[참고문헌]

[1] 한국정보통신기술협회, "정보통신표준화백서," 2002.

[2] 한국정보통신기술협회, "IT839전략 표준화로드맵 Ver2005," 2004.12.

[3] 한국전자통신연구원, "u-컴퓨팅 표준 플랫폼 기획위원회 보고서," 2006. 8.

[4] JCP - www.jcp.org

[5] OMA - www.openmobilealliance.org

[6] OSGi - http://www.osgi.org

[7] GNU - http://www.gnu.org

[8] KOTBA - http://www.kotba.org

[9] NOKIA - http://www.forum.nokia.com/main/platforms/index.html

[10] INTEL - http://developer.intel.com

[11] 모바일 자바 커뮤니티 - http://www.mobilejava.co.kr/

[12] 선 자바사이트 - http://java.sun.com/javame/index.jsp

[13] IBM - http://www.ibm.com/servicessolutions/us/

[14] 정보처리학회지 2006. 3. 제 13권 제 2호

[15] IPTV 기술워크샵 자료 2006. 4. 18 ~ 19

[16] Mobile Conference & Exhibition 2006 Proceeding, "Future of Mobile Convergence," 2006.04.28

[17] EJB(Enterprise JavaBeans) - http://java.sun.com/products/ejb

[18] Web Services Interability Organization - http://www.ws-i.org

[19] Microsoft .NET homepage - http://www.microsoft.com/net/

[20] CLR(Common Language Runtime) - http://msdn.microsoft.com/netframework/programming/clr/

[21] C# - http://msdn.microsoft.com/vcsharp

[22] Mono project - http://www.mono-project.com

[23] CORBA(Common Object Request Broker Architecture) - http://www.corba.org/

[24] Component Object Model Technology - http://www.microsoft.com/com/

[25] Liberty Alliance Project - http://www.projectliberty.org

[26] Khronos Group - http://www.khronos.org

[27] LiPS Forum - http://lipsforum.org

[28] Mobile Industry Processor Interface - http://www.mipi.org

[29] CE Linux Forum - http://www.celinuxforum.org

정보 보호 공통 플랫폼

1. 개요

1.1. 추진경과 및 중점 추진방향

■ 추진경과

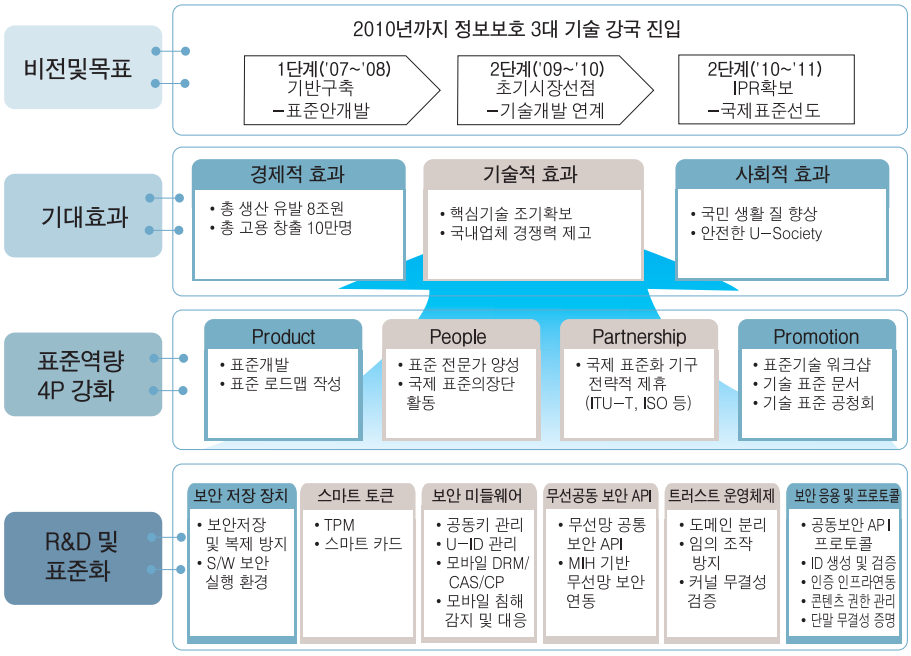
- 2006년(Ver.2007)부터 "소프트인프라웨어"상에서 사용자/단말/네트워크 간의 침해 확산을 차단하고, 융복합 서비스간의 보안 호환성을 공통적으로 제공하는데 필요한 보안 플랫폼의 보안저장장치, 스마트토큰, 보안 미들웨어, 무선공통보안API, 트러스트 운영체제, 보안 응용 및 프로토콜을 신규 중점 표준화 대상항목으로 선정하였다.

2006년(Ver.2007)		비고
정보 보호 공통 플랫폼	보안저장장치	2006년 신규 중점기술
	스마트 토큰	
	보안 미들웨어	
	무선공통보안API	
	트러스트 운영체제	
	보안 응용 및 프로토콜	
	트러스트 I/O	추후 추진 예정
	소프트웨어 다운로드 보안	추후 추진 예정

■ 중점 추진방향

- 2006년(Ver.2007)에는 "소프트인프라웨어"를 위한 정보 보호 공통 플랫폼을 신규 중점기술로 선정하고, 시장 파급성, 표준화 적시성 등을 고려하여 중점 표준화 대상항목을 선정함
- 이에 따라, 중점 표준화 분야로 보안저장장치, 스마트토큰, 무선공통보안API, 트러스트 운영체제, 보안 응용 및 프로토콜을 선정함
- 트러스트 I/O와 소프트웨어 다운로드 보안은 표준화 적시성 등을 고려하여 추후 추진할 것으로 방향을 정함
- 정보 보호 공통 플랫폼의 표준화로드맵은 소프트인프라웨어상의 연관기술(예, u-컴퓨팅 플랫폼 등)과의 연동 및 연관 서비스(예, 텔레메틱스/LBS 등)와의 표준화 연계를 통하여 표준화 성공 가능성을 높이는 추진 전략 마련

1.2. 표준화의 Vision 및 기대효과



(그림 1) 정보 보호 공통 플랫폼 기술 표준화의 비전 및 기대효과

1.2.1. 표준화의 필요성

다양한 u-IT 융 · 복합 서비스가 기대되는 유비쿼터스 환경에서 끊김없는 보안 서비스와 보안 호환성을 제공하고, 지식 콘텐츠 보호 및 모바일 침해 확산을 방지하는 기술의 표준화추진이 필요

- u-IT 융 · 복합 서비스 환경에서는 사이버 위협(개인정보 침해, 모바일 악성 코드, 지재권 침해 등)의 심화 확대가 예상된다. 또한, 이종 무선망, 이종 IT서비스간의 연동 또는 융 · 복합에 따라 컨버전스 지점이 보안 취약 지점으로 등장할 것으로 예상되며, 국부적인 피해가 전체로 확산될 위험이 증가하고 있다. 따라서, 무선망 · IT서비스간 융 · 복합화가 진행되는 u-IT 융 · 복합 서비스 환경에서, 사용자에게 통신 보안호환성과 끊김없는 신뢰 무결성을 갖는 융 · 복합 서비스 이용 환경을 제공하고, 융 · 복합 지식 서비스의 침해확산을 차단하는데 필요한 기술의 표준화가 필요하다.
- 사람과 소유물이 연계된 다양한 형태의 u-IT 융 · 복합 서비스가 개방형 스마트 단말에서 제공됨에 따라, 해당 서비스에 적합한 맞춤형 보안실행환경 지원 및 개방형 모바일 플랫폼 실행환경의 보안 Trust를 보장 (즉, 임의 조작 방지)해주는 기술의 표준화가 필요하다.
- 콘텐츠의 융 · 복합, 사용자 제작 콘텐츠, 새로운 프로슈머(Prosumer) 서비스 출현 등에 따라, 서비스 도메인별로 다르게 요구된 지재권 보호 수단(mDRM, CAS, CP, COI/UCI, 전자문서 보관소 등)의 융 · 복합화

및 기술의 국산화 및 표준화가 필요하다.

- 따라서, 국내외적으로 연구 초기 단계에 있는 융 · 복합 서비스 정보 보호의 핵심기술을 조기에 표준화를 추진해야 할 필요성이 대두되었다.

1.2.2. 표준화의 목표

u-City, u-Biz 등 다양한 u-IT 융 · 복합 서비스가 기대되는 유비쿼터스 환경에서 끊김없는 보안 서비스와 보안 호환성을 제공하기 위한 정보 보호 공통 플랫폼 핵심기술의 국내외 표준화 추진

- 1단계로 2009년까지 서비스 연동을 위한 정보 보호 공통 플랫폼 핵심 요소기술의 표준(안)을 개발하여 TTA에 국내표준화를 추진하고, 단계적으로 ITU-T, ISO 등을 통하여 국제표준화를 추진한다.
- 2단계로 2011년까지 융 · 복합 서비스를 위한 정보 보호 공통 플랫폼 핵심 요소기술의 표준(안)을 개발하여 TTA에 국내표준화를 추진하고, 단계적으로 ITU-T, ISO 등을 통하여 국제표준화를 추진한다.

1.2.3. Vision 및 기대효과

유비쿼터스 환경에서 안전한 융 · 복합 서비스 제공을 위한 정보 보호 핵심 기반 기술 표준화 선도 및 서비스를 활성화

- 안전한 융 · 복합 서비스 제공을 위한 정보 보호 핵심 기반 기술 표준화를 선도한다.
  - u-IT 융 · 복합 서비스 산업 활성화의 걸림돌인 보안 호환성 및 위협 해소
  - 정보보호 기술을 활용한 융 · 복합 서비스 활성화 및 시장 창출 유도
  - 융 · 복합 및 무선 공통 보안 분야의 de-facto 표준 기술 선도

- u-IT 융 · 복합 서비스 활성화를 위한 촉매/기폭제 역할을 한다.
  - 표준화 기술의 조기 확보를 통하여 스마트 단말 및 융 · 복합 서비스 분야에서 세계 시장 경쟁력 확보 및 국내 시장 보호
  - u-IT 융 · 복합 서비스를 위한 안전한 서비스 및 무선 보안 플랫폼 구축 및 스마트 단말 보안 표준화 기술 확보를 통해 융 · 복합 서비스 활성화 및 신시장 개척

- 국내 · 외적으로 연구 초기 단계에 있는 융 · 복합 서비스 정보 보호의 핵심기술을 조기에 표준화함으로써, 융 · 복합으로 인한 사생활 · 지재권 등의 정보화 침해 심화 또는 확산을 차단하는 안전한 u-IT 서비스 조기 정착 및 신규 보안 서비스 시장 창출에 기여한다.

2. 국내외 현황 분석

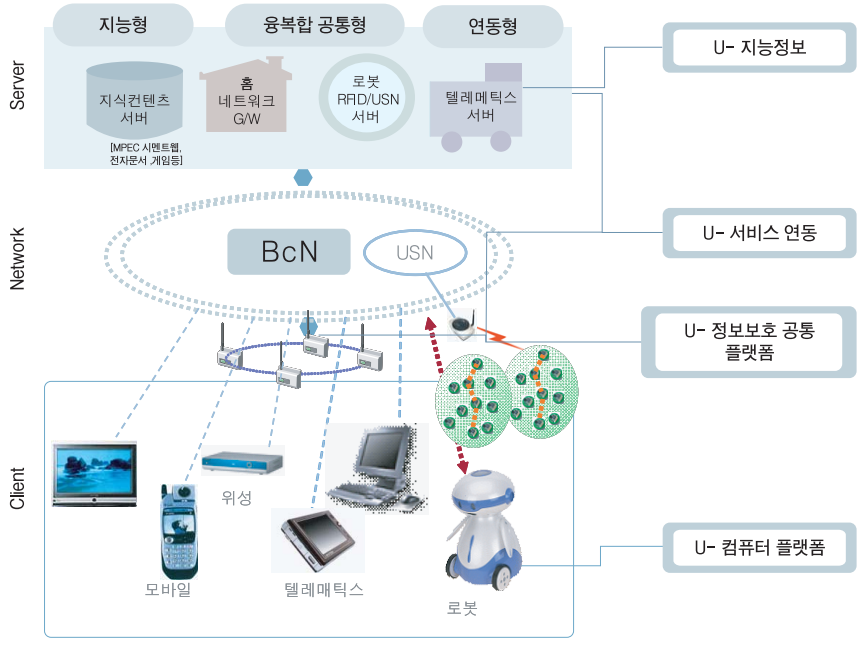
2.1. 중점기술 개요

2.1.1. 중점기술 및 표준화 대상항목의 정의

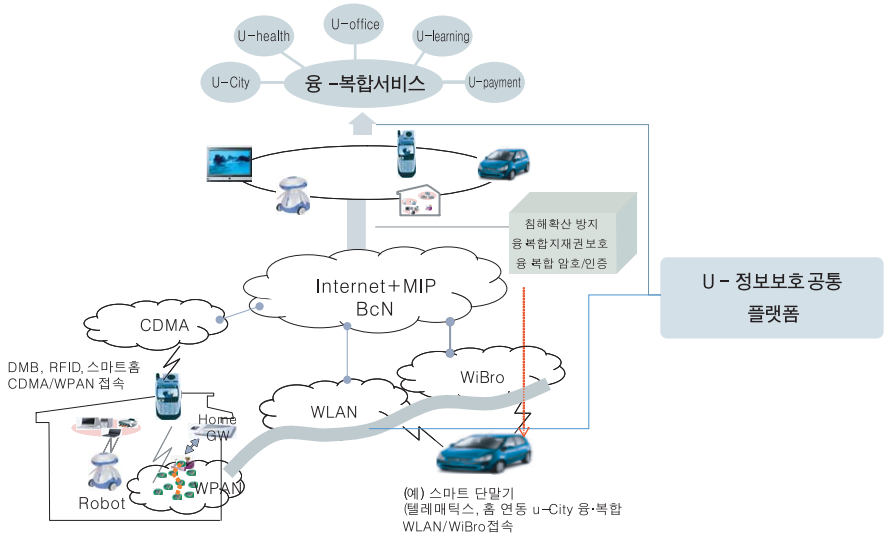
• 중점기술의 정의

정보 보호 공통 플랫폼 기술이란 안전하고 신뢰성 있는 소프트인프라웨어 구축을 위해 u-City, u-Home 등과 같은 다양한 u-IT 서비스 환경에서 1) 융 · 복합 서비스의 이용 안전성과 편리성을 제공하는 보안, 2) 융 · 복합 지식 · 콘텐츠 보호 및 모바일 침해확산을 차단하는 보안 등의 서비스를 제공하는 정보 보호 공통 소프트웨어 기술을 의미함

- 소프트인프라웨어란 차세대 이동통신, 모바일 융합 방송(DMB, m-IPTV), 스마트 차량, u-Home 등이 연계되는 환경에서 융 · 복합되거나 새롭게 창출되는 u-IT 서비스(예, u-City)를 효과적으로 구현하고, 신뢰성 있고 편리한 이용 환경을 제공하는 소프트웨어 기반으로 주요 핵심기술은 u-서비스 연동 플랫폼, u-지능정보, u-컴퓨팅 플랫폼 및 정보 보호 공통 플랫폼으로 구성된다.

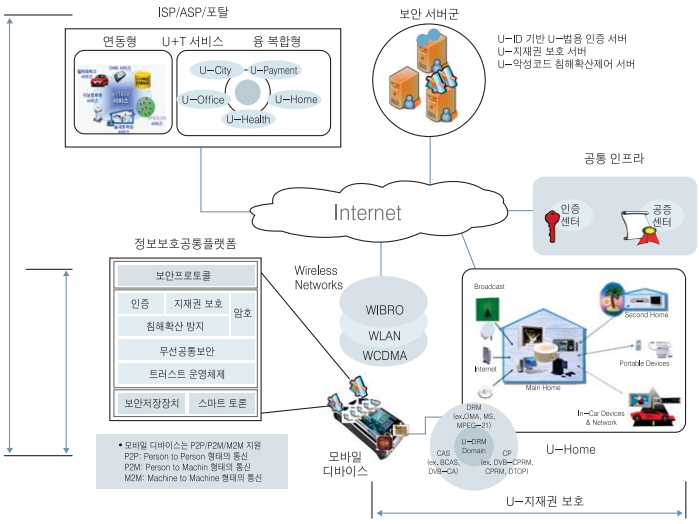


(그림 2) 소프트인프라웨어 개념도



(그림 3) 정보 보호 공통 플랫폼 지원 서비스 개념도

- 정보 보호 공통 플랫폼의 표준화 중점기술은 아래 그림과 같이 보안저장장치, 스마트토큰, 보안 미들웨어, 무선공통 보안API, 트러스트 운영체제, 보안 응용 및 프로토콜로 구성되었다.



(그림 4) 정보 보호 공통 플랫폼 개념도

- 보안저장장치는 데이터의 안전한 저장 및 지재권 보호를 위한 Right 저장 등을 가능하게 하는 저장장치로 복제 방지 기술 및 실행 환경 등에 필요한 기술이 표준화 대상항목이다.
- 스마트토큰은 u-ID 기반 범용 인증, 콘텐츠 보호 등에 활용되는 연산 프로세서로, 보안 엔진 및 프로세서, 키관리 등이 표준화 대상항목이다.(예 : TPM)
- 보안 미들웨어는 IT 융 · 복합 서비스가 기대되는 멀티도메인 환경에서 범용 인증, 지식 콘텐츠 보호 및 모바일 침해 확산을 방지하는 단말용 미들웨어 기술로서, 범용 인증, 지재권 보호, 침해확산 방지 기술 등이 표준화 대상항목이다.
- 무선공통보안API는 상이한 모바일 환경에서 무선 공통 접속 및 이동을 제공하는 표준 API 기술로서, 무선 공통 보안 인터페이스가 주요 표준화 대상항목이다.
- 트러스트 운영체제는 모바일 단말 환경에서 자원(파일, 메모리 등)에 대한 접근을 제어하고 플랫폼의 임의 조작을 방지하는 운영체제 기술로서, 도메인 분리, 임의 조작 방지 기술 등이 표준화 대상항목이다.
- 보안 응용 및 프로토콜은 정보 보호 공통 플랫폼상에서 다양한 응용서비스(u-City, u-Home 등)의 연동 보안 기능을 제공하기 위한 보안 응용 및 프로토콜 기술로서, 보안 프로토콜 및 API, 서비스가 표준화 대상항목이다.

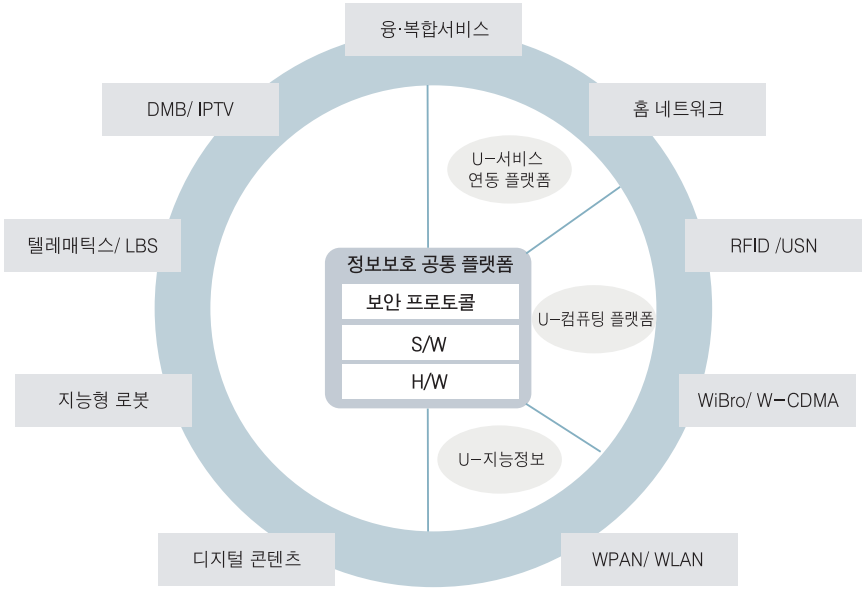
• 표준화 대상항목의 정의

표준화 대상항목	정의	요소기술	표준화내용
보안 저장 장치	데이터의 안전한 저장 및 지재권 보호를 위한 Right 저장 등을 가능하게 하는 저장 장치로 복제 방지 기술 및 실행 환경 등에 필요한 기술	- 착탈형 저장 장치의 콘텐츠 유통 권한 방지 기술 - 보안 저장 장치용 S/W 실행 환경 기술	- MMC, USB 등을 이용한 CPRM 기술 - USB와 같은 저장 장치에서 보안 기능을 제공하기 위한 표준화된 S/W 실행 환경 기술
스마트 토큰	u-ID 기반 범용 인증, 콘텐츠 보호 등에 활용되는 연산 프로세서로, 보안 엔진 및 프로세서, 키관리 등이 요소기술임 (예 : TPM)	- Hard TPM 기술 - u-ID, 콘텐츠 보안(Rights) 지원형 스마트 카드 기술	- 단말 복제 방지, 부트 코드의 임의 조작 방지 기능을 제공하는 하드웨어 TPM 기술 - u-ID, 콘텐츠 보안, 키관리 등을 지원하는 스마트 카드 플랫폼 및 API 기술
보안 미들웨어	IT 융 · 복합 서비스가 기대되는 멀티 도메인 환경에서 범용 인증, 지식 콘텐츠 보호 및 모바일 침해 확산을 방지하는 단말용 미들웨어 기술로서, 범용 인증, 지재권 보호, 침해확산 방지 기술 등이 요소기술임	- 융 · 복합 공통 보안 단말 키관리 기술 - 프로파일 기반 사용자 제어형 u-ID 관리 기술 - 모바일 DRM/CAS/CP 통합 보안 기술 - 모바일 악성코드 침해 감지 및 대응 기술	- 범용 인증(사용자, 소유물 등), 콘텐츠 보호, 플랫폼 S/W 인증 등에 활용되는 단말용 키관리 구조 및 API 기술 - 범용 ID로 융 · 복합 서비스를 지원하는 인증 프로파일, 메소드, 인증 에이전트를 포함한 범용 인증 기술 - 모바일 환경에서 융 · 복합 콘텐츠 보호 서비스를 제공하기 위한 DRM/CAS /CP 통합 보안 기술 - 모바일 악성코드 탐지를 위한 데이터 수집 메소드, 로그 포맷, 보고 절차 등을 포함하는 악성코드 침해 감지 및 대응 기술
무선공통보안API	상이한 모바일 환경에서 무선 공통 접속 및 이동을 제공하는 표준 API 기술로서, 무선 공통 보안 인터페이스가 주요 요소기술임	- 무선망 공통 보안 API 기술 - MIH 기반 무선망 보안 연동 기술	- 상이한 모바일 환경에서 무선 공통 접속 보안 API 기술 - 상이한 모바일 환경에서 무선 공통 이동(MIH 기반) 보안 API 기술

표준화 대상항목	정의	요소기술	표준화내용
트러스트 운영체제	모바일 단말 환경에서 자원(파일, 메모리 등)에 대한 접근을 제어하고 플랫폼의 임의 조작을 방지하는 운영체제 기술로서, 도메인 분리, 임의 조작 방지 기술 등이 요소기술임	- 침해 확산 방지형 도메인 분리 기술 - 플랫폼 임의 조작 방지 기술 - 커널 무결성 검증 기술	- 커널 수준에서 침해 확산을 대응하기 위한 도메인 분리용 표준 API 기술 - 플랫폼 임의 조작 방지를 위한 S/W(Core S/W, 응용 S/W 등) 인증 및 검증 기술 - 부팅용 커널 코어 이미지의 무결성을 검증하는 기술(코어 이미지 포맷, 무결성 검증 메소드 등)
보안응용 및 프로토콜	정보보호 공통 플랫폼상에서 다양한 응용서비스(u-City, u-Home 등)의 연동 보안 기능을 제공하기 위한 보안 응용 및 프로토콜 기술로써, 보안 프로토콜 및 API, 서비스가 요소기술임	- 융 · 복합 서비스용 공통 보안 프로토콜 및 API 기술 - 범용 ID(u-ID) 생성 및 검증 기술 - ID 인증 인프라 연동 게이트웨이 기술 - 사용자/디바이스간 콘텐츠 유통 권한 공유 기술 - 단말 무결성 증명 및 접속 제어 기술	- 융 · 복합 서비스를 제공하기 위한 공통 보안 프로토콜 및 API 기술(무선 공통 접속, 통신 및 데이터 보안 프로토콜 등) - 익명성 지원 범용 ID(u-ID) 생성 및 검증 기술(u-ID 포맷 및 인증 프로토콜, 무선/서비스 결합형 u-SSO 프레임워크 등) - 기존의 ID 인증 인프라의 상호 연동을 위한 게이트웨이 기술 - 모바일 환경에서 사용자/디바이스간 콘텐츠(UCC 포함) 보호를 위한 유통 권한 관리 기술 - 단말의 무결성을 증명하고 악성코드에 감염된 단말의 서비스 접속을 제어하는 기술

2.1.2. 연관기술 분석

• 연관기술 관계도



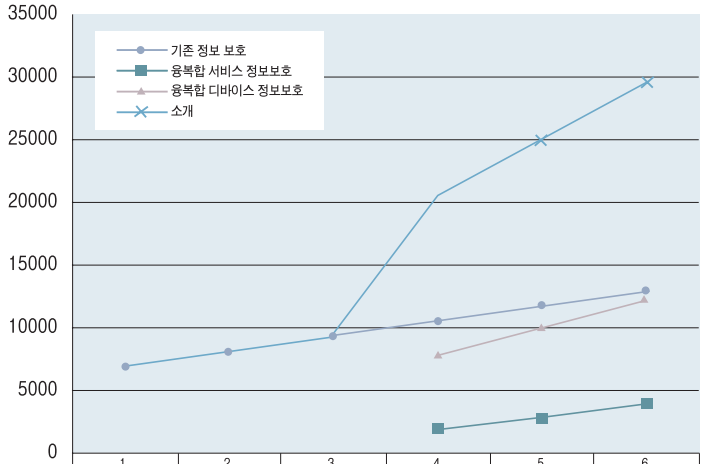
(그림 5) 정보 보호 공통 플랫폼 연관기술

• 연관기술 분석표

연관기술	내용	표준화기구/단체		표준화수준		기술개발수준	
		국내	국외	국내	국외	국내	국외
서비스 융합 플랫폼 기술	네트워크에 분산된 다양한 서비스 간에 상호운용성을 확보하여 융 · 복합 서비스 창출을 가능하게 하는 S/W 플랫폼으로 이를 위한 세부 기술	TTA	OASIS, IETF, W3C	표준 미제정	표준화 진행 중	기술기획	기술 개발 중
u-지능 정보 기술	차세대 웹 환경과 유비쿼터스 환경에서 컴퓨터가 이해할 수 있는 지능적 지식 정보 처리 서비스를 지원하기 위한 세부 기술	TTA	OASIS, IETF, W3C	표준 미제정	표준화 진행 중	기술기획	기술 개발 중
u-컴퓨팅 플랫폼 기술	유비쿼터스 컴퓨팅 환경에서 모바일 기기에 서비스 융합을 효과적으로 지원하기 위한 공통 기능 및 상호 연결 기능을 제공하기 위한 세부 기술	TTA	ELC, CELF, OMG	표준 미제정	표준화 진행 중	기술기획	기술 개발 중
u-융 · 복합 서비스 기술	u-City, u-Home, u-Health 등 서비스가 융 · 복합되거나 새롭게 창출되는 서비스를 위한 끊김없는 보안 서비스 기술	TTA	OSGi, IETF, ITU	표준 미제정	표준화 진행 중	기술기획	기술 개발 중
RFID/USN 기술	모든 사물에 센싱, 컴퓨터 및 통신 기능을 탑재하여 언제 어디서나 정보를 처리, 제공할 수 있도록 지원하는 유비쿼터스 기술	TTA	EPC, ISO, ITU	표준 제정 중	표준화 진행 중	설계	기술 개발 중
DMB/IPTV 기술	고속 이동 시청, 초고화질 방송 등 기존 방송의 한계를 극복하고 통신망과 연계되어 있는 차세대 멀티미디어 방송 서비스 기술	TTA	ITU, DVB, MPEG	표준 제정 중	표준화 진행 중	시제품	시제품
WPAN/WLAN 기술	음성, 영상, 고속 데이터 서비스를 제공하는 개인 무선인터넷 네트워크	TTA	IEEE, ISO	표준 제정 중	표준화 진행 중	시제품	시제품
차세대 이동통신 기술 (WCDMA/HSDPA 등)	WiBro, HSDPA/W-CDMA 등 이동 환경에서 음성, 영상, 고속 데이터 서비스, 이동 무선인터넷 을 제공하는 네트워크 기술	TTA	3GPP, ISO, ITU	표준 제정 중	표준화 진행 중	시제품	시제품
디지털 홈 기술	신뢰성 있는 홈네트워크 인프라 구축을 위해 단말(단말간) 인증 메커니즘 및 다양한 사용자 인증 방식 제공, 프라이버시 보호를 위한 기술	TTA	ITU, OGC	표준 제정 중	표준화 진행 중	구현	구현
텔레매틱스/ LBS 기술	통신망을 통해 확보된 위치정보를 기반으로 교통안내, 긴급 구난, 물류정보 등을 제공하는 이동형 정보 활용 서비스 기술	TTA	ISO, OGC, OMA	표준 제정 중	표준화 진행 중	구현	구현
지능형로봇	유효한 사용자를 구별하며 서비스 로봇, 차세대 PC 등 다양한 정보기기 간에 안전한 통신 및 제어 기술	TTA	ISO/IEC, ITU IEEE, OMG	표준 제정 중	표준화 진행 중	구현	구현
디지털 콘텐츠 기술	디지털 콘텐츠의 안전한 유통 및 관리를 위한 DRM/CAS, CP 기술을 포함한 콘텐츠 보호 기술	TTA	MPEG, ISO/MPEG, OMA	표준 제정 중	표준화 진행 중	구현	구현

2.2. 시장 현황 및 전망

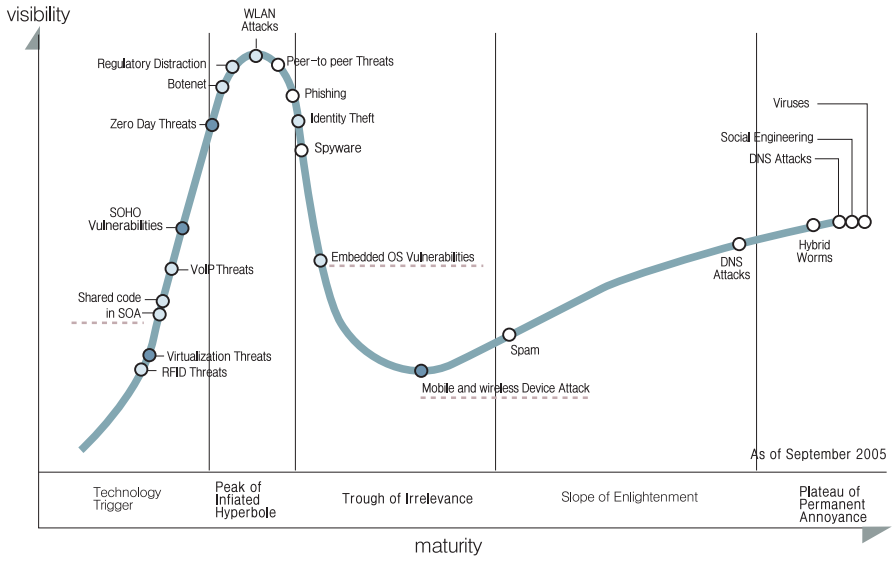
- 세계 정보 보호 시장은 연평균 16.9% 성장률로 2009년에 600억 달러에 이를 것으로 전망되며, 국내 정보 보호 시장은 연평균 10.64% 성장률로 2010년에 1조 1,544억 원 규모에 이를 것으로 전망 (출처 - IDC & KISIA, 2005.12)
- IT 서비스간 연동 및 융 · 복합화 추세에 따라 향후 2010년 정보 보호 산업 및 시장 규모가 2조 9,603억원으로 확대될 전망



	1	2	3	4	5	6
기존 정보 보호	6967	0220	9439	10363	11819	12959
융복합 서비스 정보보호				2067	2930	4112
융복합 디바이스 정보보호				7972	10011	12532
소개	6967	8228	9439	20575	24760	29600

〈표 1〉 국내 u-정보 보호 산업 전망 (단위 : 억원)

※ 전망에 활용된 모수는 KAIT 자료를 활용
※ 연도별 증가율의 경우 가트너, IDC, InStat 등 세계시장 증가율을 감안
※ 2008년 이후 국내 정보보호 시장은 IT 839 산업의 0.8~1% 추가 책정하여 추정(IITA 통계자료 2006.1.)



Acronym Key :

DNS	Domain Name System	SOHO	Small Office home Office
DOS	denial of Service	VoIP	Voice Over Internet Protocol
OS	Operating System	WLAN	Wireless local-area network
RFID	radio freqency identification	XENO	Extended Enter Networks Overseas
SOA	service-oriented architecture		

〔Hype Cycle for Cyberthreats, 2005〕 출처 : Gartner (Sep. 2005)

- u-IT 서비스가 융 · 복합되는 소프트 인프라웨어 환경에서는 개인정보 침해, 모바일 악성 코드, 지재권 침해 등 사이버 위협의 심화 확대와 무선 IT 융 · 복합 디바이스의 공통 플랫폼(예 : WIPI 플랫폼) 이 주요 해킹의 표적이 될 가능성이 크다.
  - 융 · 복합 디바이스에서 실행되는 웜 바이러스는 단말기의 성능 저하, 단말 사용자의 개인 정보 불법 수집, 다른 서비스로의 바이러스 전파 등을 야기시킬 수 있음
  - 이동통신 단말뿐 아니라 WiBro, DMB, RFID, WCDMA도 역시 WIPI 플랫폼을 적용할 것으로 전망되어, WIPI 규격의 취약점이 발견될 경우 이를 적용한 모든 단말에 공격 발생 가능성이 높음
  - P2P/P2M/M2M방식으로 연계된 u-IT 서비스가 스마트 단말에서 융 · 복합됨에 따라, 단말의 실행환경을 해커로부터 보호하고 융 · 복합 서비스에 맞춤된 트러스트 보안 플랫폼 환경 개발이 필요

2.2.1. 국내 시장 현황 및 전망

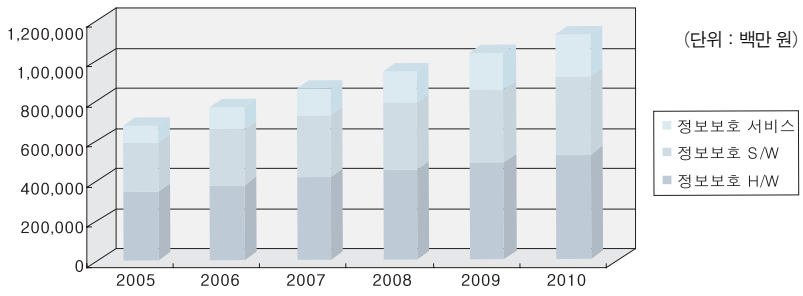
• 정보 보호 공통 플랫폼 시장

- 국내 정보 보호시장은 연평균 10.64% 성장률로 2010년에 1조 1,544억원 규모에 이를 것으로 전망된다.(출처 - IDC & KISIA, 2005.12.)
- IT 서비스간 연동 및 융 · 복합화 추세에 따라 향후 2010년 정보 보호 공통 플랫폼 산업 및 시장 규모가 6,603억 원으로 확대될 전망이다.(출처 - IITA, 2006. 8)

〈표 2〉 국내 정보 보호 시장전망 (단위 : 백만원)

구분	2005	2006	2007	2008	2009	2010	CAGR(%)
정보 보호 H/W	352,675	387,912	425,594	463,275	500,958	538,639	8.84
정보 보호 S/W	257,289	286,573	315,274	342,708	372,105	400,946	9.28
정보 보호 서비스	86,755	113,645	138,734	162,427	188,919	214,823	19.88
합계	696,719	788,130	879,602	968,410	1,061,982	1,154,408	10.64

출처 : 국내 정보보호산업 통계조사(2005-2010), KISIA, 2005.12



출처 : 국내 정보보호산업 통계조사(2005-2010), KISIA, 2005.12

(그림 6) 국내 정보 보호 시장전망

• 보안저장장치 시장

- 하드웨어 기반 저장장치를 제공하는 업체는 다수이나 데이터의 안전한 저장 및 지재권 보호를 위한 Right 저장 장치는 아직 출시하지 못하고 있으며, 향후 삼성전자의 비메모리 반도체 제품의 로드맵에 보안저장장치를 포함시켜 놓고 있다.

• 스마트토큰 시장

- 하드웨어 기반 씨큐리티 제공 보안 업체는 다수이나 TPM을 채용한 제품은 출시하고 있지 못하며 삼성전자가 유일하게 TCG에 참여하여 표준화활동을 하고 있다.
- 향후 삼성전자의 비메모리 반도체 제품의 로드맵에 TPM을 포함 시켜 놓고 있으며, 국내 모바일 단말기 시장은 세계 Top 3에 포함되고 있어서 모바일 단말용 TPM 수요는 매우 클 것으로 전망된다.

• 보안미들웨어 시장

- 국내 인터넷 가입자 3,257만 명을 Identity 관리 서비스 체계로 편입시키고, 현재 62만 3천여 개의 도메인 중 약 16% 정도가 Identity 관리 서비스에 가맹하고 연간 200만 원 정도의 Identity 관리 및 인증 대행 수수료를 지불할 것을 추정할 때, 연간 2,000억 원 규모의 인터넷 Identity 관리 서비스 시장 창출을 기대할 수 있다.
- 단순 키워드 매칭이나 DRM 기반 기밀정보 유출 방지 기술을 보유한 국내 대표 업체로는 마크애니, 엑스큐어넷 등이 있다. 마크 애니는 국내의 대표적인 내부 기밀 보안 업체로 DRM 기술을 그 근간으로 하고 있으나 문서 보안 기능이 위주이고 등록된 기밀문서에 대해서만 보호 기능을 수행하고 있다. 엑스큐어넷은 네트워크 단에서 외부로 유출되는 트래픽을 감시하는 제품으로 단순 키워드 검색 방식이며, 처리 성능이 매우 낮다.

• 무선 공통 보안API 시장

- 무선랜, 휴대인터넷, IMT-2000 및 Beyond IMT-2000내 산업을 육성하고 있다.
- 유 · 무선망 통합을 위한 핵심기술의 수입 대체 효과 출 약 3200억 원 이상이 전망되며(2006년까지 글로벌 이동 보안 시32억 달러에 이를 것으로 전망 : 2002년 Datamonitor), 서비스 시장 163조 원, 고용창출 82만 명 등의 유무선망 통합통신망 구축에 기여할 것으로 예상된다.(정통부 2003년 BcN 시장 발표)

• 트러스트 운영체제 시장

- 새로운 기술보다는 기존 기술을 개량하여 소형, 경량, 저전력 임베디드 장치내에서 키관리와 S/W 무결성 확인을 위한 트러스트 운영체제에 대한 요구가 증가할 것으로 예상된다.

• 보안응용 및 프로토콜 시장

- 펜타시큐리티의 SSO 솔루션인 eGsign은 전자 정부 및 공개키 기반 환경을 기본으로 하며 여러 도메인 간의 SSO를 지원하고 있으며, 한국 후지쓰는 국내 웹 해킹 및 피싱 패해에 대응하기 위해 '앱스캔(Appscan)을 개발하여, SSO 기능 등을 추가 지원하고 있다.

2.2.2. 국외 시장 현황 및 전망

• 정보 보호 공통 플랫폼 시장

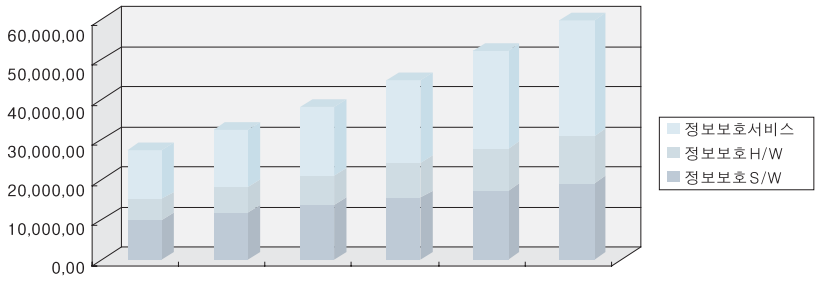
- 세계 정보 보호시장은 2004년 274억 달러 규모로 파악되며, 향후 연평균 16.9%로 성장하여 2009년에는 600억 달러에 이를 것으로 전망된다.
- IT 서비스간 연동 및 융 · 복합화 추세에 따라 향후 2010년 정보 보호 공통 플랫폼 산업 및 시장 규모가 2조 9,603억원으로 확대될 전망이다.(출처 - IITA, 2006. 8)

〈표 3〉 세계 정보 보호 시장전망 (단위 : 백만 달러)

구분	2004년	2005년	2006년	2007년	2008년	2009년	CARG(%)
정보보호 H/W	5,237	6,309	7,413	8,703	10,275	11,761	17.6
정보보호 S/W	10,000	11,852	13,689	15,552	17,396	19,222	14.0
정보보호 서비스	12,210	14,488	17,284	20,590	24,521	29,002	18.9
합계	27,447	32,649	38,386	44,845	52,192	59,985	16.9

출처 : IDC, Worldwide IT Security Software, Hardware, and Services 2005-2009 Forecast : The Big Picture, 2005.12

(단위 : 백만 달러)



출처 : IDC, Worldwide IT Security Software, Hardware, and Services 2005-2009 Forecast : The Big Picture, 2005.12

(그림 7) 세계 정보 보호 시장전망

• 보안저장장치 시장

- 2006~2008년 경에는 보안저장장치가 데스크탑 PC 및 노트북에 부착되어서 사용될 것이지만 시간이 지남에 따라 노트북 외에 신뢰&보안이 요구되는 거의 모든 신성장 산업 부분에서 사용될 것이므로 지속적으로 많은 투자를 한다면 보안 모듈의 비메모리 반도체 분야와 신뢰&보안 산업 등의 거대 시장을 창출할 수 있을 것으로 전망된다.(출처 : IDC2004).

• 스마트토큰 시장

- TPM의 전세계 시장으로는 2007년 8천900백만 개, 2008년 1.44억 개로 연평균 성장률 82.3 CAGR(%)을 기록할 것으로 전망된다, TPM을 통한 수익은 2007년 5천7백만 달러, 2008년 8천9백만 달러로 CACR

86.2(%)로 전망된다. (출처 : IDC2004).

- 모바일용 TPM은 클라이언트 씨큐리티를 PC나 노트북 및 서버와 동등 수준으로 제공해야하는 이유로 2008년 이후에 본격적인 시장이 형성될 것으로 전망된다.(출처 : Gartner2005).

• 보안미들웨어 시장

- Identity관리 시장은 2004년도에 23억35백만 달러에서 연평균 11%성장하여 2009년에는 40억 달러에 이를 것으로 예상된다.(출처 : IDC, "Worldwide IT Security Software, Hardware, and Services)
- 기밀정보나 개인정보 유출 방지 관련 기존 제품들은 암호화, 단순 필터링 등의 전통적인 보안기능 중심의 이메일 보안 업체와 저작권 보호를 위한 DRM(Digital Rights Management) 업체가 주도하고 있으나, 조직내 기밀정보나 고객의 개인정보 유출을 차단하는 데 한계점으로 인하여, 콘텐츠의 내용을 분석하여 차단하는 제품 개발에 주력하고 있다.
- Vontu, Tablus 등에서 비구조화 형태의 기밀정보 유출방지 제품을 출시하고 있으나, 처리 성능이 낮은 편이다.
- 기밀정보나 개인정보 유출 방지 관련 세계시장 2005년 378백만 달러에서 2009년 1,853백만 달러 매출규모로 연평균 48.9% 성장이 예상된다.(IDC, 2005)

• 무선공통보안API 시장

- 무선랜과 이동통신망 등 무선 네트워크의 연동시 보안에 대한 연구는 미약한 상황이나, 이들 각각의 보안에 관한 연구는 활발히 이루어지고 있다.
- 3G/무선랜/휴대인터넷의 연동은 이용자에게 편리한 무선 네트워크 환경을 제공할 뿐 아니라, 네트워크 운용과 과금 등을 위한 기존 장비의 재활용 및 중복 투자 방지로 사업자들에게도 경제적인 운영 방안을 제공할 것이다. 여기에 연동을 위한 보안 구조 제공으로 안전한 서비스가 보장됨으로써 M-commerce 등 새로운 사업 모델이 창출될 것이다.

• 트러스트 운영체제 시장

- Linux를 기반으로 Secure Enhanced Linux를 개발되었고, 현재 Linux Kernel의 기본 기능이 탑재된 운영체제가 시장을 주도할 것으로 전망된다.

• 보안 응용 및 프로토콜 시장

- 웹 기반의 SSO는 CA와 IBM, VeriSign이 30%를 차지하고 평균 20%의 성장률을 보여주고 있으며, CA/Netegrity의 SiteMinder와 IBM의 Tivoli Access Manager가 대표적인 제품이다.
- 호스트 기반의 SSO는 CA와 Novell, VeriSign, Protocom, Microsoft가 50% 이상을 점유하고 평균 30%의 성장률을 보여주고 있으며, 대표적인 제품으로는 Protocom의 SecureLogin이 있다.

2.3. 기술개발 현황 및 전망

2.3.1. 국내 기술개발 현황 및 전망

〔보안저장장치〕

• 정부정책기조

- 향후 PC, PMP 등 모든 모바일기기에는 보안저장장치가 탑재될 전망으로 MMC, USB 등 적용 가능한 기술을 중장기로드맵에 반영하여 추진 중이다.

• 기술개발

- 고속, 저전력 · 경량, 대용량 보안저장장치가 user 및 service 등의 안전성과 신뢰성을 강화시킬 목적으로 하드웨어 기반 MMC, USB 등을 이용한 CPRM 기술을 개발하고 있다.

• 국내 특허출원 현황 및 전망

- 보안저장장치 기술 관련 특허는 현재 전무한 상태이나, 향후 MMC, USB 등의 하드웨어 기술과 S/W 실행 환경 기술이 특허 출원 대상 기술로 전망된다.

〔스마트토큰〕

• 정부정책기조

- 향후 로봇, 정보가전 등 모든 기기와 칩(SoC)에는 TPM이 탑재될 전망으로 암호, 인증, 키관리, 접근제어 등 적용 가능한 스마트 토큰 기술개발을 중장기로드맵에 반영하여 추진 중이다.

• 기술개발

- 소프트웨어 기반 인증, 암호 알고리즘 및 프로토콜을 다양한 플랫폼에 개별적으로 개발 적용함으로써 security 위협은 상존하며 컴퓨터, 통신 및 디바이스에 공통으로 적용하고 user 및 service 등의 안전성과 신뢰성을 강화시킬 목적으로 하드웨어 기반 common security core module을 개발하고 있다.
- 복합 휴대 단말기 복제 혹은 ID를 위장하여 이동통신 및 텔레매틱스 서비스를 불법적으로 이용하거나 프라이버시를 침해하는 가능성이 증대되고(서비스 도용), 복합 휴대 단말 및 Mobile System의 공격을 통한 기밀정보 유출, 위장, 불법 사용, 정상적인 서비스 방해 (DOS공격)를 방지하기 위한 정보 보호 기술을 개발하고 있다.

• 국내 특허출원 현황 및 전망

- 휴대 단말 및 스마트카드 기술 관련 특허는 다수 추진되었으나 TPM과 관련된 특허는 미국, 일본 등에서 한국에 출원하고 있다.

〔보안 미들웨어〕

• 정부정책기조

- u-Korea 조기 실현을 위한 정보보호 중장기 기본전략을 범국가적으로 수립, 추진 중에 있으며, 전자정부 및 공공부문에서의 개인정보보호를 위해 "개인정보보호법(가칭)"을 상정중에 있다.

• 기술개발

- ID, 스마트카드, 인증서, 생체인식 기반의 인증 기술 및 보안 프로토콜이 상용화되고 있으며, 최근 개인정보(주민번호, ID/패스워드 등) 유출 문제로 사업자의 ID 수집 최소화를 위한 ID싱글사인온 기술이 개발 중에 있다.
  - 단일 ID로 멀티 도메인 사업자간 인증, 과금, 키관리를 통합한 범용 ID 및 인증 기술은 개념연구 단계에 있으며, 사람과 사람의 소유물(P2M, M2M)을 범용 인증하는 기술은 연구 시작 단계임
- 유비쿼터스 환경에서 위치 정보 사업 활성화 및 개인 정보보호를 위한 위치정보보호법이 2005년 제정되고 위치정보 제공 사업자가 허가되었다.
  - 사용자 또는 사용자 소유물의 위치 정보보호 기술을 탑재한 단말기(예, 휴대폰) 기술은 아직 국내에서 개발된 사례가 없음
- 디지털 콘텐츠 보호 기술은 서비스 도메인별로 다르게 요구된 지재권 보호 기술(DRM, mDRM, CAS, CP, COI/UCI, 전자문서 보관소 등)을 개발 중이다.
  - DMB 콘텐츠의 제한 수신 서비스를 제공하기 위하여 DBM-CAS 기술을 국산화 중
  - 산자부에서는 전자문서보관서 사업자를 선정하여 지재권보호 서비스를(전자문서 공증, 전자문서 시각/종적 등 위변조방지기술) 준비중
  - 문화부에서는 가짜, 불법 콘텐츠 식별 목적의 COI(Contents Object Identifier)를 이용한 모바일 문화 콘텐츠 유통 추진
  - 정통부에서는 DRM/모바일 DRM, CAS 기술을 상용화하고, 최근에는 멀티 도메인간 DRM 연동 기술을 개발 중

• 국내 특허출원 현황 및 전망

- 단일 도메인 및 조직 환경에서 한 번의 로그인으로 여러 개의 서비스를 이용할 수 있는 싱글사인온(SSO) 메커니즘에 관한 특허가 많이 등록된 상태이며, 국내의 경우 콘텐츠 차단 관련 특허가 거의 없다.

〔무선공통보안API〕

• 정부정책기조

- WiBro 기술은 2003년부터 HPi (High-speed Portable Internet) 이라는 프로젝트 명으로 한국전자통신연구원, KT, 삼성전자 등을 중심으로 개발이 추진되어 왔으며, 시내 주행속도(~60km/hr)로 이동 중에도 언제 어디서나 인터넷 접속 서비스 제공을 목표로 개발이 진행되고 있다.
- WiBro는 WiMAX라고 불리우는 세계 표준의 일부로 채택되었으며, 국내 사업자들은 802.16e 표준에 자체

기술을 포함시킨 것은 물론, 자사의 제품 및 경험을 전세계로 수출하기 위해 이에 적극적으로 참여하고 있다.

• 기술개발

- 국내 CDMA 이동 통신망 환경에서는 주로 불법도청, 복제 휴대폰, 분실 휴대폰, 휴대폰 악성코드 등의 보안 문제를 해소하는데 노력이 집중되고 있다.
  - 최근 복제 · 분실 휴대폰 차단 및 휴대폰 저장 개인정보 유출을 방지하기 위한 STPM 기술개발이 ETRI 중심으로 시작됨
  - WCDMA 환경에서 도청, 메시지 위변조, 비인가자 불법접속 문제를 해소하기 위한 USIM기술이 개발 종료 후 상용화 추진 중
- 국내 WLAN과 WiBro 망에 대한 개별 접속 보안 기술이 개발되었으나, WLAN-WLAN, WiBro-WiBro, WLAN-WiBro간 연동 및 핸드오프 관련 보안 기술은 아직 개발되지 않았다.
  - IEEE802 무선망 가입자 인증 및 키분배 기술로 IEEE802.1x(port based network access control)와 EAP(Extended Authentication Protocol) 기술이 개발됨
  - 현재, 전용 무선 단말기를 이용하여 WLAN, WiBro, CDMA 등 무선 보안 서비스가 일부 제공되고 있으나, 아직까지 정부에서 WPAN에 대한 보안 기술을 개발한 사례는 없음
  - 초기 무선 접속망에서 제공 받은 보안 강도의 손상 없이, 새로운 무선 접속망으로 빠르게 보안 접속점을 이동하는 서비스, 무선 DoS, 무선단말기 ID추적, 위장 공격 등으로부터 정당한 사용자와 무선 인프라를 보호하는 기술은 기초 연구 단계 수준임
- IT융 · 복합 디바이스 단에서 멀티모드 무선 및 서비스 컨버전스를 제공하는 기술개발이 진행 중이나, 관련 융 · 복합 보안 기술이 개발된 사례는 없다.
  - 최근 모바일 RFID 단말기, WLAN + WiBro 단말기, CDMA + WLAN 단말기 등과 같이 멀티 무선 링크를 지원하는 융 · 복합 단말기 기술이 개발되고 있는 단계임

    ※ 멀티모드 무선망 및 서비스간 인증 중복성, 상이한 보안 프로토콜 및 API등에 대한 보안 컨버전스가 요구됨

• 국내 특허출원 현황 및 전망

- WiBro의 특허가 2000년부터 2005년까지의 국내 WiBro 관련하여 출원된 특허는 644개로, WiBro의 경우 국내 출원이 압도적으로 높아 한국이 이 부분에서 기술을 리드하고 있음을 알 수 있다.

〔트러스트 운영체제〕

• 정부정책기조

- u-Korea 조기 실현을 위한 정보 보호 중장기 기본 전략을 범국가적으로 수립, 추진 중에 있으며, 국내 업체를 대상으로 기술이전을 통한 상용화를 목적으로 하는 보안 운영체제를 개발 중이다.

• 기술개발

- 1991~1992년 ETRI에서 "정보통신 시스템 기반보호를 위한 안전한 운영체제 기술 연구"를 통하여 리눅스 및 FreeBSD 에서 서버 형태로 사용할 수 있는 접근제어, 사용자 인증, 암호화 파일 시스템 등의 보안기술을 개발하고 국내 업체를 대상으로 기술 이전을 통한 상용화를 추진한 바 있다.
- 2006년부터 3년 계획으로 ETRI에서 "임베디드 보안 운영체제 기술개발" 과제를 수행 중이며, SKT, KTF, LGT 등 국내 이동통신 3사는 내년 이후 수요가 급증할 휴대폰 범용 운용체제 전략 마련을 본격화하고 있다.(리눅스, 신비안 등)

• 국내 특허출원 현황 및 전망

- 임베디드 환경에 적합한 소형, 저전력, 고속 보안기술에 대한 특허를 다수 확보하고 있다.

〔보안 응용 및 프로토콜〕

• 정부정책기조

- u-Korea 조기 실현을 위한 정보 보호 중장기 기본전략을 범국가적으로 수립, 추진 중에 있으며, 국내 업체를 대상으로 기술이전을 통한 상용화를 목적으로 하는 보안 응용을 개발 중이다.

• 기술개발

- 국내 온라인상의 사용자 인증 관련 기술은 전자서명을 이용한 기술과 OTP를 이용한 기술과 생체를 이용한 기술 등 다양한 기술이 개발되어 적용되고 있으며 인증 결과 공유 및 이를 통한 SSO를 위한 기술개발도 활발히 진행되고 있다.
- 네트워크 자체를 보호하기 위해 호스트의 네트워크 접근을 제어하는 NAC(Network Access Control) 기술, RFID 환경 하에서의 접근 제어 기술, 홈네트워크 서비스를 지원하기 위한 경량화된 접근 제어 기술 등이 연구 개발되고 있다.

• 국내 특허출원 현황 및 전망

- 단일 도메인 및 조직 환경에서 한 번의 로그인으로 여러 개의 서비스를 이용할 수 있는 싱글사인온(SSO) 메커니즘에 관한 특허가 많이 등록된 상태이다.
- 네트워크의 접근 제어를 위한 특허가 미비한 편으로, 향후 프라이버시가 보장되면서 개인정보를 유 · 무선 환경에서 공유할 수 있는 방법에 대한 특허 확보가 필요하다.

2.3.2. 국외 기술개발 현황 및 전망

〔보안 저장 장치〕

• 기술개발

- IT서비스 환경 및 특성에 맞춤된 고속, 저전력 · 경량, 대용량 보안저장장치 기술을 개발 중이다.
- 액세스망의 고속화로 Hi/Fn, Cavium. Broadcom과 같은 보안 프로세서 업체에서는 수 Gbps까지 데이터 처리를 해주는 고속 프로세서 기술을 개발 중이다.

• 주요 국가별 특허출원 동향

- PC, PMP 등 모바일기기의 보안 수준을 향상시키는 보안저장장치 기술 등의 요소기술에 대한 특허를 출원 중에 있으나 모바일 단말용에 대한 저전력 및 대용량 저장 기술에 특허는 전무한 실정이다.

〔스마트토큰〕

• 기술개발

- Trusted Computing을 위한 TPM 산업 표준인 TCG1.1 준수한 제품을 출시하고 있는 회사가 10여 개 이상이고 125개 이상의 회사가 참여 중(6 Promoter, 73 Contributor, 46 Adopter, 2005.11.) 이며 칩 제조사는 Atmel 외 4개사, 보안 제품에 적용중인 회사는 Verisign외 10여개 회사 등이며 Mobile에 적용한 사례는 현재 없으나 TCG WG을 결성하였고 산업 표준은 2006년부터 본격화될 전망이다.

• 주요 국가별 특허출원 동향

- PC 플랫폼의 보안 수준을 향상시키는 기술, 하드웨어 신뢰성을 이용한 보안 기술 등의 요소기술에 대한 특허를 출원 중에 있으나 모바일 단말용에 대한 저전력 및 제한된 자원하에 인증 및 보안 특허는 전무한 실정이다.

〔보안 미들웨어〕

• 기술개발

- 센서망, 무선 메쉬망, 스마트 차량 통신망 등 무선 M2M 통신 디바이스에 적용 가능한 무선 분산 보안 (암호, 인증) 프리미티브 기술을 기초 연구 수준에서 활발히 연구 개발 중이다.
  - 스위스 EPFL대학은 스마트 차량 PKI에 대한 기술 연구
  - 카네기 멜론대학에서는 센서노드에 적용가능한 저전력 브로드케스팅 암호 프리미티브 기술 연구
  - 다자간 secrete sharing, threshold cryptography, 동적 키관리, 핸드오프 키관리 등 무선 분산 환경에 적합한 보안 기술 상용화 연구
  - 신원(ID) 노출 보호를 위한 익명성 기반 프라이버시 보호 기술에 대한 연구를 미국 MIT대학 중심으로 기초 수준에서 진행
- 사람과 사물이 결합된 IT융 · 복합 서비스 환경에서 사람 및 소유물의 정적인 개인정보(ID, 주민번호 등)와

동적인 개인 정보(위치, 상황 등)의 유출을 보호하는 기술을 기초 연구 수준에서 진행 중이다.

※ 대부분의 인터넷 프라이버시 기술 연구는 DB암호, 프라이버시 기반 개인정보 접근제어 및 데이터 마이닝 등과 같이 정적인 개인 정보 유출을 막는 수준에 연구력을 집중하여 상용화

◦ 캐나다는 사용자의 선택에 따른 자율적 프라이버시 보호 기술(PETs, Privacy Enhancing Technologies)을 개발 중

※ 캐나다의 IPC/O(Information and Privacy Commissioner / Ontario)는 2001년부터 PET의 안전성을 공통기준 기반으로 시험/평가하려는 "PETTEP (Privacy Enhancing Technology Testing & Evaluation Project)"을 추진

◦ 유럽은 PRIME(PRivacy & Identity Management for Europe, 2004년 - 2008년) 프로젝트를 수행 중

◦ 미국 콜럼비아 대학에서는 유비쿼터스 VoIP 환경에서 사람 및 사물의 위치 프라이버시 보호 관련 기술을 연구하고, IETF Geopriv그룹에서 표준화를 추진 중

- 단일 도메인용 디지털 콘텐츠의 지재권 보호 기술이 상용화 수준에서 개발되고 있으나, 멀티도메인 통합 · 연동 지재권 보호 기술은 연구 수준이다.

◦ DRM, CAS, 복제 방지(CP) 분야에 대해서 현재 MPEG, OMA 등 국제 단체를 중심으로 기술개발이 진행됨

• 주요 국가별 특허출원 동향

- 초기에는 Identity 관리 및 SSO 분야의 특허가 주류를 이루다가 시간이 지나면서 미국, 유럽을 중심으로 익명성(Anonymity)과 Identity Federation 분야의 특허가 주류를 이루고 있으며, 국외의 경우 콘텐츠 차단과 관련된 언어기반 혹은 비언어 기반의 콘텐츠 분류 특허가 일부 출원되고 있다.

〔무선공통보안API〕

• 기술개발

- 무선 네트워크는 셀의 크기, 통신 특성, 지향하는 타겟 서비스 환경에 따라서 각기 다른 링크 액세스 보안 기술이 개발되고 있다.

◦ 현재, 무선랜, WiBro, CDMA 등 개별 무선 IT서비스는 전용 단말기를 이용하여 보안 서비스를 제공

※ WCDMA의 경우 USIM을 이용한 AKA(Authentication and Key Agreement) 기술을 상용화하여 무선 데이터 통신을 보안

※ 도청 방지, 비인가자 망 접속 차단, 위장 단말 및 기지국 차단, 무선 데이터 위변조 차단, 무선 침입탐지 등을 제공하는 전용 암호, 인증 및 보안 프로토콜을 연구 중

◦ 최근에는 동종 무선망간 핸드오프 또는 보안 구조가 서로 상이한 이종망간 핸드오프시 지연 시간을 최소화시키는 핸드오프 보안 기술이 미국을 중심으로 활발하게 연구 중이다.

※ 최근 CDMA + RFID, WLAN + Wi-bro, CDMA + WLAN 단말기 등과 같이 무선 멀티-링크간 융 · 복합 보안 서비스 기술을 미국, 유럽에서 연구개발 중

※ 미국은 IEEE802(Wireless Network) 무선 네트워크(802.11, 802.15, 802.16, 802.20)간 상호 연동 및 융 · 복합, IEEE 802 무선망과 이동 인터넷간 연동 기술을 개발 중

※ EU은 FP6의 FET(Future Emerging Technology)사업 일완으로 이종 무선망 (WLAN, CDMA, Wi-MAX)간의 융 · 복합 표준 인터페이스(Unified Link-Level API) 기술을 개발(GOLLUM 프로젝트, 2006. 3.)

- 개방형 무선(SDR : Software Defined Radio) 단말 및 기지국 기술, 멀티모드 지원 IT 컨버전스 단말기와 모바일 플랫폼 보안 기술 연구가 활발히 진행 중이다.

• 주요 국가별 특허출원 동향

- 유 · 무선 환경에서 멀티캐스트 서비스 및 시스템, 그리고 그룹 관리와 관련된 특허가 다수 출원되고 있으며, 보안과 관련하여 접근통제 및 네트워크 공격에 대한 방어 등에 대하여 특허 출원 하였다.

〔트러스트 운영체제〕

• 기술개발

- 미국의 NSA (National Security Agency) 주도 하에 정부 차원으로 국가정보기반구조 구축과 국방용으로 사용하기 위하여 1995년부터 안전한 운영체제를 개발 중이다.
- 최근에는 Linux를 기반으로 Secure Enhanced Linux를 개발하였고, 현재 Linux Kernel의 기본 기능으로 탑재되어 있다.
- 최근 퀄컴은 휴대폰 환경에서 범용 OS(μ-커널기반 L4 리눅스)fmf 지원하는 프로세스 칩셋(MSM 7000) 발표하였다.

• 주요 국가별 특허출원 동향

- 임베디드 환경에 적합한 소형, 저전력, 고속 보안기술에 대한 특허의 다수 출원되고 있다.

〔보안 응용 및 프로토콜〕

• 기술개발

- 온라인상의 사용자 인증 관련 기술은 인증 강도를 높이기 위한 방향과 상호연동성을 높이는 방향으로 개발되고 있다.
  - ◦ TPC(Trusted Computing Platform)을 통해 OTP, PW, Biometrics, SmartCard, Sim 등 여러 인증 기술이 동일한 플랫폼 하에 선택적으로 사용될 수 있도록 하는 기술이 개발되고 있음
  - ◦ RFID와 기타 무선기술을 사용한 토큰을 이용한 인증 기술이 개발되고 도입 단계에 있음
- BM, MS, Sun, CISCO 등 세계적인 기업들은 통합 보안 시스템에 대한 제품을 지원하며, 이에 핵심적인 요소로 접근 제어가 포함되어 있으며, 네트워크를 보호하는 NAC, 엔터프라이즈 솔루션 EAM, IAM 등의 기술은 많은 곳에 도입되어 운영되고 있다.

• 주요 국가별 특허출원 동향
- 미국의 IBM과 Microsoft 및 일본의 NTT를 중심으로 초기에는 ID관리 기술과 프라이버시 보호 기술이 주를 이루었으나, 점점 익명성과 ID 연계 기술로 출원 비중이 높아지고 있다.
- 미국의 IBM과 Microsoft 등이 기본적이고 핵심적인 접근제어 기술에 관한 표준을 보유하고 있고, 최근에는 접근제어를 특정 시스템에 적용할 수 있는 기술 표준이 진행되고 있다.

2.4. 표준화 현황 및 전망

2.4.1. 국내 표준화 현황 및 전망

〔보안저장장치〕
• 현재 보안저장장치에 대한 PC, PMP 등 제조사들 및 보안 제품 개발자들의 관심을 보이고 있으나 표준화활동은 미미한 상태이다.

〔스마트토큰〕
• 현재 삼성전자는 TPG에서 TPM에 대하여 Contributor로 활동하고 있으며 노트북 PC 제조사들 및 보안 제품 개발자들의 관심을 보이고 있으나 표준화활동은 미미한 상태이다.

〔보안 미들웨어〕
• 인증 관련 표준화는 한국정보보호진흥원, 인터넷보안기술포럼(ISTF)과 한국정보통신기술협회(TTA)가 정보보호에 대한 표준을 제정하고 있으며 전자서명에 관련된 일부 표준이 제정되어 있고, 현재 SAML관련 표준화가 진행되고 있으며, 한국전보통신기술협회(TTA)와 한국전자통신연구원에서 XACML 표준을 제정하고 있다.

• 프라이버시 보호 관련 표준은 아직 제정되고 있지 않으며, 정부 지침 수준에서 무선랜과 RFID 서비스에 대한 개인정보보호 가이드라인이 제정 공표되었다.(정통부 2002년, 2005년)
- 국내 PKI 관련 표준안 개발은 인터넷 보안 기술 포럼과 TTA가 주도하여 제정
- 웹서비스 및 전자상거래를 위한 XML은 ETRI, NCA, ECIF, KAIS 등이 W3C 멤버로 활동 중이며, 많은 국내업체에서 표준화가 완료된 XML 기술을 활용 중

• 디지털 콘텐츠 보호 기술은 서비스 도메인별로 다른 지재권 보호 체제(DRM, mDRM, CAS, CP, COI/UCI, 전자문서 보관소 등)로 운용되고 있다.
- 국내 DRM 표준화활동으로는 EXIM을 통해서 DRM간 데이터 교환을 위한 상호연동이 가능한 인터페이스

규격 제정 추진 중

- KTF, SKT는 OMA DRM 2.0 저작권 보호 서비스를 제공 중이나 각기 다른 도메인간 DRM 연동에 문제가 있음
- KT는 KT Home/WiBro 서비스 적용을 위한 DRM을 개발 중

〔무선 공통 보안API〕

- TTA를 중심으로한 무선 네트워크 보안기술 표준화가 진행 중이다.
  - 무선랜의 경우, 무선 접속 보안, 키관리, EAP 기반 무선 가입자 인증 관련 표준들이 초고속 무선랜 포럼과 TTA를 통하여 제정됨
  - TTA에서 WiBro 접속 보안 및 USIM을 통한 WiBro가입자 인증 관련 표준이 개발 중
  - 모바일 RFID보안 보안프임워크, 프라이버시 보호 요구사항과 관련한 표준이 모바일RFID포럼과 TTA를 통하여 표준화 추진

〔트러스트 운영체제〕

- TTA PG101 정보보호 프로젝트 그룹에서는 정보보호 기반기술 표준, Secure OS 표준 등 총 16건의 표준화 과제를 수행 중이다.

- 삼성, LG, 소니, IBM 등의 세계유수의 가전 및 임베디드 리눅스 업체들이 모여 결성한 CELF(Consumer Electronics Linux Forum)에서는 임베디드 리눅스 솔루션 및 표준 플랫폼 제정을 위해 활동 중이며 산하 기구인 Security Working Group 을 통해 기술적인 접근을 하고 있다.

〔보안 응용 및 프로토콜〕

- TTA를 중심으로 ID 생성 및 검증 기술 표준화를 진행
  - TTA PG101 정보보호 프로젝트 그룹에서는 ID 관리, 기반기술 표준, Secure OS 표준 등 총 16건의 표준화 과제를 수행 중

- TTA와 ETRI에서 접근제어를 위한 XACML (eXtensible Access Control Markup Language), XDI(XRI Data Interchange) 표준을 제정하고 있다.

2.4.2. 국외 표준화 현황 및 전망

〔보안저장장치〕

- 1999년에 설립된 TCPA의 산업체 표준화활동은 안전한 컴퓨팅 환경을 실현하자고 하는 구상 하에 TMP(Trusted Mobile Platform) 스펙을 2004년 제정하여, 모바일기기의 저장장치에 대한 규격을 제공하고 있다.

〔스마트토큰〕

- 1999년에 설립된 TCPA의 산업체 표준화활동은 보안 모듈을(Trusted Platform Module) 이용해서 안전한 컴퓨팅 환경을 실현하자고 하는 구상 하에 TPM 스펙 1.2를 2005년 제정하고 Desktop PC 및 서버와 Notebook PC에 대한 규격을 먼저 제정하였으며, Mobile에 적용하기 위하여 Nokia를 의장으로 WG을 결성하였고 산업 표준은 2006년부터 추진될 전망이다.

〔보안 미들웨어〕

- W3C에서는 XML 기반 IT 서비스 환경에 공통으로 적용할 웹보안 (WS-Security) 기술을 표준화하고 있다.
  - W3C는 XML 전자서명 · 암호화 · 키관리에 대한 표준을 제정하고 있으며, IETF는 공개키인증서, 속성인증서, LDAP에 대한 표준을 제정하고 있다.
  - OASIS는 SAML (Security Assertion Markup Language), XACML (eXtensible Access Control Markup Language), SPML (Service Provisioning Markup Language) 등의 표준을 제정하여 멀티 도메인간 ID 싱글사인온 환경을 지원하고 있다.
    ※ SUN을 중심으로 170여개 업체가 연합한 Liberty Alliance와 IBM과 Microsoft를 중심으로 여러 업체가 연합한 WS-I에서 표준화를 진행

- 프라이버시 보호 기술 관련 국제표준화
  - W3C 주도하에 P3P(Platform for Privacy Preferences) 기술 표준제정
    ※ AOL, HP, MS, CDT 등 업계와 시민단체가 공동 참여해 2004년에 개발 완료됐으며, 1년의 시험 운용 후 2005년에 표준으로 공식 승인을 받음
  - IETF Geopriv WG에서는 모바일 환경에서 사용자 동의하에 위치 정보의 수집 및 전달을 위한 보안 규격을 제정 중이며, OMA에서는 이동통신 환경에서 위치 정보의 프라이버시 보호를 위한 규격을 제정 중이다. ITU-T에서는 RFID 프라이버시 프레임워크에 대한 표준화를 추진하고 있다.

- 디지털 콘텐츠의 지재권 보호 표준화현황
  - 국제 디지털 콘텐츠 보호 기술 (지재권 보호 기술)은 DRM, CAS, 복제 방지(CP) 분야에 대해서 현재 MPEG, OMA 등 국제표준화 단체를 중심으로 기술표준화가 진행 중이다.

※ 저작권 보호기술 분야는 MPEG-21, OMA, DVB-CPCM, DHWG, TV-Anytime, IDRM, SDMI, OeBF, XrML, ODRL에서 추진중이다.

※ 디지털 방송 & 셋톱박스 분야 (CAS 포함)는 OpenCable POD Copy Protection (케이블방송), ATSC CA (지상파), DVB-CA, ISMACryp 에서 추진중이다.

※ 복제 방지 기술 (Copy Protection Technology) 분야는 CPTWG, CSS, CPSA, CPPM, CPRM, DTCP, HDCP, SmartRight에서 추진 중이다.

〔무선 공통 보안API〕

- IEEE802, IETF를 중심으로한 무선 네트워크 보안 기술 표준화
  - 개별 무선 네트워크에 대한 보안 규격은 IEEE 802 (Wireless Network) 그룹을 중심으로 WLAN, WMAN(WiBro), WPAN 등에 대한 보안 기술의 표준화가 진행 중이다.
  - 차량 - 기지국간 DSRC 통신 보안은 IEEE802.11i 표준 규격을 따르고, 홈네트워크용 무선 메시통신, 차량간 통신 등에 활용되는 무선 메쉬 네트워크 보안은 IEEE802.11s, IEEE802.15.5에서 표준화추진 중이다.
  - IEEE802 계열 이종 무선망, 이동통신망(CDMA, GSM), 그리고 이동인터넷망(MIP)간의 개방형 핸드오프(Media Independent Hand-off) 규격 표준화를 IEEE 802.21에서 진행하고 있다.

〔트러스트 운영체제〕

- TCPA(Trusted Computing Platform Alliance)는 PC 기반의 산업 플랫폼, 운영체제, 응용 등의 보안규격을 개발이 목표이다. 표준 규격인 TCPA 1.0 의 범위는 안전한 저장매체, 플랫폼 인증 등의 전형적인 보안 기능 블록과 BIOS의 자가 진단, 마스터 부트 레코드, OS 부트 로더 등의 플랫폼 무결성 확인 표준화가 진행 중이다.

〔보안응용 및 프로토콜〕

- ISO, IETF를 중심으로한 보안 프로토콜 표준화
  - ISO/IEC JTC1/SC27에서는 3개의 워킹그룹을 구성하여, IT 시스템 보안을 위한 정보보호 원천 기술과 구현 방법들에 대한 표준화가 추진 중이다.
    ※ WG1에서는 보안요구사항, 정보보호 관리, 보안서비스 가이드라인 제정
    ※ WG2에서는 암호 알고리즘과 보안서비스 구현 기술을 표준화
    ※ WG3에서는 보안시스템에 대한 평가기준, 평가 방법론, 보호프로파일 작성 절차들을 표준

- SSO 및 인증 공유와 관련해서 OASIS는 SAML(Security Assertion Markup Language), Sun을 중심으로 170여개 업체가 연합한 Liberty Alliance와 IBM과 Microsoft를 중심으로 여러 업체가 연합한 WS-I에서 표준화를 진행하고 있다.

• 현재 진행되고 있는 접근제어 표준은 OASIS 그룹의 XACML(eXtensible Access Control Markup Language), XDI(XRI Data Interchange) 등이 있다.

- 최근에는 접근 제어 표준에 프라이버시 부분을 추가하는 추세이다. IBM에서 개발하고 W3C에서 진행하고 있는 EPAL(Enterprise Privacy Authorization Language)은 프라이버시 접근제어 표준이고, OASIS의 XACML 또한 새로운 버전에 프라이버시를 위한 스펙이 추가되고 있다.

2.5. 표준화 대상항목별 현황 분석표

표준화 대상항목		보안 저장장치	스마트 토큰	보안 미들웨어
시장 현황 및 전망	국내	전망국내데이터의 안전한 저장 및 지재권 보호를 위한 Right 저장 장치는 아직 출시하지 못하고 있음	하드웨어 기반 씨큐리티 제공 보안 업체는 다수이나 TPM을 채용한 제품은 출시하고 있지 못함	연간 2,000억 원 규모의 인터넷 Identity 관리 서비스 시장 창출 기대
	국외	보안저장장치가 신뢰&보안이 요구되는 거의 모든 신성장 산업 부분에서 사용될 것으로 전망됨	TPM의 전세계 시장으로는 2007년 8천900백만 개, 2008년 1.44억 개로 연평균 성장률 82.3 CAGR(%)을 기록할 것으로 전망	Identity관리 시장은 2004년도에 23억 35백만 달러에서 연평균 11%성장하여 2009년에는 40억 달러로 예상
기술 개발 현황 및 전망	국내	하드웨어 기반 MMC, USB 등을 이용한 CPRM 기술을 개발하고 있음	user 및 service 등의 안전성과 신뢰성을 강화시킬 목적으로 하드웨어 기반 common security core module을 개발하고 있음	- ID, 스마트카드, 인증서, 생체인식 기반의 인증 기술 상용화 - 디지털 콘텐츠 보호 기술은 서비스 도메인별로 다르게 요구된 지재권 보호 기술을 개발 중
	국외	액세스망의 고속화로 Hi/Fn, Cavium. Broadcom과 같은 보안 프로세서 업체에서는 수 Gbps까지 데이터 처리를 해 주는 고속 프로세서 기술개발	Trusted Computing을 위한 TPM 산업 표준인 TCG1.1 준수한 제품을 출시하고 있는 회사가 10여 개 이상이고 125개 이상의 회사가 참여 중	- 무선 M2M 통신 디바이스에 프리미티브 기술을 기초연구 - 단일 도메인용 디지털 콘텐츠의 지재권 보호 기술이 상용화 수준
기술 개발 수준	국내	기술기획(일부 설계)	기술기획	기술기획
	국외	설계(일부 구현)	설계(일부구현)	설계
	기술격차	1.5년	2년	1년
	관련제품	보안저장장치	스마트 토큰	보안 미들웨어
IPR 보유현황	국내	현재 전무한 상태임	스마트카드 기술 관련 특허는 다수	싱글사인온(SSO) 메커니즘에 관한 특허가 많이 등록된 상태이나, 콘텐츠 차단 관련 특허가 거의 없음
	국외	보안저장장치 기술 등의 요소기술에 대한 특허를 출원 중	보안 수준을 향상시키는 기술, 하드웨어 신뢰성을 이용한 보안 기술 등의 요소기술에 대한 특허를 출원 중	Identity 관리 및 SSO 분야의 특허가 주류를 이루며, 콘텐츠 차단 특허가 일부 출원되고 있음
IPR확보 가능분야		MMC, USB 등	Hard TPM, 스마트카드 플랫폼 등	보안 프로토콜 구조 등
IPR확보 가능성		높음	보통	높음
표준화현황 및 전망		- 국내 : 제조사들 및 보안 제품 개발자들의 관심을 보이고 있으나 표준화활동은 미미한 상태임 - 국외 : TMP(Trusted Mobile Platform) 스펙을 2004년 제정하여, 모바일기기의 저장장치에 대한 규격을 제공하고 있음	- 국내 : 현재 삼성전자는 TPG에서 TPM에 대하여 Contributor로 활동하고 있다 - 국외 : TPM 스펙 1.2를 2005년 제정하고 Desktop PC 및 서버와 Notebook PC에 대한 규격을 제정2006년부터 추진될 전망임	- 국내 : TTA를 중심으로 ID 생성 및 접근제어 표준화 진행 - 국외 : W3C에서는 웹보안 기술. 프라이버시 보호, MPEG-21, OMA, 에서는 DRM 표준화추진
표준화 기구/ 단체	국내	TTA	TTA	TTA
	국외	ISO, OMA 등	ISO, OMA 등	ITU-T, ISO, W3C, MPEG 등
	국내참여 업체 및 기관현황	ETRI, 삼성 등	ETRI, 삼성 등	ETRI, KT, 삼성, SK 등
	국내기여도	보통	낮음	높음
표준화 수준	국내	표준안 기획(일부 표준항목승인)	표준안 기획	표준안 기획
	국외	표준안 항목 승인(일부 표준안 개발)	표준안 항목 승인(일부 표준안 개발)	표준안 항목 승인
국내표준화의 인프라수준 (시장요구정도 및 참여도)		보통	낮음	높음

표준화 대상항목		무선공통보안API	트러스트 운영체제	보안응용 및 프로토콜
시장 현황 및 전망	국내	수입 대체 효과 출 약 3200억 이상 (2006년까지 글로벌 이동 보안 시32억 달러에 이를 것으로 전망)	소형, 경량, 저전력 임베디드 장치 내에서 키 관리와 S/W 무결성 확인을 위한 트러스트 운영체제가 시장 독점 전망	SSO 솔루션인 eGsign은 전자 정부 및 공개키 기반 환경을 기본으로 하며 여러 도메인간의 SSO를 지원함
	국외	연동을 위한 보안 구조 제공으로 안전한 서비스가 보장됨으로써 새로운 사업 모델이 창출될 것임.	Linux Kernel의 기본 기능이 탑재된 운영체제가 시장을 주도	웹 기반의 SSO는 CA와 IBM, VeriSign이 30%를 차지하고 평균 20%의 성장률을 보여주고 있으며, CA/Netegrity의 SiteMinder와 IBM의 Tivoli Access Manager가 대표적인 제품임
기술 개발 현황 및 전망	국내	IT융 · 복합 디바이스 단에서 멀티모드 무선 및 서비스 컨버전스를 제공하는 기술개발이 진행 중이나, 관련 융 · 복합 보안 기술이 개발된 사례는 없음	2006년 부터 3년 계획으로 ETRI에서 "임베디드 보안 운영체제 기술개발" 과제를 수행 중	- 온라인 상의 사용자 인증 관련 기술은 전자서명을 이용한 기술과 OTP를 이용한 기술과 생체를 이용한 기술 등 다양한 기술이 개발 - 네트워크 자체를 보호하기 위해 호스트의 네트워크 접근을 제어하는 기술 등이 연구 개발되고 있음
	국외	개방형 무선 단말 및 기지국 기술, 멀티모드 지원 IT 컨버전스 단말기와 모바일 플랫폼 보안 기술 연구가 활발히 진행 중	최근에는 Linux를 기반으로 Secure Enhanced Linux를 개발	- 온라인 상의 사용자 인증 관련 기술은 인증 강도를 높이기 위한 방향과 상호 연동성을 높이는 방향으로 개발되고 있다. - BM, MS, Sun, CISCO 등 세계적인 기업들은 통합 보안 시스템에 대한 제품을 지원
기술 개발 수준	국내	기술기획(일부설계)	기술기획	기술기획
	국외	설계(일부구현)	설계(일부구현)	설계
	기술격차	1년	1.5년	1년
	관련제품	무선보안API	도메인 분리 API, 임의조작 방지 S/W	보안 프로토콜 및 API
IPR 보유현황	국내	WiBro의 특허가 2000년부터 2005년까지의 644개	임베디드 환경에 적합한 소형, 저전력, 고속 보안기술에 대한 특허의 다수 확보	싱글사인온(SSO) 메커니즘에 관한 특허가 많이 등록된 상태임
	국외	유무선 환경에서 접근통제 및 네트워크 공격에 대한 방어 등 특허 출원	소형, 경량, 저전력에 대응할 수 있는 특허권을 확보함으로써 시장 선점	미국의 IBM과 Microsoft 및 일본의 NTT를 중심으로 ID관리 기술과 핵심적인 접근제어 기술에 관한 특허를 보유
IPR확보 가능분야		가입자 인증 및 키관리 기술 등	도메인 분리, 접근제어, 감사추적 등	ID 생성 및 검증, 접근 제어 등
IPR확보 가능성		높음	보통	높음
표준화현황 및 전망		- 국내 : TTA를 중심으로한 무선 네트워크 보안기술 표준화가 진행 중이다. - 국외 : IEEE802, IETF를 중심으로한 무선 네트워크 보안 기술 표준화	- 국내 : CELF에서 임베디드 리눅스 솔루션 및 표준 - 국외 : TCPA는 PC 기반의 산업 플랫폼, 운영체제, 응용 등의 보안규격을 개발	- 국내 : TTA를 중심으로 SSO 및 접근제어에 대한 표준화를 진행 - 국외 : OASIS는 중심으로 SSO 관련 SAML, 접근제어 관련 XACML표준 진행 중
표준화 기구/ 단체	국내	TTA	TTA	TTA
	국외	ITU-T, ISO, IEEE 등	ITU-T, ISO, TCPA 등	ITU-T, ISO, OASIS 등
	국내참여 업체 및 기관현황	ETRI, KT, SK 등	ETRI, 삼성, SK, Secuve 등	ETRI, KT, SK 등
	국내기여도	높음	보통	높음
표준화 수준	국내	표준안 기획(일부 표준항목승인)	표준안 기획	표준안 기획(일부 표준항목승인)
	국외	표준안 항목 승인(일부 표준안 개발)	표준안 항목 승인	표준안 항목 승인(일부 표준안 개발)
국내표준화의 인프라수준 (시장요구정도 및 참여도)		높음	보통	높음

3. 중점 표준화 대상항목의 표준화 추진전략

3.1. 중점기술의 표준화 환경분석

3.1.1. 표준화 추진상의 문제점 및 현안사항

- 표준화추진을 위한 전담 포럼 구성 시 정보 보호 공통 플랫폼에 대한 연구 및 기술개발을 진행 중인 산업체가 많지 않으므로, 컨소시엄 및 포럼 구성에 어려움을 겪을 수 있다. 또한, 정보 보호 업체가 영세하여 표준화 여력이 부족하므로, 적극적으로 참여를 유도하는 정부의 노력이 필요하다.
- 서비스별로 유관 단체(포럼 등)가 전용 표준안을 개발하는 국내 상황에서 보안 공통화를 추진하기 위한 상호 의견 조율 및 협력이 필요하며, 보안 공통화를 추진하려는 단말과 서비스의 타겟팅이 표준화의 주요한 관건이다.
- 국제표준화추진 시(ISO, ITU-T 등) 정보 보호 공통 플랫폼 관련된 표준화 그룹이 산재되어 있어, 산업적 파급 효과를 고려한 선택과 집중 전략이 필요하다.

3.1.2. SWOT 분석 및 표준화 추진방향

국내 역량요인 / 국외 환경요인			강점 요인 (S)	약점 요인 (W)
		시장	- 통방융합, 유무선융합 등 컨버젼스 네트워크 시장 증대 - WiBro, DMB 등 융복합 서비스의 세계 최초 상용 서비스 시장 형성	시장 - 국내 이동통신 시장 규모의 한계 - 국내 이동통신사업자의 경쟁에 따른 저가의 모바일 단말 요구
		기술	- 소프트인프라웨어가 IT839 전략의 3대 첨단 인프라 기술로 부각 - 보안미들웨어(인증, 프라이버시) 및 보안 운영체제 기술 보유	기술 - 보안 칩 등 H/W 해외 의존도 높다. - 핵심 원천 기술에 대한 분쟁 가능성 높음
		표준	- ITU-T SG17 정보보호 표준화 주도 - IT839 전략에 따른 정부의 일관된 표준 정책	표준 - 산업체 사업자의 표준화 참여도 미흡 - 기존 표준과의 호환성 유지를 위한 비효율성 존재
기회요인 (O)	시장	- WiBro 등 초고속 네트워크 환경 구축 및 융복합 서비스 환경 다양화 - 디지털 콘텐츠 및 프라이버시 보호를 위한 모바일 환경의 요구	- 현황분석에 의한 우선순위 : 1 - 모바일 환경에서 융 · 복합 서비스의 시장 증대에 따른 무선공통보안 API 기술개발 및 IEEE 802 표준화추진 - ITU-T SG17 정보보호 표준화 경험 활용을 통한 보안미들웨어(인증 및 침해확산) 및 트러스트 운영체제 기술의 국제표준 선점	- 현황분석에 의한 우선순위 : 2 - IT839 전략을 기반으로 DMB, WiBro 등 융복합 서비스의 지재권 보호 기술개발 및 ISO 표준의 조기 정립을 통한 국외 시장 개척 - 중장기적인 전략으로 국제표준화활동을 통한 해외 의존도 높은 모바일 단말 H/W(보안저장장치) 기술 확보
	기술	- 세계적으로 기획 단계인 DMB, 등 융복합 서비스 보호 기술 확보 - 위치추적, 통합 인증 등 새로운 패러다임의 보안 기술 요구		
	표준	- DMB, WiBro 등 융복합 서비스 실현을 위한 선행 표준 주도 - 모바일 환경에서 네트워크 및 단말 보호를 위한 표준화 요구		
			〈SO전략 : 공격적 전략(강점사용-기회활용)〉	〈WO전략 : 만회 전략(약점극복-기회활용)〉
			〈ST전략 : 다각화 전략(강점사용-위협회피)〉	〈WT전략 : 방어적 전략(약점최소화-위협회피)〉
위협요인 (T)	시장	- 미국, 유럽 등에서 독자적인 모바일 시장 개척을 위한 추진체 구성 - 모바일 단말 시장이 선진 업체에 의해 형성됨	- 현황분석에 의한 우선순위 : 3 - 진 업체가 주도하고 있는 모바일 단말 H/W(스마트토큰) 기술 등에 대한 산 · 학 · 연 표준화 협력 체계를 구축을 통한 ISO, OMA 국제표준 추진 - ISO/IEC 등 선도 표준 기구의 진입을 위한 국제표준 전문가 그룹과의 연대를 통한 국제표준의 협력 및 보안 응용 및 프로토콜 기술의 경쟁력 확보	- 현황분석에 의한 우선순위 : 4 - 기술 경쟁이 치열하고 시장 규모가 큰 트러스트 I/O 및 소프트웨어 다운로드 보안 기술의 국제표준 수용 및 적용 - 산 · 학 · 연 표준 협력 체계 구축으로 국제표준화활동의 지속적인 참여를 통한 기존 표준과의 호환성 유지 및 표준 전문 인력 양성
	기술	- 선진 업체와 기술 파급 효과가 큰 모바일 단말 H/W 기술 경쟁이 치열 - 기술 선진국과의 공동 연구 및 기술 개발 미흡		
	표준	- 선도 모바일 단말 보안 표준 기구의 진입 장벽 - 미국, 유럽 등의 모바일 단말 개발 방향에 따라 표준 기술이 주도		

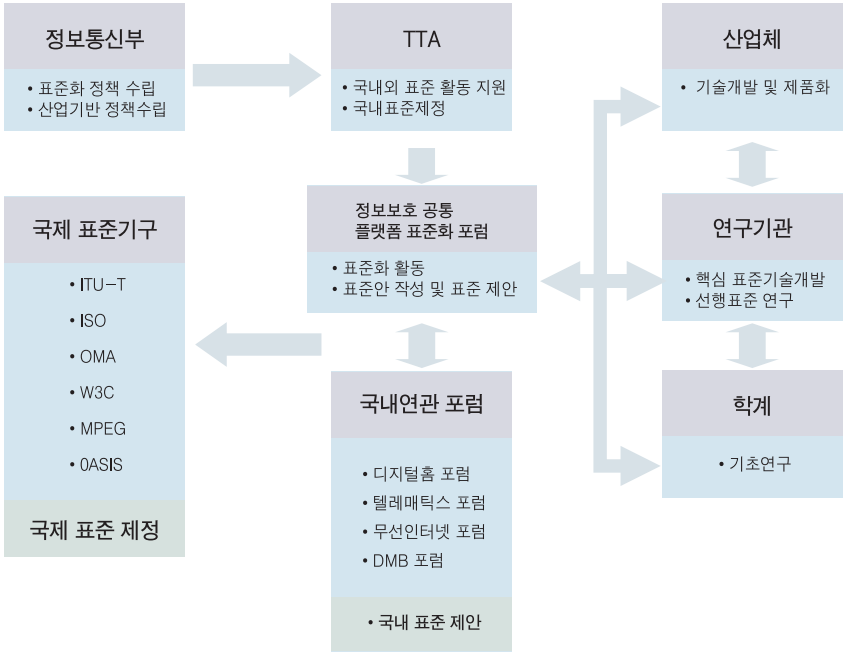
- 현황 분석을 통한 우선순위
  - 기술성숙도와 시장잠재력이 우수한 정보 보호 공통 플랫폼의 보안 미들웨어 및 무선 공통 보안 API 기술은 국내 관련 산업의 인프라가 비교적 양호한 기술 분야로 국내 산업의 강점을 최대한 활용하여 국제표준을 선도 한다.
  - 기술 의존도가 높고 원천 기술 확보가 취약한 보안저장장치 및 스마트 토큰 등 정보 보호 공통 플랫폼의 H/W 분야는 국제표준을 수용하여 국내 관련 산업의 기술 기반을 마련한다.

• 표준화 추진방향

- 정보 보호 공통 플랫폼 기술은 현재 모바일 환경에서 적용 가능한 기술로, 소프트인프라웨어 구축과 함께 시급히 요구되는 기술이며, 기본적인 H/W의 저장장치 및 무선 접속 기술에 대한 표준화작업은 국제적으로 상당히 진행되어 있으므로 이들 분야에 대해서는 국내 환경에 신속히 적용하기 위한 국제표준 수용작업을 지속적으로 추진하여야 한다.
- 국제표준 수용과 프로파일 표준 개발 작업을 추진함에 있어 산업체의 제품 경쟁력과 관련이 깊은 핵심기술에 대해서는 선행 시제품 개발을 병행하여 추진함으로써 표준 개발의 품질 제고 및 확보되는 핵심 표준 기술을 산업체에 제공하여 개발 표준이 조기 상용화되도록 추진한다.
- 정보 보호 공통 플랫폼의 보안 미들웨어 및 보안응용 및 프로토콜 등 최근 국제표준화 기구에서 논의가 시작되고 있거나 미래 표준기술 분야에 대해 선행 표준 기술 연구 활동을 적극 추진하여 신규 표준화 분야에 대한 국제표준 선점을 위한 국제표준화활동을 강화한다.

3.1.3. 표준화 추진체계

- 표준화 과정에서 신속한 대응을 위해서는 (그림 8)와 같이 산 · 학 · 연의 정보보호 전문가들이 관련 기술에 대한 이해와 문제점 도출, 표준화 방향 등을 협의 할 수 있는 정보 보호 공통 플랫폼 표준화 포럼을 설립하여 표준화를 추진한다.
- 표준안 개발은 국내 시장 및 국제 환경에 효과적으로 적응하는 기술 규격을 분석하고, 이를 기반으로 표준안을 개발한다.
- 또한, TTA는 표준과제를 통하여 국내 및 국제표준안을 개발하고, 국제표준 전문가 과제를 통하여 국제표준화활동을 지원한다.
- 기존의 국내 연관 포럼(디지털홈포럼 등)과 협력을 통하여 융 · 복합 서비스 공통 보안 응용 및 프로토콜 표준화를 추진한다.



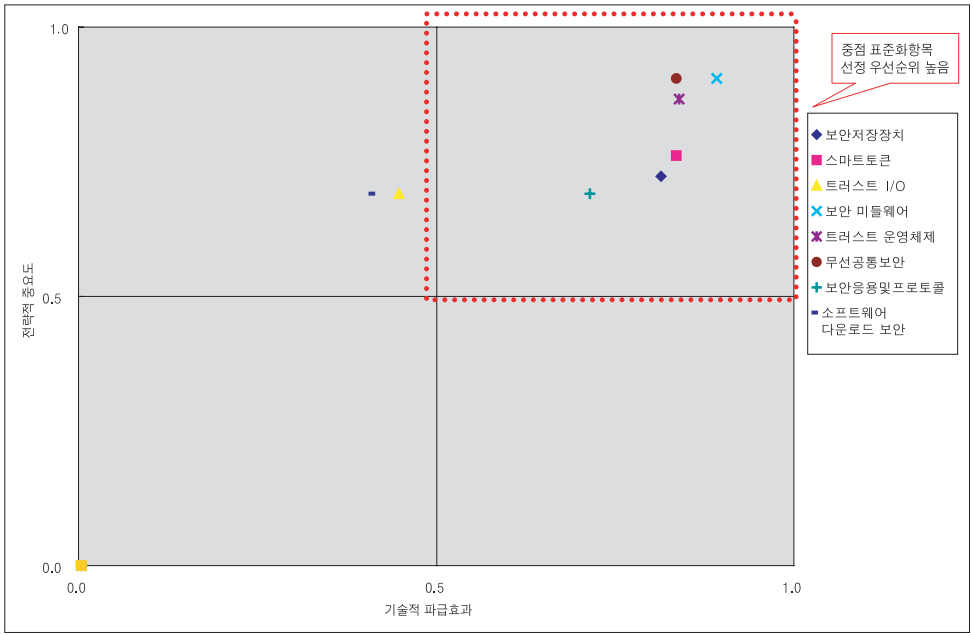
(그림 8) 표준화 추진체계

3.2. 중점 표준화 대상항목 선정

3.2.1. 중점 표준화 대상항목 선정방법

표준화 대상항목별 전략적 중요도 및 기술적 파급효과 분석								
고려요소	전략적 중요도					기술적 파급효과		
	P1 정부의지	P2 산업체의지	P3 공공성	P4 (Priority Index)	PI	E1 기술 내 중요도	E3 산업적 파급효과	EI
고려요소별 가중치	0.21	0.17	0.09	0.11		0.28	0.26	
보안저장장치	4	5	4	4	0.8	4	4	0.6
스마트토큰	4	5	4	5	0.9	4	4	0.7
트러스트 I/O	2	2	3	2	0.5	3	3	0.8
보안 미들웨이	5	4	5	5	0.9	5	4	0.7
트러스트 운영체제	5	4	4	5	0.9	5	4	0.9
무선공통보안	4	4	5	4	0.9	5	4	0.9
보안응용 및 프로토콜	3	4	3	5	0.7	3	3	0.9
소프트웨어 다운로드 보안	3	2	2	1	0.4	3	3	0.7

* 표준화 대상항목의 각 고려요소별 평가점수는 해당 중점기술의 전문가들 의견을 종합하여 산출
* 각 고려요소별 평가점수는 1(매우 낮음), 2(낮음), 3(보통), 4(높음), 5(매우 높음)의 5점 척도



3.2.2. 중점 표준화 대상항목 선정사유

• 전략적 중요도 및 기술적 파급효과의 요소

- 정보 보호 공통 플랫폼 기술 표준화항목의 선정은 전략적 중요도 및 기술적 파급효과를 고려한다.
- 전략적 중요도의 요소인 정부의지, 산업체 의지, 공공성, 적시성, 시장파급성, 기술적 선도 가능성, 국제표준화 이슈 정도, 사용화 가능성 등 8개 항목에 대한 가중치는 이 분야 전문가들의 설문을 통하여 선정되었다. 이들 8개 항목 중 정부의 의지가 0.175로 가장 높게 나타나고, 국제표준화 이슈 정도가 가장 낮게 나타나고 있다.
- 기술적 파급효과의 요소인 기술 내 중요도, 타기술에 파급효과, 산업적 파급효과, 미래 영향력 등 4개 항목에 대한 가중치는 이 분야 전문가들의 설문을 통하여 선정되었다. 이 4개 항목 중 산업적 파급효과가 0.3으로 가장 높게 나타나고, 미래 영향력이 가장 낮게 나타나고 있다.

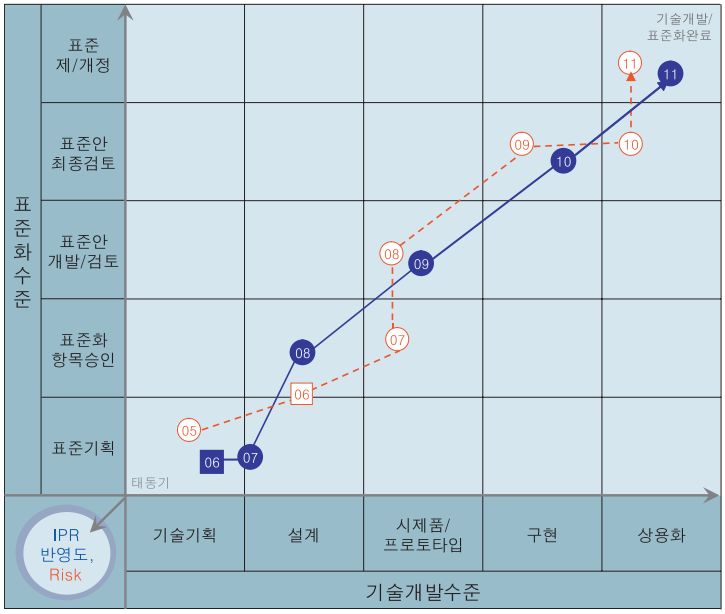
• 중점 표준화 대상항목별 선정사유

- 최근 ITU-T, ISO 등 국제표준화기구를 중심으로 진행되고 있는 정보 보호 공통 플랫폼 기술 표준화 동향을 중심으로 표준화 대상항목을 선정하였으며, 또한 국제적으로 우리나라가 표준화를 주도하거나, 주도할 잠재력을 가진 분야, 기술 개발 시 국내외적으로 시장경쟁력을 확보할 수 있는 분야를 중심으로 표준화 대상항목을 선정하였다.
- 이와 같은 기준에 따라 선정된 보안저장장치, 스마트토큰, 트러스트 I/O, 무선공통보안API, 트러스트 운영체제, 보안 응용 및 프로토콜, 소프트웨어 다운로드 보안 등을 표준화 대상항목을 선정하였다.
- 전략적 중요도 및 기술적 파급효과의 가중치를 8개 표준화 대상항목에 적용하여 보안저장장치, 스마트토큰, 무선공통보안API, 트러스트 운영체제, 보안 응용 및 프로토콜 등 6개 표준화 대상항목이 정보 보호 공통보안플랫폼 기술의 중점 표준화항목으로 선정되었다.
- 한편, 트러스트 I/O 및 소프트웨어 다운로드 보안 등의 2개 표준화 대상항목은 적시성과 시급성 등의 요소가 낮게 나타나는데, 이는 정보 보호 공통 보안 플랫폼의 상용화가 예상되는 2009년부터 본격적으로 표준화의 논의가 시작될 것으로 예상된다.

3.3. 중점 표준화 대상항목별 세부전략(안)

3.3.1. 보안저장장치

• 표준상태전이도(표준화 & 기술 개발 연계 분석)

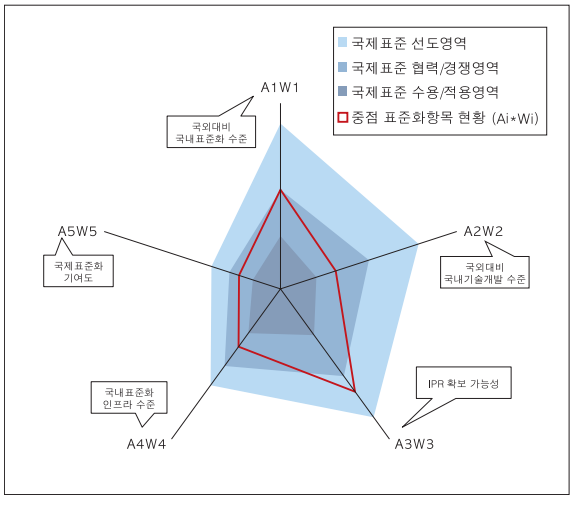


표준화 중요도	국내 개발주체		관련 국제 표준화 기구
고(★★★) 중(★★☆) 저(★☆☆)	표준개발	기술개발	
★★★	TTA	ETRI	ISO, OMA

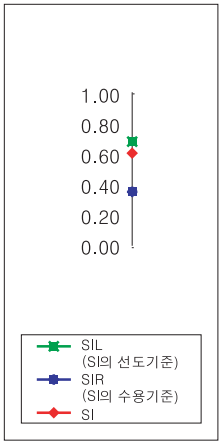
범 례

06 : 중점 표준화항목의 국내상태
06 : 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	
SI_L (SI의 선도기준)	0.68
SI_R (SI의 수용기준)	0.35
SI	0.60



∴ 국제표준 협력/경쟁

• 세부전략(안)

- 표준화추진

◦ 보안저장장치는 데이터의 안전한 저장 및 지재권 보호를 위한 Right 관리 및 S/W 실행 등을 가능하게 하는 저장장치로 하드웨어 기반 MMC, USB 등을 이용하여 2008년 1차 규격으로 착탈형 저장 장치의 콘텐츠 유통 권한 방지 기술의 표준화를 추진한다.

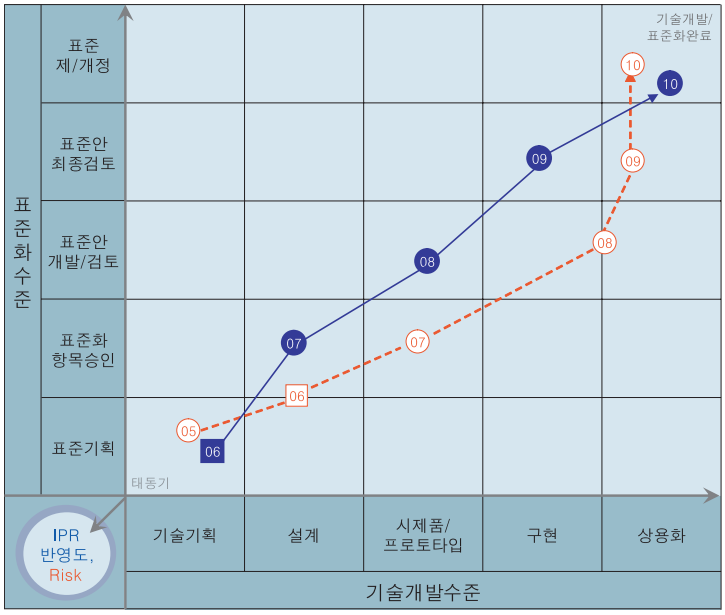
◦ USB와 같은 저장장치에서 보안 기능을 제공하기 위한 S/W 실행 환경 기술을 2010년 2차 규격으로 표준화를 추진한다.

- IPR 확보 방안

◦ 국제표준 협력/경쟁을 확보하기 위해서 1차적으로 기술개발과 동시에 국내표준을 추진한 후 OMA, ISO에서 국제표준과 함께 IPR 확보를 추진한다.

3.3.2. 스마트토큰

• 표준상태전이도(표준화 & 기술 개발 연계 분석)

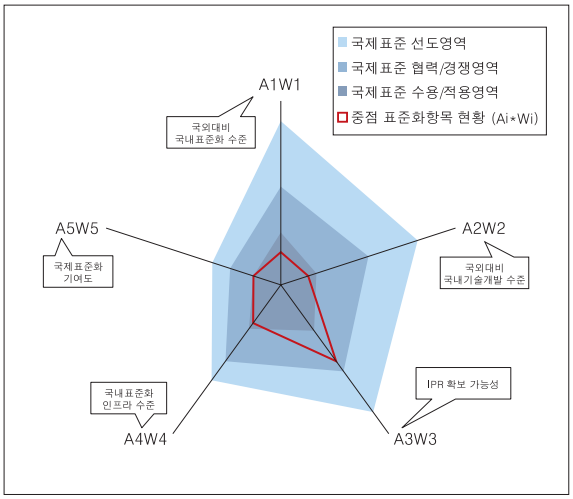


표준화 중요도	국내 개발주체		관련 국제 표준화 기구
고(★★★) 중(★★☆) 저(★☆☆)	표준개발	기술개발	
★★★	TTA	ETRI	ISO, OMA

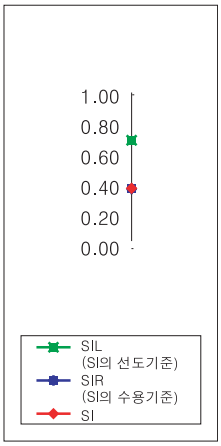
범 례

06 : 중점 표준화항목의 국내상태
06 : 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	
SI_L (SI의 선도기준)	0.68
SI_R (SI의 수용기준)	0.35
SI	0.35



∴ 국제표준 수용/적용

• 세부전략(안)

- 표준화추진

◦ TPM 기반 단말의 (가칭) 정보 보호 공통 플랫폼포럼을 중심으로 산 · 학 · 연 표준화 협력 체계를 구축하여 TPM 산업 표준인 TCG 단체 규격을 수용하고, 2008년도 단말 복제 방지, 부트 코드의 임의 조작 방지 기능을 제공하는 하드웨어 TPM의 구현 기술에 대한 국내 고유 표준 개발을 추진한다.

◦ 2008년 u-ID, 콘텐츠 보안, 키관리 등을 지원하는 스마트카드 플랫폼 기술에 대한 국내 고유 표준 개발을 추진하고, 2009년 TCG 단체 규격으로 제안하여 국제표준화를 추진한다.

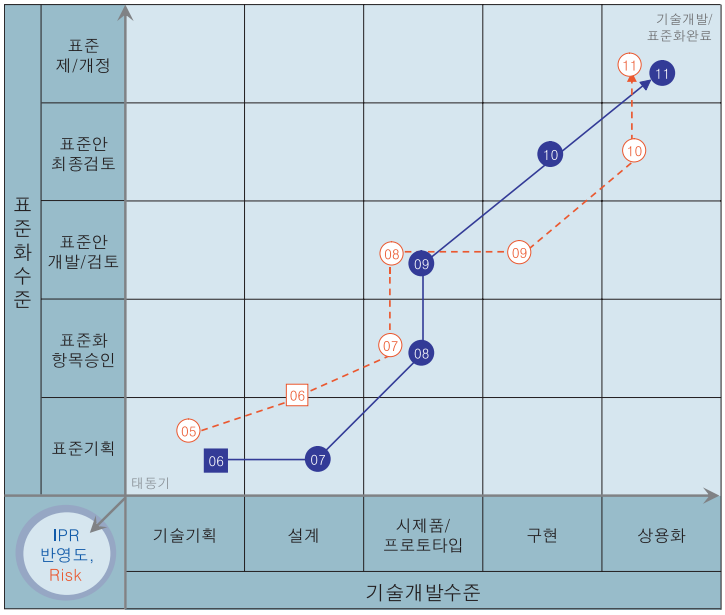
- IPR 확보 방안

◦ 미국 인텔을 중심으로 보안 프로세서 등의 요소기술에 대한 IPR을 주도하고 있다.

◦ TPM과 관련된 특허는 미국, 일본 등에서 IPR을 독점하고 있는 실정이나, 이를 극복하기 위한 방안으로 표준 수용 및 기술개발을 동시에 추진하여 ISO, OMA에서 스마트 토큰 응용 API 등 응용서비스 인터페이스 부분에 대한 IPR 확보하는 방안을 추진한다.

3.3.3. 보안미들웨어

- 표준상태전이도(표준화 & 기술 개발 연계 분석)

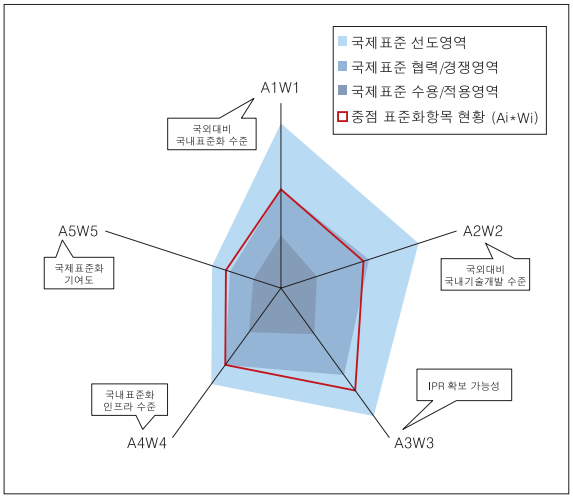


표준화 중요도	국내 개발주체		관련 국제 표준화 기구
고(★★★) 중(★★☆) 저(★☆☆)	표준개발	기술개발	
★★★	TTA	ETRI	ITU-T, ISO, W3C, MPEG

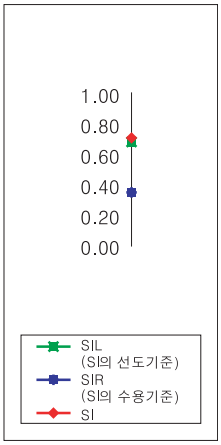
범 례

06 : 중점 표준화항목의 국내상태
06 : 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	
SI_L (SI의 선도기준)	0.68
SI_R (SI의 수용기준)	0.35
SI	0.71



∴ 국제표준 선도

• 세부전략(안)

- 표준화추진

◦ 보안저장장치, 스마트토큰 등의 표준을 응용 모델에 반영하여 2009년 국내표준을 추진한다.

◦ 융복합 공통 보안 키관리 기술, 프로파일 기반 사용자 제어형 u-ID 관리 기술은 국내표준을 바탕으로 2009년 ITU-T(인증)에 국제표준을 추진한다.

◦ 모바일 환경에서 융 · 복합 콘텐츠 보호 서비스를 제공하기 위한 DRM/CAS/CP 통합 지재권 보호 기술은 국내표준을 바탕으로 2008년 ISO(지재권)에 국제표준을 추진한다.

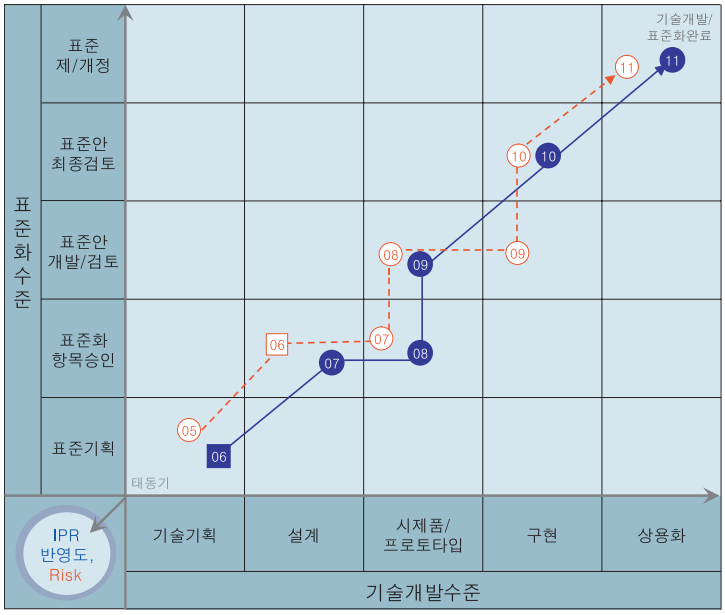
◦ 모바일 악성코드 탐지를 위한 데이터 수집 메소드, 로그 포맷, 보고 절차 등을 포함하는 악성 코드 침해 감지 및 대응 기술은 국내표준을 바탕으로 2009년 ITU-T(침해확산방지)에 국제표준을 추진한다.

- IPR 확보 방안

◦ 특히, 지재권 보호 기술은 OMA, 5C DTCP, DVB CPCM, DLNA 등에서 모바일 및 홈기기의 지재권 보호 관련한 Defactor 표준 추진을 통해 IPR 및 로열티 수익을 확보한다.

3.3.4. 무선공통보안API

• 표준상태전이도(표준화 & 기술 개발 연계 분석)



표준화 중요도	국내 개발주체		관련 국제 표준화 기구
고(★★★) 중(★★☆) 저(★☆☆)	표준개발	기술개발	
★★★	TTA	ETRI	ITU-T, ISO, IEEE

범 례

06 : 중점 표준화항목의 국내상태

06 : 중점 표준화항목의 국제상태

→ : 중점 표준화항목의 국내 표준상태전이

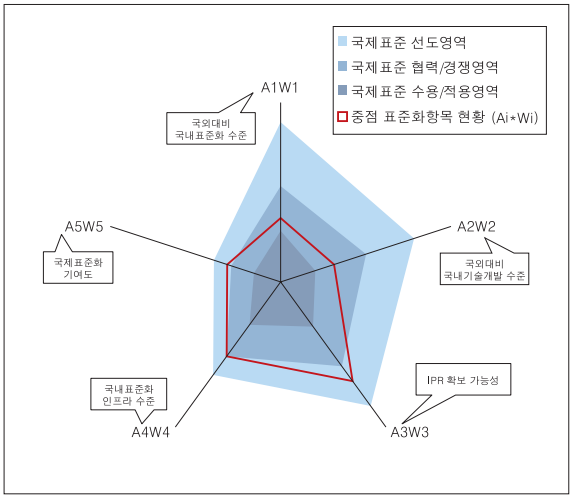
⇢ : 중점 표준화항목의 국제 표준상태전이

↑ : 선행표준(선 표준화 후 기술개발)

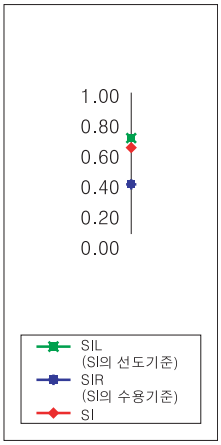
↗ : 동시표준(표준화&기술개발 동시추진)

↓ : 후행표준(선 기술개발 후 표준화)

• 국제표준화 전략목표 도출



SI	
SI_L (SI의 선도기준)	0.68
SI_R (SI의 수용기준)	0.35
SI	0.61



∴ 국제표준 협력/경쟁

• 세부전략(안)

- 표준화추진

◦ 무선API 경우 서비스/디바이스에 공통 적용됨으로 국내 고유 표준 개발을 위한 단말기 제조업체, 서비스 개발업체간의 협력/조율이 필요하며, 무선공통보안API의 경우 무선네트워크 고유의 보안 규격을 보유하고 있으므로, 2007년 1차적으로 적용규격을 국내표준안으로 수용한 후, 2008년 공통된 단일규격 API를 별개의 표준안으로 추진한다.

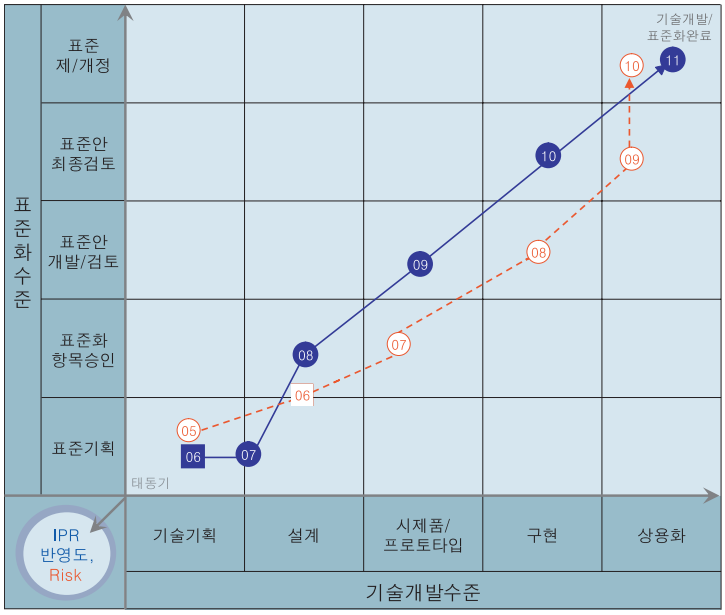
◦ 상이한 모바일 환경에서 무선 공통 이동(MIH 기반) 보안 API 기술은 2007년 IEEE 802, 3GPP2, IETF 등의 국제표준을 수용하고, MIH 기반 보안 API 구현 기술이 확보되는 2009년 IEEE 802에 국제표준화를 추진한다.

- IPR 확보 방안

◦ MIH 기반 무선망 보안 연동 기술의 경우 상이한 무선망간의 이동 보안 규격을 다루고 있으므로, IEEE 802, 3GPP2, IETF 등과 협력 경쟁하여 국제표준화 및 IPR 확보를 추진한다.

3.3.5. 트러스트 운영체제

• 표준상태전이도(표준화 & 기술 개발 연계 분석)

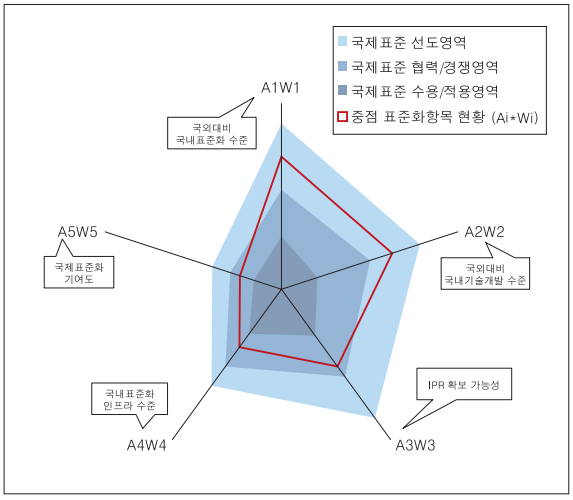


표준화 중요도	국내 개발주체		관련 국제 표준화 기구
고(★★★) 중(★★☆) 저(★☆☆)	표준개발	기술개발	
★★★	TTA	ETRI	ITU-T, ISO, TCPA

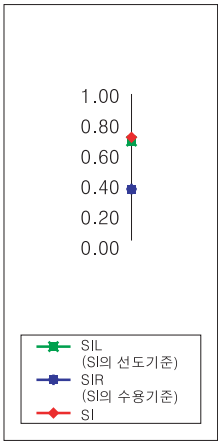
범 례

06 : 중점 표준화항목의 국내상태
06 : 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	
SI_L (SI의 선도기준)	0.68
SI_R (SI의 수용기준)	0.35
SI	0.69



∴ 국제표준 선도

• 세부전략(안)

- 표준화추진

◦ 침해 확산 방지형 도메인 분리 기술, 플랫폼 임의 조작 방지기술과 커널 무결성 검증 기술은 TCG의 모바일 단말 환경에서 플랫폼 임의 조작 및 침해 확산을 방지하는 TMP(Trusted Mobile Platform) 및 네트워크의 신뢰성을 제공하는 TNC(Trusted Network Connection) 규격을 수용하고, 2009년 구현 기술에 대한 국내 고유 표준 개발을 추진한다.

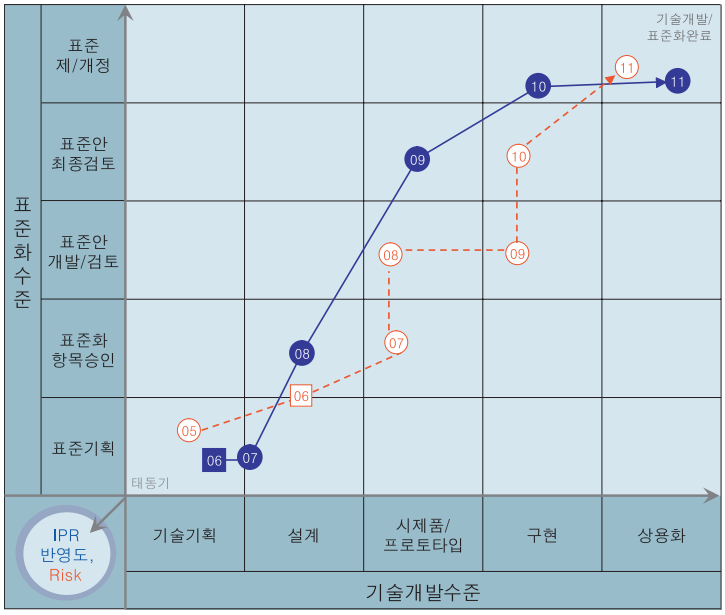
◦ 2008년 트러스트 운영체제 기술은 ISO 표준 규격을 바탕으로 모바일 단말은 트러스트 운영체제 국제표준을 추진함으로써 표준화를 선도한다.

- IPR 확보 방안

◦ 침해 확산 방지형 도메인 분리 기술은 새로운 개념의 분리 커널 표준화 분야로, Common Criteria를 기반으로 ISO에서 국제표준화 및 IPR 확보를 추진한다.

3.3.6. 보안 응용 및 프로토콜

• 표준상태전이도(표준화 & 기술 개발 연계 분석)



표준화 중요도	국내 개발주체		관련 국제 표준화 기구
고(★★★) 중(★★☆) 저(★☆☆)	표준개발	기술개발	
★★★	TTA	ETRI	ITU-T, ISO, OASIS

범 례

06 : 중점 표준화항목의 국내상태

06 : 중점 표준화항목의 국제상태

→ : 중점 표준화항목의 국내 표준상태전이

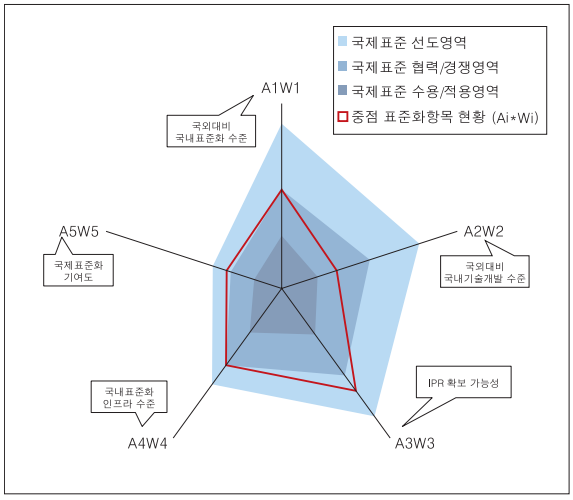
⇢ : 중점 표준화항목의 국제 표준상태전이

↑ : 선행표준(선 표준화 후 기술개발)

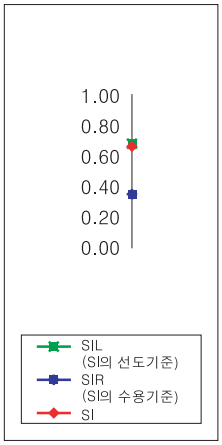
↗ : 동시표준(표준화&기술개발 동시추진)

↓ : 후행표준(선 기술개발 후 표준화)

• 국제표준화 전략목표 도출



SI	
SI_L (SI의 선도기준)	0.68
SI_R (SI의 수용기준)	0.35
SI	0.66



∴ 국제표준 협력/경쟁

• 세부전략(안)

- 표준화추진

◦ 보안 응용 및 프로토콜은 정보보호 공통 플랫폼상에서 다양한 응용서비스(u-City, u-Home 등)의 연동 보안 기능을 제공하는 기술로서, 공통 보안 프로토콜 및 API, 범용 ID 생성 및 검증, 단말 무결성 검증 및 접근제어 기술, 사용자/디바이스간 콘텐츠 유통 권한 공유 기술이 표준화 대상항목으로, 일부 기술에 대한 표준화 및 이에 따른 IPR 확보가 상당히 진행되었다.

◦ 융복합 서비스용 공통 보안 프로토콜 API 기술의 경우 IT 839 서비스 유관 포럼(홈네트워크 등)과 협력하여 2009년 국내 단일 표준안 마련을 추진한다.

◦ 범용 ID 생성 및 검증, ID 인증 인프라 연동 게이트웨이 기술의 경우 네트워크 및 서비스 통합 인증(u-SSO) 프레임워크의 표준화에 집중하고, 2008년 IETF, ITU-T에서 국제표준화를 추진한다.

◦ 모바일 환경에서 사용자/디바이스간 콘텐츠(UCC 포함) 보호를 위한 유통 권한 관리 기술은 국내표준을 바탕으로 2008년 ISO(유통 권한 공유 기술)에 국제표준을 추진한다.

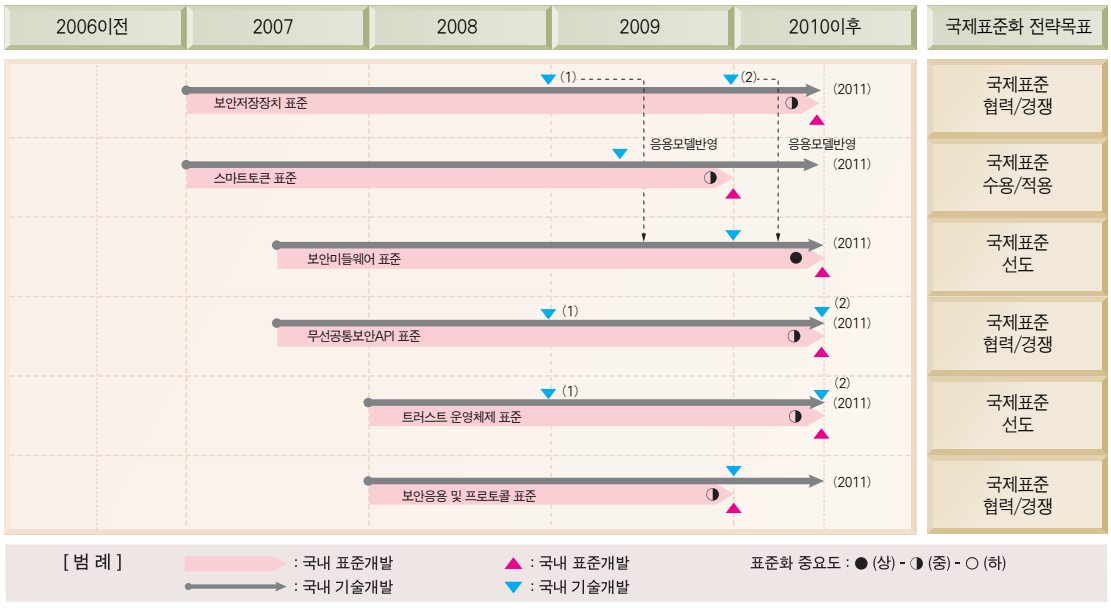
◦ 단말의 무결성을 증명하고 악성코드에 감염된 단말의 서비스 접속을 제어하는 기술은 국내표준을 바탕으로 2009년 ITU-T(단말 무결성 증명 및 접속제어 기술)에 국제표준을 추진한다.

- IPR 확보 방안

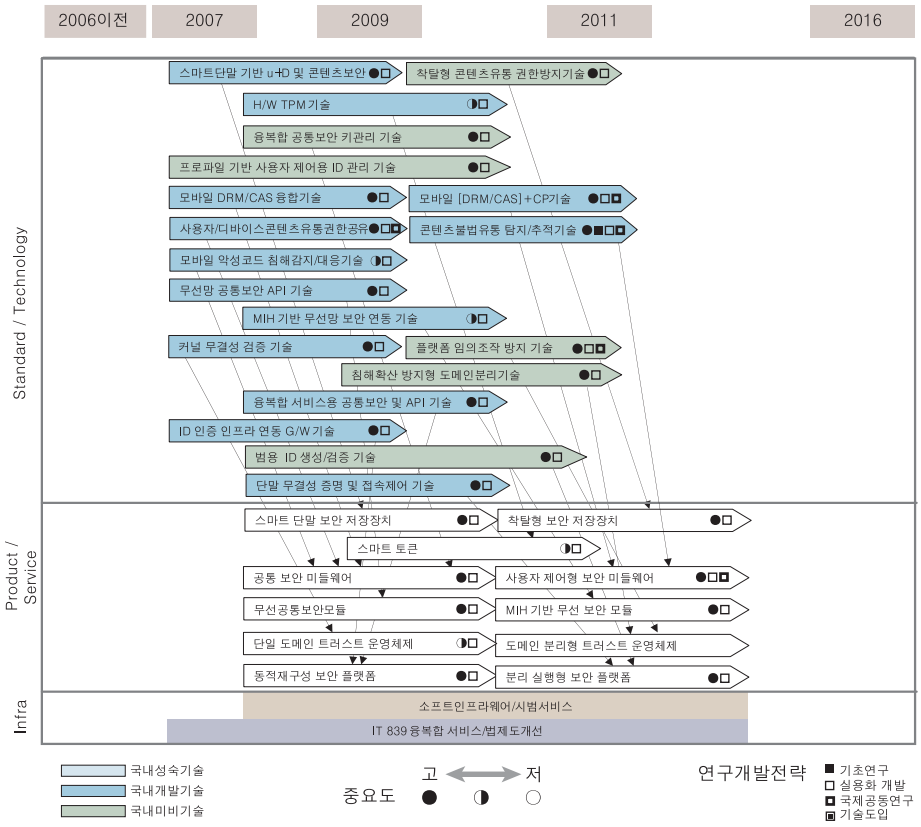
◦ 사용자/디바이스간 콘텐츠 유통 권한 공유기술의 경우 Web 2.0(UCC) 및 u-홈 환경에서 지재권 보호를 위한 핵심기술이므로 개발과 표준화를 병행하여 IPR을 우선 확보 전략을 추진한다.

3.4. 중장기 표준화로드맵

3.4.1. 중기(2007~2009) 표준화로드맵



3.4.2. 장기 표준화로드맵(10년 기술 예측)



〔국내외 관련표준 대응리스트〕

구분	표준화 항목	표준명	기구 (업체)	제정 연도	재개정 현황	국내관련표준	국내 추진기구
보안저장장치	보안저장장치	CPRM(Content Protection for Recordable Media)	4C	1998	제정		
		DTCP(Digital Transmission for Copy Protection)	5C	1998	제정		
스마트 토큰	스마트 토큰	Smart cards; Vocabulary for Smart Card Platform specifications V3.0.0	ETSI	2005	개발 중		
		Open Platform Card Specification	비공식기구	2004	제정	개방형 구조 카드 표준	TTA
		Smart Cards; Extensible Authentication Protocol support in the UICC; V6.1.0; Release 6	ETSI	2004	제정		
		Smart cards; UICC Application Programming Interface (UICC API) for Java Card (TM) (Release 6) V6.0.1; Includes Diskette	ETSI	2004	제정		
		Smart cards; Secured packet structure for UICC based applications V6.4.0; Release 6	ETSI	2005	개발 중		
		Smart Cards; Security Mechanisms for UICC Based Applications - Functional Requirements V6.0.0; Release 6	ETSI	2005	개발 중		
보안 미들웨어	키 관리 기술	Wireless Key Distribution Algorithm Standard	ITU-T	2002	제정	무선 키 분배 알고리즘 표준	TTA
		Directory : public-key and attribute certificate frameworks standard	ITU-T	2003	제정	디렉토리 : 공개키와 속성 인증서에 대한 프레임 워크 표준	TTA
		Guideline for Key Management and Certificate on Encryption Key Distribution	ITU-T	2004	제정	암호키분배용 인증서 및 키 관리 지침	TTA
		Advanced Encryption Standard(AES) Key Wrap Algorithm	ITU-T	2005	제정	AES 키 싸기 알고리즘	TTA
		Triple-DES and RC2 Key Wrapping	ITU-T	2005	제정	3-DES와 RC-2 키 싸기	TTA
		ENTITY AUTHENTICATION MECHANISM STANDARD USING SYMMETRIC CRYPTOGRAPHIC TECHNIQUES	ISO/IEC	1999	제정	대칭형 암호화 기법을 이용한 실체인증 기술 표준	
	ID 관리 기술	ENTITY AUTHENTICATION STANDARD USING A CRYPTO GRAPHIC CHECK FUNCTION	ISO/IEC	1999	제정	암호학적 확인함수를 이용한 실체인증 기술 표준	TTA
		Wireless Transport Layer Security Certificate Profile Standard	ITU	2002	제정	무선 WTLS 인증서 프로파일 표준	TTA
		Wirelss Certificate Request Format Protocol Standard	ITU	2002	제정	무선 인증서 요청형식 프로토콜 표준	TTA
		OCSP(Online Certificate Status Protocol) Standard	IETF	003	제정	실시간 인증서 상태 확인 프로토콜 표준	TTA
		Wireless Certification Management Protocol	ITU	2004	제정	무선 인증서 관리 프로토콜	TTA
		Wireless Certification Request Message Format Protocol	ITU	2004	제정	무선 인증서 요청형식 프로토콜	TTA
		Framework for Certificate Policy and Certification Practice Statement	ITU	2004	제정	인증서정책 및 인증업무 준칙 프레임워크	TTA
		Subscriber Identification Based on VID	ITU	2005	제정	식별번호를 이용한 본인 확인 기술	TTA
		Extensible Authentication Protocol(EAP)	ITU-T	2005	제정	EAP 프로토콜	TTA
	지재권 보호	IMT-2000 3GPP-Digital Rights Management (DRM); Stage 1(R6)	3GPP	2005	제정	IMT-2000 3GPP-DRM; 1단계(R6)	TTA
		Universal Mobile Telecommunications System (UMTS); Digital Rights Management (DRM); Stage 1 3GPP TS 22.242 version 6.2.0 Release 6	ETSI	2003	제정		

구분	표준화 항목	표준명	기구 (업체)	제정 연도	재개정 현황	국내관련표준	국내 추진기구
보안 미들웨어	지재권 보호	Universal Mobile Telecommunications System (UMTS); Digital Rights Management (DRM); Stage 1 3GPP TS 22.242 Version 6.3.0 Release 6	ETSI	2003	제정		
		Digital Radio Mondiale (DRM); Specific Restrictions for the use of the Distribution and Communication Protocol (DCP) V1.1.1	ETSI	2003	제정		
	침해감지및 대응기술	FIREWALL SYSTEM SELECTION GUIDELINE	ISO/IEC	1999	제정	침입차단시스템 선정 지침	TTA
		Intrusion Detection System Security Functional Package	ITU-T	2003	제정	침입탐지시스템 기능패키지	TTA
무선 공통 보안	보안 API	IP 계층에서의 VPN 보안기술 표준	ITU-T	2001	제정	IP 계층에서의 VPN 보안 기술 표준	TTA
		User Authentication Mechanisms for Home Network using Home Server	ITU-T	2005	제정	홈서버 중심의 홈네트워크 사용자 인증 메커니즘	TTA
		PPP EAP TLS Authentication Protocol	IETF	2005	제정	EAP-TLS 인증 프로토콜	TTA
		IP Encapsulating Security Payload(ESP)	IETF	2005	제정	IP 캡슐화 보안 페이로드	TTA
		IP Authentication Header	IETF	2005	제정	IP 인증헤더	TTA
	보안 연동 기술	Secure Use Guide for Wireless LAN	ITU-T	2005	제정	안전한 무선랜 사용을 위한 가이드	TTA
		Security Architecture for the Internet Protocol	IETF	2005	제정	인터넷 프로토콜을 위한 보안구조	TTA
트러스트 운영 체제	트러스트 운영 체제	Standard for Information Technology Portable Operating System Interface (POSIX) Part 26 : Device Control Application Program Interface (API) (C Language) IEEE Computer Society Document	IEEE	2003	제정		
		"Standard for Information Technology - Portable Operating System Interface (POSIX) IEEE Computer Society Document; Includes Vol 1 -Base Definitions, Vol 2-System Interfaces, Vol 3-Shell and Utilities, Vol 4-Rationale (Informative)"	IEEE	2003	제정		
		Information Technology - Portable Operating System Intenistration First Edition; ANSI/IEEE Std 1387.2	ISO/IEC	2003	제정		
		Information technology Portable Operating System Interface (POSIX) Test methods for measuring conformance to POSIX Part 2 : Shell and utilities First Edition; IEEE Std 2003.2-1996	ISO/IEC	2003	제정		
		Information technology - Portable Operating System Interface (POSIX) - Part 2 : System Interfaces Third Edition; IEEE Std 1003.1 : 2003; Corrigendum 1 : 9/15/2004	ISO/IEC	2004	제정		
		Information Technology - Portable Operating System Interface (POSIX) - Part 1 : Base Definitions Fourth Edition; IEEE 1003.1; Corrigendum 1 : 9/15/2004	ISO/IEC	2005	제정		
		PROTABLE OPERATING SYSTEM INTERFACE (POSIX) PART 2 : SHELL AND UTILITIES	ISO/IEC	2005	제정	POSIX - PART 2 : 쉘과 유틸리티 표준 - ISO/IEC 9945-2	TTA
		A STANDARD FOR PORTABLE OPERATING SYSTEM INTERFACE(POSIX)	ISO/IEC	2005	제정	개방형 운영체제 인터페이스(POSIX.1)표준	TTA
		PORTABLE OPERATING SYSTEM INTERFACE(POSIX) PART 1 : SYSTEM APPLICATION PROGRAMMING INTERFACE(API) (C LANGUAGE)	ISO/IEC	2005	제정	POSIX - PART 1 : C언어를 위한 시스템 응용 프로그래밍 인터페이스(API) 표준 - ISO/IEC 9945-1	TTA
		Sensor Operating System API Framework for USN	ISO/IEC	2005	제정	USN용 센서 운영체제 API 프레임워크	TTA

구분	표준화 항목	표준명	기구 (업체)	제정 연도	재개정 현황	국내관련표준	국내 추진기구
보안 응용 및 프로토콜	공통보안 프로토콜	OPEN SYSTEMS INTERCONNECTION - THE DIRECTORY ; AUTHENTICATION FRAMEWORK	ITU-T	1993	제정	디렉토리 기본표준 ; 인증골격	TTA
		DIRECTORY SYSTEM AUTHENTICATION FRAMEWORK STANDARD	ITU-T	2000	제정	디렉토리시스템 인증 프레임워크 표준	TTA
		The Standard for Information Security Management	ISO/IEC	2002	제정	정보보호관리 표준	TTA
	ID 생성 및 검증 기술	DIGITAL SIGNATURE MECHANISM WITH APPENDIX - PART 2 : CERTIFICATE-BASED DIGITAL SIGNATURE ALGORITHM	ITU-T	1998	제정	부가형 전자서명 방식 표준- 제2부 : 확인서 이용 전자 서명 알고리즘	TTA
		Digital Signature Certificate Profile	ITU-T	2000	제정	전자서명 인증서 프로파일 표준	TTA
		Digital Signature Mechanism with Appendix - Part 2 : Certificate-based Digital Signature Algorithm	ITU-T	2000	제정	부가형 전자서명 방식 표준 -제 2 부 : 인증서 기반 전자서명 알고리즘	TTA
		Digital Signature Mechanism with Appendix - Part 3 : Korean Certificate-based Digital Signature Algorithm Using Elliptic Curves	ITU-T	2001	제정	부가형 전자서명 방식 표준-제3부 : 타원곡선을 이용한 인증서 기반 전자 서명 알고리즘	TTA
		Wireless Digital Signature Algorithm Standard	ITU	2002	제정	무선 전자서명 알고리즘 표준	TTA
		Wirelss Digital Signature Certificate Revocation List Profile Standard	ITU	2002	제정	무선 전자서명 인증서 효력정지 및 폐지 목록 프로파일 표준	TTA
		Wireless Digital Signature Certificate Profile Standard	ITU	2002	제정	무선 전자서명 인증서 프로파일 표준	TTA
		Path Processing Algorithm for Digital Signature Certificate	ITU	2005	제정	전자서명 인증서 경로처리 알고리즘	TTA
	연동 게이트웨이 기술	OPEN SYSTEMS INTERCONNECTION - THE DIRECTORY(1993) ; AUTHENTICATION FRAME WORK(REVISION)	ITU-T	1995	제정	개방 시스템 상호접속 -등록부 표준(1993) ; 인증 골격(개정)	TTA
		OPEN SYSTEMS INTERCONNECTION - SECURITY FRAMEWORK IN OPEN SYSTEMS - PART 4 : NON-REPUDIATION	ISO/IEC	1999	제정	개방 시스템 상호접속 -개방시스템에서의 보안 골격 - 제4부 : 부인 방지	TTA
	증명 및 접속 제어 기술	Canonical XML Version 1.0	W3C	2004	제정	정규 XML 버전 1.0	TTA
		XML-Signature Syntax and Processing	W3C	2004	제정	확장성 생성 언어 전자서명 구문과 처리	TTA
		Diameter Base Protocol for Authentication, Authorization and Accounting	IETF	2005	제정	인증과 권한 제어 및 과금용 다이아메터(Diameter) 베이스 프로토콜	TTA

〔참고문헌〕

〔1〕 FIPS PUB 140-2 Security Requirements for Cryptographic Modules

〔2〕 FIPS PUB 180-1 Securie Hash Standard

〔3〕 FIPS PUB 197? Advanced Encryption Standard

〔4〕 FIPS PUB 46-3 Data Encryption Standard

〔5〕 RFC 1321 The MD5 Message Digest Algorithm

〔6〕 PKCS #11 Cryptographic Token Interface Standard

〔7〕 RFC 2119

〔8〕 Trusted Computing Group(TCG) Design Philosophies and Concepts Version 1.0

〔9〕 Trusted Computing Group(TCG) Main Specification Version 1.1b, http://www.trustedcomputinggroup.org/, February 2002 (also known as Trusted Computing Platform Alliance(TCPA) Main Specification Version 1.1b)

〔10〕 TCG Software Stack(TSS) Specification Version 1.0

〔11〕 Trusted Mobile Platform Security Requirements

〔12〕 Trusted Mobile Platform Hardware Architecture Description

〔13〕 Trusted Mobile Platform Protocol Specification Documents

〔14〕 Provosioning Bootstrap 1.1? Open Mobile Alliance

〔15〕 ANSI X9.63

〔16〕 Common Criteria Part : Security functional requirements, Aug 1999, Ver.2.1

〔17〕 Schneier, Bruce : Applied Cryptographic, Second Edition, John Wiley & Sons, 1996, "Section 22.1 Diffie-Hellman

〔18〕 Schneier, Bruce : Applied Cryptographic, Second Edition, John Wiley & Sons, 1996, "Section 20.1 Digital Signature Algorithms"

〔19〕 3GPP TS 31.101 : " UICC-Terminal Interface; Physical and Logical Characteristics".

〔20〕 3GPP TS 31.102 : "Characteristics of USIM Application".

〔21〕 3GPP TS 33.102 : "3G Security; Security architecture".

〔22〕 3GPP TS 11.11 : "Specification of the Subscriber Identity Module - Mobile Equipment Interface".

〔23〕 3GPP TS 51.0 11 : "Specification of the Subscriber Identity Module - Mobile Equipment Interfaces".

〔24〕 TS 03.20 : Digital Cellular telecommunications system (Phase 2+); Security related network functions?

〔25〕 TS 23.048 : Security mechanisms for the (U)SIM application toolkit ?

〔26〕 BioAPI Specification Version 1.1? March 16, 2001, The BioAPI Consortium, http://www.bioapi.org.

〔27〕 S. Prabhakar, S. Pankanti, A. Jain, Biometric Recognition : Security and Privacy Concerns? IEEE Security and Privacy, March/April 2003, pp33-42.

〔28〕 "Content Protection for Recordable Media Specification : SD Memory Book Common Part", Rev 0.96, Nov. 26, 2001. by Intel, Matsushita, and Toshiba

〔29〕 Trusted Mobile Platform Software Architecture Description

〔약어〕

ACL	Access Control List
AES	Advanced Encription Standard
AKA	Authentication and Key Agreement
API	Application Program Interface
B2B	Business to Buisiness
B2E	Business to Employee
BD	Biometric Devices
BIS	Boot Integrity Services
CA	Certificate Authority
CACS	Common Access Control Service
CAS	Conditional Access System
CBC	Cypher Blocking Chaining
CDMA	Code Division Multiple Access
CDSA	Common Data Security Architecture
COI	Content Object Identifier
CORBA	Common Object Request Broker Architecture
CP	Copy Protection
CRTM	Core Root of Trust Measurement
DAC	Discretionary Access Control
DCE	Distributed Computing Environment
DES	Data Encryption Standard
DH	Diffie-Hellman
DIR	Data Integrity Register
DMB	Digital Multimedia Broadcasting
DRM	Digital Rights Management
DSA	Digital Signature Algorithm
F/W	Firewall
GSM	Global System for Mobile Communications
HTTP	Hyper Text Transfer Protocol
HTML	Hyper Text Markup Language
IPS	Intrusion Prevention System
MAC	Mandatory Access Control
MIH	Media Independent Handoff

MPEG	Moving Picture Experts Group
OMA	Open Mobile Alliance
OpenSSL	Open Source version of cryptogrphic library
OSAP	Object Specification Authorization Protocol
OSGi	Open Service Gateway initiative
PEK	Platform Encryption Key
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PRNG	Pseudo Random Number Generator
RFID	Radio Frequency IDentification
SAML	Security Assertion Markup Language
SHA	Secure Hash Algorithm
SIM	Subscriber Identity Module
SMTP	Single Mail Transfer Protocol
SOAP	Simple Object Access Protocol
SSH	Secure Shell
SSL	Secure Sockets Layer
TBC	Trusted Boot Code
TBH	Trusted Boot Hardware
TCB	Trusted Code Base
TCG	Trusted Computing Group
TCPA	Trusted Computing Platform Alliance
TLS	Transport Layer Security
TMD	Trusted Mobile Device
TMP	Trusted Mobile Platform
TP	Trusted Platform
TPM	Trusted Platform Module
TUI	Trusted User Interface
UCI	Universal Content Identifier
USIM	Universal Subscriber Identity Module
UUID	Universal Unique Identifier
VM	Virtual Machine
WAP	Wireless Application Protocol
WIM	WAL Identity Module

WiBro	Wireless Broadband
WiMAX	World Interoperability for Microwave Access
WLAN	Wireless Local Area Network
WPAN	Wireless Private Access Network
XACML	Entensible Access Control Markup Language
XML	Extensible Markup Language

1. 본 분석자료는 정보통신부의 국책사업인 "정보통신표준화 계획 수립 및 대응전략 연구"의 일환으로 발간된 자료입니다.

2. 본 분석자료의 무단 복제를 금하며, 내용을 인용할 시에는 반드시 정보통신부 정보통신 연구개발사업의 연구결과임을 밝혀야 합니다.

○ 총괄책임자 : 진병문 (TTA 표준화본부장)
○ 사업책임자 : 손 홍 (TTA 전략기획팀장)
○ 전략기획팀 : 장종표, 진수경, 전철기, 박정환, 전덕중
박종봉, 강부미

IT839 전략 표준화로드맵 Ver.2007
종합보고서9

2006년도 12월 26일 인쇄
2006년도 12월 30일 발행

발 행 소 : 한국정보통신기술협회
발 행 인 : 김 홍 구
발간번호 : TTA-06091-SA
인 쇄 인 : 다강 (02-3461-5789)

한국정보통신기술협회
Telecommunications Technology Association

463-824, 경기도 성남시 분당구 서현동 267-2
Tel : 031-724-0062, Fax : 031-724-0109
http://www.tta.or.kr