안 제품에 대한 국내 경쟁력 약화		

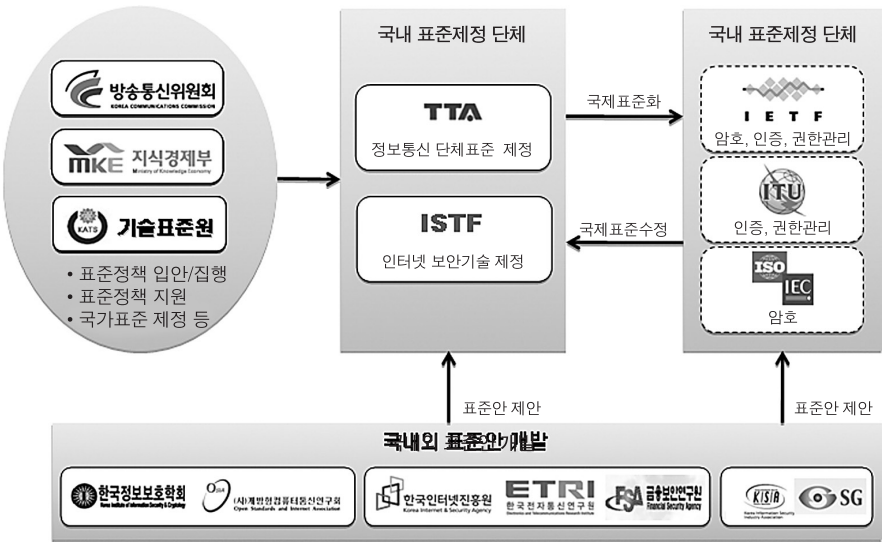
• **현황분석을 통한 우선순위 : ST전략 → SO전략 → WO전략 → WT전략**

- ST 전략 : 한-미, 한-EU 등 FTA 체결 확산에 따라 국산 정보보호 제품에 대한 국내 경쟁력 강화를 위해 우선적으로 국내 원천기술을 다양한 응용서비스에 적용하기 위한 표준 개발이 시급. 이를 위해, 향후 급속히 확산될 수 있는 IPTV, VoIP 등 신규 방송·통신 융합 서비스에 선도적으로 적용하기 위한 국제 표준 개발
- SO전략 : ITU-T 국제 표준화 기구에 의장단 진출 및 우수 국제 표준 전문가 보유 확대를 통해 국내에서 개발한 우수한 정보보호 기술에 대해 국제 표준 개발을 확대하고, 이를 통해 국내에 상대적으로 적은 IPR 보유 기반도 확대
- WO전략 : 정보보호 기반 기술의 경우 국내 산업에 직접적으로 영향력을 미칠 수 있는 기술이 아니기 때문에 가능한 시장 친

화적이고 산업 친화적인 분야를 발굴하고 이를 통해 정부 및 산업체의 투자 및 참여 확대를 도모
- WT전략 : 장기적인 국제 표준 전문 인력 양성시스템 구축 및 운영을 통해 국내 IPR 보유 노력 미흡 및 국제 표준 인식 저하 문제를 해결하고, 궁극적으로 국내 정보보호 기술에 대한 국제 경쟁력 강화 기반 마련

• **표준화 추진방향 : ST전략의 중점추진을 통한 WO전략의 보완**
- 국산 암호알고리즘 등 국내 원천기술을 다양한 응용서비스에 적용하기 위한 표준화를 우선적으로 추진하는 ST 전략을 적극 활용하여 국내 정보보호 제품 산업 보호 및 육성을 위한 기반을 마련
- 이를 기반으로 정부 및 산업체의 국제 표준 개발 참여 유도 확산을 통해 궁극적으로 국내 표준화 인프라 및 산업을 확산하여 국내 IPR 확보를 위한 선순환 구조를 마련
- 또한, 국내 뿐 아니라 국제 표준화 전문가가 점차적으로 확산되고 있기 때문에 이를 활용하는 SO 전략을 중점 추진함으로써 국제 표준 개발 시 소요되는 시간 및 노력을 절감하고 다양한 분야에서 다양한 표준들이 채택될 수 있도록 적극 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 기술 홍보 뿐 아니라 국내 정보보호 제품에 대한 국제 시장 진출 활성화가 가능

3.1.3. 표준화 추진체계



• 학계 및 산업계의 경우 개인 자격 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

• 한국인터넷진흥원, ETRI, 금융보안연구원 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

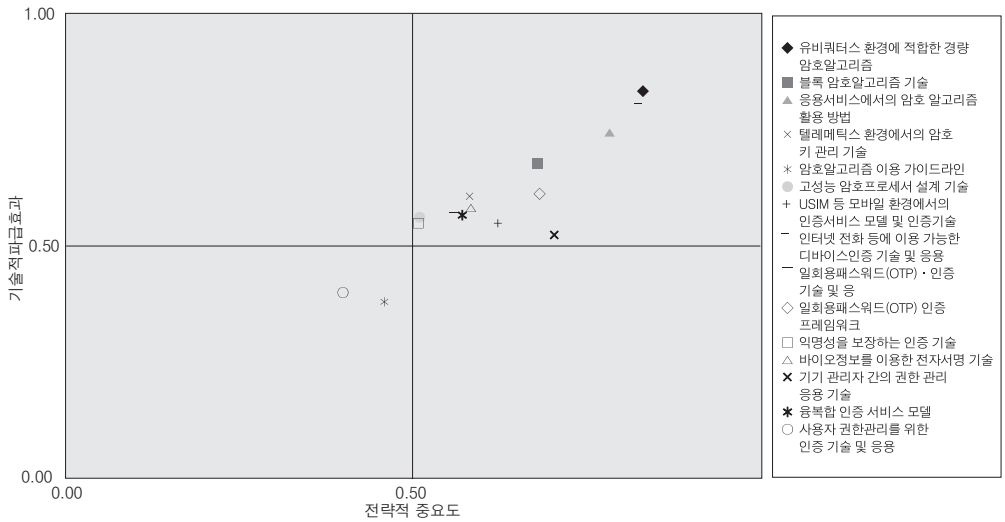
3.2. 중점 표준화항목 선정

3.2.1. 중점 표준화항목 선정방법

• 표준화 대상항목별 전략적 중요도 및 기술적 파급효과 분석

중점기술 후보별 전략적 중요도 및 기술적 파급효과 분석

평가지표	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	P4 기술적 선도 가능성(국제표준경쟁력, IPR 확보 등)	P5 국제표준화 이슈정도	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	0.16	0.17	0.24	0.24	0.19	-	0.25	0.16	0.22	0.20	0.18	-
유비쿼터스 환경에 적합한 경량 암호알고리즘	3.64	3.21	4.50	4.79	4.21	0.83	4.50	4.07	4.07	3.93	4.21	0.83
블록 암호알고리즘 기술	3.80	3.07	3.47	3.47	3.20	0.68	4.20	3.40	2.93	3.00	3.20	0.68
응용서비스에서의 암호 알고리즘 활용 방법	3.83	3.56	4.00	4.17	3.94	0.79	3.61	3.89	3.67	3.83	3.72	0.75
텔레메틱스 환경에서의 암호 키 관리 기술	2.94	3.13	2.69	3.25	2.56	0.58	2.88	2.81	3.13	3.25	3.06	0.61
암호알고리즘 이용 가이드라인	2.56	4.11	2.56	1.39	1.22	0.46	1.61	2.33	2.00	1.83	1.83	0.38
고성능 암호프로세서 설계 기술	2.08	2.25	3.50	2.58	2.08	0.51	3.58	2.92	2.75	2.17	2.42	0.56
USIM 등 모바일 환경에서의 인증서비스 모델 및 인증기술	3.44	2.88	3.36	3.24	2.60	0.62	2.88	2.96	2.48	2.64	2.76	0.55
인터넷 전화 등에 이용 가능한 디바이스 인증 기술 및 응용	4.38	4.14	4.45	4.00	3.48	0.82	3.48	4.41	4.24	4.03	4.10	0.80
일회용패스워드(OTP) 인증 기술 및 응용	2.75	4.06	3.25	2.25	1.94	0.56	2.69	2.00	3.56	2.88	3.00	0.57
일회용패스워드(OTP) 인증 프레임워크	3.63	4.06	3.50	3.31	2.69	0.68	3.06	2.94	3.19	2.88	3.25	0.61
익명성을 보장하는 인증 기술	2.60	2.25	2.30	3.10	2.40	0.51	3.65	2.55	2.40	2.15	2.75	0.55
바이오정보를 이용한 전자서명 기술	2.56	2.75	2.88	3.44	2.81	0.58	3.38	3.06	2.13	2.50	3.56	0.58
기기 관리자 간의 권한 관리 응용 기술	3.00	2.59	2.76	1.71	1.47	0.46	2.47	2.24	2.35	2.12	2.12	0.45
융복합 인증 서비스 모델	2.19	3.43	2.90	2.76	3.00	0.57	3.00	3.00	2.52	2.71	2.90	0.56
사용자 권한관리를 위한 인증 기술 및 응용	2.18	1.88	2.06	1.88	2.00	0.40	2.18	1.88	2.00	1.71	2.18	0.40



3.2.2. 중점 표준화항목 선정사유

• 전략적 중요도 및 기술적 파급효과 평가 결과

- 암호/인증/권한관리 분야의 중점 표준화 항목으로 선정된 6가지의 표준화 항목은 우선적으로 기술적 선도 가능성, 적시성, 정부 및 산업체 의지 등 전략적 중요도와 타기술의 파급효과, 시장파급성 및 상용화 가능성, 산업적 파급효과 등 기술적 파급효과에서 모두 0.5점 이상(평균 0.73점)의 높은 점수를 획득한 표준화 항목을 대상으로 선정
- 또한, 최근 국제적으로 이슈화가 되고 있고 국내에서 선도적으로 추진 가능한 아이템을 중심으로 전략적 중요도 및 기술적 파급효과를 고려하여 선정

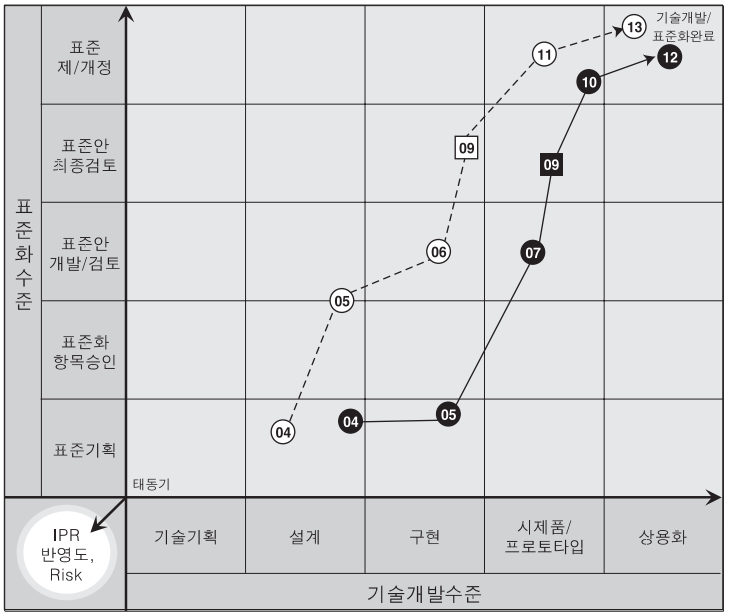
• 중점 표준화항목별 선정사유

- 유비쿼터스 환경에 적합한 경량 암호알고리즘 항목은 신규 u-인증 서비스에서는 컴퓨팅 파워가 적은 단말기를 사용하는 서비스가 주를 이루기 때문에 이를 위해서는 저전력/경량 알고리즘이 필요. 이에 따라 해당 아이템의 경우 기술 선도 가능성 및 적시성 등의 전략적 중요도가 높으며, 기술적 파급효과에서는 미래영향력 및 기술적 중요도가 높아 선정
- 블록 암호알고리즘 기술 항목은 해킹 기술의 발달 등으로 인해 매년 알고리즘의 안전성이 위협을 받게 됨에 따라 기존 128비트의 알고리즘을 192, 256비트로 확장하는 기술로써 기술적 파급효과가 높아 중점 표준화 항목으로 선정
- 응용서비스에서의 암호 알고리즘 활용 방법 항목은 국내 원천기술인 암호알고리즘을 VoIP, IPTV 등의 신규 IT 응용서비스에 적용시키기 위해 필요한 표준화로써, 최근 국내 정보보호 제품에 대한 국제 경쟁력 강화를 위해 정부 및 산업체에서 관심이 많은 분야임. 이에 따라, 전략적 중요도 측면에서 영향력이 높은 아이템으로 중점 표준화 항목으로 선정
- 인터넷 전화 등에 이용 가능한 디바이스 인증 기술 및 응용 항목은 유비쿼터스 환경의 도래에 따라 인증의 범위가 사람 뿐 아니라 인터넷 전화, CCTV, IPTV 등의 다양한 디바이스로 확산되고 향후 u-시티, u-헬스 등의 산업에서 활발히 적용 가능한 기술이기 때문에 전략적 중요도 측면에서 영향력이 높은 아이템으로 중점 표준화 항목으로 선정
- 일회용패스워드(OTP) 인증 기술 및 응용 항목은 강한 인증을 제공하면서 상대적으로 편리하게 사용할 수 있는 OTP 인증 기술을 포함하고 있으며, 해당 OTP 인증 기술은 현재 온라인 게임 등 다양한 분야에서 적용되어 사용되고 있어 기술적 파급효과 및 전략적 중요도가 높아 중점 표준화 항목으로 선정
- 일회용패스워드(OTP) 인증 프레임워크 항목은 엄격한 사용자 및 거래 인증 수단으로 금융권에서 구현되어 서비스 중인 OTP 인증을 포괄하는 프레임워크 기술로써 산업적 파급효과 등 기술적 파급효과가 높아 중점 표준화 항목으로 선정

3.3. 중점 표준화항목별 세부전략(안)

3.3.1. 유비쿼터스 환경에 적합한 경량 암호알고리즘

• 표준화-기술개발-IPR 연계분석



표준화 중요도	국내 개발주체		활용도	관련 국제 표준화 기구
고(★★★) 중(★★☆) 저(★☆☆)	표준개발	기술개발		
★★★	KISA TTA ETRI	KISA, ETRI 등	센서, RFID, VoIP 등	ISO/IEC JTC1, IETF, ITU-T 등

범 례

09 : 중점 표준화항목의 국내상태

09 : 중점 표준화항목의 국제상태

→ : 중점 표준화항목의 국내 표준상태전이

-→ : 중점 표준화항목의 국제 표준상태전이

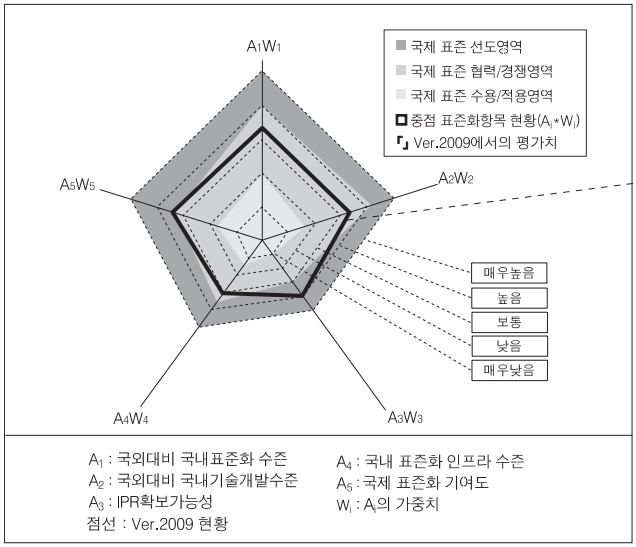
↑ : 선행표준(선 표준화 후 기술개발)

↗ : 동시표준(표준화&기술개발 동시추진)

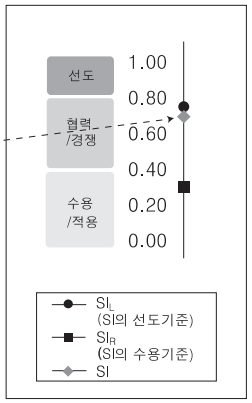
→ : 후행표준(선 기술개발 후 표준화)

표준화 특성	선행표준
표준화-기술개발- IPR 연계방안	경량 암호알고리즘 관련 기술에 대해 IPR을 확보하는 것은 어려울지라도 기술 표준화를 통해서 국제 시장에서의 국내 기술의 경쟁력 강화

• 국제표준화 전략목표 및 세부전략(안)



SI (표준화 전략지수)	
SI_L (SI의 선도기준)	0.74
SI_R (SI의 수용기준)	0.32
SI	0.67



$0 < SI \leq 1$

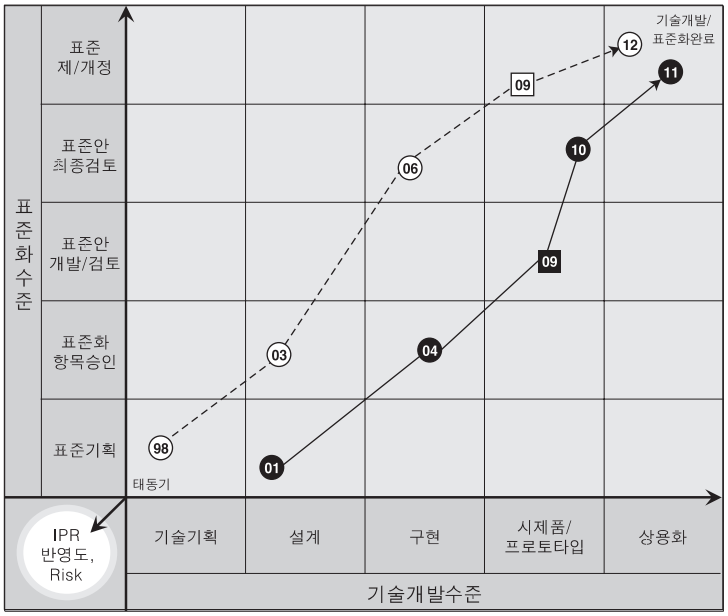
- $SI \geq SI_L$: 선도항목
- $SI_R \leq SI < SI_L$: 협력/경쟁항목
- $SI < SI_L$: 수용/적용항목

국제표준
협력/경쟁(Ver.2010)

국제표준화 전략목표	국제표준 협력/경쟁(Ver.2010)
Trace Tracking (Ver.2009 ⟼ 2010)	본 중점 표준화 항목의 경우 Ver.2010 신규 항목임. 다만, 현재 저전력 RFID에 적합한 암호기술 뿐만 아니라 경량화된 블록 암호알고리즘의 표준화를 위해 국제 표준화 기구에서 editor로 활동 하는 등 표준화 수준은 점차적으로 상향되는 경향임
세부전략(안)	- 국외대비 국내표준화수준 분석에 따른 전략: 유 • 무선의 고전 암호알고리즘에 대한 기술 개발은 이미 국내외 적으로 표준화 추진이 완료되었기 때문에, RFID/USN, IPTV 등에 활용 가능한 경량화된 암호 알고리즘에 대해 국내 표준화 선행 추진 후 이를 기반으로 ISO/IEC, IETF 등에서 국제 표준화 추진 - 국외대비 국내기술개발수준 분석에 따른 전략: 2000년 초기부터 기술개발이 다양하게 이루어져왔고, 최근에는 경량화된 암호 기술 등 유비쿼터스 환경에 필요한 암호기술에 대한 연구가 진행되고 있기 때문에 관련 산업계에서 국내외 표준화의 중요성을 인지하고 관련 기술에 대한 표준화 활동을 강화할 수 있는 기반 마련 필요 - IPR확보가능성 분석에 따른 전략: 국내에서 경량 암호알고리즘에 대한 자체 특허는 이미 존재하므로, 국내 IPR 확보가 어려울 것으로 판단됨. 반면, 국외에서 경량화 암호알고리즘에 대한 관심이 높으므로 국외 IPR 확보를 고려해볼 필요가 있음 - 국내표준화인프라수준 분석에 따른 전략: 암호기술과 관련된 표준화의 경우 TTA, KSIC 등에서 지속적으로 추진되고 있기 때문에 국내 표준화 인프라는 좋은 편이며, 이를 기반으로 국제 경쟁력 있는 표준화 인프라 구축 노력에 주력 - 국제표준화기여도 분석에 따른 전략: ISO/IEC, IETF 등에서 다양한 암호기술에 대한 표준화 추진이 활발히 진행되고 있기 때문에 국내 전문가들이 해당 표준화 기구에 적극적으로 참여하여 국내 기술에 대한 국제 표준화 채택에 기여 필요
IPR 확보방안	- 국내 암호 알고리즘에 대한 개발이 활발하지 않기 때문에 IPR 확보가 어려울 수 있으므로, 경량 암호 알고리즘에 대한 관심이 높은 국제 표준화 기구에서의 표준화 활동을 통해 국제 IPR 확보 추진

3.3.2. 블록 암호알고리즘 기술

• 표준화-기술개발-IPR 연계분석



표준화 중요도	국내 개발주체		활용도	관련 국제 표준화 기구
고(★★★) 중(★★☆) 저(★☆☆)	표준개발	기술개발		
★★★	KISA TTA ETRI	KISA, ETRI 등	금융, 무선통신, 공공, 민간, 보안장비 등	ISO/IEC JTC1, IETF, ITU-T 등

범 례

09 : 중점 표준화항목의 국내상태

09 : 중점 표준화항목의 국제상태

→ : 중점 표준화항목의 국내 표준상태전이

-→ : 중점 표준화항목의 국제 표준상태전이

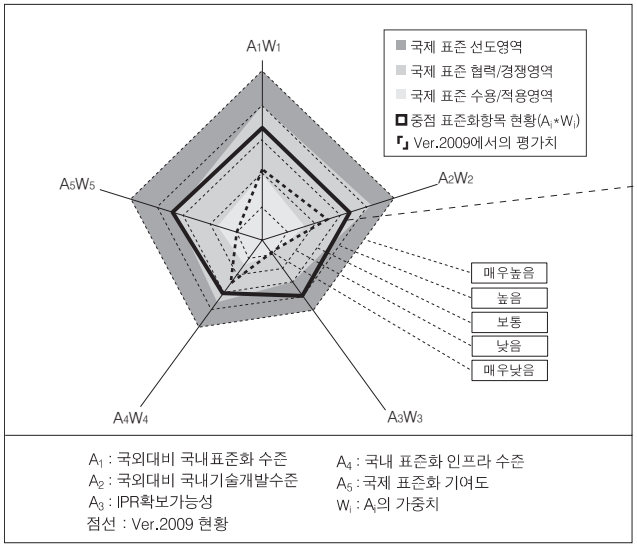
↑ : 선행표준(선 표준화 후 기술개발)

↗ : 동시표준(표준화&기술개발 동시추진)

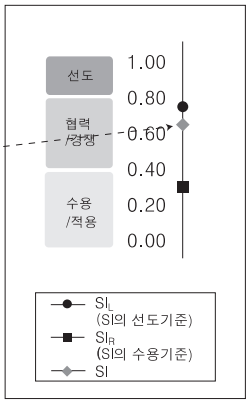
→ : 후행표준(선 기술개발 후 표준화)

표준화 특성	후행표준
표준화-기술개발- IPR 연계방안	블록 암호알고리즘에 대해서는 이미 국내외에서 오래전부터 표준화 및 IPR을 확보하고 있기 때문에 신규 IPR 확보는 어렵지만, 최근 해킹피해가 증가하고 있기 때문에 이에 대응하기 위해 암호강도가 증가된 블록 암호알고리즘에 대한 국내외 표준화를 통해 향후 IPR 확보 노력 필요

• 국제표준화 전략목표 및 세부전략(안)



SI (표준화 전략지수)	
SI_L (SI의 선도기준)	0.74
SI_R (SI의 수용기준)	0.32
SI	0.63



$0 < SI \leq 1$

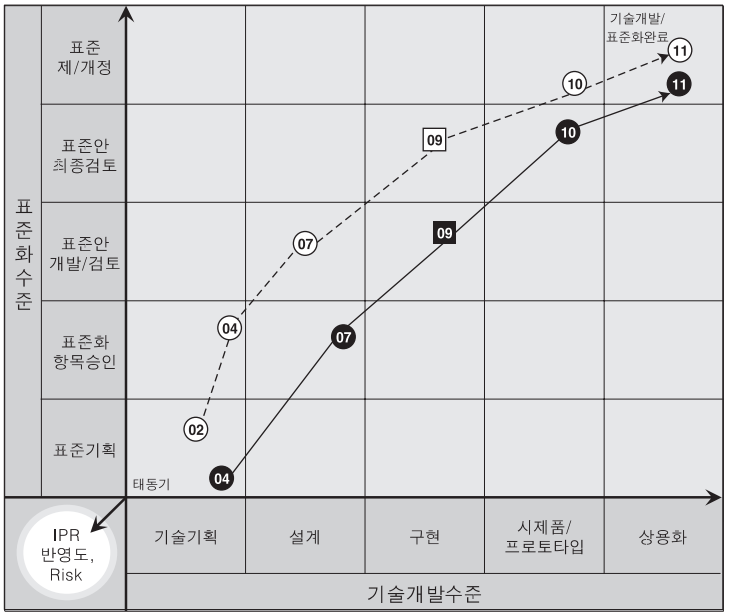
- $SI \geq SI_L$: 선도항목
- $SI_R \leq SI < SI_L$: 협력/경쟁항목
- $SI < SI_L$: 수용/적용항목

국제표준
수용/적용(Ver.2009)
⬇
국제표준
협력/경쟁(Ver.2010)

국제표준화 전략목표	국제표준 수용/적용(Ver.2009) ⟼ 국제표준 협력/경쟁(Ver.2010)
Trace Tracking (Ver.2009 ⟼ 2010)	- Ver.2009이전부터 국외대비 국내 표준화 수준이 낮음으로 분석되었으나, 최근에는 지능화-고도화된 해킹 공격에 대응하기 위해 안전성이 강화된 암호알고리즘에 대한 국내외 표준화 추진을 통해 Ver.2010에서는 표준화 수준이 상향 평가됨
세부전략(안)	- 국외대비 국내표준화수준 분석에 따른 전략: 미국, 유럽, 일본 등 국외에서 AES, Blowfish, Camellia 등을 개발하여 ISO/IEC, IETF 등 다양한 분야에 표준화를 추진하고 있지만 국내에서도 자체 개발한 블록 알고리즘에 대한 국내외 표준화 추진 경험이 있기 때문에 해당 경험을 기반으로 안전성이 강화된 암호 알고리즘에 대한 표준안을 국내외 동시에 추진 - 국외대비 국내기술개발수준 분석에 따른 전략: 블록 암호 알고리즘의 경우 1990년대 말부터 기술개발이 다양하게 이루어져왔고, 최근에는 RFID/USN 등과 같이 특정 환경을 고려한 암호 알고리즘에 대한 연구가 활발히 이루어지고 있으나, 이러한 암호 알고리즘은 특정 환경 이외에서는 적합하지 않을 수도 있음. 이에 특정 환경에 적합한 암호 알고리즘 개발 이외에 웹 서비스, 보안 장비 등에서도 활용 될 수 있는 암호 알고리즘을 개발하고 이에 대한 국내 및 국제 표준화 추진 - IPR확보가능성 분석에 따른 전략: 국내에 암호 알고리즘 자체에 대한 특허는 이미 존재하므로, 국내 IPR 확보가 어려울 것으로 판단됨. 반면, 다양한 해킹 공격에 대응하기 위한 안전성이 강화된 블록 암호 알고리즘에 대한 제한적 IPR 발굴 노력 필요 - 국내표준화인프라수준 분석에 따른 전략: 암호기술과 관련된 표준화의 경우 TTA, KSIC 등에서 지속적으로 추진되고 있기 때문에 국내 표준화 인프라는 좋은 편임. 따라서, 해당 인프라를 활용하여 실효성 있는 국내 표준 개발을 통해 국제 경쟁력 있는 표준화 인프라 구축 노력에 주력 - 국제표준화기여도 분석에 따른 전략: ISO/IEC, IETF 등에서 다양한 암호기술에 대한 표준화 추진이 활발히 진행되고 있기 때문에 국내 전문가들이 해당 표준화 기구에 적극적으로 참여하여 국내 기술에 대한 국제 표준화 채택에 기여 필요
IPR 확보방안	- 국내 암호 알고리즘에 대한 개발이 활발하지 않기 때문에 IPR 확보가 어려울 수 있으나, 지속적으로 암호 알고리즘을 개발하기 위해 산•학•연을 기반으로 알고리즘 개발에 주력, 이를 기반으로 국내외 IPR 확보

3.3.3. 응용서비스에서의 암호알고리즘 활용 방법

• 표준화-기술개발-IPR 연계분석



표준화 중요도	국내 개발주체		활용도	관련 국제 표준화 기구
고(★★★) 중(★★☆) 저(★☆☆)	표준개발	기술개발		
★★★	KISA TTA ETRI	KISA, ETRI 등	VoIP IPsec 등	ISO/IEC JTC1, IETF, ITU-T 등

범 례

09 : 중점 표준화항목의 국내상태

09 : 중점 표준화항목의 국제상태

→ : 중점 표준화항목의 국내 표준상태전이

-→ : 중점 표준화항목의 국제 표준상태전이

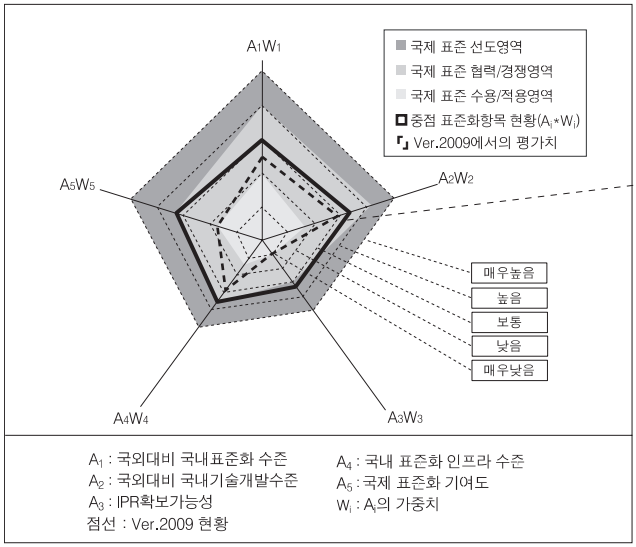
↑ : 선행표준(선 표준화 후 기술개발)

↗ : 동시표준(표준화&기술개발 동시추진)

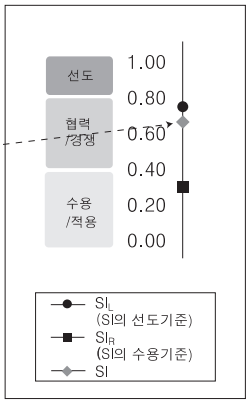
→ : 후행표준(선 기술개발 후 표준화)

표준화 특성	동시표준
표준화-기술개발- IPR 연계방안	국내에서 추진하는 신규 IT서비스 관련 선도 기술에 암호 알고리즘을 활용하는 노력을 통해 분야별 필요한 응용 기술 개발 및 국내외 표준화 추진을 통해 관련 기술의 국제 IPR 선점

• 국제표준화 전략목표 및 세부전략(안)



SI (표준화 전략지수)	
SI_L (SI의 선도기준)	0.74
SI_R (SI의 수용기준)	0.32
SI	0.65



$0 < SI \leq 1$

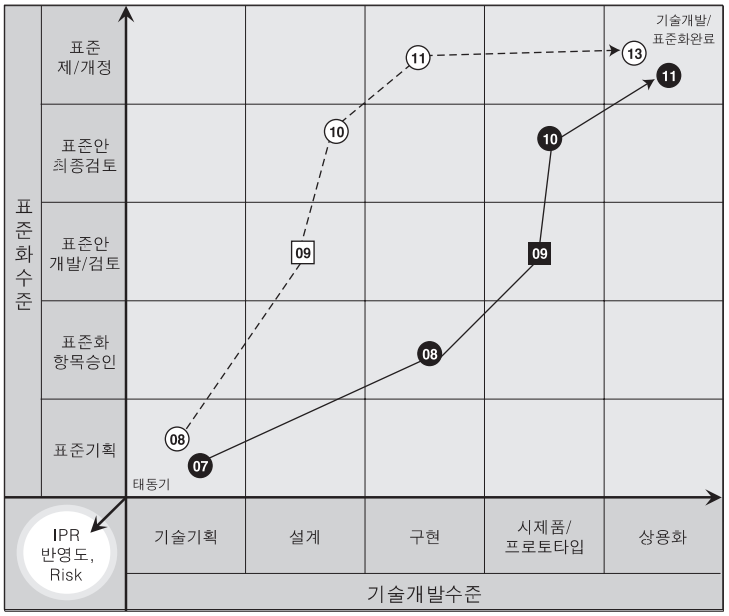
- $SI \geq SI_L$: 선도항목
- $SI_R \leq SI < SI_L$: 협력/경쟁항목
- $SI < SI_L$: 수용/적용항목

국제표준
협력/경쟁(Ver.2009)
⬇
국제표준
협력/경쟁(Ver.2010)

국제표준화 전략목표	국제표준 협력/경쟁(Ver.2009) ⟼ 국제표준 협력/경쟁(Ver.2010)
Trace Tracking (Ver.2009 ⟼ 2010)	- Ver.2009 현황과 동일
세부전략(안)	- 국외대비 국내표준화수준 분석에 따른 전략: 블록 암호 알고리즘 등과 같은 고전적 암호기술은 이미 국내외 적으로 표준화 추진이 완료되었기 때문에, IPTV, VoIP 등에 활용되는 암호응용기술에 대해 국제 경쟁력 있는 표준안을 TTA에서 선행 개발하고 이를 기반으로 IETF, ISO/IEC, IEEE 등에서 국제 표준화 선도 - 국외대비 국내기술개발수준 분석에 따른 전략: 암호응용기술의 경우 2000년 초기부터 기술개발이 다양하게 이루어져왔고, 최근에는 IP 기반 VoIP, IPTV 등 신규 IT 응용 서비스들에 대한 연구가 진행되고 있기 때문에 관련 산업계에서 국내외 표준화의 중요성을 인지하고 관련 기술에 대한 표준화 활동을 강화할 수 있는 기반 마련 필요 - IPR확보가능성 분석에 따른 전략: 국내에서 개발한 암호 알고리즘과 관련된 기술 및 서비스 특허가 많이 존재하고 있어 국내 IPR 확보가 어려울 것으로 판단됨. 다만, 다양한 IT서비스들이 계속적으로 개발 • 적용되고 있기 때문에 해당 서비스에 제한적인 IPR 발굴 노력 필요 - 국내표준화인프라수준 분석에 따른 전략: 암호 알고리즘 및 응용 기술과 관련된 표준화의 경우 TTA, KSIC 등에서 지속적으로 추진되고 있기 때문에 국내 표준화 인프라는 좋은 편임. 따라서, 해당 인프라를 활용하여 실효성 있는 국내 표준 개발을 통해 국제 경쟁력 있는 표준화 인프라 구축 노력에 주력 - 국제표준화기여도 분석에 따른 전략: ISO/IEC, IETF 등에서 다양한 응용 서비스에서 적용 가능한 암호 알고리즘에 대한 표준화 추진이 활발히 진행되고 있기 때문에 국내 전문가들이 해당 표준화 기구에 적극적으로 참여하여 국내 기술에 대한 국제 표준화 채택에 기여 필요
IPR 확보방안	- 국내 암호 알고리즘을 다양한 IT 서비스들에 적용하여 응용 서비스 분야 도출, 응용 환경에 적용 가능한 방법 개발하여 국내외 IPR 확보

3.3.4. 인터넷 전화기 등에 이용 가능한 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 등	제조업 서비스 공공	IETF ITU-T

범 례

09 : 중점 표준화항목의 국내상태

09 : 중점 표준화항목의 국제상태

→ : 중점 표준화항목의 국내 표준상태전이

-→ : 중점 표준화항목의 국제 표준상태전이

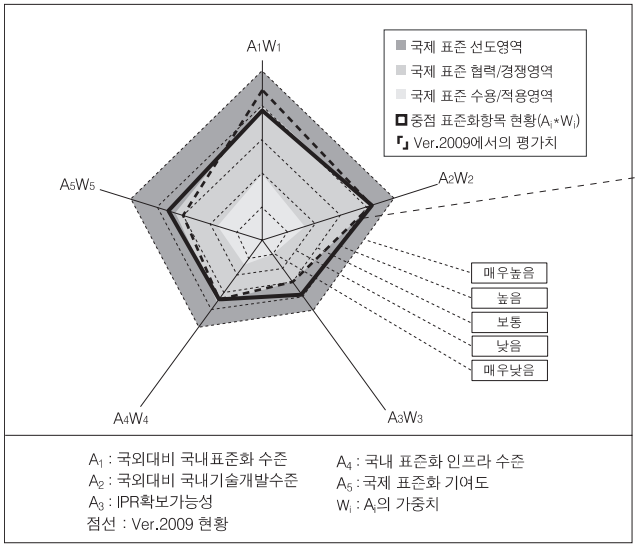
↑ : 선행표준(선 표준화 후 기술개발)

↗ : 동시표준(표준화&기술개발 동시추진)

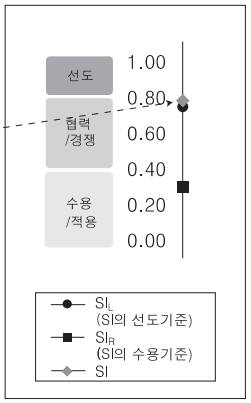
→ : 후행표준(선 기술개발 후 표준화)

표준화 특성	동시표준
표준화-기술개발- IPR 연계방안	유비쿼터스 환경에 필요한 디바이스 인증 기술 개발이 산학연을 중심으로 활발히 진행되고 있기 때문에 해당 기술에 대한 표준화를 국내 및 국제 표준화 기구에 동시에 추진하고 이를 기반으로 국내 디바이스 인증기술에 대한 IPR 확보 기반 마련

• 국제표준화 전략목표 및 세부전략(안)



SI (표준화 전략지수)	
SI_L (SI의 선도기준)	0.74
SI_R (SI의 수용기준)	0.32
SI	0.76



$0 < SI \leq 1$

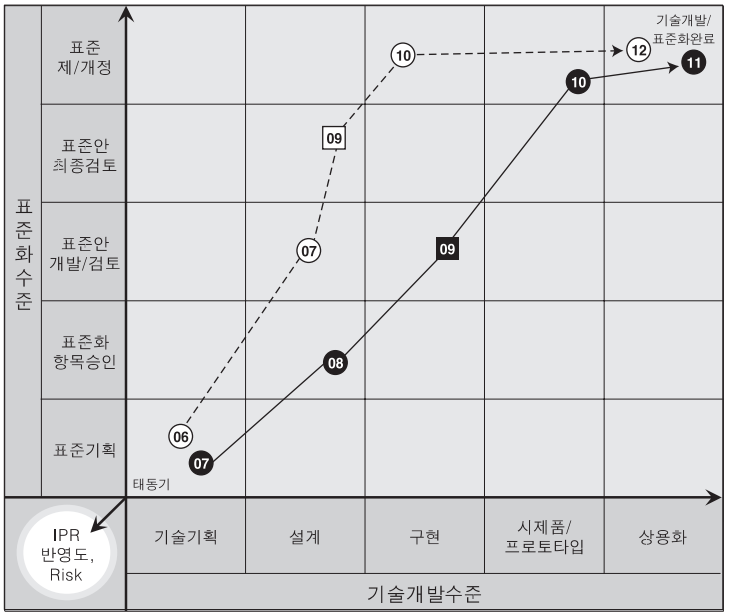
- $SI \geq SI_L$: 선도항목
- $SI_R \leq SI < SI_L$: 협력/경쟁항목
- $SI < SI_L$: 수용/적용항목

국제표준
협력/경쟁(Ver.2009)
⬇
국제표준
선도(Ver.2010)

국제표준화 전략목표	국제표준 선도(Ver.2009) ⟼ 국제표준 선도(Ver.2010)
Trace Tracking (Ver.2009 ⟼ 2010)	- Ver.2009 현황과 동일
세부전략(안)	- 국외대비 국내표준화수준 분석에 따른 전략: ITU-T, IETF, TTA 등 국내외 표준화 단체에서 홈 네트워크 기반의 디바이스 인증서 프로파일 표준이 국내 전문가 주도로 개발되는 등 디바이스 인증 분야 표준화 개발이 활발히 진행됨에 따라, 향후 다양한 분야의 디바이스 인증기술에 대해 지속적인 국제 표준화 추진 - 국외대비 국내기술개발수준 분석에 따른 전략: 국내에서 u-시티 구축 사업 등 정부 및 산업체 주도로 다양한 디바이스를 활용한 사업이 추진 중에 있음. 이에 따라, 산업계 전문가와 공동으로 유비쿼터스 환경에 적합한 디바이스 인증 기술을 개발하고, 해당 기술에 대한 국내 및 국제 표준화 병행 추진 - IPR확보가능성 분석에 따른 전략: 홈네트워크 및 디바이스에서의 인증 방법에 대해서는 국내 특허가 출원되어져 있긴 하지만 그 외 신규 디바이스들에 대한 인증 기술에 대한 특허는 출원이 가능할 것으로 판단됨. 이에 따라, 신규 IT 서비스에 적용될 수 있는 디바이스 인증기술 표준화 추진 시 IPR 확보 가능성 확인 후 병행 추진 - 국내표준화인프라수준 분석에 따른 전략: 디바이스 인증 관련 국내 기술 개발은 ETRI, KISA, LG CNS 등 연구소 및 산업계에서 활발히 진행되고 있으며 관련 기술은 TTA를 통해 국내 표준화로 추진하고 있기 때문에 현재와 같은 선순환 구조를 유지하여 국내 및 국제 표준화 활성화 추진 - 국제표준화기여도 분석에 따른 전략: 국제적으로도 ITU-T, ISO, IETF 등 다양한 표준화 기구에서 디바이스 인증에 많은 관심을 가지고 있고, 국내 디바이스 인증 기술이 다른 국가에 비해 뒤떨어지지 않기 때문에 디바이스 인증 분야에 국내 전문가가 지속적으로 참가한다면 표준화 선도도 가능할 것으로 판단됨
IPR 확보방안	- 기존 인증기술에 대한 표준화 및 특허 등은 이미 출원되어져 있지만 IPTV, VoIP, 센서 등 다양한 디바이스에 대한 기술 개발 및 IPR은 미미한 상태임. 이에 따라, 국내 산업체 및 연구소 등을 통해 개발된 디바이스 인증기술에 대한 국제 표준화를 선행적으로 추진하고, 이를 기반으로 관련 IPR 확보 노력 필요

3.3.5. 일회용패스워드(OTP) 인증 기술 및 응용

• 표준화-기술개발-IPR 연계분석



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

범 례

09 : 중점 표준화항목의 국내상태

09 : 중점 표준화항목의 국제상태

→ : 중점 표준화항목의 국내 표준상태전이

-→ : 중점 표준화항목의 국제 표준상태전이

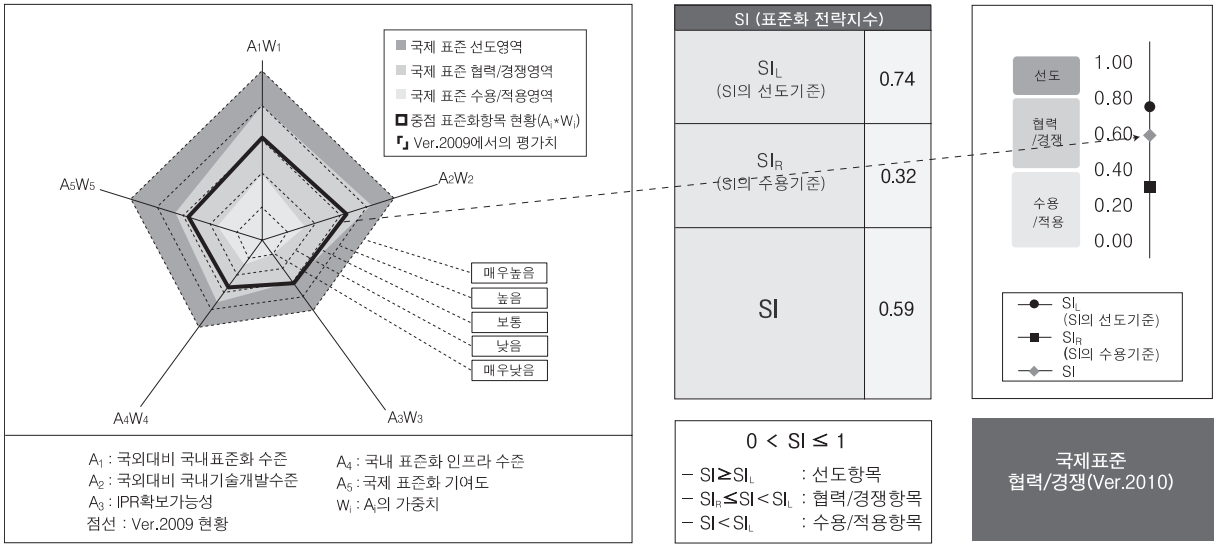
↑ : 선행표준(선 표준화 후 기술개발)

↗ : 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 국제 표준화 추진을 통해 IPR 확보 기반 마련 필요

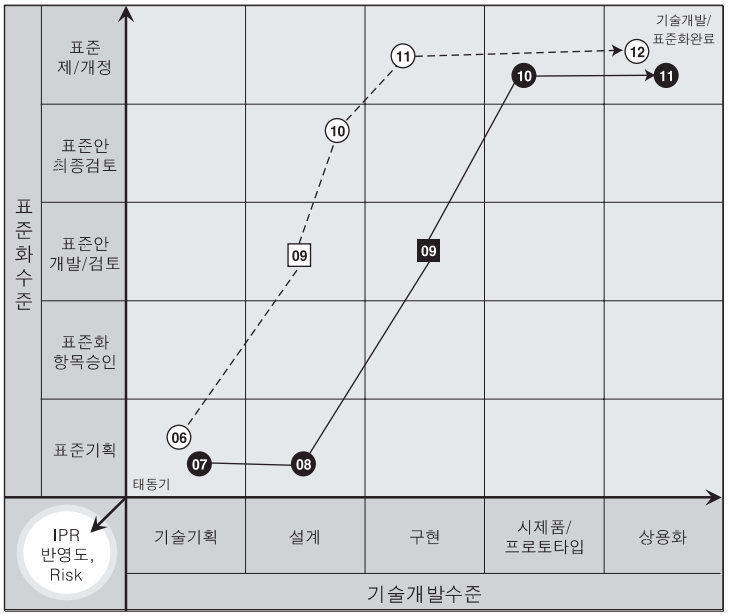
• 국제표준화 전략목표 및 세부전략(안)



국제표준화 전략목표	국제표준 협력/경쟁(Ver.2010)
Trace Tracking (Ver.2009 ⟼ 2010)	- 본 중점 표준화 항목의 경우 Ver.2010 신규 항목임
세부전략(안)	- 국외대비 국내표준화수준 분석에 따른 전략: OTP 인증 기술 및 응용과 관련한 분야의 표준화는 IETF를 통해 OTP 기본 인증기술 들이 표준화되어 있으며, 기존의 TLS, Kerberos 등의 인증 프로토콜과 응용하는 방안도 이미 표준화 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. - 국외대비 국내기술개발수준 분석에 따른 전략: 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 - IPR확보가능성 분석에 따른 전략: 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 - 국내표준화인프라수준 분석에 따른 전략: OTP와 관련한 국내 금융분야의 인프라는 전 세계적으로 매우 우수한 상황이며, 2009년 6월 기준으로 약 300만의 사용자가 OTP를 사용 중에 있음. 또한, 최근 국내 표준화에 대한 인프라도 금융보안연구소 등 금융권 분야를 중심으로 확대되고 있기 때문에, 국내의 선진 기술 및 인프라를 활용한 표준 개발을 통해 국제 경쟁력 확보도 가능 - 국제표준화기여도 분석에 따른 전략: 현재 ITU-T 등 국제 표준화 기구를 통해 OTP 관련 인증 기술에 대한 표준화를 추진하고 있기 때문에, 이를 기반으로 현재 국내 OTP 업체 및 관련 기관의 협조 및 지원을 받아 중장기적으로 OTP 인증기술에 대한 표준화 주도권 확보 가능
IPR 확보방안	- 현재 OTP 기반 기술에 대한 특허가 국내외적으로 많이 출원되어져 있기 때문에 고전적인 OTP 기술에 대한 IPR 확보보다는 다양한 응용에 적용 가능한 OTP 인증기술을 개발하고 이에 대한 IPR 확보 노력 필요

3.3.6. 일회용패스워드(OTP) 인증 프레임워크

• 표준화-기술개발-IPR 연계분석



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

범 례

09 : 중점 표준화항목의 국내상태

09 : 중점 표준화항목의 국제상태

→ : 중점 표준화항목의 국내 표준상태전이

-→ : 중점 표준화항목의 국제 표준상태전이

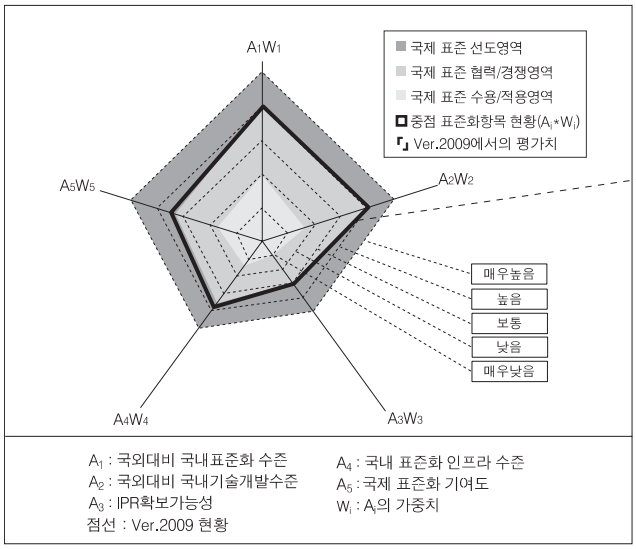
↑ : 선행표준(선 표준화 후 기술개발)

↗ : 동시표준(표준화&기술개발 동시추진)

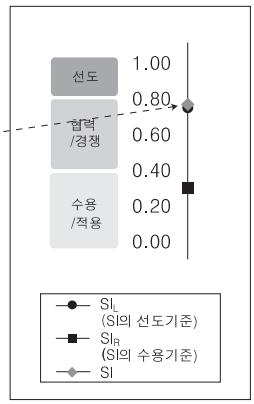
→ : 후행표준(선 기술개발 후 표준화)

표준화 특성	동시표준
표준화-기술개발- IPR 연계방안	OTP 인증 프레임워크 기술의 경우 현재 국내에서 유일하게 추진하고 있는 OTP 관련 기술이기 때문에 해당 기술개발 및 표준화를 동시에 추진하고 이를 통해 국내 및 국제 IPR 확보

• 국제표준화 전략목표 및 세부전략(안)



SI (표준화 전략지수)	
SI_L (SI의 선도기준)	0.74
SI_R (SI의 수용기준)	0.32
SI	0.75



$0 < SI \leq 1$

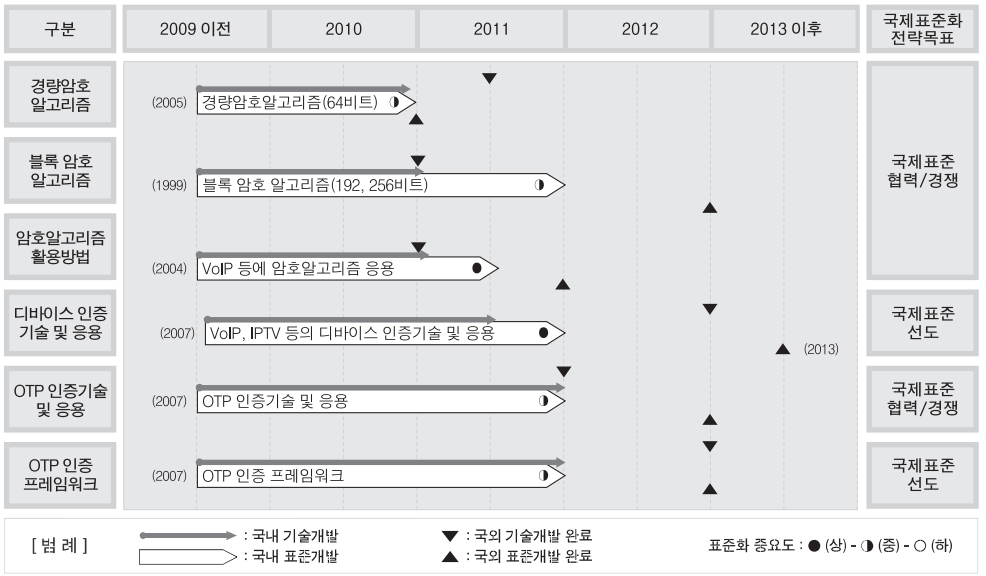
- $SI \geq SI_L$: 선도항목
- $SI_R \leq SI < SI_L$: 협력/경쟁항목
- $SI < SI_L$: 수용/적용항목

국제표준 선도(Ver.2010)

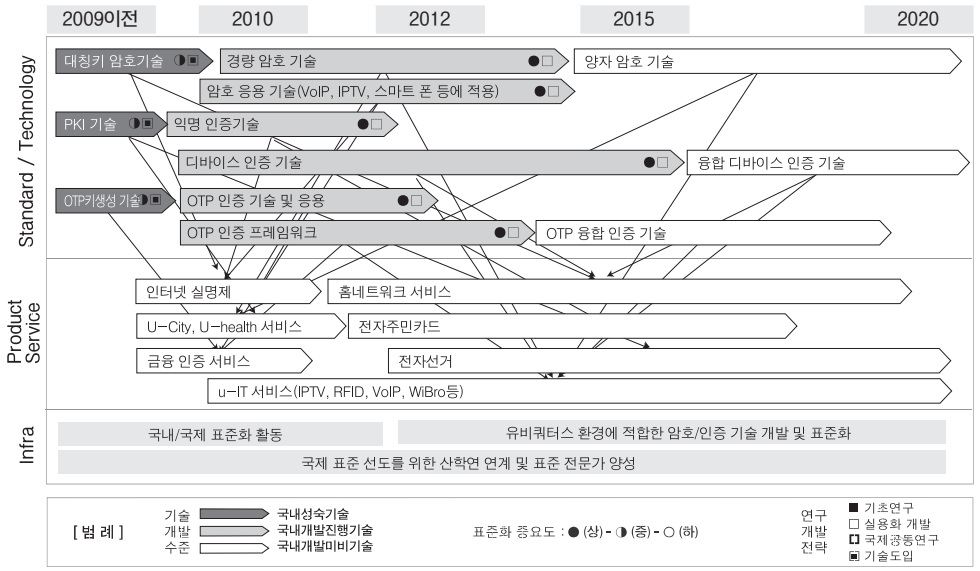
국제표준화 전략목표	국제표준 선도(Ver.2010)
Trace Tracking (Ver.2009 ⟼ 2010)	- 본 중점 표준화 항목의 경우 Ver.2010 신규 항목임
세부전략(안)	- 국외대비 국내표준화수준 분석에 따른 전략: 국제적으로 OTP 생성 알고리즘, 응용 보안 프로토콜, 키 프로비저닝 프로토콜 등의 표준화가 이미 IETF에서 추진 중이지만, 관련 인프라를 구축하고 서비스를 제공 및 관리하는 프레임워크가 존재하지 않음. 따라서 본 중점 표준화 항목과 기존의 표준화된 분야의 차이점을 부각시켜 해당 분야에 대한 국제 표준화 선도가 가능하도록 추진 - 국외대비 국내기술개발수준 분석에 따른 전략: 최근 행안부 등 공공기관, 인터넷 게임 사이트에서 사용자 편의성 제공을 위한 OTP 인증 서비스 관리 및 연동기술 개발 요구가 있기 때문에, 해당 기술 개발에 대한 노하우를 기반으로 OTP 인증에 대한 전반적인 프레임워크 기술을 개발한다면 국내 뿐아니라 국제 표준화 선도 가능 - IPR확보가능성 분석에 따른 전략: 2008년 일회용 패스워드 인증 프레임워크에 대한 특허 출원상태이며 국제 특허 분야에 대한 가능성 확인 후 추진 필요 - 국내표준화인프라수준 분석에 따른 전략: OTP에 관련한 주요 메커니즘의 표준화 인프라는 국외에 비해 뒤쳐진 것으로 판단되지만, 모바일 기기와 OTP의 결합과 같은 융합 환경에서의 응용서비스 기술에 대한 표준화는 국내가 앞서기 때문에 지속적인 관심과 표준화 참여가 이루어진다면 향후 국제 표준화에도 선도적인 역할이 가능할 것으로 판단됨 - 국제표준화기여도 분석에 따른 전략: PKI기반 공인인증서, 바이오인증 등의 멀티팩터 형태로 사용되는 강한 인증 방식들에 대한 개별 관리 프레임워크 표준화가 ITU-T, IETF등에서 제정 및 추진 상태이기 때문에 해당 국제 표준화 인프라를 기반으로 OTP 인증 프레임워크 및 멀티팩터 인증프레임워크들간 연동 및 관리에 대한 국제 표준화 적극 추진
IPR 확보방안	- OTP 인증 프레임워크의 경우 현재 국내에서 유일하게 추진하는 표준이기 때문에 해당 기술에 대한 국내 및 국제 표준화 선행 추진 후 이를 기반 국내외 IPR 확보 추진

3.4. 중장기 표준화로드맵

3.4.1. 중점 표준화항목별 중기('10~' 12) 표준화로드맵



3.4.2. 장기 표준화로드맵(10년 기술예측)



[국내외 관련 표준 대응리스트]

구 분	표준명	기구(업체)	제정연도	제개정현황	국내 관련표준	국내 추진기구
암호 기술	FIPS 46-3 Data Encryption Standard	NIST	1999	재재개정	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	재개정		TTA/ISTF
	FIPS 185 Escrowed Encryption Standard(EES)	NIST	1994	초안		TTA/ISTF
	FIPS 186-2 Digital Signature Standard (DSS)	NIST	2001	재개정		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 J/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
	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

구 분	표준명	기구(업체)	제정연도	제개정현황	국내 관련표준	국내 추진기구
암호 기술	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 RFC 3820 Internet X.509 Public Key Infrastructure Proxy Certificate Profile	JTC1/SC27 /WG2 IETF	1997 2004	초안 초안		TTA/ISTF TTA/ISTF
인증기술	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
	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

구 분	표준명	기구(업체)	제정연도	제개정현황	국내 관련표준	국내 추진기구
인증기술	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 /WG2	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	ISO/IEC JTC1/SC6	2000	초안	TTAS.IT -X.509/R2	TTA/ISTF
	X.509 Information Technology - OSI - The Directory: Public-key and Attribute Certificate framework	ITU SG7	2000		TTAS.IT -X509/R2	TTA/ISTF
일반 응용중 전자우편보안	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
	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]

〔2〕 TTA, 정보통신표준활용맵2009, 2009.4.
〔3〕 KISA, 건전한 암호이용 활성화 방안 마련을 위한 보고서, 2002.12.
〔4〕 KIISC, 국내외 암호관련 법제도 현황, 2005.4.
〔5〕 KISA, 다양한 보안프로토콜에서의 SEED 이용 가이드라인, 2008.6.
〔6〕 KIISC, 선진국 민간분야 암호사용실태 및 사용정책동향연구, 1998.11.
〔7〕 KISA, 암호 알고리즘 및 키 길이 이용 안내서,
〔8〕 KISA, 암호이용 가이드라인, 2007.12.
〔9〕 KISA, 암호이용기반구축 보고서, 2004.12.
〔10〕 KISA, 암호정책 수립 기준 설명서, 2008.10.
〔11〕 전자통신동향분석, NIST의 키 관리 표준, 17권 제5호, 2002.10.
〔12〕 KISA, SEED 소스코드 매뉴얼 v1.0, 2008.6.
〔13〕 TTA, IT 839전략 표준화 로드맵 Ver. 2007, 2006.12
〔14〕 2006년도 정보통신 기술수준 조사 보고서, 2006.7
〔15〕 텔레매틱스 표준화 포럼, www.kotba.or.kr
〔16〕 정보통신용어사전, www.tta.or.kr
〔2〕 KIPA, 국내 정보보호 시장 동향과 전망
〔3〕 IDC, Worldwide and U.S Security Services 2006-2011 Forecast and Analysis
〔4〕 씨큐어넷, 2007년 정보보호 동향
〔5〕 KISA, 2008 국내 정보보호 산업 시장 및 동향 조사, 2008. 12
〔6〕 www.verisign.com
〔7〕 www.cm-la.com
〔8〕 www.ietf.org
〔9〕 www.wimaxforum.org
〔10〕 http://www.trustedcomputinggroup.org/
〔11〕 www.utrend.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