정보통신 중점기술 표준화로드맵
Ver. 2008

TTA-07100-SA

Telecommunications Technology Association

ICT Standardization Roadmap 2008

종합보고서 6
지식 · 정보보호 분야

Contents

지식 · 정보보호 분야 : 총괄 염흥렬 PM

정보통신 중점기술

표준화로드맵

Ver. 2008 종합보고서❻

ICT Standardization Roadmap 2008

지식 · 정보보호 분야

- 암호 · 인증 · 권한관리
- 개인정보보호 및 ID관리
- 네트워크 및 시스템보안
- 응용보안/평가인증
- 바이오인식

암호 · 인증 · 권한관리

1. 개요

1.1. 기술개요

1.1.1. 중점기술 및 표준화항목의 정의

• 중점기술의 정의

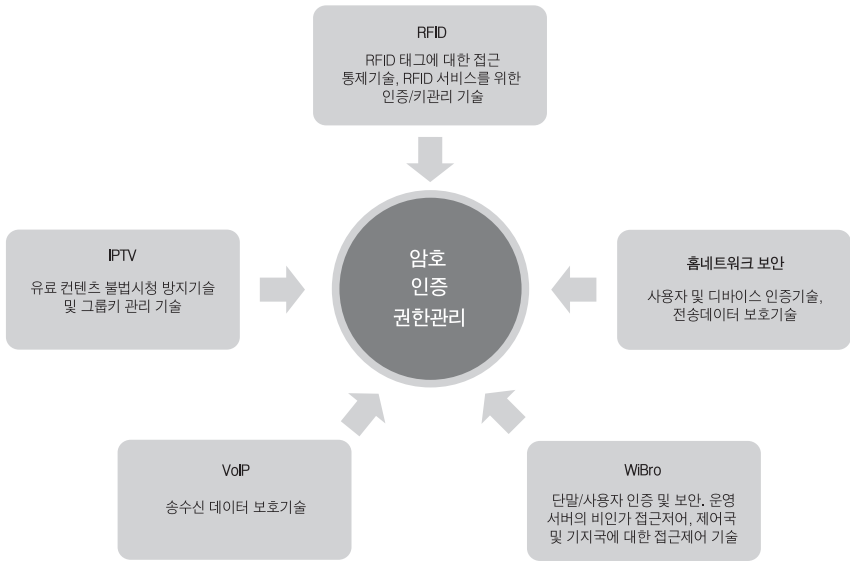
- 암호 · 인증 · 권한관리는 정보통신망을 통한 정보의 안전한 전송 및 이용, 정보통신망 상의 상대방에 대한 신원 확인, 정보통신망을 통한 불법적인 접근을 통제하기 위한 기반기술임
- 암호기술은 정보통신망을 통한 안전한 정보의 송수신을 위한 프리미티브로서 암호 알고리듬, 암호 키 관리 기술, 암호 응용기술 등으로 구분할 수 있음
- 인증기술은 정보통신망에서 상대방의 신원을 확인하기 위한 기술로서 PKI, 익명인증기술 등으로 분류할 수 있음
- 권한관리기술은 정보통신망을 통해 정보를 이용하고자 하는 자가 적절한 권한을 가지고 있는지를 판단하기 위한 것으로서 PMI, 하드웨어 기반의 접근제어 등으로 구분할 수 있음

• 표준화항목의 정의

구분	정의	대상 표준화항목	표준화 내용
암호	암호기술은 기밀성, 무결성, 메시지 인증, 사용자 인증, 부인방지 등의 보안서비스를 위해 요구되는 핵심 보안알고리듬을 정의	암호 알고리듬	암호알고리듬은 블럭 암호 알고리듬, 스트림 암호 알고리듬, 공개키 암호알고리듬, 키분배 알고리듬, 해쉬 알고리듬, 전자서명 알고리듬, 난수발생기 및 양자 암호알고리듬 등으로 분류
		암호 키 관리	개인키 암호화 기술, 패스워드 기반의 암호화 기술, 비밀정보 교환기술, 보안토큰내의 비밀정보 저장기술, 암호 키 복구 기술 등 암호 키를 안전하게 생성 · 분배 · 복구 · 폐기하는 기술
		암호 응용 기술	암호메시지 전송기술, 암호토큰 인터페이스 기술 등 응용서비스에서 암호기능에 대한 공통 플랫폼을 제공하는 기술
인증	인증은 사용자의 신원을 확인하기 위한 기술	PKI (Public Key Infrastructure)	인증서 프로파일, 인증서 관리 프로토콜, 인증서 운영프로토콜, 인증서 검증 프로토콜, 사용자 인터페이스 기술, 전자서명 키 보호기술 등을 이용하여 전자거래에서 부인방지, 무결성, 인증 등의 정보보호서비스를 제공하기 위한 기술
		익명 인증 (Anonymous Authentication)	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
권한관리	기업 및 기관 단위에서 사용자들에게 특정 시스템 및 애플리케이션에 접근할 수 있는 권한을 차등 부여해주는 기술	PMI (Privilege Management Infrastructure)	속성인증서 프로파일, 속성인증서 관리프로토콜, 속성인증서 운영프로토콜, 속성인증서 검증프로토콜, 사용자 인터페이스 기술 등 속성인증서를 이용하여 사용자에 대한 권한을 관리하기 위한 기술
		HW 기반 접근제어	OTP, 스마트카드, RFID, USB토큰 등 하드웨어를 기반으로 권한관리 프로토콜, 권한관리 API, 관한관리 운영지침 등으로 분류

1.1.2. 연관기술 분석

• 연관기술 관계도



• 연관기술 분석표

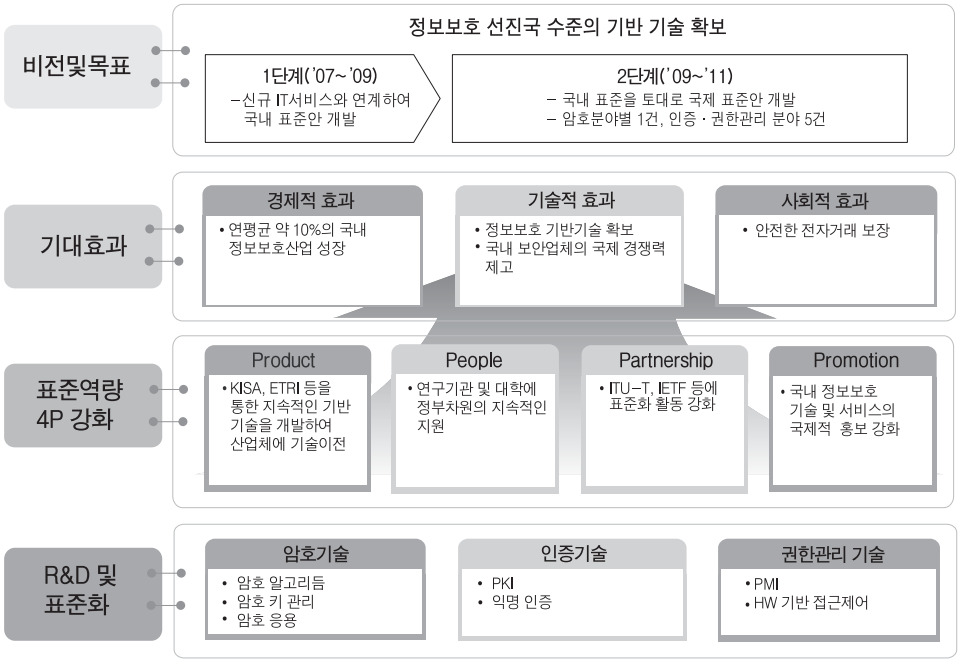
연관기술	내용	표준화기구/단체		표준화수준		기술개발수준	
		국내	국외	국내	국외	국내	국외
RFID	RFID 태크의 접근을 제어할 수 있는 인증 및 키 관리 기술	TTA/USN 포럼	IETF, ITU-T	표준안 개발/검토	표준안 개발/검토	상용화	상용화
IPTV	IPTV 서비스에서 유료 컨텐츠의 불법시청 및 복제을 방지하기 위한 기술	TTA	IETF, ITU-T	표준안 개발/검토	표준안 개발/검토	상용화	상용화
홈 네트워크 보안	안전한 홈 네트워크 서비스를 제공하기 위해 홈 내부 및 원격 사용자에게 보안서비스를 제공하기 위한 기술	TTA/홈네트워크 보안포럼	ITU-T	표준안 개발/검토	표준안 개발/검토	구현	구현
VoIP	송 · 수신 데이터에 대한 보호기술	TTA	ITU-T	표준안 개발/검토	표준안 개발/검토	구현	구현
WiBro	와이브로 서비스에서 단말 및 사용자에 대한 인증기술 및 제어국 · 기지국의 접근을 제어할 수 있는 기술	TTA	IEEE	표준제정	표준제정	상용화	구현

1.2. 추진경과 및 중점 추진방향

- 추진경과
  - 2004년도에는 모든 분야에 대한 표준화 항목을 정리하였음
  - 2005년도에는 TTA를 통하여 수행되지 않고 한국정보보호진흥원을 통하여 수행되었으며, 주로 IT839와 연계된 정보보호 표준분야를 정리함
  - 2006년도에는 정부의 추진의지가 강한 VoIP 분야를 포함한 응용서비스 정보보호분야와 최근 ITU-T와 IETF 등의 국제표준화기구에서 활발하게 국제표준화가 추진 중인 네트워크 정보보호분야를 중점적으로 정리함
  - 2007년에는 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 정리함

- 중점 추진방향
  - 유비쿼터스 사회에 적합하도록 사람, 사물, 기기 등을 포괄할 수 있도록 암호, 인증, 권한관리 기술에 대한 표준화를 중점 추진
  - 암호기술과 관련하여 사이드채널 공격을 고려하여 암호의 하드웨어 구현에 관한 표준화 가능성을 모색하고 해쉬함수의 안전성에 대한 문제가 제기됨에 따라 미국에서 차세대 해쉬 함수 공모가 시작될 것으로 보이는 바, 이에 부응한 차세대 해쉬 함수 개발 가능성을 모색할 필요가 있음. 또한 사이버 범죄에 대한 대책과 개인정보보호의 필요성이 충돌하는 것을 해결하기 위하여 개인 정보를 암호화하여 저장하고 합법적인 요구 발생시 추적할 수 있는 기술에 대한 표준화도 필요
  - 더불어, 무조건적인 안전성을 보장하는 양자암호는 미래 IT 환경 및 양자 컴퓨팅 환경에서 정보보호문제를 해결할 수 있는 핵심원천기술로서 기술적, 산업적 파급효과가 매우 커 양자암호의 요소기술에 대한 표준화가 필요함
  - 인증기술과 관련하여 지금까지는 사람에 대한 신원확인을 목적으로 하는 인증에서 기기, 사물을 포괄하는 인증기술로 표준화를 확대하고, 더불어 인터넷 실명제 등에 적합한 익명인증 기술로서 익명인증체계, 익명인증 프로토콜 및 익명인증서 프로파일 등에 대한 표준화를 중점 추진
  - 권한관리 기술과 관련하여 PMI 등 속성인증에 대한 표준화가 국외에 비해 거의 이루어지고 있지 않으므로 이 분야를 중심으로 표준화 추진하는 한편 유비쿼터스 사회에서의 정보시스템에 대한 접근 방법은 단순히 패스워드에 의존하는 것이 아니라 스마트카드 등 다양한 하드웨어를 접근매체로의 사용이 확대될 것으로 예측되므로 이러한 분야에 대해서도 기술 및 표준화 추진

1.3. 표준화의 Vision 및 기대효과



1.3.1. 표준화의 필요성

- 암호, 인증, 권한관리는 정보보호 기반 기술이므로 정보보호 시스템의 상호호환성, 안전성, 신뢰성을 보장하기 위해서는 표준화가 필수적으로 중요한 요소임
- 따라서 유비쿼터스 사회의 정보보호시스템을 준비하기 위해서는 암호알고리듬에 대한 원천기술은 물론 암호 응용기술, 익명인증 및 하드웨어 기반 접근제어 기술 등에 대한 표준화가 필요

- 암호, 인증, 권한관리는 정보보호에서 기반이 되는 기술임. 따라서 기반기술에 대한 상호호환성, 안전성, 신뢰성은 매우 중요한 요소임. 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 옴. 특히 암호알고리듬의 경우, SEED, KCDSA, HAS-160 등을 포함하여 차세대 암호로서 HIGHT, FORK256 등 컴퓨팅 및 정보보호 기술의 변화에 따라 기술개발 및 표준화를 추진하여 옴. 인증기술의 경우는 국내에서 가장 많이 활용되고 있는 PKI 관련하여 국제 표준의 수용 및 국내 자체 기술개발을 통하여 전반적 표준화를 진행하여 전체 PKI 체계가 원활히 움직일 수 있도록 하였음
- 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

- 그러나 아직도 암호응용, 익명인증, 권한관리 관련 분야에서는 표준화가 미미하기 때문에 다가오는 유비쿼터스 사회의 정보보호 시스템 개발을 위한 준비에는 부족한 부분이 있다. 따라서 이러한 부분에 있어서 좀 더 적극적인 표준화 활동이 필요

1.3.2. 표준화의 목표

- 암호 기술과 관련해서는 유비쿼터스 사회에 적합한 대칭키 · 공개키 · 스트림 암호 알고리듬에 대한 원천기술을 확보하여 2012년까지 각 분야별 국제표준 1건 보유
- 인증 및 권한관리 기술과 관련해서는 현재 표준화가 미미한 분야인 익명인증, 하드웨어 접근관리 등에 대한 표준화 추진하여 이 분야에 대해 2012년까지 국제표준 5건 보유

※ 2007년 6월 현재 국제 표준 전무

- 암호 기술의 경우 국내에서 개발한 경량 암호 알고리듬, 256비트 해쉬 알고리듬, 스트림 암호 알고리듬 등에 대해 2008년부터 경량 암호 알고리듬부터 단계적으로 국제 표준화를 추진하여 2012에는 분야별 1개 이상의 국제 표준을 보유할 수 있도록 추진
- 인증 기술의 경우 2008년까지 익명인증체계 및 익명인증서 프로파일, 2009년까지 익명인증 프로토콜에 대한 국내 표준을 개발하여 2009년부터 단계적으로 국제 표준화 추진
- 권한관리 기술의 경우 국내 표준도 아직 준비되지 않은 상황이므로 2008년부터 2009년까지 속성인증 및 하드웨어 접근관리 분야에 대한 기술 및 표준안을 준비하여 2010년부터 국제 표준화 추진

1.3.3. Vision 및 기대효과

- 국내 정보보호 제품의 국제 경쟁력 강화
- 암호 · 인증 · 권한관리 기반을 구축하여 안전하고 신뢰할 수 있는 u-사회 구축에 기여

- 암호, 인증, 권한관리 기술은 모든 정보보호 제품의 기반 기술이므로 이러한 기반 기술 확보를 통해 국내 제품의 국제 경쟁력을 제고
- 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

- 한국정보보호진흥원이 발표한 2006년도 국내 정보보호 매출은 2005년 보다 7.9% 증가한 약 7,348억 원으로 나타났으며, 분야별로는 정보보호제품이 7.2% 성장한 약 6,252억 원에 이르렀으며, 정보보호서비스는 이보다 성장률이 높은 12.7%로 약 1,096억 원의 시장을 형성함
- 전체 매출에서 시스템 및 네트워크 정보보호제품은 약 85%, 정보보호서비스는 약 15%를 차지했는데 다른 IT산업 분야와 마찬가지로 정보보호 산업도 서비스분야의 증가율이 높음
- 암호 응용분야 중에 하나인 콘텐츠 보안 분야는 정보보호제품 중에서 성장률이 두드러진 분야임
- 콘텐츠 보안은 2006년도에 약 326억 원으로 나타나 2005년 약 273억 원보다 19.1% 높게 성장했으며, 향후에도 전체적으로 12%대의 성장률을 보여 2011년에는 555억 원 정도의 시장을 형성할 것으로 예상되는 가운데 특히 DRM 분야의 성장률이 약 24% 예상되어 DB보안의 5% 성장보다 훨씬 높게 시장이 형성될 것으로 전망
- 또한 양자 암호기술에 대한 국내 시장은 2011년 약 855 억원의 시장이 형성될 것으로 예측되고, 이는 양자암호기술의 응용서비스인 VPN의 정보보호 시장 점유율인 7.2%를 반영한 것이지만 아직 양자 암호기술은 이론 및 실증실험 단계에 머물고 있어 아직 상용화 제품은 전무하지만 가까운 미래에 상용화가 이루어지면 절대적 안전성이 요구되는 국방, 금융, 외교 분야에 수요가 급증할 것으로 예상

〈표1〉 콘텐츠 보안 분야 매출전망(단위 : 억원)

구 분	2005년	2006년	2007년	2008년	2009년	2010년	2011년	CAGR(%)
DB보안	195	208	220	232	244	256	268	5,41
DRM	78	118	158	190	222	254	286	24,28
합 계	273	326	378	422	466	510	554	12,52

※ 출처 : 한국정보보호진흥원, 2006 국내 정보보호산업 통계조사, 2006

- 공개키기반구조(PKI)는 2006년도에 약 177억 원으로 2005년 약 161억 원보다 약 10% 증가한 것으로 나타났으며, 향후 2011년까지 8%대의 연평균 성장률을 보여 260억 원대 규모에 이를 것으로 전망
- 또한 인증서비스는 2006년에 약 75억 원으로 2005년도 약 65억 원보다 14% 성장하였으며, 전체적으로 2011년까지 연평균 성장률이 약 11%에 달해 약 120억 원에 이를 것으로 전망

〈표2〉 콘텐츠 보안 분야 매출전망(단위 : 억원)

구 분	2005년	2006년	2007년	2008년	2009년	2010년	2011년	CAGR(%)
PKI	161	177	194	210	227	243	260	8,32
인증서비스	65	75	84	93	102	111	120	10,69

※ 출처 : 한국정보보호진흥원, 2006 국내 정보보호산업 통계조사, 2006

- 통합접근관리(EAM), 싱글사인온(SSO), 통합계정관리(IM/IAM) 등이 포함된 접근관리 분야는 2006년도에 약 91억 원으로 나타나 2005년 약 112억 원보다 19% 감소했지만 2007년도에는 약 113억 원으로 다시 증가해 2011년에는 약 191억 원의 시장을 형성하며 연평균 9.28%의 성장을 보일 것으로 전망

〈표3〉 접근관리 분야 매출전망(단위 : 억원)

구 분	2005년	2006년	2007년	2008년	2009년	2010년	2011년	CAGR(%)
EAM	62	39	46	53	60	67	74	2,94
SSO	19	30	40	48	56	63	70	24,46
IM/IAM	31	22	28	34	39	43	47	7,16
합 계	112	91	114	135	155	173	191	9,28

※ 출처 : 한국정보보호진흥원, 2006 국내 정보보호산업 통계조사, 2006

- 2006년 국내 정보보호산업 통계조사(한국정보보호진흥원)에 따르면 전체적으로 국내 정보보호 산업의 시장규모는 완만한 성장을 보이고 있는 가운데 2006년도 7,348억 원대인 매출규모는 2011년에는 1조 1,823억 원대 규모에 이를 것으로 전망되며, 이 기간 연평균 성장률은 전체 9.64%로 예상되며 서비스가 조금 높은 성장률을 보일 것으로 전망

2.1.2. 국외 시장 현황 및 전망

- 세계 정보보호시장은 과거 3년간 17.84%의 고성장을 지속하였으며, 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
- 국내 정보보호시장은 과거 3년간 연평균 8.3% 성장하였으나 세계 정보보호시장 성장률과 비교하면 절반수준에 불과함

〈표5〉 국내외 정보보호 시장 성장률

(단위:억원(국내), 백만달러(세계), 환율 1,000원)

구분	2004	2005	2006	3년간 CAGR(%)
세계(A)	27,447	32,331	38,114	17.84
국내(B)	6,261	6,807	7,348	8.33
점유비율(B/A, %)	2.28	2.11	1.93	

※ 출처 :국내정보보호시장(KISA), 세계 정보보호시장(IDC, 2006 Black-Book)

- 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

〈표7〉 u-정보보호 관련 현 정보보호 요소기술 경쟁력 분석

구분	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
인프라 측면	인프라보호기술	BcN 보안(IPv6 포함)	0.7	95.0
		소프트인프라웨어 보안	1.3	90.0
		RFID/USN 보안	0.5	95.0
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

〈표8〉 미국과의 정보보호 제품 경쟁력

구분	미국과의 제품 경쟁력 조사		수출비중	수입시장
	격차	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%
합계	1.40년	84%	100%	100%

※ 출처 2005년 국내 정보보호산업 통계조사, KISA

2.2. 기술개발 현황 및 전망

2.2.1. 국내 기술개발 현황 및 전망

• 정부정책기조

- 정보통신부는 2006년 유비쿼터스 정보보호 기본전략에서 안전한 정보인프라 구축, IT서비스 신뢰기반 확보, 이용자의 프라이버시 보호 등 세 부분으로 구분하여 기술개발 전략을 수립
- 안전한 정보인프라 구축에서는 'u-IT 인프라 보호 및 무선 보안 기술 개발', '침해확산 방지 및 디지털 포렌식 기술개발'을, IT서비스 신뢰기반 확보에서 '범용 인증기술 개발', 'u-지식 및 지재권 보호기술 개발'을, 이용자의 프라이버시 보호에서는 '개인정보보호 및 프라이버시 보호기술개발', 'RFID/USN 정보보호기술' 등을 중점과제로 정하고 있음
- 특히, 범용인증기술 개발과 관련하여 기존 인터넷 사업자별로 보유한 전용 ID를 사용하는 환경에서, 향후에는 네트워크 및 서비스 사업자와 무관하게 사용자의 대표 ID로 모든 서비스를 이용할 수 있는 환경으로 변화할 것을 예상하여 최소한의 ID로 다양한 서비스를 끊김 없이 제공하기 위한 u-ID카드, u-ID 인증 인프라 등 범용 인증 체계의 기반기술을 개발하고 BcN, UsN, 소프트인프라웨어 등 유비쿼터스 인프라를 이용하여 사용자의 프라이버시를 보호할 수 있도록 범용 ID를 제공할 수 있는 기술을 개발할 계획
- 더불어 2007년 정보통신 국제표준화 추진전략(안)에서도 10대분야 36대 중점기술에 정보보호를 포함하고 있어, 정보보호 관련 국제표준화도 한층 더 힘을 받을 것으로 전망

• 암호기술

- 국내 암호기술은 대칭 암호 알고리듬인 SEED, 전자서명 알고리듬인 KCDSA, 해쉬 알고리듬인 HAS-160, 패스워드 기반 키 분배 방식인 AMP, C2C-PAKA를 가지고 있으나, 공개키 암호 알고리듬, 난수 생성 함수 및 키 합의 알고리듬 등 일부 알고리듬에 대한 개발 및 표준이 부족한 상태임
- 따라서 이러한 일부 원천 기술의 미흡으로 인하여 선진국에 비하여 1.3년 정도 뒤져있다고 판단
- 국내의 경우, 2001년 암호 키 관리 시스템을 시범 구축하는 등 암호기술 개발을 위한 기반을 마련하여 왔으며, 현재 ARIA, HIGHT 등 다양한 암호 알고리듬이 개발되었고, FORK256 등 해쉬 알고리듬이 개발되는 등 선진국 수준과 기술 격차를 줄이고 있다고 할 수 있음

◦ 대칭키 암호 : 1998년 민간 표준으로 사용하기 위한 블록 암호 SEED가 개발된 이후로, 신규 대칭키 암호 설계에 대한 연구가 활발히 진행되고 있으며, 2004년에는 블록 암호 ARIA가 한국 산업 규격 KS 표준으로 제정되었고 2006년에는 초경량 환경에 적합한 블록 암호 HIGHT와 T 함수 기반 스트림 암호 TSC-4가 개발되었지만, 대칭키 암호에 대한 안전성 분석 기술에 대한 연구는 차분 공격법이 제안된 이후로 활발히 진행되고 있음. 초기에는 국내에서 독창적으로 제안된 안전성 분석법이 없어 선진국에서 제안된 공격법을 활용하는 수준에 불과하였지만, 현재는 선진국과 동등한 수준의 기술력을 가지고 있음. 그 결과, 일부 대학에서는 신규 합성 분석 기법인 연관키-렉탱글

공격, 포화-비선형 공격, 연관키 차분-비선형 공격 기법을 개발함. 그러나 대칭키 암호 기술은 KISA, ETRI, NSRI, 고려대학교 등과 같은 소수 그룹에 한정되어 연구되고 있는 실정임

◦ 공개키 암호 연산 고속화 : 일부 국내대학과 연구소에서 RSA 공개키 암호 시스템과 DLP(Discrete Logarithm Problem)기반의 암호시스템을 위한 효율적인 지수승 알고리듬, 타원곡선 암호시스템을 위한 효율적인 유한체 연산 기법과 타원곡선 연산 속도 개선 알고리듬을 발표하였고, ID 기반 암호시스템에서 사용되는 pairing 연산을 고속화하기 위한 방법들이 발표된 사례가 있음

◦ 사이드 채널 공격 : 국내의 대학과 연구소에서 주로 연구가 이루어지고 있지만 선진국 수준에 비하여 미흡한 실정임. 주로 알고리듬 차원에서 DPA(Differential Power Analysis Attack) 또는 Timing attack을 피할 수 있는 방법들에 대한 연구가 일부에서 이루어지고 있으며 SEED, ARIA 등에 대한 다양한 분석 방법과 대응 방법에 대한 연구가 활발히 진행되고 있음

◦ 키 설정 메커니즘 : 주로 표준화된 기술들을 제품에 그대로 적용하고 있는 실정

◦ 암호 응용 프로토콜 : 주요 대학에서 연구 결과를 발표하고 있으며, 전체적으로 세계적인 수준에 근접하고 있는 것으로 파악되고 있음

◦ 해쉬 알고리듬 : 해쉬 알고리듬 설계 및 분석 기술은 세계 수준에 근접한 것으로 판단됨. 국내 표준 알고리듬인 HAS-160이 개발된 이후로 지속적으로 MD4 기반 해쉬 함수와 FORK-256 해쉬 함수가 개발됨

◦ 양자 암호기술: ETRI, KIAS 등의 연구소와 국내 대학을 중심으로 연구가 이루어지고 있으 나, 선진국에 비해 매우 미흡한 수준. 광섬유를 이용한 양자 암호통신의 이론 및 기초 실증 실험에 대한 연구가 수행되고 있음

- 암호 모듈 평가와 관련하여 국내에서는 독창적인 통계적 검증 방법 또는 암호 모듈 안전성 평가 기술이 일부 확보되었으나 아직까지는 미흡한 실정. 현재 NIST의 CMVP와 유사한 암호 모듈 평가 체계에 대한 연구가 NSRI 등에서 진행되고 있고, 최근 암호 모듈 평가를 2005년도 시범사업을 거쳐서 2006년부터 본격적으로 시행 중. 현재 우리나라와 정보보호 선진국간의 기술 격차는 1-2년 정도가 되는 것으로 평가

• 인증기술

- PKI 기술개발업체는 무선 공개키 인증 분야에서 세계 최초로 상용 서비스를 개발하는 등, 일부 분야에서 선진국과 거의 비슷한 정도의 기술력을 갖고 있는 것으로 판단되나, 아직 원천 기술 및 프로토콜 설계 분야에서 뒤쳐져 있다고 볼 수 있음. 또한 다양한 인증 서비스를 위한 응용 기술이 실용화되고 있으며, 인터넷 뱅킹 등의 금융 분야를 중심으로 하는 인증 응용 분야에서는 상당한 기술경쟁력을 갖고 있는 것으로 평가

- PKI, PKCS, 그리고 커버로스 보안 기술은 PKI 기술을 중심으로 개발, PKI 기술의 경우, 국제 표준의 채용을 통한 상호연동성 보장, 인증서 정책 기능의 강화 및 용이한 적용, 소규모에서 대규모까지 시스템 규모 가변성 보장 등이 이루어지고 있음. 또한 무선 공개키 기반구조를 위한 시스템 기술이 개발되고 있고, 온라인 인증서 상태 확인 프로토콜 등의 VA(Validation Authority) 기능의 강화, 키 복구 기능의 강화, 사용자의 이동성을 보장하기 위한 스마트카드 등 이동성 저장매체 이용, 전자서명 알고리듬으로 타원곡선 암호 도입, 유 · 무선 통합형 인증 제품,

의료 · 교육 분야 등의 다양한 응용 서비스 분야에 연계되고 있는 제품이 속속 개발되고 있음

- 또한 정보통신부는 한국정보보호진흥원 및 한국 PKI 포럼을 중심으로 2001년부터 1,000만명 전자서명 인증서 갖기 운동을 대대적으로 추진함. 이를 위해 정보통신부는 6개의 공인인증기관을 전자서명법에 의하여 지정한바 있음. 또한 보편적 서비스 차원에서 공인인증서의 용도에 관계없이 모든 개인 및 법인의 인증서를 전자민원에 사용하도록 하는 정책, 범용 공인인증서에 대한 수수료정책 등 정부차원의 정책적 지원도 다양하게 이루어 짐. 따라서 현재 PKI 기반의 인증서비스는 세계적 경쟁력을 가질 수 있는 수준에 도달함
- 무선 인터넷 보안은 무선 공개키 기반구조를 토대로 인증 제품, 서비스, 그리고 응용이 개발되었고 타원곡선 암호를 이용한 공개키 기반구조 제품과 응용들도 개발되고 있음. 이는 우리나라가 상당한 서비스 제공 능력과 무선 공개키 기반구조 분야에서 상당한 기술력을 보유하고 있다는 증거
- 향후에는 인터넷 실명제에 적용할 수 있는 익명 인증뿐만 아니라 무선 인터넷에서 간편하게 사용할 수 있는 인증 방법들에 대한 연구가 필요할 것으로 전망. 현재 익명 인증은 공개키 기반 구조를 위한 익명 인증 기술 및 서비스 등이 학술적인 단계에서 연구가 이루어지고 있으나, 상용 서비스는 이루어지고 있지 않음

• 권한관리기술

- 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 되었고, ITU-T는 PKI와 덧붙여 권한관리 기반구조(PMI : Privilege Management Infrastructure)를 표준화함. 권한관리 기반구조는 다양한 응용환경에서 특정자원에 접근할 수 있는 권한을 차등 부여함으로써 관련 자원과 소유자간의 관계를 신뢰기관이 보증하고 유지하는 체계를 의미
- 20001년부터 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
- HW 기반의 접근제어 기술의 경우 2005년 고액 금융거래 이용자에 대해 OTP 또는 보안토큰의 이용을 의무화하면서 점차적으로 기술개발에 대한 관심이 높아짐. 2007년에는 금융거래 분야에서 OTP 사용을 위한 시스템 및 서비스를 준비 중에 있고, 보안토큰에 대해서도 KISA가 중심이 되어 이용기반을 마련 중에 있음. 향후 u-IT 서비스가 증가하면서 다양한 HW 기반의 접근제어 기술이 개발될 것으로 전망

2.2.2. 국외 기술개발 현황 및 전망

• 주요국가의 정책기조

- 미국의 경우 NIST는 정보보호기반 기술에 대한 표준, 평가 지수, 시험 및 실증 방법을 개발하여 IT 보안성을 높이기 위한 계획, 관리, 운용, 실용화에 대한 가이드라인을 개발하며, NIST의 STG(Security Technology Group)에서 연방 정부에 필요한 정보의 기밀성, 완전성 및 정당성을 지키기 위해 암호 기법을 개발. 표준 제정 이후에도 NIST는 5년마다 암호 알고리듬과 암호 표준을 수정하도록 하여 지속적인 기술 개발을 요구. 양자 암호의 경우 국가차원의 R&D 및 상용화 로드맵(ARDA) 마련하여 연구개발을 촉진하고 있음
- 유럽의 경우 유럽 연합의 정보사회기술 프로그램(Information Societies Technology Programme)의 일환으로 실시되고 있는 ECRYPT에서 2004년부터 EU의 정보보호 연구자를 지원하고 있으며, STVL(Symmetric Techniques Virtual Lab), ATVL(Asymmetric Techniques Virtual Lab), PVL(Protocols Virtual Lab), SEIVL(Secure and Efficient Implementation Virtual Lab), WPHVL(Watermarking and Perceptual Hashing Virtual Lab) 등 5개 분야로 나누어 활동하고 있음. 현재 2007년부터 2013년, 또는 그 이후에 사용될 수 있는 정보보호 기반 기술 개발 및 양자 암호에 대한 기술개발을 계획하고 있음
- 일본의 경우 IPA/SEC에서 기술 개발 상황을 파악하여 기술 개발이 이루어지고 있으나 아직 상용화되지 않은 기술 또는 위험성이 큰 기술에 대한 개발 또는 연구를 수행하고 있음. 전자정부에서 사용하고 있는 암호 알고리듬, 전자서명 알고리듬, 해쉬 함수 등의 기반 기술에 대한 안전성 및 구현에 대한 연구 및 평가를 CRYPTREC에서 매년 수행하고 있으며, 새로운 정보보호 기반 기술에 대한 공모를 수시로 시행하고 있음

• 암호기술

- 국외 암호 기술은 미국, 일본, 유럽의 일부 선진국들이 주도하고 있다. 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 알고리듬들을 제안함. 그리고 현재 ECRYPT 프로젝트의 일부인 스트림 암호 공모사업 eSTREAM을 진행하고 있음. 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

  ◦ 대칭키 암호 : DES가 표준으로 채택된 이후, DES와 유사한 구조를 갖는 다양한 블록 암호들 (FEAL, GOST, LOKI 등)이 개발. 하지만 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

기술 에 대한 활발한 연구가 진행되고 있고 MISTY1, SHACAL-2, IDEA 표준 권고 알고리듬들에 대한 안전성 분석 연구가 지속되고 있음. 그리고 스트림 암호의 경우, 1990년대 이전에는 LFSR 기반 스트림 암호에 대한 연구가 유럽을 중심으로 이루어졌고 1990년대 이후 암호 기술의 일반화와 다양한 암호 응용 환경이 등장하면서 약 10여개의 소프트웨어 기반 스트림 암호 (RC4, SEAL, SOBER 등)등이 개발됨. 현재는 경량의 고속 암호화를 요구하는 신규 IT 환경에 적합한 스트림 암호들이 유럽의 eSTREAM 프로젝트를 통해 여러 알고리듬 (Trivium, HC-256, Endon 등)이 제안되고 있고 동시에 안전성 분석이 진행 중

◦ 공개키 암호 : 1970년대 말 Diffie-Hellman에 의해서 개념이 정립된 후 RSA, ECC, Rabin, ElGamal, XTR, NTRU 등 다양한 공개키 암호가 개발되었으나, 현재는 RSA와 ECC 만이 실용화되어 있는 상태. 공개키 암호의 실용화 장애 요인인 계산 효율성 문제를 해결하기 위한 다양한 연구가 진행 중에 있으며, 특히, 모듈러 연산, 유한체 연산, 타원곡선 연산 등의 효율성을 높이기 위한 연구가 진행 중에 있음. 특히, RSA의 안전성 판단의 기준이 되는 인수분해 알고리듬에 대한 연구가 많이 진행되고 있고, 시빙(Sieving) 단계와 행렬 연산 단계를 위한 인수분해 전용 하드웨어 SHARK 등이 제안되기도 함

◦ 해쉬 알고리듬 : 2005년 Crypto 2005에서 SHA-1의 충돌 가능성에 대한 논문이 발표된 이래, MD4, MD5, HAVAL의 충돌쌍과 부분 라운드 HAS-160의 충돌쌍을 찾는 이론적인 결과들이 다수 제시됨. 현재는 이를 보완하기 위한 연구가 진행 중에 있고 실질적으로 충돌쌍을 찾는 구현 연구가 활발히 이루어지고 있음. 2008년에는 차세대 해쉬 함수 공모가 미국의 NIST를 중심으로 진행될 예정

◦ 키 교환 프로토콜 : ISO에서 대칭키 기반과 공개키 기반의 다양한 프로토콜들을 국제 표준으로 규정한 이후 많은 연구가 이루어지고 있으며, NIST는 현재 키 설정에 대한 미 연방 표준화 작업을 진행하고 있음

◦ 암호 응용 프로토콜 : 전자 상거래에 이용되는 암호 기술인 은닉 서명이 D.Chaum에 의해서 처음 제안된 이래 Brand 등을 중심으로 전자 지불, 전자 지갑 등을 위한 응용 프로토콜 연구가 진행되고 있음. 또한 프락시 서명 프로토콜, 패스워드 기반 인증 및 키 분배 프로토콜 등의 다양한 암호 응용 프로토콜들이 발표되고 있다. 최근 다양한 공격 방법이 개발되어, PAKE(Password Authentication Key Exchange) 프로토콜이 개발되었고, 다시 오메가 프로토콜이 2006년 8월 CRYPTO2006에서 제안됨

◦ 대칭키 분야의 안전성 분석 기술 : DC/LC의 파생 공격, 대수적 공격 등의 다양한 분석 기술이 AES의 실용화를 앞두고 활발히 연구되고 있음

- 최근 타원곡선 암호에 대한 관심이 이동 시스템을 중심으로 증대되고 있음. 타원곡선 암호의 장점은 RSA 1024 비트 만큼의 안전성을 유지하면서 타원곡선 서명문의 길이가 320비트 정도로 줄어드는 특징이 있어서, 많은 표준화 기구에서 이에 대한 표준화를 수행하고 있음. 이의 대표적인 경우가 PKCS#13과 IETF PKIX 인터넷 드래프트 문서인 NIST Recommended EC Domain Parameters For PKIX를 들 수 있음

• 인증기술

- PKI, PKCS, 그리고 커버로스 보안 기술은 PKI 기술을 중심으로 개발되고 있고, PKI 기술의 경우, 표준의 채용을

통한 상호 연동성 보장, 키 및 인증서 수명 관리의 자동화, 인증서 정책 기능의 강화 및 용이한 적용, 소규모에서 대규모까지 시스템 규모 가변성, 사용자 인증을 위하여 바이오 인증 방식의 도입되고 있음. 특히 OpenCable은 공개키 기반 인증서를 이용하여 정당한 기기에 대한 인증 및 과금 등을 처리하고 있음

- 양자암호기술의 경우 미국에서는 ARDA 프로젝트를 통해 양자암호기술 로드맵을 작성하여 향후 관련 분야의 발전을 위해 필요한 기술 분야 및 발전 가능성에 대해 분석하였고 유럽은 SECOQC (Secure Communication based on Quantum Cryptography) 프로젝트를 중심으로 양자 암호기술 개발에 박차를 가함. 현재, 자유공간/위성통신기반 양자 통신의 경우 100km 급의 양자통신에 성공하였고 중국에서는 양자 라우터 실험에 성공하였다. 양자 암호 인터넷 서비스 상용화에 대한 기술을 연구 중

• 권한관리 기술

- 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 커스터 마이징하여 적용하고 있음
- 그러나 일부업체에서 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 Technoloies사의 SelectAccess, Entrust Technologies사의 Entrust GetAccess, RSA Security사의 ClearTrust, Netegrity사의 SiteMinder 등이 있음
- 최근에는 OTP, IC 칩 등 하드에어 기반의 접근제어 기술들이 응용서비스에 적합하도록 다양한 형태로 개발되고 있음

2.3. 표준화 현황 및 전망

2.3.1. 국내 표준화 현황 및 전망

국내 암호 · 인증 · 권한관리 관련 표준은 인터넷보안기술포럼(ISTF) 및 정보통신표준협회(TTA)에서 추진되고 있음. 인터넷보안기술포럼은 인터넷 보안 기술 분야의 민간 업체들이 중심이 되어 구성된 민간 포럼으로 인터넷 보안 기술 관련 국제 표준화 활동에 공동 대응하고 시장 수요를 반영한 사실 표준의 개발을 위해 2000년 6월에 창립된 한국정보보호진흥원 산하 포럼임. TTA는 한국정보보호진흥원, 한국전자통신연구원, 정보통신업체 등이 주도가 되어 추진하고 있는 정보통신단체표준임. 2006년까지 표준화 현황은 표9 및 표10과 같으며, 특히 TTA에서의 암호 · 인증 · 권한관리 표준화는 공통기반기술위원회(TC1) 산하 정보보호기반그룹(PG101)에서 추진되고 있음

- 암호기술
  - 1997년부터 1999년에 걸쳐 전자서명 알고리듬인 KCDSA와 해쉬 알고리듬 HAS-160 및 128 비트 블록 암호 알고리듬인 SEED를 개발하여 표준화 하였으며, 2001년 암호 키 관리 시범 시스템을 구축하고, 2001년에는 공개키 암호인 타원곡선 암호를 이용한 전자서명 알고리듬인 ECKCDSA를 국내 표준으로 제정하였고 TTA TC1 위원회에서 패스워드 기반 인증 프로토콜에 대한 표준화를 추진하고 있음
  - NSRI에서는 독자적인 대칭형 암호 알고리듬인 ARIA를 개발했으며, 산업기술표준으로 표준화되었고, 또한 2004년도에 국가정보원은 KISA, NSRI와 함께 암호 모듈 평가를 발표하였고, 이를 위하여 국내에서 사용될 암호 알고리듬에 대한 선정 작업을 수행함. 따라서 국내 공공기관에 적용될 선정 알고리듬에 대한 평가 방법이 개발됨
  - 2006년에 KISA, NSRI, 고려대학교 등은 공동으로 경량화된 대칭형 암호알고리듬으로 HIGHT, 256비트 해쉬알고리듬으로 FORK256, 스트림 암호알고리듬으로 TSC-4를 개발하여 국제적인 검증을 거쳐 TTA 표준으로 제정함
  - 양자 암호의 경우 세계적으로 원천기술연구 및 기초 실증 실험차원에 머무르고 있어 표준화는 아직 시기상조이나 선진국의 기술 발전 추이를 예의 주시하면서 국내 기술개발 여력을 축적하여 표준화에 대비하여야 함

- 인증 기술
  - 국내 PKI 표준안 개발은 인터넷보안기술포럼 및 TTA 표준화 그룹에서 진행되고 있음. 표준화 방식은 일반적으로 인터넷보안기술포럼에서 사실 표준을 제정한 후 TTA를 통해 단체표준화 하는 형식을 취하고 있음. 인터넷보안기술포럼는 국내 PKI 보안 솔루션 업체, 한국정보보호진흥원, 한국전자통신연구원, 공인인증기관 등으로 구성된 민간을 중심으로 하는 국내 PKI 관련 기술의 표준화 작업을 주도하고 있음
  - 인터넷보안기술포럼은 2000년 8월 한국정보보호진흥원에서 15개 업체의 PKI 관련 개발자를 중심으로 시작되었으며 2006년 12월에 "전자서명 인증서프로파일 표준", "전자서명 인증서 효력정지 및 폐지목록 표준" 등 20건의 유 · 무선 PKI 표준을 제 · 개정하였으며, 이와 더불어 전자서명 인증서 프로파일 표준, 전자서명 인증서 효력정지 및

폐지 목록 프로파일 표준, 인증서 검증 알고리듬 표준, 암호톤큰을 위한 PKCS#11 프로파일 표준, 식별번호를 이용한 본인확인 기술 등 10건의 표준안을 TTA에 상정하여 단체표준으로 제정함

- 또한, 국제적인 표준화 기구에 대한 기술 동향 파악과 국내 기술의 국제 표준화를 위한 준비로서 PKI 콘퍼런스, ISO 표준화 회의 참석, IETF 표준 회의를 참석을 통해 PKI 분과위원회의 지속적인 발전과 중장기적인 계획 수립하고 있음. 2006년도 IETF PKIX에서 SIM 표준이 완료되어 RFC 로 표준화가 완료됨
- 향후의 인증관련 표준화 방향은 인터넷 실명제 등에 맞추어 익명 인증에 대한 표준화가 진행될 전망. 더불어 유비쿼터스에 적합하도록 사람에 대한 인증뿐만 아니라 기기 및 사물을 포괄하는 인증기술이 개발되어 표준화될 전망임

• 권한관리 기술

- 국내에서는 권한관리 기술과 관련된 표준화는 국외에 비교하여 상당히 늦게 시작함. 그 결과 현재 권한관리 기술과 관련된 표준화는 ISTF의 '속성인증을 이용한 응용 서비스모델 표준'가 유일한 표준임. 따라서, 국내에서도 권한관리 관련하여 속성인증서와 연관된 표준 및 응용분야로서 EAM 등에 대한 표준화 활동이 필요함
- 또한, 인터넷을 이용한 전자거래가 활성화되면서 OTP, 스마트카드 등 HW에 기반한 접근매체에 대한 활용도가 지속적으로 증가할 것으로 전망되며 이에 따라 표준화도 증가할 것으로 전망

〈표9〉 암호 · 인증 · 권한관리 관련 인터넷보안기술포럼 표준현황

관련분야	표준 번호	표준 내용	제정 년도	비고
암호	ISTF-006	암호 메시지 규격 표준	2002	
	ISTF-007	Diffie-Hellman 키합의 방식 표준	2002	TTAS.IF-RFC2631
	ISTF-011	CMS에서 CAST-128 암호화 알고리즘의 사용 표준	2002	
	ISTF-015	무선 전자서명 알고리즘 표준	2002	TTAS.KO-12.0020
	ISTF-016	무선 키분배 알고리즘 표준	2002	TTAS.KO-12.0021
	ISTF-022	무선 응용계층 보안 프로토콜 표준	2003	
	ISTF-024	암호메시지 규격에서 사용되는 알고리즘 표준	2004	TTAS.IF-RFC3370
	ISTF-025	암호메시지 규격에서 AES 알고리즘의 사용 표준	2004	TTAS.IF-RFC3394
	ISTF-026	암호메시지 규격에서 SEED 알고리즘의 사용 표준	2004	
	ISTF-026/R	암호메시지 규격에서 SEED 알고리즘의 사용	2006	개정
	ISTF-027	AES 키 싸기 알고리즘 표준	2004	TTAS.IF-RFC3394
	ISTF-028	3-DES와 RC2 키 싸기 표준	2004	TTAS.IF-RFC3217
PKI	ISTF-001	전자서명 인증서 프로파일 표준	2000	TTAS.KO-12.0012
	ISTF-002	전자서명 인증서 효력정지 및 폐지목록 프로파일 표준	2000	TTAS.KO-12.0013
	ISTF-002/R	전자서명인증서 효력정지 및 폐지 목록 프로파일 표준	2006	개정
	ISTF-012	무선 전자서명 인증서 프로파일 표준	2002	TTAS.KO-12.0016
	ISTF-013	무선 전자서명 인증서 효력정지 및 폐지목록 프로파일 표준	2002	TTAS.KO-12.0017
	ISTF-014	무선 WTLS 인증서 프로파일 표준	2002	TTAS.KO-12.0019
	ISTF-017/R	무선 인증서 요청형식 프로토콜 표준	2003	TTAS.KO-12.0018/R1

관련분야	표준 번호	표준 내용	제정 년도	비고
PKI	ISTF-018	공인인증기관간 상호연동을 위한 PKI 표준	2002	
	ISTF-021	무선 인증서 관리 프로토콜 표준	2003	TTAS.OT-12.0001
	ISTF-023	암호 토큰을 위한 PKCS#11 프로파일 표준	2003	TTAS.OT-12.0002
	ISTF-030	인증서 경로검증 알고리즘 표준	2004	TTAS.KO-12.0028
	ISTF-031	식별번호를 이용한 본인확인 기술 표준	2004	TTAS.KO-12.0029
	ISTF-036	공인인증기관간 상호연동을 위한 사용자 인터페이스 표준	2005	
	ISTF-037	인증서 정책 및 인증업무준칙 프레임워크 표준	2005	TTAS.IF-RFC3267
	ISTF-038	전자서명인증체계 공인인증서 갱신 표준	2005	
	ISTF-039	공개키 인증서를 이용한 개체인증 프로토콜 표준	2005	
	ISTF-040	인증기관간 상호연동을 위한 CTL 기술 표준	2005	
	ISTF-043	웹서버보안, 코드서명, 보안메일용 인증서 프로파일 표준	2006	
	ISTF-045	XML 전자서명 X.509 인증서 토큰 프로파일	2006	
	ISTF-046	익명성을 갖는 전자서명 인증 기술 표준	2006	
권한관리	ISTF-044	속성인증을 이용한 응용 서비스모델 표준	2006	

〈표10〉 암호 · 인증 · 권한관리 관련 TTA 표준현황

분야	표준번호	제목	표준제정상태	년도	비고
암호	TTA.KO-12.0001	부가형 전자서명 방식표준 - 제2부 : 확인서 이용 전자서명 알고리즘	제정완료	1998	KCDSA
	TTAS.KO-12.0011	해쉬함수표준 - 제2부 : 해쉬함수알고리즘표준(HAS-160)	제정완료	1998	
	TTA.KO-12.0004	128비트 블록암호알고리즘 표준	제정완료	1999	SEED
	TTA.IS-10181.4	개방시스템 상호접속-개방시스템에서의 보안 골격-제4부:부인방지	제정완료	1999	ISO/IEC 10181 -4, X.813
	TTAS.KO-12.0001/R1	부가형 전자서명 방식 표준-제 2 부 : 인증서 기반 전자서명 알고리즘	개정완료	2000	KCDSA
	TTAS.KO-12.0011/R1	해쉬함수표준-제2부 : 해쉬함수알고리즘표준(HAS-160)	개정완료	2000	
	TTAS.KO-12.0015	부가형 전자서명 방식 표준-제3부 : 타원곡선을 이용한 인증서 기반 전자서명 알고리즘	제정완료	2001	EC-KCDSA
	TTAS.IF-RFC2631	Diffie-Hellman 키합의 방식	제정완료	2003	
	TTAS.KO-12.0025	블록암호알고리즘 SEED의 운영모드	제정완료	2003	
	TTAS.IF-RFC3217	3-DES와 RC-2 키 싸기	제정완료	2005	
	TTAS.IF-RFC3394	AES 키 싸기 알고리즘	제정완료	2005	
	TTAS.KO-12.0004/R1	128비트 블록암호알고리즘 SEED	개정완료	2005	
	TTAS.KO-12.0011/R2	해쉬함수표준-제2부 : 해쉬함수알고리즘표준(HAS-160)	개정완료	2005	
	TTAS.IF-RFC3370	암호 메시지 규격에서 사용되는 알고리즘	제정완료	2005	
	TTAS.KO-12.0039	해쉬함수 알고리즘 FORK-256	제정완료	2006	
	TTAS.KO-12.0040	64비트 블록암호알고리즘 HIGHT	제정완료	2006	
	TTAS.IF-RFC3369	암호 메시지 규격	제정완료	2006	
	TTAS.KO-12.0041	스트림암호알고리즘 TSC-4	제정완료	2006	
	TTAR-12.0001	MD5 메시지-다이제스트 알고리즘	제정완료	2006	

분야	표준번호	제목	표준제정상태	년도	비고
암호	TTAS.IF-RFC4196	IPsec을 위한 SEED 암호알고리즘	제정완료	2006	
	TTAS.IF-RFC4162	TLS를 위한 SEED 암호알고리즘	제정완료	2006	
	TTAS.IF-RFC4010	CMS를 위한 추가암호 알고리즘 : Part1 SEED	제정완료	2006	
	TTAS.IF-RFC3565	CMS를 위한 추가암호 알고리즘 : Part2 AES	제정완료	2006	
	2004-008	패스워드 기반의 공개키 암호기술 표준(AMP)	제정예정	2007	
인증	TTA.KO-12.0005	암호학적 확인함수를 이용한 실체인증 기술 표준	제정완료	1999	ISO/IEC 9798-4
	TTA.KO-12.0006	대칭형 암호화 기법을 이용한 실체인증 기술 표준	제정완료	1999	ISO/IEC 9798-2
	TTAS.IT-X.509/R2	디렉토리 시스템 인증 프레임워크 표준	개정완료	2000	ITU-T X.500
	TTAS.KO-12.0012	전자서명 인증서 프로파일 표준	제정완료	2000	PKI
	TTAS.KO-12.0013	전자서명 인증서 효력정지 및 폐지 목록 프로파일 표준	제정완료	2001	PKI
	TTAS.KO-12.0016	무선 전자서명 인증서 프로파일 표준	제정완료	2002	무선 PKI
	TTAS.KO-12.0017	무선 전자서명 인증서 효력정지 및 폐지목록 프로파일 표준	제정완료	2002	무선 PKI
	TTAS.KO-12.0018	무선 인증서 요청형식 프로토콜 표준	제정완료	2002	무선 PKI
	TTAS.KO-12.0019	무선 WTLS 인증서 프로파일 표준	제정완료	2002	무선 PKI
	TTAS.KO-12.0020	무선 키분배 알고리즘 표준	제정완료	2002	무선 PKI
	TTAS.KO-12.0021	무선 전자서명 알고리즘 표준	제정완료	2002	무선 PKI
	TTAS.IT-X509/R3	디렉토리 : 공개키와 속성 인증서에 대한 프레임워크 표준	개정완료	2003	PKI
	TTAS.KO-12.0024	실시간 인증서 상태확인 프로토콜 표준	제정완료	2003	PKI
	TTAS.IF-RFC3267	인증서정책 및 인증업무준칙 프레임워크	제정완료	2004	PKI
	TTAS.KO-12.0027	암호키분배용 인증서 및 키 관리 지침	제정완료	2004	PKI
	TTAS.OT-12.0002	암호 토큰을 위한 PKCS#11 프로파일	제정완료	2004	PKI
	TTAS.OT-12.0001	무선 인증서 관리 프로토콜	제정완료	2004	무선 PKI
	TTAS.KO-12.0018/R1	무선 인증서 요청형식 프로토콜	개정완료	2004	무선 PKI
	TTAS.KO-12.0028	전자서명 인증서 경로처리 알고리즘	제정완료	2005	PKI
	TTAS.KO-12.0029	식별번호를 이용한 본인확인 기술	제정완료	2005	PKI
	TTAS.KO-09.0003/R1	부가형 디지털 전자서명방식 - 제 1 부 : 기본 구조 및 모델	개정완료	2005	PKI
	TTAE.IF-RFC2716	EAP-TLS 인증 프로토콜	제정완료	2005	인증
	TTAE.IF-RFC3748	EAP 프로토콜	제정완료	2005	인증
	TTAE.IF-RFC3588	인증과 권한제어 및 과금용 다이아메터(Diameter) 베이스 프로토콜	제정완료	2005	인증
	TTAS.KO-12.0030	홈서버 중심의 홈네트워크 사용자 인증 메커니즘	제정완료	2005	인증
	TTAS.KO-12.0038	본인확인서비스 중복가입 확인정보	제정완료	2006	인증
	TTAS.KO-12.0012/R	전자서명 인증서 프로파일	개정완료	2006	PKI
	TTAI.KO-12.0035	홈네트워크를 위한 보안기술 프레임워크	제정완료	2006	인증
	TTAS.IT-X800	개방시스템 상호접속-개방시스템에서의 보안공격-제4부 부인방지	제정완료	2006	PKI
	2006-478	사용자 익명성을 갖는 전자서명 인증 기술	제정예정	2007	PKI
	2007-001	홈네트워크 등에 적용 가능한 디바이스 인증서 프로파일	제정예정	2007	PKI
	2007-002	전자서명 인증서 효력정지 및 폐지목록 프로파일	개정예정	2007	PKI
	2007-290	디렉토리 : 공개키와 속성 인증서에 대한 프레임워크 표준	개정예정	2007	인증
	2007-344	i-PIN 서비스 프레임워크	제정예정	2007	인증
	2007-345	i-PIN 서비스 전달 메시지 형식	제정예정	2007	인증

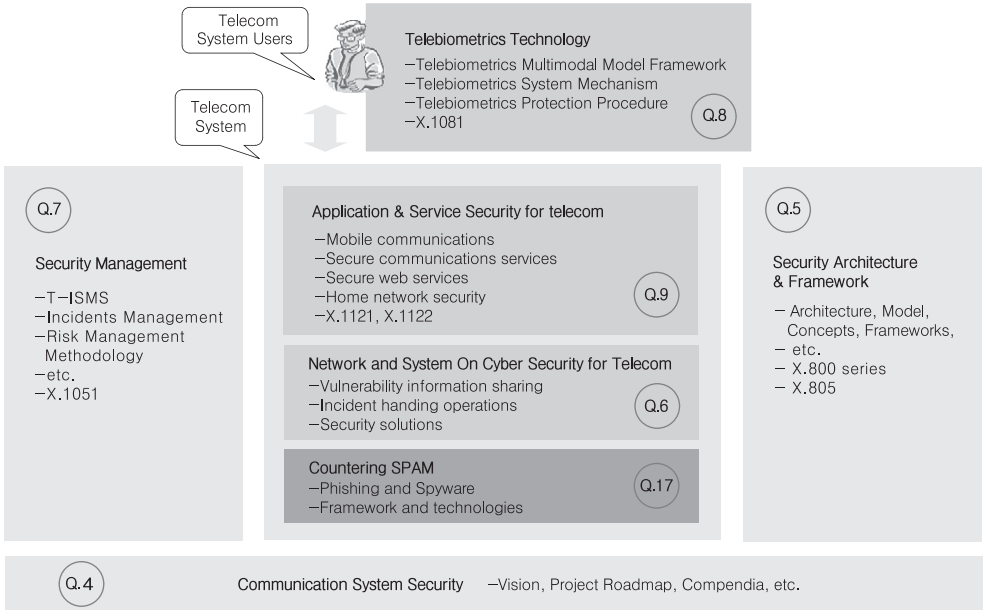
2.3.2. 국외 표준화 현황 및 전망

- 국외 암호 · 인증 · 권한관리 분야의 표준화는 다양한 표준화 기구 또는 기관에서 이루어지며 이들 중에 대표적인 기구들로는 IETF, ISO/IEC JTC1 SC27, ITU-T, RSA 등이 있음
- IETF에서의 암호 · 인증 · 권한관리 기술에 대한 표준화 작업은 Security Area의 17개 작업반에서 이루어지고 있음. 각각의 작업반은 응용분야와 연관이 되어 있기 때문에 암호와 같은 기반기술을 전담하는 작업반은 없으며 각 응용분야에서 적절하게 암호에 대한 표준을 진행하고 있음. 인증 및 권한관리 부분에 대해서도 응용분야에 따라 나누어져 있으나 PKI 관련 분야의 경우에는 PKIX에서 전담하여 진행하고 있음. 표11는 IETF security area의 표준화 작업반임

〈표〉 11 IETF security area 표준화 작업반

작업반	관련 내용
BTNS	better than nothing
DKIM	Domain Keys Identified Mail
EMU	EAP Method update
INCH	Extended Incident Handling
ISMS	Integrated Security Model for SNMP
KITTEN	Kitten(GSS API Next Generation)
KRB-WG	Kerberos WG
LTANS	Long-term Archive and Notary Service
MSEC	Multicast Security
OPENPGP	An Open Specification for Pretty Good Privacy
PKI4IPSEC	Profiling Use of PKI in IPSEC
PKIX	Public Key Infrastructure (X.509)
SASL	Simple Authentication and Security Layer
SECSH	Secure Shell
SMIME	S/MIME Mail Security
SYSLOG	Security Issues in Network Event Logging
TLS	Transport Layer Security

- ITU-T SG17에서는 정보통신 보안에 관한 표준을 선도하는 그룹으로 WP2 산하에 통신 시스템 보안 프로젝트, 보안 구조 및 프레임워크, 사이버 보안, 보안 관리, 바이오인식, 안전한 통신 서비스, 기술적인 스팸대응 등의 7개 연구과제로 구성되어 보안 표준들을 추진하고 있음. WP2의 연구영역은 그림 1과 같으며, 암호 · 인증 · 권한관리 관련 연구과제로 패스워드 기반 인증 및 키 교환, 패스워드 기반 인증 등이 표준화 추진 중



〈그림 1〉 ITU-T SG17 WP2 연구영역

〈표 12〉 ITU-T SG17 연구과제

연구과제	연구과제 제목	기개발된 표준 (Draft 표준)
4/17	통신 시스템 보안 프로젝트 (Communications systems security project)	
5/17	보안 구조 및 프레임워크 (Security architecture and framework)	X.800, X.802, X.803, X.805, X.810, X.811, X.812, X.813, X.814, X.815, X.816, X.830, X.831, X.832, X.833, X.834, X.835, X.841, X.842, X.843
5/17	패스워드 기반 인증 및 키 교환 (EAP-based authentication and key management)	X.akm
6/17	사이버 보안 (Cyber security)	E.409
7/17	보안 관리 (Security management)	X.1051
8/17	텔리바이오메트릭 (Telebiometrics)	X.1081
8/17	텔레바이오메트릭 인증(Telebiometrics authentication)	X.tai, X-tsm-1
9/17	안전한 통신 서비스 (Secure communication services)	X.1121, X.1122, X.1141, X.1142
9/17	홈네트워크 보안 (Security for home network)	X.1111, X.homesec-2, 3, 4
9/17	모바일 보안 (Mobile security)	X.1121, X.1122, X.msec-4
9/17	패스워드 기반 인증(Secure password-based authenticaion)	X.sap-1
17/17	기술적인 SPAM 대응 (Countering SPAM by technical means)	-

• 암호기술

– 국제 표준화 기구인 ISO/IEC JTC 1/SC27에서는 블록 암호 알고리듬, 전자서명 알고리듬, 공개키 암호 알고리듬,

해쉬 함수 등 수십 종의 암호 알고리듬을 표준화하고 있음. 또한, 암호분야에서는 미국, 유럽, 일본이 주도적으로 표준화를 진행하고 있음

- 미국의 경우, 오랫동안 대표적인 대칭키 암호 알고리듬이었던 DES에 대하여 키 전수조사가 가능해지고 다양한 분석 기법의 발견 등으로 안전성에 논란이 커지자 NIST는 새로운 차세대 암호를 공모하여 2000년 11월 AES를 선정 발표함. 그리고 NIST는 기존의 모드를 개선하고 AES에 적합한 새로운 모드 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 902.11 WLAN 표준으로도 채택된 알고리듬임. 하지만 NIST는 지속적으로 SP 800-38 시리즈를 업데이트 할 것으로 보임. 현재 계획으로는 1개 이상의 인증-암호화 모드를 추가적으로 선정할 것으로 예상되며 그 대상은 키와 같은 특정 대상을 인증-암호화하기 위한 AES KEY Wrap(AESKW) 알고리듬임. 또한, 미국 주도의 IEEE P1363에서는 공개키 기반의 키 교환, 암호화, 서명 등에 대한 알고리듬의 DB 작업을 시작하여 완성하고 있으며 lattice 기반, 패스워드 기반 인증 등을 위하여 p1363.1, p1363.2 등을 새롭게 작성하여 정리하고 있음. 게다가, NIST에서는 FIPS 180-2로 제정된 SHA-1 해쉬 함수를 대체하기 위하여 2008년 9월까지 해쉬 함수를 공모할 예정임
- 유럽에서는 전자상거래, 전자정부 및 전자서명 등을 구현하기 위해 필수적 요소인 암호 원천 기술에 대한 공모 사업 NESSIE를 통해 2003년 블록 암호, MAC 알고리듬, 해쉬 함수, 공개키 암호, 전자서명 알고리듬 등 다수를 선정함. 현재, ECRYPT 프로젝트의 일부인 스트림 암호 공모사업 eSTREAM이 추진 중에 있으며 30여개 알고리듬이 제안되어 공개 검증이 수행되고 있음. 이 공모사업은 고속 소프트웨어 환경용과 제한적인 하드웨어 환경용의 두 가지 분야로 진행되고 있으며, 특히 제한적인 하드웨어 분야에 제안된 알고리듬들은 RFID 태그에 탑재가 가능할 것으로 예상되고 있음
- 일본에서는 전자정부 구축을 위한 암호 원천 기술을 공모하여 역시 2003년 2월에 대칭키 암호, 공개키 암호, 해쉬 함수, 의사 난수 생성기 등을 선정함
- 한국은 2005년도 블록 암호 SEED가 ISO 국제 표준으로 채택되었고, EC-KCDSA 역시 이미 국제 표준으로 채택되었음. 최근에는 블록 암호 HIGHT를 ISO 표준으로 상정하기 위한 절차가 진행중임

• 인증기술

- ITU-T의 경우, 정보보호분야의 표준화가 활발하게 이루어지지 못하여 왔으나, X.500 디렉토리 서비스와 관련하여 개발된 X.509 인증서는 PKI 표준의 기초가 되었으며, 데이터구조를 표현하는 ASN.1 구문과 BER(Basic Encoding Rules)과 DER(Distinguished Encoding Rules) 부호화 규칙은 IETF의 많은 표준에서 활용되고 있음. 또한 현재 보안관련 선도그룹인 SG17의 Q.10에서는 통신시스템 보안 구조, 정보시스템을 위한 관리 보안, 이동망을 위한 보안 구조, 모바일 보안, 그리고 텔레바이오메트릭 분야의 보안 프로토콜이 표준화하고 있음

- ISO/IEC JTC1/SC27 WG2는 보안서비스 구현을 위한 다양한 보안기술과 관련된 여러 메커니즘의 표준화 작업과 비암호 방식의 보안기술도 취급하고 있으며, 인증서비스의 기반이 되는 핵심 알고리듬에 대한 표준화가 이루어지고 있음. 또한, 본 표준화 기구에서 제정된 알고리듬은 IETF 및 ITU-T의 표준에서 활용되고 있음
- PKCS 표준은 RSA암호 표준, DH(Diffie-Hellman) 키 합의 표준, 패스워드-기반 암호 표준, 확장된 인증서 구문 표준, 암호학적 메시지 구문 표준, 개인키 정보 구문 표준, 선택된 속성 타입, 인증 요구 구문 표준, 암호학적 토큰 인터페이스 표준, 개인 정보 교환 구문 표준, 타원곡선 암호 표준, 암호학적 토큰 정보 포맷 표준 등을 다루고 있음. 이 표준은 PKIX와 관련된 표준과 S/MIME 표준에 영향을 미친 아주 중요한 사실 표준임

〈표 13〉 PKCS 표준

문서명	주요 내용
PKCS #1	이 표준은 암호학적 프리미티브, 암호 기법, 서명 기법 등을 포함하는 RSA 알고리듬에 기반을 둔 공개키 암호에 대한 구현 방법을 기술한 권고안임
PKCS #3	이 표준은 DH(Diffie-Hellman) 키 일치를 실현하기 위한 방법을 규정한다. 이 프로토콜은 안전한 통신을 구축하기 위한 프로토콜에서 이용될 수 있음
PKCS #5	이 표준은 키 도출 함수, 암호 기법, 그리고 메시지 인증 기법을 포함한 패스워드-기반 암호를 실현하기 위한 규정을 제공함
PKCS #6	이 표준은 인증서와 여러 속성들로 구성되는 확장된 인증서를 위한 구문을 기술함
PKCS #7	이 표준은 디지털 서명과 디지털 봉투와 같은 데이터의 일반적인 구문을 기술한다.
PKCS #8	이 표준은 공개키 알고리듬과 인증서에 대한 개인키를 포함하는 개인키 정보에 대한 구문을 기술한다. 이 이 표준은 암호화된 개인키에 대한 구문을 기술함
PKCS #9	이 표준은 PKCS #6 확장된 인증서, PKCS #7 디지털 서명 메시지, PKCS #8 개인키 정보, PKCS #10 인증서 요구 메시지에서 사용 가능한 속성 타입을 정의함
PKCS #10	이 표준은 공개키에 대한 인증을 위한 요구를 위한 구문을 정의함
PKCS #11	이 표준은 암호 정보를 보관하고 암호기능을 수행하는 장치로의 Cryptoki 라 불리는 API를 규정하고 있다. Cryptoki는 암호학적 토큰 인터페이스를 지칭하며, 단순한 객체-기반 접근방식을 따르며, 기술 독립과 자원 공유의 목적을 달성하고, 응용에게 암호학적 토큰의 공통의 논리적 관점을 제공함
PKCS #12	이 표준은 사용자 개인키, 인증서, 그리고 다양한 비밀정보를 저장하고 전달하기 위한 이동 가능한 형태를 규정함
PKCS #13	PKCS #13은 타원곡선 암호 표준으로써, 현재 개발중에 있다. 이는 파라메터, 키 생성과 검증, 디지털 서명, 공개키 암호, 키 일치 등의 타원곡선 암호의 다양한 측면을 제공하고 있음
PKCS #15	PKCS #15는 응용의 토큰 인터페이스 제공자와 무관하게, 사용자가 여러 표준-준용 응용에게 자신의 신분을 확인하기 위한 암호학적 토큰을 사용할 수 있도록 보장하는 표준임

- IETF는 실제 구현의 관점에서 표준화를 진행하는 사실표준화 기관으로 PKIX, TAM BOF, KeyProv, HoKey, Kerberos, TLS, EMU, S/MIME, SASL, LANS 등의 워킹그룹에서 인증관련 표준화가 진행되고 있음

〈표 14〉 IETF Security Area 표준화 진행 현황(2007.8.)

Working Group	RFC	Draft	현재 상태
Public-Key Infrastructure (X.509) (pkix)	40	8	작업중
EAP Method Update (EMU)	-	2	작업중
Simple Authentication and Security Layer(SASL)	5	3	작업중
Long-Term Archive and Notary Services (ltans)	1	5	작업중
Kitten(KITTEN)	4	3	작업중
Kerberos WG(KRB-WG)	7	10	작업중
합 계	57	31	

◦ 공개키 기반(Public-Key Infrastructure, PKIX) 워킹그룹은 X.509 기반의 PKI에 관련된 인터넷 표준을 개발하는 워킹그룹으로, X.509 V3 인증서와 v2 인증서 폐지 목록에 대한 프로파일, 공개키 인증서의 관리와 요청과 상태 표시 등을 위한 프로토콜, LDAP/FTP/HTTP 등에 의한 PKI 작업, Diffie-Hellman 소유 증명 알고리듬, 적격인증서 프로파일, 데이터 검증/인증 서버 프로토콜, 타임스탬프 프로토콜 등을 규정하고 있음. 현재 서버기반의 인증서 경로검증 프로토콜(DPD/DPV), CMS 기반의 인증서 관리 프로토콜, OCSP 경량 프로토콜 등 8건의 Internet Draft에 대한 표준화를 추진 중. 또한, SHA-224, 256, 384, 512 등 해쉬 알고리듬을 지원하는 타원곡선 전자서명 알고리듬 OID, 인증서 및 CRL 공고 프로토콜로써 HTTP 기반의 WebDAV 프로토콜, 인증서 초기등록, 갱신, 인증기관 인증서 검색 등을 위한 간소화된 인증서 등록 프로토콜(SCEP), PKI Resource Query Protocol 등 다양한 드래프트 문서들이 제안되어 논의 중에 있음

◦ 최상위인증서 관리(Trust Anchor Management, TAM) BOF에서는 최상위인증서를 온라인으로 저장소에 추가 · 삭제 · 검색할 수 있도록 하는 프로토콜 및 인증서 경로 검증시 최상위인증서 이름, 공개키 정보, 용도 등 표현 요구사항 등을 정의하기 위해 새로운 워크그룹의 신설을 추진 중임. 현재 최상위인증서 저장소 관리하기 위한 프로토콜이 표준화되어 있지 않기 때문에 PKI 정책기관에 의해 관리되지 못함을 지적하고 최상위인증서 관리 프로토콜이 적용될 수 있는 분야로써 핸드폰, 파이어월 등 디바이스 등을 예시하고 있다. 현재 참석자 대부분 최상위인증서 관리(TAM)을 워킹그룹으로 신설하여 표준을 추진하는 방안에 동의하고 있음

◦ 키 관리(Key Provisioning, KeyProv) 워킹그룹 기 출시되어 보안 프로그램이 설치되어 있지 않을 수 있는 휴대전화, 보안토큰, USB 등 단말기에 동적으로 대칭키를 안전하게 전달할 수 있는 통신 프로토콜 및 메시지 형식을 표준화하는 워킹그룹으로, 보안토큰 키 초기화 프로토콜 웹서비스, 동적 대칭키 관리 프로토콜 등 5개 Internet Draft에 대한 표준화가 진행 중임

◦ 핸드오버 키관리(Handover keying, Hokey) 워킹그룹 무선 네트워크에서 핸드오버시 효율적인 인증을 위한 인증 절차 간소화 및 안전한 키 관리를 위한 계층적인 키 관리 방안 등에 대한 표준화를 추진 중임. '08년 3월까지 총 4개의 Internet Draft을 RFC로 등록할 계획임

◦ 커버로스(Kerberos) 워킹그룹 커버로스 사용자 인증 시스템(Version 5)의 안전 · 편의성 제고 및 키관리 방법 개선을 위한 표준을 추진 중임. 사용자 인증키 해킹 방지를 위한 확장필드 개발, KDC 클라이언트 통신 프로토콜에

GSS-API 추가, 사용자 정보관리를 위한 LDAP 스키마 등 10개 Internet Draft를 검토 중이며, '08년 3월까지 RFC로 추진할 계획임

◦ TLS(Transport Layer Security) 워킹그룹 '96년에 개발된 TLS v1.1 프로토콜을 개선하는 워킹그룹으로, 최근 취약점이 발견된 MD5와 SHA1 등 해쉬알고리듬을 제거하고 신규로 개발되는 암호 알고리듬 표준을 추가하는 추세임. 현재, SHA-256/384 및 AES 알고리듬 추가 및 OpenPGP Key 인증 프로토콜 등 6개 Internet Draft에 대해서 표준화를 추진 중임

◦ 확장가능한 인증프로토콜 방식 개선(EAP Method Update, EMU) 워킹그룹 40여개 이상의 확장가능한 인증 프로토콜(EAP) 방법간 구현상의 상호연동 확보를 위한 표준화를 추진 중. 여기서 EAP는 무선 AP(Access Point)에서 Kerberos, 공개키, OTP 등 다양한 인증메커니즘 구현에 대한 부담을 줄이기 위해 개발된 Pass-Through 프로토콜로써 인증 메시지 및 통신 프로토콜에 대한 내용을 수록하고 있음. 특히, EAP-TLS 메커니즘에서의 인증 및 채널 암호화 방식 및 EAP 메커니즘에서 비도 높은 비밀키 공유방식의 RFC3748 및 RFC4017 요구사항 충족 등을 위한 표준화 진행 중임

◦ 보안메일(S/MIME,Longterm Archive and Notary Services)SASL) 워킹그룹 보안메일 메시지 형식(RFC3369) 및 알고리듬(RFC3370) 표준의 개선을 추진하는 워킹그룹으로 SHA2, AES 등 보안메일 암호 알고리듬 추가, Multiple Signatures 등 메시지 형식 추가 등을 위한 Internet Draft 10종이 검토 중임

◦ 간소화된 인증 및 보안 계층(Simple Authentication and Security Layer, SASL) 워킹그룹 클라이언트와 서버가 인증, 무결성, 암호화 등 다양한 정보보호 메커니즘을 상호 협상할 수 있도록 하는 프로토콜을 표준화하는 워킹그룹으로, GSS-API 기반의 SASL 메커니즘, 메시지 축약 인증을 이용한 SASL 메커니즘 등 3개 Internet Draft의 표준화를 추진 중임

◦ 장기전자서명(Longterm Archive and Notary Services) 워킹그룹 장기 전자서명에 대한 기술적인 방안을 마련하기 위한 워킹그룹으로, 기록 증명 메시지 형식, 장기보관 프로토콜 등 6개 Internet Draft에 대한 표준화가 진행 중임

〈표 15〉 PKIX 표준

구분	문서명	문서이름	상태	발표월일
암호	RFC 3874	A 224-bit One-way Hash Function: SHA-224	표준	2004.9.
	RFC 3279	Additional Algorithms and Identifiers for RSA Cryptography for use in the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile	표준	2005.6.
	RFC4491/3279	Using the GOST R 34.10-94, GOST R 34.10-2001, and GOST R 34.11-94 Algorithms with the Internet X.509 Public Key Infrastructure Certificate and CRL Profile	표준	2006.5.
	RFC4055	Additional Algorithms and Identifiers for RSA Cryptography for use in the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile	표준	2005.6
인증서	RFC 2459/3280	Internet X.509 Public Key Infrastructure Certificate and CRL Profile	표준	1999.1./ 2002.4
	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.

구분	문서명	문서이름	상태	발표 월일
인증서	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.
인증서 정책	RFC 2527	Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework	정보	1999.3.
	RFC 3628	Policy Requirements for Time-Stamping Authorities	정보	2003.11
	RFC 3647	Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework	표준	2003.11.
운영/관리	RFC 2510	Internet X.509 Public Key Infrastructure Certificate Management Protocols	표준	1999.3.
	RFC 2511	Internet X.509 Certificate Request Message Format	표준	1999.3.
	RFC 2559	Internet X.509 Public Key Infrastructure Operational Protocols - LDAPv2	표준	1999.4.
	RFC 2585	Internet X.509 Public Key Infrastructure Operational Protocols: FTP and HTTP	표준	1999.5.
	RFC 2587	Internet X.509 Public Key Infrastructure LDAPv2 Schema	표준	1999.6.
	RFC 2875	Diffie-Hellman Proof-of-possession algorithm	표준	2000.7.
	RFC 2797	Certificate Management Messages over CMP	표준	2000.4.
	RFC 4158	Internet X.509 Public Key Infrastructure: Certification Path Building	정보	2005.9.
	RFC 4210/2510	Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP	표준	2005.9.
	RFC 4211/2511	Internet X.509 Public Key Infrastructure Certificate Request Message Format (CRMF)	표준	2005.9.
	RFC 4387	Internet X.509 Public Key Infrastructure Operational Protocols: Certificate Store Access via HTTP	표준	2006.2.
	RFC 4630	Update to DirectoryString Processing in the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile	표준	2006.8
응용 프로토콜	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.

• 권한관리 기술

- 현재 PMI 관련 표준화는 ITU-T 및 IETF에서 이루어지고 있으며, ITU-T는 X.509 3rd Edition에서 버전1의 속성 인증서 기본구조를 정의하고 있고, X.509 4th Edition에서 보다 명확한 PMI 프레임워크를 정의함. X.509 4th Edition에서는 버전 2 속성인증서 구조의 정의, PMI 모델의 정의, 위임 경로 처리 과정의 명시, 표준 확장 필드의

정의 및 디렉토리 스키마 오브젝트 정의의 추가 등을 들 수 있음

- IETF는 2002년에 RFC 3281 'An Internet Attribute Certificate Profile for Authorization'이라는 제목의 표준으로 인터넷 환경에서 사용될 수 있는 속성 인증서 프로파일을 제시하고 있고. 또한 이와 관련하여 속성 인증서 정책 관련된 확장을 다루고 있는 'Attribute Certificate policies Extension' 등을 표준화함
- 향후에는 EAM 등 속성 인증서를 이용한 다양한 응용서비스 모델에 따라 상호 호환성 보장을 위한 표준화가 필요함

2.4. 표준화 대상항목별 현황 분석표

구분		암호인증권한관리 기술		
표준화 대상항목		암호기술	인증기술	권한관리 기술
시장 현황 및 전망	국내	- 2006년도 국내 정보보호 매출은 2005년보다 7.9% 증가한 약 7,348억원으로 지속적으로 증가추세 - SEED, DES, 3DES, AES 등 정보보호 제품에 탑재된 정보보호 제품이 출시 중 - 전자서명 알고리듬의 경우 국내 공인인증서비스 확대와 더불어 사용이 급속히 증가하고 있음 - ECC 탑재 암호 제품이 널리 상용화되고 있음 - 2006년부터 국내에서도 상용 암호모듈평가프로그램이 시작됨 - 인터파크, G마켓 등의 인터넷 쇼핑몰에서 결제 정보의 암호화 및 CD/ATM에서 은행서버로 계좌번호, 비밀번호 등의 금융정보 암호화에 SEED 사용	- CA, RA, OCSP, SCVP 서버가 개발되고 있음 - AA, PMI 서버 등의 제품이 개발되고 있음 - 무선 PKI 시스템을 위한 제품이 상용화되고 있음 - 2004년도부터 개인용 상호연동용 인증서가 유료화됨에 따라서 인증시장의 규모가 증가할 것으로 개대됨 - 2006년도에는 인터넷뱅킹, 사이버증권거래, 전자입찰, 교육, 세금 등 사회전반에 PKI가 적용되어 활성화되고 있음 - 향후 인터넷 실명제 등에 적합한 익명인증 및 유비쿼터스 사회에 적합한 사람, 기기 등에 대한 인증기술 개발이 활성화 될 것으로 전망됨	- PMI 등 권한관리 기술은 접근제어 제품, EAM, 포털관리 및 e-비지니스 시스템에 내장되어 개발 - 펀타시큐리티의 iSIgn, 소프트포럼의 SafeSignOn, 시큐아이닷컴의 Trust SSO 등 SSO(Single Sign-On) 형태의 제품들이 출시 - HW 기반의 접근매체에 대한 필요성은 인식하고 있으나, 사용편의성 문제로 보급은 지연 - 2005년 고액의 금융거래의 경우 OTP 또는 HW 기반의 접근매체 이용을 의무화 - 2007년 금융기관 공동으로 고액의 금융거래에 OTP 사용 - 향후 자격, 접근통제 관련하여 다양한 형태의 제품들이 출시될 전망
	국외	- 인증 기술, 시스템, 네트워크 정보보호 기술, 응용 정보보호 기술은 모두 기반 기술인 암호 기술에 의존하고 있음 - 정보보호 시장의 제품이 점차 토털 솔루션의 형태로 발전하여 암호 제품이 포함되어 시장을 형성함 - 독자적인 암호 모듈 제품이 상용화되고 있고, 시장을 형성하고 있음 -양자암호는 MagiQ Tech., id Quantique 등의 벤처회사를 중심으로 초기 형태의 상용화 제품 출시하여 조기시장이 형성되어 있음	- PKI 제품이 주로 지금까지 상용화되어 서비스되고 있으나, 앞으로는 PMI 관련 제품의 개발이 이루어질 것으로 예측되며, 네트워크 디비이스를 위한 각종 디바이스 인증 제품에 대한 수요가 증가할 것으로 예측됨 - I&AM 일부 제품이 상용화되고 있음	- PMI 관련하여 Baltimore Technoloies사의 SelectAccess, Entrust Technologies사의 Entrust GetAccess, RSA Security사의 ClearTrust, Netegrity사의 SiteMinder 등의 제품이 출시 - 스마트카드, OTP 등 다양한 HW 기반의 접근매체 출시
기술 개발 현황 및 전망	국내	- 가 2001년 암호 키 관리 시스템을 구축하여 기술이전함 - 대칭키 암호 분야는 민간 표준으로 사용하기 위한 블록 암호 SEED 개발하였고, 2004년 ARIA 알고리듬이 개발되었음 - 2006년 대칭형 암호알고리듬으로 HIGHT, 256비트 해쉬 알고리듬으로 FORK256, 스트림 암호알고리듬으로 TSC-4 등을 개발 - 2006년부터 국정원에 의한 암호모듈평가프로그램 시작 - 공개키 암호 연산 고속화 분야에서는 지수승 알고리듬, 유한체 연산 기법, 타원곡선 연산 속도 개선 알고리듬을 발표 - 패스워드 인증 및 키공유, 특수 전자서명 알고리듬 등의 분야, DES 등의 암호해독 분야에서 주목할 만한 연구 실적이 있으나, 공개키 암호 알고리듬 설계 분야에서 연구 실적 없음 - SEED, ARIA 등 대칭형 암호 알고리듬을 개발했으나, 공개키 암호를 위한 암호해독 및 암호 알고리듬 설계 분야가 다소 뒤떨어짐 - 미국, 영국, 프랑스, 캐나다, 호주 드에서 암호키관리 장비(HSM) 및 스마트카드 등에 SEED가 탑재되어 상용화됨 - 현재 암호 분야의 ITRC를 통하여 다양한 암호 기술들이 개발되고 있고, NSRI와 KISA 암호 팀에 의한 관련 연구가 수행되고 있어서 독자적인 암호 기술의 자립이 가능할 것으로 예측됨 - 25km급 양자암호통신 실험 성공, 상용화를 위한 양자암호 기술 연구 개발 중임	- 국내에서도 전문보안업체에서 많은 유형의 PKI 제품을 개발하고 있음 - I&AM에 관한 연구개발이 ETRI에 의하여 2004년부터 시작되어 관련 제품과 표준이 개발될 예정임 - 국내 인증기술의 표준화는 ISTF에서 개발된 사실 표준을 근거로 TTA에 의한 정보통신단체 표준이 개발되고 있음 - 많은 PKI 관련 산업체에서 IETF PKIX에서 표준화되고 있는 프로토콜을 이용한 제품을 개발하고 있고, 대부분 IETF 표준에 호환성이 있는 제품을 개발하고 있음 - 이 분야의 기술수준은 국내도 상당한 수준이라고 평가되며, 특히 무선 공개키 기반구조 분야의 경우, 세계 선진 수준과 견줄만 하다고 판단됨	- PMI 기능들은 접근제어 제품, EAM, 포털관리 및 e-비지니스 시스템 등에 끼어 들어가는 형태로 동작하고 있지만, 앞으로는 XML 기반으로 발전할 것으로 전망 - 국내 스마트카드, OTP 등 업체에서는 보안성이 뛰어나며 사용이 편리한 접근매체 개발 중 - 2007년 KISA에서는 보안토큰 기반의 공인인증서 이용기술 등을 발표 - HW 기반의 접근매체의 경우 세계 선진 수준에는 아직 미치지 못하고 있음
	국외	- 대칭키 암호 알고리듬은 1970년대 중반 미 연방 표준 암호 알고리듬으로 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		

	국외	- RSA, ECC, Rabin, ElGamal, XTR, NTRU 등 다양한 공개키 암호가 개발되었으나, 현재는 RSA와 ECC 만이 실용적 이용됨 - 키 설정 프로토콜은 ISO/IEC JTC1에서 대칭키 또는 공개키 기반의 다양한 프로토콜을 국제 표준으로 규정한 후 많은 연구 진행됨 - IETF의 경우 ECC 알고리듬을 포함한 다양한 암호 알고리듬에 대한 확인자를 개발하고 있고, 관련 보안 프로토콜의 기반 알고리듬으로 활용하고 있음 - ITU-T의 경우, 접근제어 프레임워크, 부인방지 프레임워크, 키관리 프레임워크 등의 다양한 프레임워크를 개발완료하였음 - AES, 가변 길이 해쉬 알고리듬이 개발되는 등 핵심 암호 알고리듬 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 해쉬알고리듬의 개발이 활발히 수행될 예정이고, 2005년과 2006년 두 차례에 걸쳐 NIST 주관 해쉬 워크샵이 개최되어 2011년까지 해쉬 알고리듬을 개발할 목적으로 공개 공모과정을 2007년부터 시작하는 것을 골자로 하는 로드맵이 확정되어 있음 - 양자암호의 경우 유사단일광자(수 개)통신, 자유공간 100km에 성공하였고 양자암호 인터넷 서비스 기술을 연구 중임	- IETF의 경우, 기존의 하나의 작업반인 (PKIX) 외에 4개의 세로운 작업반(IPSec을 위한 PKI, 안전한 크리덴셜 저장 및 전달 프로토콜, 초기 등록 등) 이 만들어져 관련 표준을 개발하고 있음 - IETF에서 기존의 확장 가능한 인증 방법을 갱신하기 위한 UEAP 작업반을 구성하고, 이에 대한 표준을 2006년부터 시작함 - OASIS는 PKI 활성화 방안을 마련하고 전자서명 및 공개키 기반구조 관련 표준을 개발하고 있고, 웹서비스 보안을 위한 SAMLv2, XACMLv2 등의 표준을 개발하고, 이를 ITU-T을 통하여 2006년 4월 승인함 - 미국의 경우 150개 이상의 조직이 결합한 Liberty alliance 라는 프로젝트를 통하여 연합된 네트워크 구조를 이용한 싱글사인에 대한 표준과 공통의 플랫폼을 개발하고 있음.	- 선도적인 다국적 정보보호업체의 경우에는 PMI 관련 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	국내	상용화	상용화	기술기획/구현
	국외	상용화	상용화	구현/상용화
	기술격차	1.93년	1년	
	관련제품	- 암호 모듈, 암호 칩, 암호 알고리듬을 구현한 각종 암호 API, 암호모듈 평가	- CA, AA, RA, OCSP 서버, SCVP서버 등	- SSO, EAM 등 - OTP, 보안토큰 등
IPR 보유 현황	국내	- KCDSA 전자서명 알고리듬 - SEED, ARIA 등의 대칭형 암호 알고리듬	-	-
	국외	- 공개키, 대칭키, 전자서명, 키분배 알고리듬, ECC 알고리듬	-	-
IPR확보 가능분야		- 전자서명 및 대칭형 암호 알고리듬, 패스워드기반 인증 및 키교환, 타원곡선기반 전자서명, 고속화 공개키 암호 매커니즘 등의 분야에서 고속동작이 가능한 알고리듬 실현 분야 - 미래 USN을 고려하면, ECC 실현 기술에 대한 IPR 확보는 매우 중요한 과제임 - decoy 상태에 대한 양자 암호 원천기술 및 각종 상용화를 위한 요소기술에서 IPR 확보가 가능함	-	-
IPR확보 가능성		- 높음	- 보통	- 낮음
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 알고리듬을 시스템 특성에 따라서 선택적으로 협상을 통하여 사용할 수 있도록 하는 암호 알고리듬 스위트에 대한 표준화를 진행중에 있음, 이의 대표적인 경우가 IPSec, TLS, 그리고 PKIX에서의 표준 암호 스위트를 들 수 있음 - 우리나라가 제안한 SEED가 2005년에 ISO/IEC JTC1 및 IETF에서 표준으로 선정되었음 - 블록 암호 HIGHT와 해쉬 함수 FORK-256이 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 - 양자암호는 현재 원천기술 연구 개발 중이므로 아직 표준화는 시기상조이	- IETF의 경우, IPSec을 위한 PKI 등에 대한 표준이 개발될 예정임 - 2006년 IETF에서는 기존의 EAP에 대한 향상된 버전의 EAP를 표준화하기 위한 BOF 를 만듬 - 공개키 기반구조에 대한 표준화는 거의 성숙 상태에 있으나, 앞으로도 IETF PKIX 작업반, ITU-T 디렉토리 연구반, 그리고 OMA에서 무선 공개키 기반구조에 대한 표준화가 지속적으로 추진될 것으로 예측됨 - OASIS의 경우, 공개키 기반구조 활성화를 위한 표준을 개발하고 있고, 특히 SSO에 적용될 수 있는 SAMLv2, EXACMLv2를 2004년에 완성하고, XML 보안에 대한 표준화를 추진하고 있음 - 2006년 4월 ITU-T에서는 OASIS SAML, XACML을 ITU-T X.1141, X.1142로 표준화함 - 2006년 ITU-T SG13에서 NGN 보안 및 인증 요구사항 문서를 개발 중에 있음 - 향후 익명인증 분야에서 표준화활동을 강화할 필요가 있음	- PMI 관련한 국내 표준안 아직 진행되고 있지 않으며 2008년부터 표준안을 마련할 예정 - HW 기반의 접근제어의 경우 KISA에서 보안토큰 기반의 인증서 이용기술 등에 대한 표준안을 준비 중에 있음 - PMI와 HW 기반의 접근제어에 대한 표준화는 u-IT 서비스가 증가하면서 점차 증가할 것으로 전망됨
표준화 기구/ 단체	국내	TTA, 기술표준원	TTA,	TTA
	국외	IETF, ISO/IEC JTC1, ITU-T	IETF, I ITU-T	IETF, I ITU-T
	국내참여 업체 및 기관현황	KISA, ETRI, KIISC, TTA	KISA, ETRI, TTA	KISA, ETRI, TTA
	국내기여도	- 국내 암호 알고리듬(SEED)이 ISO/IEC JTC1 에서 국제 표준화되었음	-	
표준화 수준	국내	표준제/개정	표준제/개정	표준안 기획
	국외	표준제/개정	표준제/개정	표준안 개발/검토
국내표준화의 인프라수준 (시장요구정도 및참여도)		보통	높음	낮음

3. 중점 표준화항목의 표준화 추진전략

3.1. 중점기술의 표준화 환경분석

3.1.1. 표준화 추진상의 문제점 및 현안사항

- 암호, 인증, 권한관리는 정보보호 기반 기술이기 때문에 사회적으로 지속적인 관심이 부족하여 정부차원의 지속적인 투자를 이끌어내기가 어렵다. 또한 암호, 인증, 권한관리는 보안서비스 제공을 위한 인프라로 인식되기 때문에 업체의 신규 기술 개발 및 표준 활동이 미미한 실정임
- 따라서, 신규 IT 서비스에 적합한 정보보호 기반기술의 확보를 위한 경량 암호 기술, 양자암호 기술, 암호 평가 기술 등 차세대 함호기술에 대한 정부차원의 지속적인 지원이 필요
- 또한 유비쿼터스 사회에서는 사람, 사물, 기기 등이 하나의 네트워크로 연결되게 되므로 이러한 환경에 적합하도록 다양한 인증대상 및 인증수단 및 인증수단을 고려한 차세대 인증기술의 개발이 필요
- 마지막으로 해킹 기술의 발달로 정보시스템에 대한 접근 시 하나 이상의 접근통제 수단을 필요로 하고 있고, 특히 하드웨어를 기반으로 하는 접근통제가 필수적인 수단으로 등장할 것으로 예측되므로 이에 대한 기술 개발 및 표준화도 필요

3.1.2. SWOT 분석 및 표준화 추진방향

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

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

• 현황분석을 통한 우선순위

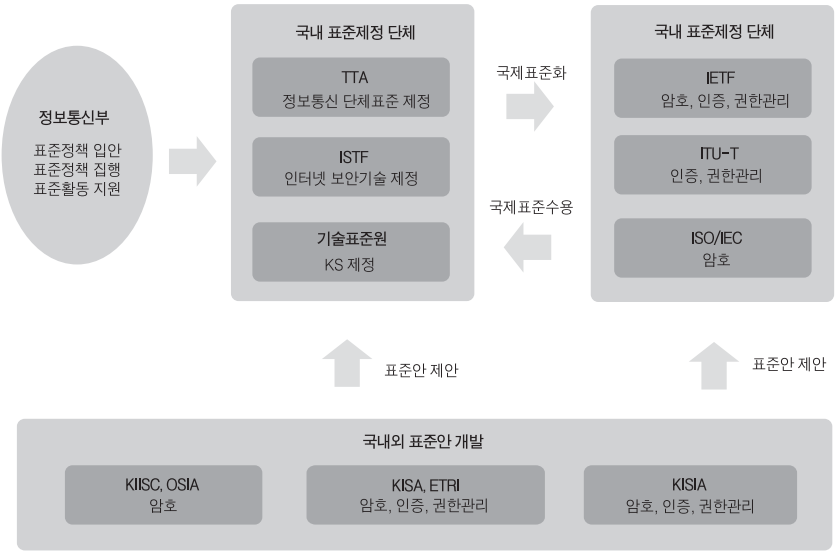
- 암호기술 분야는 이미 원천기술을 확보하고 있고 국제표준화를 통해 국제적인 입지를 갖추고 있으므로 아직 시장 및 응용분야에서 적용이 활성화되지 않은 익명인증, 암호응용기술 분야에서 유비쿼터스 사회의 다양한 응용서비스와 연계하여 IPR 및 국제 표준화 추진

• 표준화 추진방향

- 정부차원의 지속적인 선도 기반 기술 개발 및 지속적인 인력양성을 통해 암호 키 관리 및 HW 기반 접근제어 기술을 개발하여 IPR 확보 및 국제표준화 추진

3.1.3. 표준화 추진체계

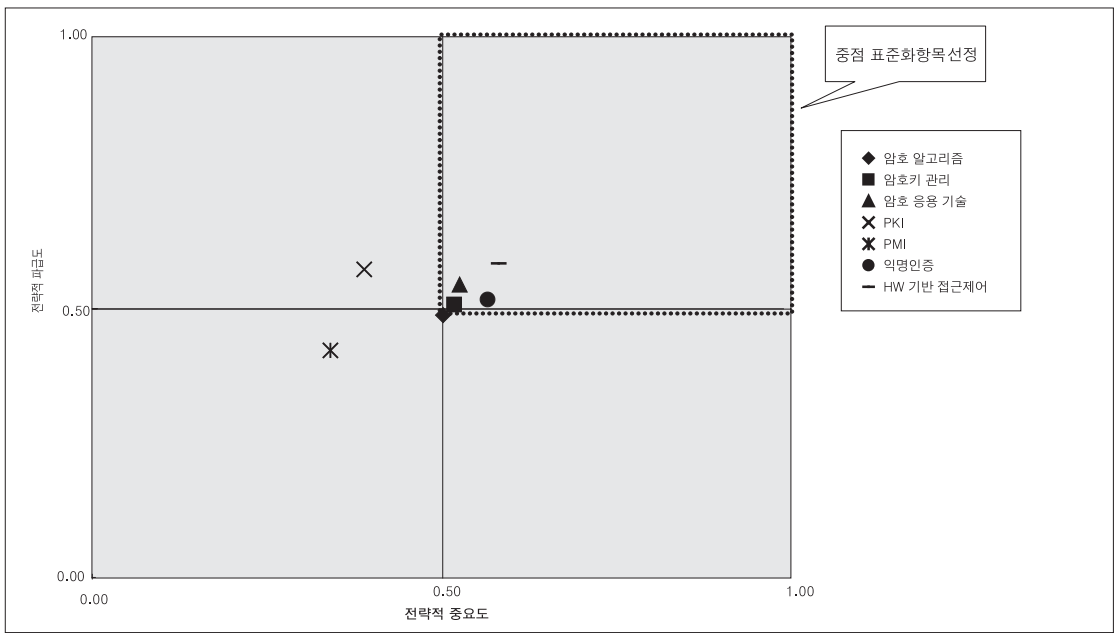
• 암호인증권한관리 분야



3.2. 중점 표준화항목 선

3.2.1. 중점 표준화항목 선정방법

표준화 대상항목별 전략적 중요도 및 파급도 분석												
	전략적 중요도						전략적 파급도					
고려요소	P_1 산학연 관심도 (투자 등)	P_2 정부 관심도 (정책 등)	P_3 표준선도 가능성 (표준 투자정도)	P_4 표준(기술) 개발의 시급성	P_5 기술(표준) 격차	PI (Priority Index)	E_1 타 산업 파급효과	E_2 경제적 파급효과	E_3 국내외 시장규모	E_4 IPR확보 가능성 (로얄티 수입)	E_5 사용자편의 (호환성/ 공공성 등)	EI (Effect Index)
고려요소별 가중치(합계 1)	0.1	0.1	0.2	0.4	0.2	1	0.3	0.4	0.1	0.1	0.1	1
암호 알고리듬	1.0	4.0	1.0	2.5	4.0	0.50	4.0	2.0	1.0	1.0	2.5	0.49
암호키 관리	2.0	4.0	2.0	3.0	2.0	0.52	2.0	3.0	2.0	2.0	3.5	0.51
암호 응용 기술	3.0	3.5	2.5	2.5	2.5	0.53	3.0	2.5	3.0	2.0	3.5	0.55
PKI	2.5	3.5	1.0	1.0	3.0	0.36	3.0	3.0	2.5	2.0	3.5	0.58
익명인증	2.0	3.0	3.0	3.0	3.0	0.58	2.5	2.5	2.0	2.5	4.0	0.52
PMI	2.0	2.0	1.0	1.0	2.5	0.30	2.0	2.0	2.0	2.0	3.0	0.42
HW 기반 잡근제어	3.5	3.0	3.0	3.5	2.0	0.61	3.5	2.5	3.0	2.0	3.5	0.58



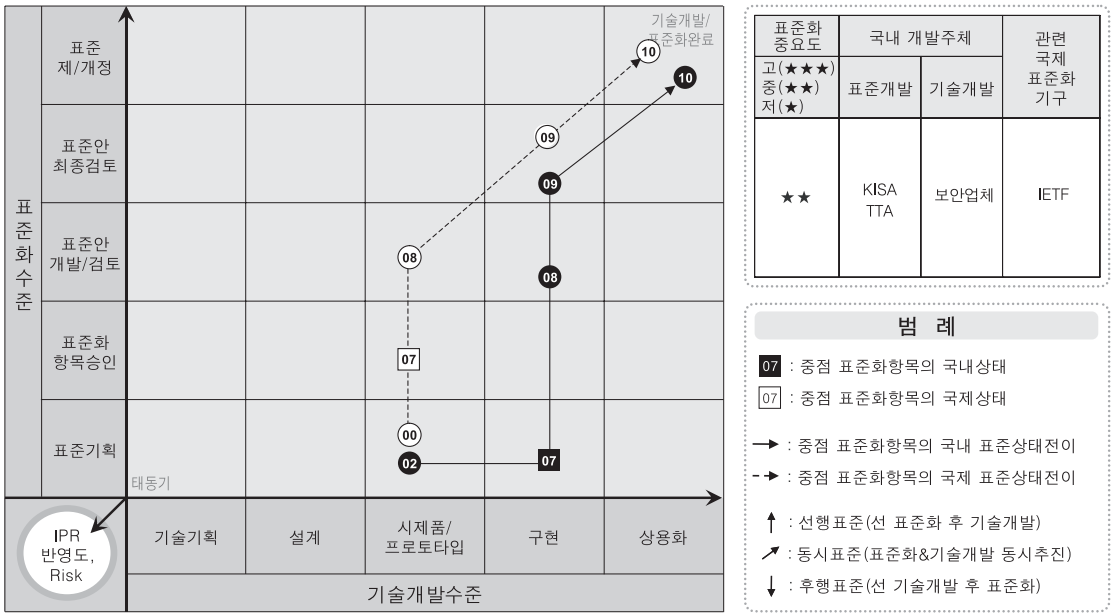
3.2.2. 중점 표준화항목 선정사유

- 전략적 중요도 및 기술적 파급효과의 요소
  - 유비쿼터스 사회에서 핵심적 기반기술인지 여부
  - u-IT 서비스 또는 환경에서 자체 기술 확보 또는 국제 경쟁 가능 여부
  - 현재 표준화 정도 및 향후 표준화 가능성 여부
- 중점 표준화항목별 선정사유
  - 암호 키 관리의 경우 전자정부 구현에 따라 암호통신이 활성화되면서 키 복구 기술 등이 중요
  - 암호응용기술의 경우 해킹 등으로부터 전자거래의 안전성을 확보하기 위한 핵심기술임. 국내 원천기술이 부족하여 대부분 국제표준에 따라 적용
  - 익명인증기술의 경우 인터넷 실명제 등에서 개인의 프라이버시를 보호하기 위한 기술로서 아직 표준화가 미흡한 상황
  - HW 기반의 접근제어 기술은 u-사회로 발전하면서 한 가지 이상의 접근통제 수단을 요구함에 따라 HW 기반 접근제어 기술은 필수적인 요소가 됨

3.3. 중점 표준화항목별 세부전략(안)

3.3.1. 암호 키 관리

• 표준상태전이도 (표준화 & 기술개발 연계분석)



표준화 중요도	국내 개발주체		관련 국제 표준화 기구
고(★★★) 중(★★) 저(★)	표준개발	기술개발	
★★	KISA TTA	보안업체	IETF

범 례

07 : 중점 표준화항목의 국내상태

07 : 중점 표준화항목의 국제상태

→ : 중점 표준화항목의 국내 표준상태전이

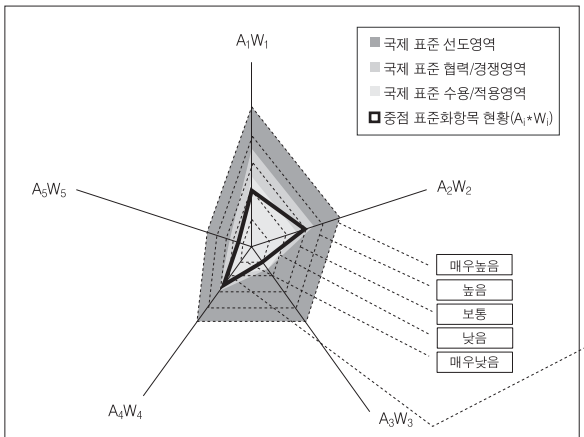
⇢ : 중점 표준화항목의 국제 표준상태전이

↑ : 선행표준(선 표준화 후 기술개발)

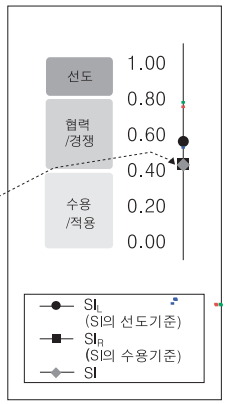
↗ : 동시표준(표준화&기술개발 동시추진)

↓ : 후행표준(선 기술개발 후 표준화)

• 국제표준화 전략목표 도출



SI (표준화 전략지수)	
SI_L (SI의 선도기준)	0.58
SI_R (SI의 수용기준)	0.42
SI	0.41



$$SI = (\sum_{i=1}^{5} A_i \cdot W_i) / 5$$

$$(0 < W_i < 1, 0 < SI \leq 1)$$

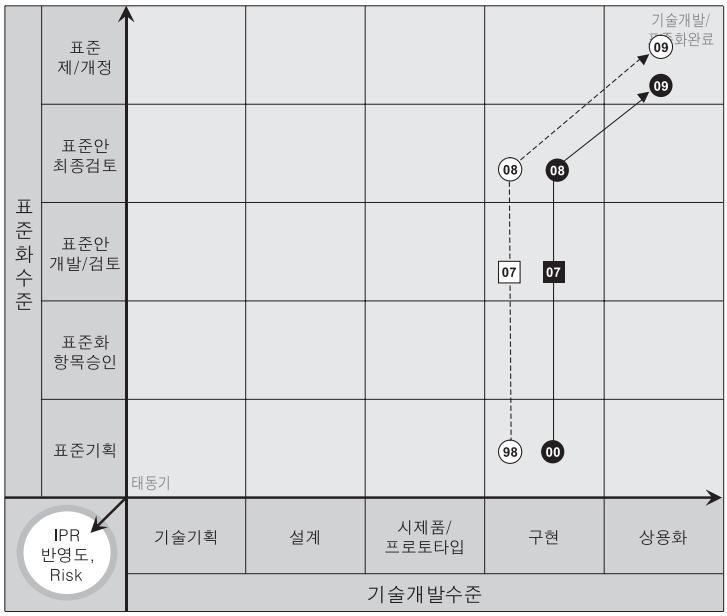
국제표준 협력/경쟁

• 세부전략(안)

- 국내 암호 키 관리 시스템 개발 경험을 토대로 표준화 항목을 도출하고 KISA 및 보안업체가 중심이 되어 국내 표준화를 추진
- 또한, 현재 IETF 보안분야의 KeyProv 워킹그룹에서는 암호 키와 관련하여 표준화를 추진 중에 있으므로 국내 암호 키 관리 시스템 개발 경험을 토대로 IETF 표준화에 적극적으로 참여하여 원천 기술보다는 서비스 관점에서 표준(안)을 제시

3.3.2. 암호 응용 기술

• 표준상태전이도 (표준화 & 기술개발 연계분석)



표준화 중요도	국내 개발주체		관련 국제 표준화 기구
고(★★★) 중(★★) 저(★)	표준개발	기술개발	
★★	KISA ETRI TTA	ETRI 보안업체	IETF

범 례

07 : 중점 표준화항목의 국내상태

07 : 중점 표준화항목의 국제상태

→ : 중점 표준화항목의 국내 표준상태전이

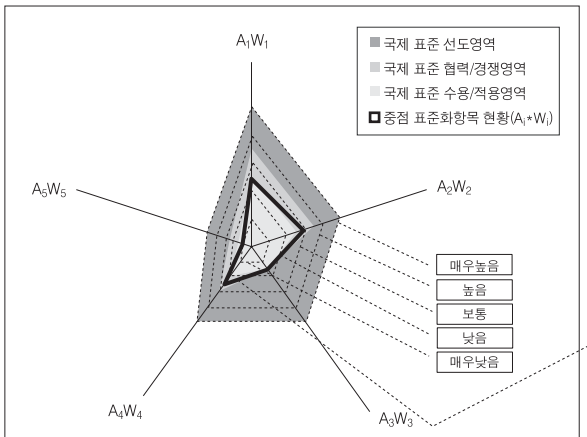
-→ : 중점 표준화항목의 국제 표준상태전이

↑ : 선행표준(선 표준화 후 기술개발)

↗ : 동시표준(표준화&기술개발 동시추진)

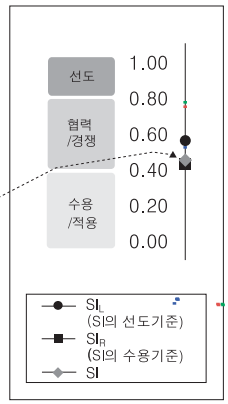
↓ : 후행표준(선 기술개발 후 표준화)

• 국제표준화 전략목표 도출



A_1 : 국외대비 국내표준화 수준
A_2 : 국외대비 국내기술개발수준
A_3 : IPR확보가능성
A_4 : 국내 표준화 인프라 수준
A_5 : 국제 표준화 기여도
W_i : A_i의 가중치

SI (표준화 전략지수)	
SI_L (SI의 선도기준)	0.58
SI_R (SI의 수용기준)	0.42
SI	0.45



$$SI = (\sum_{i=1}^{5} A_i \cdot W_i) / 5$$

$$(0 < W_i < 1, 0 < SI \leq 1)$$

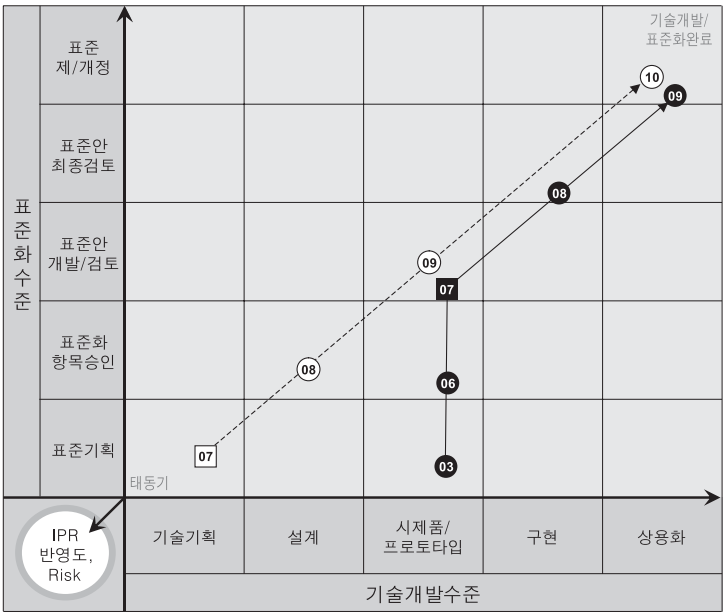
국제표준 협력/경쟁

• 세부전략(안)

- 기존 암호 메시지 전송, 암호토큰 인터페이스 기술 등은 이미 국제 표준화가 되어 있는 분야이므로 국내에서는 신규 IT서비스 및 최근 지속적으로 발전하는 해킹기술에 대응할 수 있는 암호응용기술 관점에서 표준안을 발굴하여 TTA를 중심으로 국제 경쟁력있는 표준화를 추진
- 더불어 국내 표준을 토대로 IETF 또는 ITU-T 등에서 국제 표준화 추진

3.3.3. 익명 인증

- 표준상태전이도 (표준화 & 기술개발 연계분석)

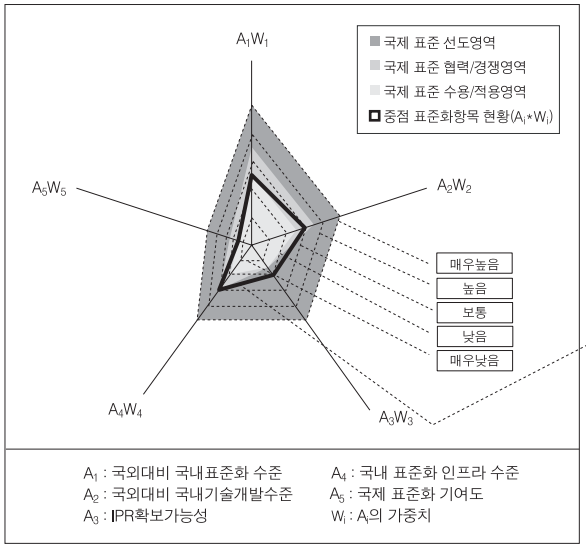


표준화 중요도	국내 개발주체		관련 국제 표준화 기구
고(★★★) 중(★★) 저(★)	표준개발	기술개발	
★★	KISA TTA	보안업체	IETF

범 례

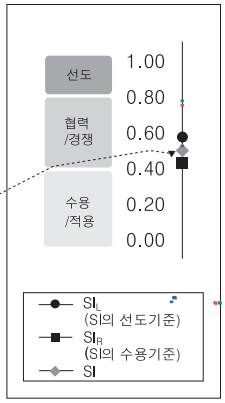
- 07 : 중점 표준화항목의 국내상태
- 07 : 중점 표준화항목의 국제상태
- → : 중점 표준화항목의 국내 표준상태전이
- ⇢ : 중점 표준화항목의 국제 표준상태전이
- ↑ : 선행표준(선 표준화 후 기술개발)
- ↗ : 동시표준(표준화&기술개발 동시추진)
- ↓ : 후행표준(선 기술개발 후 표준화)

- 국제표준화 전략목표 도출



A1 : 국외대비 국내표준화 수준
A2 : 국외대비 국내기술개발수준
A3 : IPR확보가능성
A4 : 국내 표준화 인프라 수준
A5 : 국제 표준화 기여도
Wi : Ai의 가중치

SI (표준화 전략지수)	
SI_L (SI의 선도기준)	0.58
SI_R (SI의 수용기준)	0.42
SI	0.50



$$SI = (\sum_{i=1}^{5} A_i \cdot W_i) / 5$$
$$(0 < W_i < 1, 0 < SI \leq 1)$$

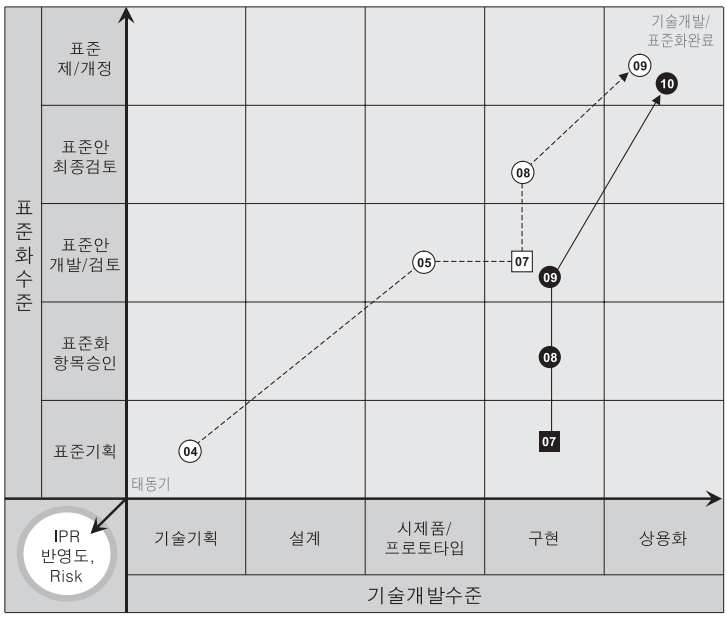
국제 표준 협력/경쟁 (일부선도)

• 세부전략(안)

- 익명인증기술 분야는 아직 표준화가 추진되고 있지 않는 분야이므로, 우선 KISA, ETRI를 중심으로 국내 표준안을 제정하여 TTA에 표준화를 추진하고
- 국내 표준을 바탕으로 IETF 등 국제 표준화 기구에 표준으로 제안

3.3.4. HW 기반 접근제어

• 표준상태전이도 (표준화 & 기술개발 연계분석)



표준화 중요도	국내 개발주체		관련 국제 표준화 기구
고(★★★) 중(★★) 저(★)	표준개발	기술개발	
★★	KISA ETRI TTA	전문 보안업체	IETFI TU-T

범 례

07 : 중점 표준화항목의 국내상태

07 : 중점 표준화항목의 국제상태

→ : 중점 표준화항목의 국내 표준상태전이

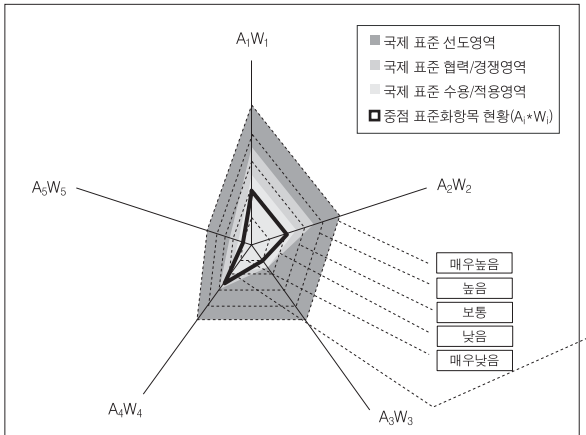
⇢ : 중점 표준화항목의 국제 표준상태전이

↑ : 선행표준(선 표준화 후 기술개발)

↗ : 동시표준(표준화&기술개발 동시추진)

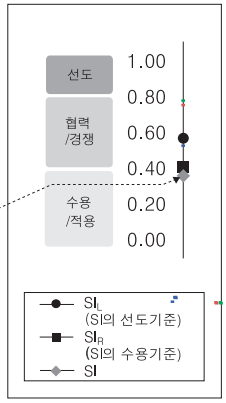
↓ : 후행표준(선 기술개발 후 표준화)

• 국제표준화 전략목표 도출



A_1 : 국외대비 국내표준화 수준
A_2 : 국외대비 국내기술개발수준
A_3 : IPR확보가능성
A_4 : 국내 표준화 인프라 수준
A_5 : 국제 표준화 기여도
W_i : A_i의 가중치

SI (표준화 전략지수)	
SI_L (SI의 선도기준)	0.58
SI_R (SI의 수용기준)	0.42
SI	0.36



$$SI = (\sum_{i=1}^{5} A_i \cdot W_i) / 5$$
$$(0 < W_i < 1, 0 < SI \leq 1)$$

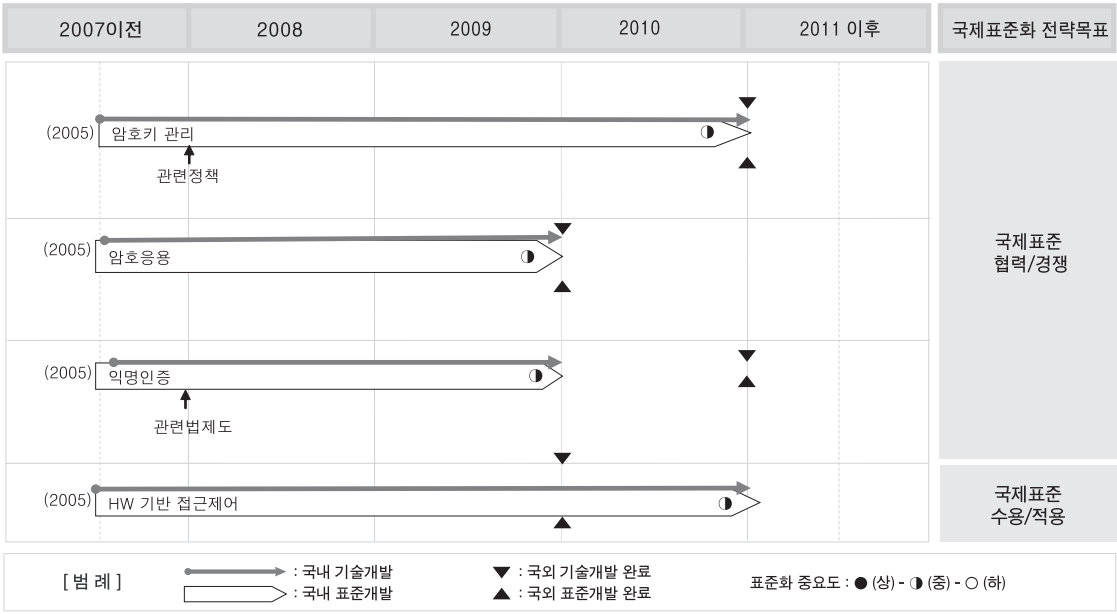
국제표준
수용/적용

• 세부전략(안)

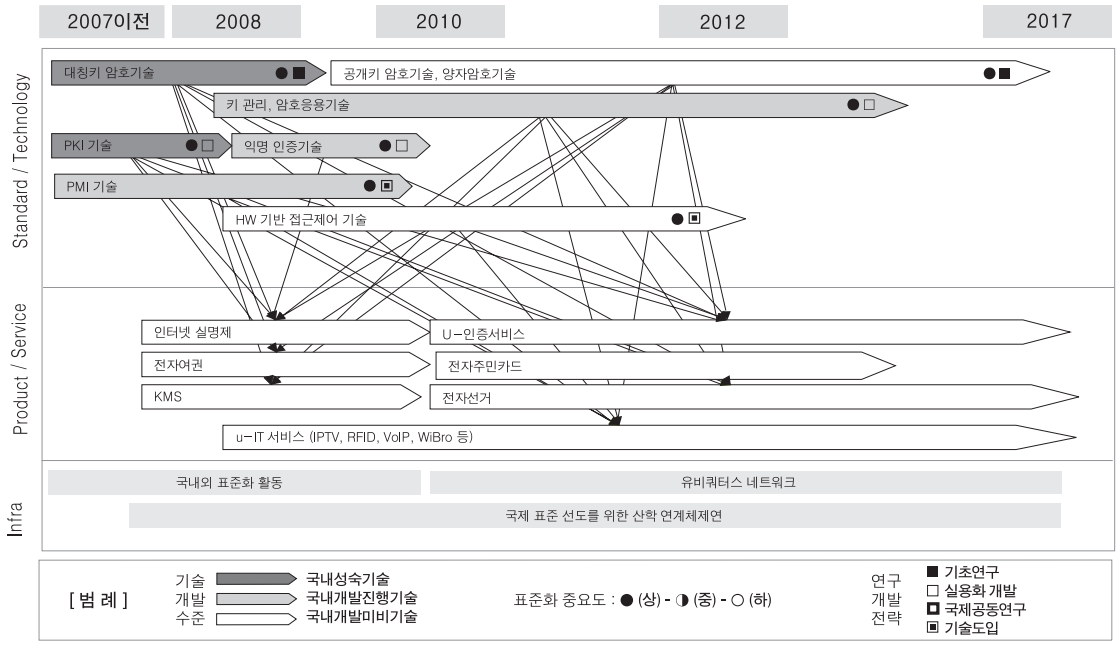
- 하드웨어 기반 접근제어 기술은 이미 OTP 등 일부 하드웨어 매체를 통하여 이루어지고는 있으나 유비쿼터스 사회에서는 모든 사물, 기기, 사람이 네트워크를 통해 연결되기 때문에 현재 보다 고도화된 하드웨어 기반의 접근제어 기술이 필요할 것으로 보임
- 따라서, 우리나라는 유비쿼터스 환경을 고려한 하드웨어 기반의 접근제어 기술을 개발하여 국제 표준안을 개발할 필요가 있음

3.4. 중장기 표준화로드맵

3.4.1. 중기('08~'10) 표준화로드맵



3.4.2. 장기 표준화로드맵(10년 기술예측)



[국내외 관련표준 대응리스트]

구분	표준명	기구(업체)	제정 연도	재개정 현황	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/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

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

구분	표준명	기구(업체)	제정	연도	재개정	현황
인증 기술	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
	RFC 2692 SPKI Requirements	IETF	1999	초안		[illegible]
	RFC 2693 SPKI Certificate Theory	IETF	1999	초안		[illegible]
	ISO/IEC 18014-1 Time stamping services and protocols- Part 1 : Framework	ISO/IEC JTC1/SC27/WG1	2002	초안		TTA/ISTF
	ISO/IEC 18014-2 Time stamping services and protocols - Part 2 : Mechanisms producing independent tokens	ISO/IEC JTC1/SC27/WG2	2002	초안		TTA/ISTF
	ISO/IEC 18014-3 Time stamping services and protocols - Part 3 : Mechnisms producing linked tokens	ISO/IEC JTC1/SC27/WG2	2000	초안		TTA/ISTF
	ISO/IEC 15945 Specification of TTP services to support the application of digital signatures	ISO/IEC JTC1/SC27/WG1	2002	초안		TTA/ISTF
	ISO/IEC9979 Information technology-Security techniques-Procedures for the registration of cryptographic algorithms(Revision of ISO/IEC 9979:1991)	JTC1/SC27/WG1	1999	초안	KS X 1209	TTA/ISTF
	ISO/IEC 9594-8 Information technology-OSI-The Directory-Public-key and Attribute Certificate framework	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 응용 중 전자 우편 보안	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

구분	표준명	기구(업체)	제정	연도	재개정	현황
일반 응용 중 전자 우편 보안	RFC 3156 MIME Security with OpenPGP	IETF	2001	초안		TTA/ISTF
	RFC 2984 Use of the CAST-128 Encryption Algorithm in CMS	IETF	2000	초안	ISTF-011	TTA/ISTF
	RFC 2634 Enhanced Security Services for S/MIME	IETF	1999	초안	ISTF-010	TTA/ISTF
	RFC 2633 S/MIME Version 3 Message Specification	IETF	1999	초안	ISTF-009	TTA/ISTF
	RFC 2632 S/MIME Version 3 Certificate Handling	IETF	1999	초안	ISTF-008	TTA/ISTF
	RFC 2631 Diffie-Hellman Key Agreement Method	IETF	1999	초안	ISTF-007	TTA/ISTF
	RFC 2630 Cryptographic Message Syntax	IETF	1999	초안	ISTF-006	TTA/ISTF
	RFC 3125 Electronic Signature Policies	IETF	2001	초안		TTA/ISTF
	RFC 3183 Domain Security Services using S/MIME	IETF	2001	초안		TTA/ISTF
	RFC 2857 The Use of HMAC-RIPEMD-160-96 within ESP and AH	IETF	2000	초안		TTA/ISTF
	RFC 2440 OpenPGP Message Format	IETF	1998			TTA/ISTF

[참고문헌]

〔1〕 KISA, 정보보호 표준화 로드맵, 2004.7.

〔2〕 염흥열, 2003년도 정보보호일반 표준화 로드맵, TTA, 2003.

〔3〕 KISA, http://www.kisa.or.kr/, 정보보호 표준화 목록, 2003.

〔4〕 IETF, http://www.ietf.org/, IETF, PKIX, IPSec, S/MIME, MSEC 등의 작업반 홈페이지, 2003.

〔5〕 OMA, http://www.wapforum.org/, OMA 홈페이지, 2003.

〔6〕 ITU, http://www.itu.int/home/index.html, ITU 홈페이지, 2003.

〔7〕 NIST, http://www.nist.gov/, NIST 홈페이지, 2003

〔8〕 ISO/IEC JTC1, http://www.jtc1.org/, ISO 홈페이지, 2003

〔9〕 TTA, http://www.tta.or.kr, TTA홈페이지, 2003.

〔10〕 MIC, http://www.mic.go.kr/index.jsp, MIC 홈페이지, 2003.

〔11〕 MIC, 정통부 정보보호 중장기 기술개발계획서, 초안, 2003

〔12〕 MIC, 정통부 정보보호 중장기 기술개발계획서, 2002.

〔13〕 이계상, 류재철, 이광수, 이재광, 염흥열, 정수환, 채기준, IETF 정보보호 표준화 동향 분석에 관한 연구, 한국정보보호진흥원, 2002.12.

〔14〕 과기처, 정보보호분야 국가기술지도 맵, 김홍근, 염흥열, 이희조, 2003.7.

〔15〕 Rivest, R., "The MD5 Message-Digest Algorithm", RFC 1321, April 1992.

〔16〕 Eastlake, D. and P. Jones, "US Secure Hash Algorithm 1 (SHA1)", RFC 3174, September 2001.

〔17〕 Housley, R., Ford, W., Polk, W. and D. Solo, "Internet X.509 Public Key Infrastructure Certificate and CRL Profile", RFC 3280, April 2002.

〔18〕 Housley, R., Ford, W., Polk, W. and D. Solo "Internet X.509 Public Key Infrastructure: Certificate and CRL Profile", RFC 2459, January, 1999.

〔19〕 Myers, M., Ankney, R., Malpani, A., Galperin, S. and C. Adams, "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP", RFC 2560, June 1999.

〔20〕 Pinkas, D., Ross, J. and N. Pope, "Electronic Signature Policies", RFC 3125, September 2001.

〔21〕 Pinkas, D., Ross, J. and N. Pope, "Electronic Signature Formats for long term electronic signatures", RFC 3126, September 2001.

〔22〕 Housley, R. and P. Hoffman, "Internet X.509 Public Key Infrastructure. Operational Protocols: FTP and HTTP", RFC 2585, May 1999.

〔23〕 Boeyen, S., Howes, T. and P. Richard, "Internet X.509 Public Key Infrastructure Operational Protocols LDAPv2", RFC 2559, April 1999.

〔24〕 Hoffman, P., "Enhanced Security Services for S/MIME", RFC 2634, June 1999.

[25] Kent, S., "Privacy Enhancement for Internet Electronic Mail: Part II: Certificate-Based Key Management", RFC 1422, February 1993.

[26] Balenson, D., "Privacy Enhancement for Internet Electronic Mail: Part III: Algorithms, Modes, and Identifiers", RFC 1423, February 1993.

[27] Bradner, S., "Key Words for Use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[28] Kaliski, B., "PKCS #1: RSA Encryption Version 1.5", RFC 2313, March 1998.

[29] US National Computer Security Center, "Department of Defense Trusted Computer System Evaluation Criteria", DoD 5200.28-STD, US Department of Defense, Ft. Meade, MD., December 1985.

[30] US National Computer Security Center, "Trusted Network Interpretation of the Trusted Computer System Evaluation Criteria", NCSC-TG-005, Version 1, US Department of Defense, Ft. Meade, MD., 31 July 1987.

[31] Haller, N., and R. Atkinson, "On Internet Authentication", RFC 1704, October 1994.

[32] Harkins, D., and D. Carrel, "The Internet Key Exchange (IKE)", RFC 2409, November 1998.

[33] SDNS Secure Data Network System, Security Protocol 3, SP3, Document SDN.301, Revision 1.5, 15 May 1989, published in NIST Publication NIST-IR-90-4250, February 1990.

[34] Shacham, A., Monsour, R., Pereira, R., and M. Thomas, "IP Payload Compression Protocol (IPComp)", RFC 2393, August 1998.

[35] Thayer, R., Doraswamy, N., and R. Glenn, "IP Security Document Roadmap", RFC 2411, November 1998.

[36] John Ioannidis and Matt Blaze, "Architecture and Implementation of Network-layer Security Under Unix", Proceedings of USENIX Security Symposium, Santa Clara, CA, October 1993.

[37] Kent, S., and R. Atkinson, "IP Authentication Header", RFC 2402, November 1998.

[38] Kent, S., and R. Atkinson, "IP Encapsulating Security Payload (ESP)", RFC 2406, November 1998.

[39] Kent, S., "US DoD Security Options for the Internet Protocol", RFC 1108, November 1991.

[40] Maughan, D., Schertler, M., Schneider, M., and J. Turner, "Internet Security Association and Key Management Protocol (ISAKMP)", RFC 2408, November 1998.

[41] Orman, H., "The OAKLEY Key Determination Protocol", RFC 2412, November 1998.

[43] Piper, D., "The Internet IP Security Domain of Interpretation for ISAKMP", RFC 2407, November 1998.

[43] ITU-T X680, Abstract Syntax Notation One (ASN.1): Specification of Basic Notation, ITU-T Recommendation X.680 (1997) | ISO/IEC International Standard 8824-1:1998.

[44] ITU-T X690, ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules(DER), ITU-T Recommendation X.690 (1997)| ISO/IEC

International Standard 8825-1:1998.

〔45〕 CCITT Recommendation X.208: Specification of Abstract Syntax Notation One (ASN.1), 1988.

〔46〕 ITU-T Recommendation X.660 Information Technology -ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER), 1997.

〔47〕 X9.62-1998, "Public Key Cryptography For The Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)", January 7, 1999.

〔48〕 ISO/IEC 9594-8/ITU-T Recommendation X.509, "Information Technology - Open Systems Interconnection: The Directory: Authentication Framework," 1997 edition.

〔49〕 ISO/IEC JTC1/SC6, Network Layer Security Protocol, ISO-IEC DIS 11577, International Standards Organisation, Geneva, Switzerland, 29 November 1992.

〔50〕 Federal Information Processing Standards Publication (FIPS PUB) 180-1, Secure Hash Standard, 17 April 1995.

〔51〕 Federal Information Processing Standards Publication (FIPS PUB) 186, Digital Signature Standard, 27 January 2000. 〔Supersedes FIPS PUB 186-1 dated 15 December 1998.〕

〔52〕 ANSI X9.42-2000, "Public Key Cryptography for The Financial Services Industry: Agreement of Symmetric Keys Using Discrete Logarithm Cryptography", December, 1999.

〔53〕 ANSI X9.63-2001, "Public Key Cryptography For The Financial Services Industry: Key Agreement and Key Transport Using Elliptic Curve Cryptography", Work in Progress.

〔54〕 IEEE P1363, "Standard Specifications for Public-Key Cryptography", 2001.

〔55〕 Bruce Schneier, Applied Cryptography, Section 8.6, John Wiley & Sons, New York, NY, 1994

〔56〕 ITU-T Recommendation X.1121, "X.1121: Framework of security technologies for mobile end-to-end data communication", ITU-T SG17, March 2004.

〔57〕 ITU-T Recommendation X.1122, "X.1122: Guideline for implementing secure mobile systems based on PKI ", ITU-T SG17, March 2004.

〔58〕 ITU-T Recommendation J.190 "Architecture of MediaHomeNet that supports cable based services" defines a reference model of home network based on cable network and describes security requirements for the reference model.

〔59〕 ITU-T Recommendation J.192 "Residential Gateway to support the delivery of cable data services" describes home gateway security.

〔60〕 Heung-Youl Youm, Heung-Ryong Oh, "Updated first draft Recommendation X.homesec-1: Framework of security technologies for home network", ITU-T SG17, COM17-D172-E, April 2006.

〔61〕 Dong-Young Yoo, Gang-Shin Lee, Jae-IL Lee, Heung-Youl Youm, "Draft text on X.homesec-2 : Device

certificate profile for the home network", ITU-T SG17, COM17-D173-E, April 2006.

〔62〕 Hyung-Kyu Lee, Hong-IL Ju, Yun-Kyung Lee, Jong-Wook Han, Kyo-IL Chung, Heung-Youl Youm, "Proposal for the first draft of X.homesec-3 User authentication mechanism for home network services", ITU-T SG17, COM17-D176-E, April 2006.

〔63〕 Jianyoung Chen, Feng Zhang, "First draft—General security service (policy) for secure mobile end to end data communication, X.msec-3, ITU-T SG17, TD2330, Arpil 2006.

〔64〕 Zheng Zhibin, Wei Jiwei, "Revised text of X.msec-4 from the Editor", ITU-T SG17, COM17-187-E, April 2006.

〔65〕 Liu Shuling, Wei Jiwei, Zheng Zhibin, "New draft text of X.crs: Correlative reacting system in mobile data communication", ITU-T SG17, COM17-189Rev.1-E, April 2006.

〔66〕 Heung-Youl Youm, Young-Man Park, "New Draft Text of X.sap-1: Guideline on secure password-based authentication protocol with key exchange", ITU-T SG17, COM17-D171-E, April 2006.

〔67〕 Tadashi KAJI, "Proposal on the process model of secure communications for X.sap-2", ITU-T SG17, COM17-D143-E, April 2006.

〔68〕 Yutaka Miyake, "Proposal of Recommendation X.p2p-1 structure", ITU-T SG17, COM17-D144-E, April 2006.

〔69〕 Hyeok-Chan Kwon, Jae-Hoon Nah, Jong-Soo Jang, "Secure Routing on P2P Overlay Networt 외 3편", ITU-T SG17, COM17-D193~6-E, April 2006.

〔70〕 Abbie Barbir, "ITU-T Candidate Recommendation X.websec-1 - Security Assertion Markup Language (SAML)", ITU-T SG17, TD2273Rev.2, April 2006.

〔71〕 Abbie Barbir, "Extensible Access Control Markup Language Version 2.0 (XACML)", ITU-T SG17, TD2278Rev.3, April 2006.

〔72〕 Jae-Seung Lee, Ki-Yoong Moon, Kyo-IL Chung, "Guideline on Security Architecture for Message Security in Mobile Web Services", ITU-T SG17, COM17-D174—E, April 2006.

〔73〕 염흥열, "ITU-T 모바일 보안 표준 분석 및 전망", TTA IT Standard Weekly, 2004.4.

〔74〕 오흥룡, 염흥열, "ITU-T SG17 정보보호 표준화 동향과 Mobile Security 표준 분석", 한국정보보호진흥원, 2004.12.

〔75〕 염흥열, "ITU-T SG17 WP2 Q.9(안전한 통신 서비스) 표준화 동향 및 향후 전망", 한국정보보호진흥원, 2005.12.

〔76〕 염흥열, ITU-T SG17 종단간 이동 통신 보안을 위한 보안 정책 및 홈 네트워크 보안 프레임워크에 관한 표준화 동향 , TTA IT Standard Weekly, 2005.1.

〔77〕 염흥열, "ITU-T가 홈 네트워크 보안 표준을 주도할 수 있을까?", TTA IT Standard Weekly, 2005.5.

〔78〕 진병문, 오흥룡, 염흥열, 정교일, "ITU-T SG17 모스크바 회의", TTA 저널, 99호, 2005.6.

〔79〕 진병문, 오흥룡, 염흥열, 정교일, "ITU-T SG17 제네바 회의", TTA 저널, 102호, 2005.12.

〔80〕 진병문, 오흥룡, 염흥열, 강신각, "2005년 ITU-T SG17 연구동향", TTA, ITU-T 연구활동 보고서, 2005.12.

〔81〕 정보통신부, "유비쿼터스 정보보호 기본전략", 2006. 12.

〔82〕 한국정보보호진흥원, "2006 국내 정보보호산업통계조사 ' 2006. 11.

〔82〕 한국정보보호진흥원, "국내외 정보보호산업 현황 및 주요 정책진단 : FTA등 시장개방화 환경을 중심으로", 정보보호 이슈리포트 2007-06, 2007. 5.

[약어]

AAA	Authentication, Authorization, Accounting
AES	Advanced Encryption Standard
AMP	Authentication and key agreement via Memorable Passwords
AP	Access Point
API	Application Program Interface
BcN	Broadband Convergence Network
CA	Certification Authority
CC	Common Criteria
CMVP	Cryptographic Module Validation Program
DES	Data Encryption Standard
DLP	Discrete Logarithm Problem
DPA	Differential Power Analysis Attack
DRM	Digital Rights Management
EAM	Extranet Access Management
ECC	Elliptic Curve Cryptosystem
ETRI	Electronic Telecommunications Research Institute
ETSI	European Telecommunications Standards Institute
FIPS	Federal Information Processing Standards
HAS-160	160-bit Hash Algorithm Standard
IETF	Internet Engineering Task Force
IM/IAM	Identity Management/Identity Access Management
IPSec	Internet Protocol Security
ISO/IEC	International Organization for Standardization/International Electrotechnical Commission
ITU-T	Intgernational Telcommunication Union-Telecommunication
KCDSA	Korea Information Security AgencyKorea Certificate-based Digital Signature Algorithm
KISA	Korea Information Security Agency
LDAP	Lightweight Directory Access Protocol
NIST	National Institute of Standards and Technology
NSRI	National Security Research Institute
OMA	Open Mobile Alliance
OTP	One Time Password

PAKE	Password Authentication Key Exchange
PKCS	Public-Key Cryptography System
PKI	Public Key Infrastructure
PMI	Privilege Management Infrastructure
RFID	Radio Frequence Identification
RSA	Rivest-Shamir-Adelman)
RSA-OAEP	RSA-Optimal Asymmetric Encryption Padding
SIM	Subject Identity Module
SSL	Secure Socket Layer
SSO	Single Sign-on
TLS	Trnansport Layer Security
TTA	Telecommunications Technology Association
USN	Ubiquitous Sensor Network
WIM	Wireless Identity Module
XML	extensible Markup Language