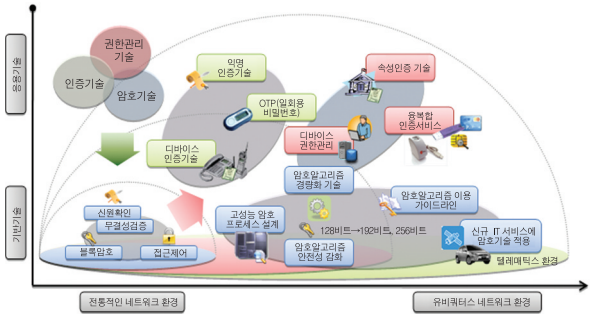
정보보호 분야

암호 / 인증 / 권한관리

■ 기술개요

• 인터넷상에서 유통되고 있는 다양한 정보에 대해 안전하고 신뢰성 있게 전송 및 이용하기 위한 기반 기술로, 안전한 정보의 송수신을 위한 프리미티브 기술인 암호 기술, 인터넷상에서 사용자의 신원확인 및 전송되는 정보에 대한 무결성 보장을 제공하는 인증기술, 인터넷상에서의 불법적인 정보 접근을 통제하기 위한 권한관리 기술로 구분

• 또한, 최근 급속한 인터넷 해킹 기술의 발전과 유비쿼터스 환경이 도래됨에 따라 사회적으로 요구되고 있는 안전성이 강화되고 경량화된 암호 · 인증 · 권한관리 기술을 포함

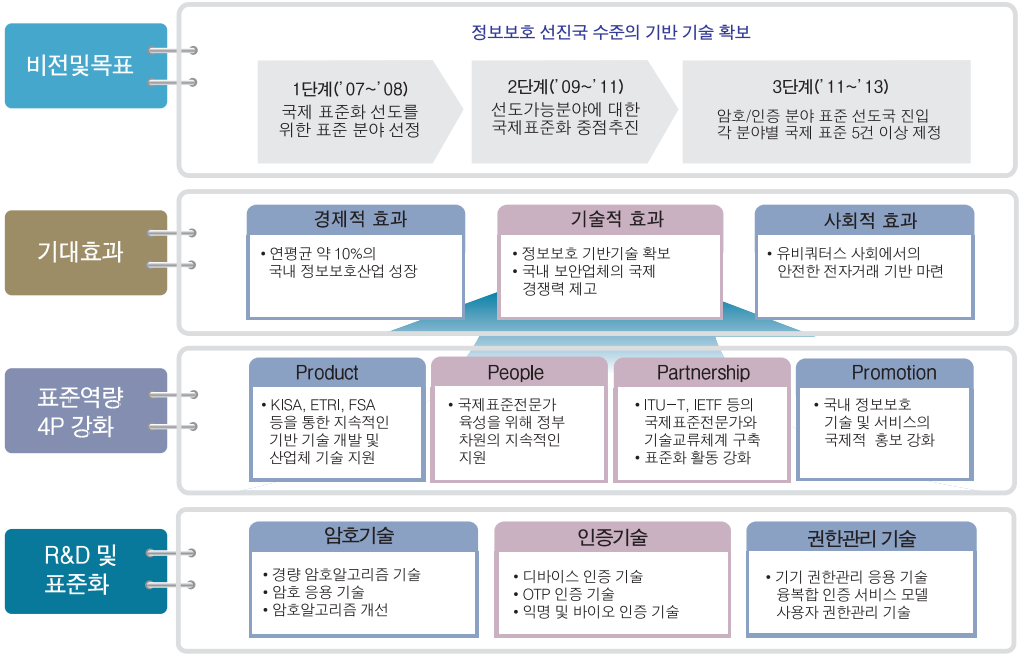


■ 표준화의 필요성

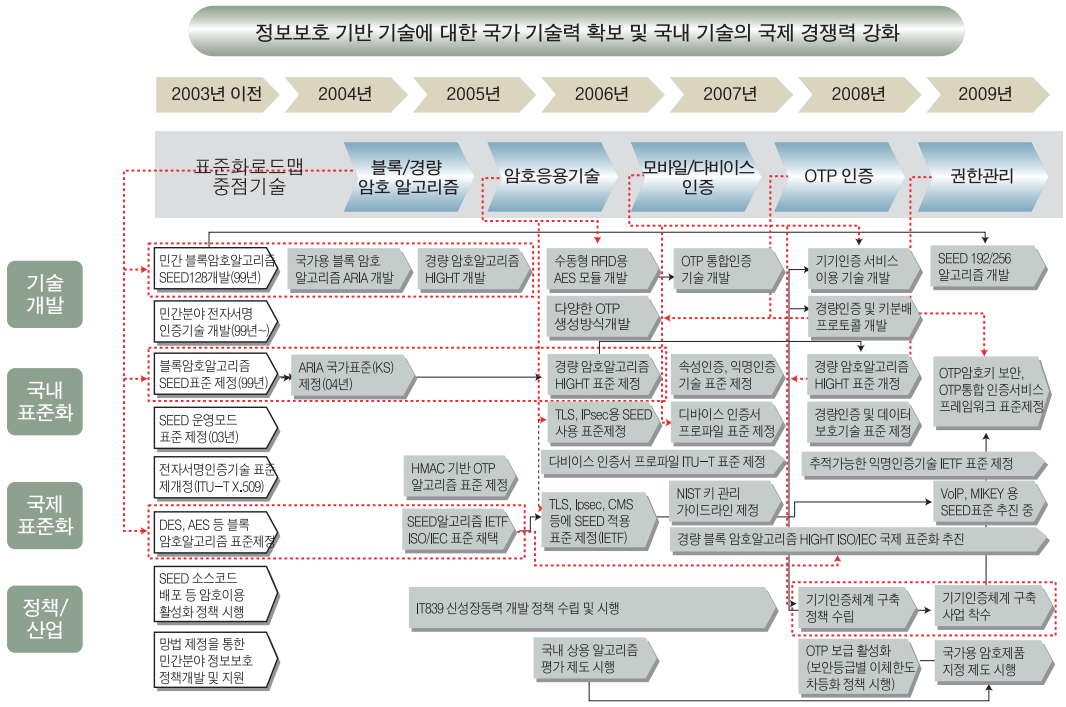
• 암호 · 인증 · 권한관리 분야는 인터넷상에서 안전한 정보의 전송 및 이용을 위해 반드시 필요한 정보보호 기반 기술로써 인프라 성격을 띠고 있기 때문에 정보보호 시스템의 상호호환성, 인터넷 이용자의 안전성 및 신뢰성 보장을 위해 해당 기반 기술에 대한 표준화 개발이 필요

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

■ 표준화의 비전 및 기대효과



■ 연도별 주요현황 및 이슈

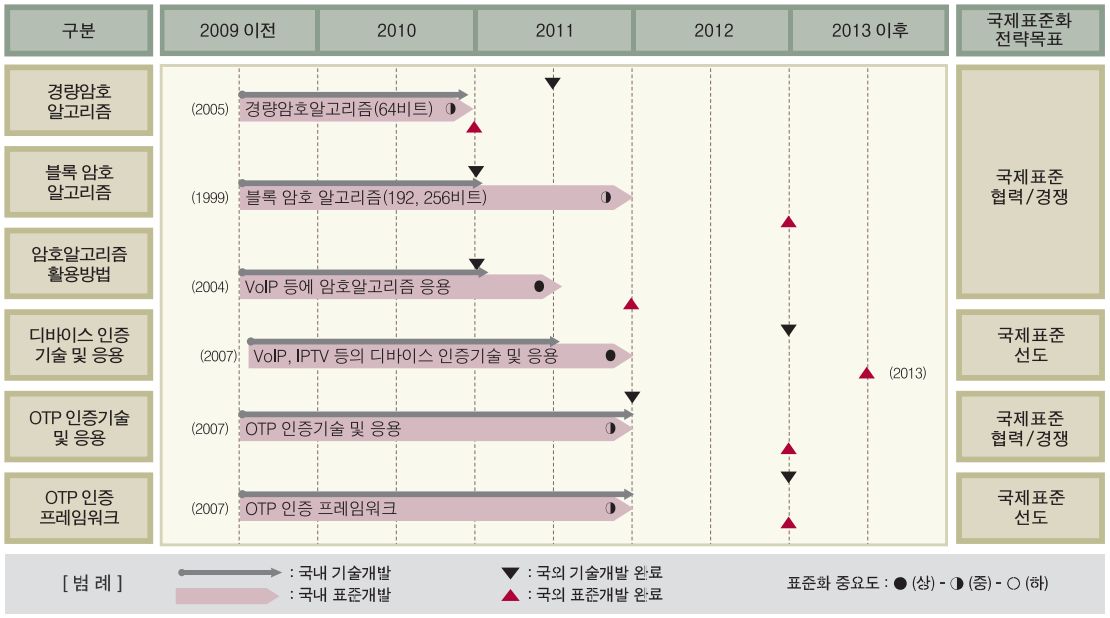


■ 표준화 대상항목

표준화 대상항목 (중점 표준화항목)		표준화 내용	대응 표준화기구	국내참여 기관/업체	표준화수준	
					국내	국제
암호	유비쿼터스 환경에 적합한 경량 암호알고리즘	유비쿼터스 환경 등에서 이용되는 다양한 디바이스에서 안전한 데이터 전송을 위해서는 해당 디바이스에 적합한 경량화된 암호알고리즘이 필요. 경량화 된 블록 암호알고리즘에 대한 키 생성 및 암 · 복호화 과정 정의 ※ 경량 블록 암호알고리즘 HIGHT 등이 국제 표준화 추진 중	IETF, ISO/IEC JTC1	KISA, ETRI, KIISC, TTA	최종 검토	최종 검토
	블록 암호알고리즘 기술	전자상거래, 금융, 무선 통신 등에서 전송되는 정보의 안전성 강화를 위해 개발된 암호 알고리즘에 대한 키 확장, 암복호화 과정, S-box 생성방법 및 테이블, 라운드 키 생성 과정 등을 정의 ※ 최적화된 범용 알고리즘인 ARIA, 192/256비트 블록 암호알고리즘 SEED 등의 블록암호알고리즘 포함			개발/ 검토	제/ 개정
	응용서비스에서의 암호 알고리즘 활용 방법	VoIP, IPTV 및 IPSec 등에서 음성 데이터의 암호화, 키 관리 및 네트워크 프로토콜 등에서의 암호 알고리즘의 활용 및 적용 방안 ※ SRTP 및 MIKEY 키관리 기술에서 SEED 알고리즘 활용 방법, IPTV 내의 멀티캐스트 기법에서 SEED 알고리즘 활용 방법, IPsec 프로토콜에서의 SEED 운영모드 사용 규격 등 연구 진행 중			개발/ 검토	최종 검토
	텔레메틱스 환경에서의 암호 키 관리 기술	텔레메틱스 기술은 자동차와 정보통신 등 이종산업간 융합적 특성을 지닌 기술로, 차량 내부와 외부 통신, 차량간 통신시스템에서 정보를 실시간으로 주고받는 기술로써, 원격정보 서비스 및 차량안전, 보안, 개인화된 정보서비스에서의 안전한 통신을 위한 키 관리 기술을 정의	IETF, ISO/IEC JTC1, ITU-T, 3GPP	KISA, ETRI, KIISC, 현대기아자동차, KT, LG텔레콤, SK텔레콤	기획	기획
	암호알고리즘 이용 가이드라인	전자서명, 암 · 복호화, 메시지 인증 코드 등 다양한 암호학적 응용분야를 세분화하고 각 응용분야에서 암호 알고리즘을 안전하게 사용하기 위한 요구사항들을 정의	IETF, ISO/IEC, ITU-T	KISA, ETRI, KIISC, TTA, 방송통신위원회	개발 검토	개발 검토
	고성능 암호프로세서 설계 기술	암호알고리즘은 다량의 연산처리 등으로 인해 SW적인 수행의 경우 속도 문제가 발생하므로 고속으로 다량의 데이터를 처리하는 차세대 네트워크 서비스에서 고속 암호처리를 지원하고 안전한 보안 서비스를 제공하기 위한 암호프로세서의 구현 요구사항을 정의	TCG, ITU-T	ETRI, 삼성전자, 보안업체 등	–	기획
인증	USIM 등 모바일 환경에서의 인증서비스 모델 및 인증기술	USIM 칩이 탑재된 스마트폰, 3G폰 등의 보급 확대에 따라, 모바일 환경에서 인증서 기반의 다양한 인터넷 서비스 이용을 위한 USIM 기반의 인증서비스 이용 모델 및 관련 기술에 대해 정의	ETSI SCP, 3GPP, OMA	SKT, KT, KISA, TTA	기획	기획

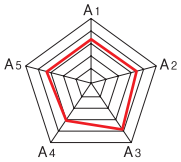
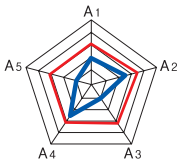
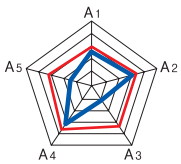
표준화 대상항목 (중점 표준화항목)		표준화 내용	대응 표준화기구	국내참여 기관/업체	표준화수준	
					국내	국제
인증	인터넷 전화 등에 이용 가능한 디바이스 인증 기술 및 응용	인터넷 전화기, CCTV, 휴대단말기, 지능형 가전 등 네트워크에 참여하는 디바이스에 대한 신뢰된 인증서비스를 제공하기 위한 기술로써, 디바이스 인증모델, 디바이스 인증서 프로파일, 인증서 관리 및 검증 기술, 전자서명키 보호기술 등 정의	ITU-T, IETF	KISA, TTA, 한국정보인증, 한국전자인증	개발/검토	개발/검토
	일회용패스워드(OTP) 인증 기술 및 응용	일회용 패스워드(OTP) 보안 서비스 제공을 위한 암호키 관리 및 정책 요구사항, 배포절차 및 요구사항, 인증 보증레벨 등 OTP 인증기술과 응용에 대해 정의 ※ 일회용 패스워드(OTP) 암호키 관리보안 요구사항, 일회용 패스워드(OTP)키 컨테이너, 일회용패스워드(OTP)인증서비스를 위한 보증레벨과 응용 가이드라인 등에 대해 연구 진행 중	ITU-T, IETF	금융보안연구원	개발/검토	최종검토
	일회용패스워드(OTP) 인증 프레임워크	OTP 인증 기본 모델, 통합인증 모델, 대체인증서버가 있는 통합인증 모델, 센터간 통합인증 모델 등 총 4개의 인증 서비스 모델을 포함하는 OTP 인증서비스 프레임워크를 정의하고, 서비스 요구사항, 기본 업무, 보안 고려 사항 및 참고사항을 정의	ITU-T	금융보안연구원	개발/검토	개발/검토
	익명성을 보장하는 인증 기술	웹사이트 가입, 성인인증 등 개인의 실명이 필요 없는 곳에서 프라이버시 보장을 위해 가명 또는 익명을 사용할 수 있도록 보장하면서 익명성 남용을 방지하기 위한 기술로서 익명인증체계, 익명인증서 프로파일, 익명인증 프로토콜, 익명인증서 검증기술, 익명에 대한 추적기술 등으로 분류	ITU-T, IETF	KISA, TTA, 한국정보인증	제/개정	개발/검토
	바이오정보를 이용한 전자서명 기술	기존 공개키 기반의 전자서명 기술에서의 단점을 보완하기 위해 지문, 홍채 등 바이오정보를 포함한 전자서명 인증 기술 및 이용 효율성 제고를 위한 융합 기술 등 정의	ITU-T, IETF	KISA, ETRI	기획	기획
권한관리	기기 관리자 간의 권한 관리 응용 기술	센서, 무선 네트워크 장치, 기능형 가전, CCTV 등 다양한 디바이스에 대한 인증 서비스의 필요성이 대두. 따라서 디바이스를 관리하는 기기 관리자나 기기 소유자의 디바이스에 대한 권한관리 모델 및 시나리오, 기기 식별체계 등을 개발	OMA, ITU-TS, CableLabs, ISO, IET	KISA, ETRI, Samsung	기획	기획
	융복합 인증 서비스 모델	다양한 IC카드의 사용, USIM 카드, 신용카드 등이 복합적으로 활용되므로 이에 대한 융복합 인증 서비스 모델 및 시나리오 개발이 필요	IETF, ITU, IEEE	KISA, TTA	기획	기획
	사용자 권한관리를 위한 인증 기술 및 응용	속성인증서 프로파일, 속성인증서 관리프로토콜, 속성인증서 운용 프로토콜, 속성인증서 검증프로토콜, 사용자 인터페이스 기술 등 속성인증서를 이용하여 사용자에 대한 권한을 관리하기 위한 기술	IETF, ITU-T	KISA, TTA	개발/검토	개발/검토

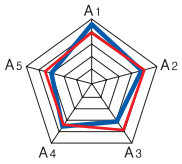
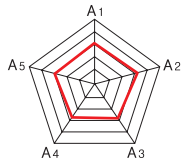
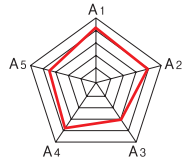
■ 중점 표준화항목별 중기(3개년) 표준화로드맵



■ 중점 표준화항목별 세부전략(안)

* A1: 국외대비 국내 표준화 수준, A2: 국외대비 국내 기술개발 수준, A3: IPR 확보 가능성, A4: 국내 표준화 인프라 수준, A5: 국제표준화 기여도　　* 파란색: Ver.2009, 빨간색: Ver.2010

중점 표준화항목	세부전략(안)
유비쿼터스 환경에 적합한 경량 암호알고리즘	*** 국제표준화 전략목표 : 국제표준 협력/경쟁(Ver.2010)**
	• 국외대비 국내표준화수준 분석에 따른 전략: 유 • 무선의 고전 암호알고리즘에 대한 기술 개발은 이미 국내외 적으로 표준화 추진이 완료되었기 때문에, RFID/USN, IPTV 등에 활용 가능한 경량화된 암호 알고리즘에 대해 국내 표준화 선행 추진 후 이를 기반으로 ISO/IEC, IETF 등에서 국제 표준화 추진 • 국외대비 국내기술개발수준 분석에 따른 전략: 2000년 초기부터 기술개발이 다양하게 이루어져왔고, 최근에는 경량화된 암호 기술 등 유비쿼터스 환경에 필요한 암호기술에 대한 연구가 진행되고 있기 때문에 관련 산업계에서 국내외 표준화의 중요성을 인지하고 관련 기술에 대한 표준화 활동을 강화할 수 있는 기반 마련 필요 • IPR확보가능성 분석에 따른 전략: 국내에서 경량 암호알고리즘에 대한 자체 특허는 이미 존재하므로, 국내 IPR 확보가 어려울 것으로 판단됨. 반면, 국외에서 경량화 암호알고리즘에 대한 관심이 높으므로 국외 IPR 확보를 고려해볼 필요가 있음 • 국내표준화인프라수준 분석에 따른 전략: 암호기술과 관련된 표준화의 경우 TTA, KSIC 등에서 지속적으로 추진되고 있기 때문에 국내 표준화 인프라는 좋은 편이며, 이를 기반으로 국제 경쟁력 있는 표준화 인프라 구축 노력에 주력 • 국제표준화기여도 분석에 따른 전략: ISO/IEC, IETF 등에서 다양한 암호기술에 대한 표준화 추진이 활발히 진행되고 있기 때문에 국내 전문가들이 해당 표준화 기구에 적극적으로 참여하여 국내 기술에 대한 국제 표준화 채택에 기여 필요
선행표준	IPR확보가능분야 : 안전한 시스템 구축을 위한 각종 상용화를 위한 요소기술에서 IPR 확보가 가능함
블록 암호알고리즘 기술	*** 국제표준화 전략목표 : 국제표준 수용/적용(Ver.2009) → 국제표준 협력/경쟁(Ver.2010)**
	• 국외대비 국내표준화수준 분석에 따른 전략: 미국, 유럽, 일본 등 국외에서 AES, Blowfish, Camellia 등을 개발하여 ISO/IEC, IETF 등 다양한 분야에 표준화를 추진하고 있지만 국내에서도 자체 개발한 블록 알고리즘에 대한 국내외 표준화 추진 경험이 있기 때문에 해당 경험을 기반으로 안전성이 강화된 암호 알고리즘에 대한 표준안을 국내외 동시에 추진 • 국외대비 국내기술개발수준 분석에 따른 전략: 블록 암호 알고리즘의 경우 1990년대 말부터 기술개발이 다양하게 이루어져왔고, 최근에는 RFID/USN 등과 같이 특정 환경을 고려한 암호 알고리즘에 대한 연구가 활발히 이루어지고 있으나, 이러한 암호 알고리즘은 특정 환경 이외에서는 적합하지 않을 수도 있음. 이에 특정 환경에 적합한 암호 알고리즘 개발 이외에 웹 서비스, 보안 장비 등에서도 활용 될 수 있는 암호 알고리즘을 개발하고 이에 대한 국내 및 국제 표준화 추진 • IPR확보가능성 분석에 따른 전략: 국내에 암호 알고리즘 자체에 대한 특허는 이미 존재하므로, 국내 IPR 확보가 어려울 것으로 판단됨. 반면, 다양한 해킹 공격에 대응하기 위한 안전성이 강화된 블록 암호 알고리즘에 대한 제한적 IPR 발굴 노력 필요 • 국내표준화인프라수준 분석에 따른 전략: 암호기술과 관련된 표준화의 경우 TTA, KSIC 등에서 지속적으로 추진되고 있기 때문에 국내 표준화 인프라는 좋은 편임. 따라서, 해당 인프라를 활용하여 실효성 있는 국내 표준 개발을 통해 국제 경쟁력 있는 표준화 인프라 구축 노력에 주력 • 국제표준화기여도 분석에 따른 전략: ISO/IEC, IETF 등에서 다양한 암호기술에 대한 표준화 추진이 활발히 진행되고 있기 때문에 국내 전문가들이 해당 표준화 기구에 적극적으로 참여하여 국내 기술에 대한 국제 표준화 채택에 기여 필요
후행표준	IPR확보가능분야 : 안전한 시스템 구축을 위한 각종 상용화를 위한 요소기술에서 IPR 확보가 가능함
응용서비스에서의 암호 알고리즘 활용 방법	*** 국제표준화 전략목표 : 국제표준 협력/경쟁(Ver.2009) → 국제표준 협력/경쟁(Ver.2010)**
	• 국외대비 국내표준화수준 분석에 따른 전략: 블록 암호 알고리즘 등과 같은 고전적 암호기술은 이미 국내외 적으로 표준화 추진이 완료되었기 때문에, IPTV, VoIP 등에 활용되는 암호응용기술에 대해 국제 경쟁력 있는 표준안을 TTA에서 선행 개발하고 이를 기반으로 IETF, ISO/IEC, IEEE 등에서 국제 표준화 선도 • 국외대비 국내기술개발수준 분석에 따른 전략: 암호응용기술의 경우 2000년 초기부터 기술개발이 다양하게 이루어져왔고, 최근에는 IP 기반 VoIP, IPTV 등 신규 IT 응용 서비스들에 대한 연구가 진행되고 있기 때문에 관련 산업계에서 국내외 표준화의 중요성을 인지하고 관련 기술에 대한 표준화 활동을 강화할 수 있는 기반 마련 필요 • IPR확보가능성 분석에 따른 전략: 국내에서 개발한 암호 알고리즘과 관련된 기술 및 서비스 특허가 많이 존재하고 있어 국내 IPR 확보가 어려울 것으로 판단됨. 다만, 다양한 IT서비스들이 계속적으로 개발?적용되고 있기 때문에 해당 서비스에 제한적인 IPR 발굴 노력 필요 • 국내표준화인프라수준 분석에 따른 전략: 암호 알고리즘 및 응용 기술과 관련된 표준화의 경우 TTA, KSIC 등에서 지속적으로 추진되고 있기 때문에 국내 표준화 인프라는 좋은 편임. 따라서, 해당 인프라를 활용하여 실효성 있는 국내 표준 개발을 통해 국제 경쟁력 있는 표준화 인프라 구축 노력에 주력 • 국제표준화기여도 분석에 따른 전략: ISO/IEC, IETF 등에서 다양한 응용 서비스에서 적용 가능한 암호 알고리즘에 대한 표준화 추진이 활발히 진행되고 있기 때문에 국내 전문가들이 해당 표준화 기구에 적극적으로 참여하여 국내 기술에 대한 국제 표준화 채택에 기여 필요
동시표준	IPR확보가능분야 : 안전한 시스템 구축을 위한 각종 상용화를 위한 요소기술에서 IPR 확보가 가능함

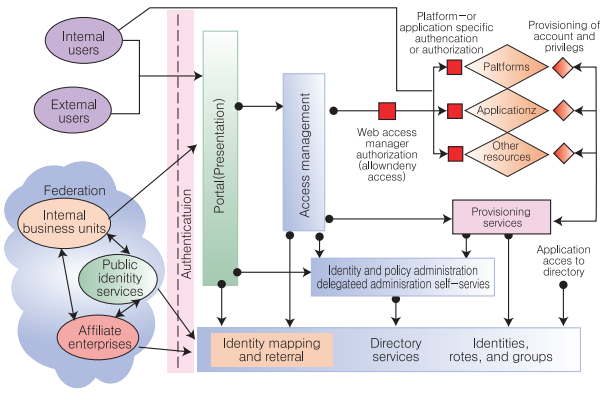
중점 표준화항목	세부전략(안)
인터넷 전화 등에 이용 가능한 디바이스 인증 기술 및 응용	* 국제표준화 전략목표 : 국제표준 선도(Ver.2009) → 국제표준 선도(Ver.2010)
	• 국외대비 국내표준화수준 분석에 따른 전략: ITU-T, IETF, TTA 등 국내외 표준화 단체에서 홈 네트워크 기반의 디바이스 인증서 프로파일 표준이 국내 전문가 주도로 개발되는 등 디바이스 인증 분야 표준화 개발이 활발히 진행됨에 따라, 향후 다양한 분야의 디바이스 인증기술에 대해 지속적인 국제 표준화 추진 • 국외대비 국내기술개발수준 분석에 따른 전략: 국내에서 u-시티 구축 사업 등 정부 및 산업체 주도로 다양한 디바이스를 활용한 사업이 추진 중에 있음. 이에 따라, 산업계 전문가와 공동으로 유비쿼터스 환경에 적합한 디바이스 인증 기술을 개발하고, 해당 기술에 대한 국내 및 국제 표준화 병행 추진 • IPR확보가능성 분석에 따른 전략: 홈네트워크 및 디바이스에서의 인증 방법에 대해서는 국내 특허가 출원되어져 있긴 하지만 그 외 신규 디바이스들에 대한 인증 기술에 대한 특허는 출원이 가능할 것으로 판단됨. 이에 따라, 신규 IT 서비스에 적용될 수 있는 디바이스 인증기술 표준화 추진 시 IPR 확보 가능성 확인 후 병행 추진 • 국내표준화인프라수준 분석에 따른 전략: 디바이스 인증 관련 국내 기술 개발은 ETRI, KISA, LG CNS 등 연구소 및 산업계에서 활발히 진행되고 있으며 관련 기술은 TTA를 통해 국내 표준화로 추진하고 있기 때문에 현재와 같은 선순환 구조를 유지하여 국내 및 국제 표준화 활성화 추진 • 국제표준화기여도 분석에 따른 전략: 국제적으로도 ITU-T, ISO, IETF 등 다양한 표준화 기구에서 디바이스 인증에 많은 관심을 가지고 있고, 국내 디바이스 인증 기술이 다른 국가에 비해 뒤떨어지지 않기 때문에 디바이스 인증 분야에 국내 전문가가 지속적으로 참가한다면 표준화 선도도 가능할 것으로 판단됨
동시표준	IPR 확보가능분야 : 다양한 IT기기에 대한 인증 기술 및 관련 프로토콜 , 인증서 발급/검증 기술 및 활용 서비스 등
일회용패스워드(OTP) 인증 기술 및 응용	* 국제표준화 전략목표 : 국제표준 협력/경쟁(Ver.2010)
	• 국외대비 국내표준화수준 분석에 따른 전략: OTP 인증 기술 및 응용과 관련한 분야의 표준화는 IETF를 통해 OTP 기본 인증기술 들이 표준화되어 있으며, 기존의 TLS, Kerberos 등의 인증 프로토콜과 응용하는 방안도 이미 표준화 추진됨. 국내 TTA에서는 2008년부터 OTP와 관련한 암호키 관리, 키 배포 파일, 인증 프레임워크 등이 표준화 추진 중에 있음. OTP 인증기술의 상호연동 및 보안성 강화를 위한 표준 기술들은 여전히 개발 중이며, 특히 OTP 응용과 관련한 표준기술에 대한 표준안의 개발 노력이 활발히 요구됨. • 국외대비 국내기술개발수준 분석에 따른 전략: OTP 기기 및 인증 기술의 개발은 국내외적으로 상당한 완성도를 가지고 있으며, 많은 분야에서 이미 사용 중임. 해외의 제품은 대부분 상호연동을 고려하지 않고 해당 도메인에서만 사용되는 방식으로 구현되어 있으나, 국내의 경우 금융분야에서 OTP 통합인증센터를 통해 OTP 상호인증이 제공되고 있음. 국내의 OTP 상호인증 기술의 우월성을 기반으로 한 표준안 개발 및 모바일 OTP 등의 최신 응용기술에 대한 표준기술 개발 필요 • IPR확보가능성 분석에 따른 전략: 금융분야의 활발한 이용으로 인해 국내 IPR 현황은 약 50여건의 관련된 특허가 출원되어 있으며, 현재도 꾸준하게 관련 특허 출원이 진행되고 있음. 표준기술을 기반으로 하는 국내 특허의 개발 및 확보도 가능할 것으로 전망되며, 표준화를 통해 실효성 있는 IPR의 추진을 가능하도록 함 • 국내표준화인프라수준 분석에 따른 전략: OTP와 관련한 국내 금융분야의 인프라는 전 세계적으로 매우 우수한 상황이며, 2009년 6월 기준으로 약 300만의 사용자가 OTP를 사용 중에 있음. 또한, 최근 국내 표준화에 대한 인프라도 금융보안연구소 등 금융권 분야를 중심으로 확대되고 있기 때문에, 국내의 선진 기술 및 인프라를 활용한 표준 개발을 통해 국제 경쟁력 확보도 가능 • 국제표준화기여도 분석에 따른 전략: 현재 ITU-T 등 국제 표준화 기구를 통해 OTP 관련 인증 기술에 대한 표준화를 추진하고 있기 때문에, 이를 기반으로 현재 국내 OTP 업체 및 관련 기관의 협조 및 지원을 받아 중장기적으로 OTP 인증기술에 대한 표준화 주도권 확보 가능
동시표준	IPR 확보가능분야 : 유비쿼터스 환경에 접목한 OTP 응용 기술 등
일회용패스워드(OTP) 인증 프레임워크	* 국제표준화 전략목표 : 국제표준 선도(Ver.2010)
	• 국외대비 국내표준화수준 분석에 따른 전략: 국제적으로 OTP 생성 알고리즘, 응용 보안 프로토콜, 키 프로비저닝 프로토콜 등의 표준화가 이미 IETF에서 추진 중이지만, 관련 인프라를 구축하고 서비스를 제공 및 관리하는 프레임워크가 존재하지 않음. 따라서 본 중점 표준화 항목과 기존의 표준화된 분야의 차이점을 부각시켜 해당 분야에 대한 국제 표준화 선도가 가능하도록 추진 • 국외대비 국내기술개발수준 분석에 따른 전략: 최근 행안부 등 공공기관, 인터넷 게임 사이트에서 사용자 편의성 제공을 위한 OTP 인증 서비스 관리 및 연동기술 개발 요구가 있기 때문에, 해당 기술 개발에 대한 노하우를 기반으로 OTP 인증에 대한 전반적인 프레임워크 기술을 개발한다면 국내 뿐아니라 국제 표준화 선도 가능 • IPR확보가능성 분석에 따른 전략: 2008년 일회용 패스워드 인증 프레임워크에 대한 특허 출원상태이며 국제 특허 분야에 대한 가능성 확인 후 추진 필요 • 국내표준화인프라수준 분석에 따른 전략: OTP에 관련한 주요 메커니즘의 표준화 인프라는 국외에 비해 뒤쳐진 것으로 판단되지만, 모바일 기기와 OTP의 결합과 같은 융합 환경에서의 응용서비스 기술에 대한 표준화는 국내가 앞서기 때문에 지속적인 관심과 표준화 참여가 이루어진다면 향후 국제 표준화에도 선도적인 역할이 가능할 것으로 판단됨 • 국제표준화기여도 분석에 따른 전략: PKI기반 공인인증서, 바이오인증 등의 멀티팩터 형태로 사용되는 강한 인증 방식들에 대한 개별 관리 프레임워크 표준화가 ITU-T, IETF등에서 제정 및 추진 상태이기 때문에 해당 국제 표준화 인프라를 기반으로 OTP 인증 프레임워크 및 멀티팩터 인증프레임워크들간 연동 및 관리에 대한 국제 표준화 적극 추진
동시표준	IPR 확보가능분야 : 일회용패스워드 통합 인증 프레임워크 등

ID관리 / 개인정보보호

■ 기술개요

• ID관리 기술은 인증정보를 비롯한 개인의 특징, 신상정보, 선호도와 같은 ID의 생성부터, 변경, 유통, 폐기 등에 대한 라이프 사이클을 인터넷 및 통신망 환경에서 안전하고 통합적으로 관리하는 기술이며, 개인정보보호 기술은 사용자의 개인정보를 보호하기 위한 기술 및 정책

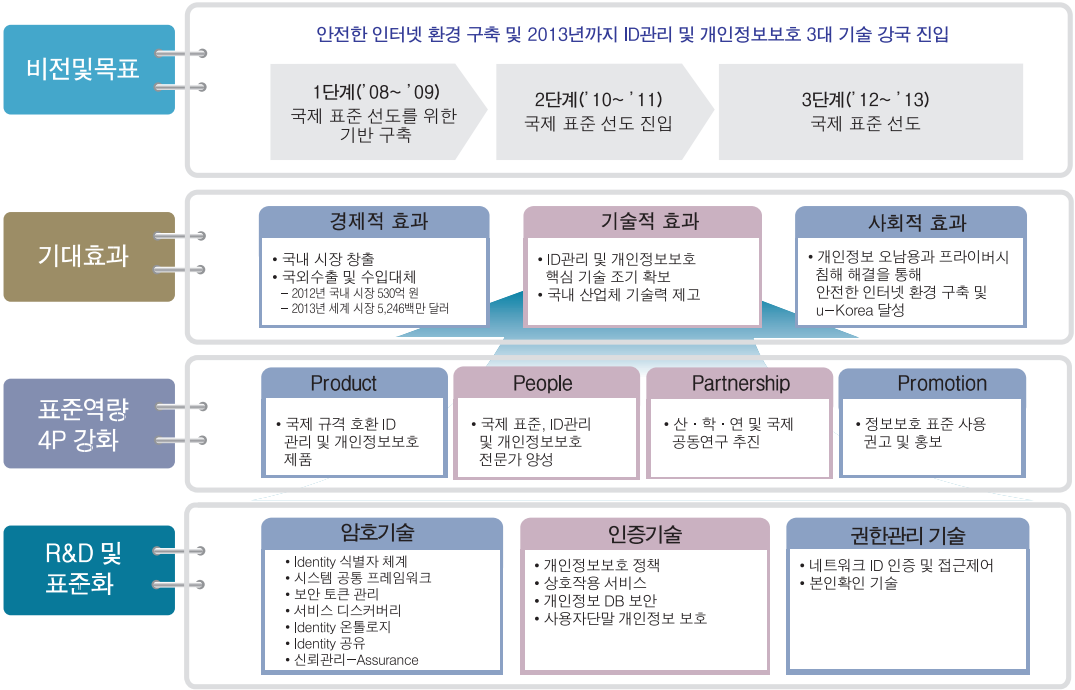
• 사용자의 편의성과 안전성, 개인정보보호 수준을 높이고 사업자의 관리비용 감소와 시스템 보호 및 조직 간 서비스 연계 등을 지원하는 기술이며, 차세대 웹 환경을 위한 필수 정보보호 기술 및 IP 기반의 통합망인 NGN/BcN의 상용화와 클라우드 컴퓨팅의 활성화를 위해서도 역시 필수적인 기술



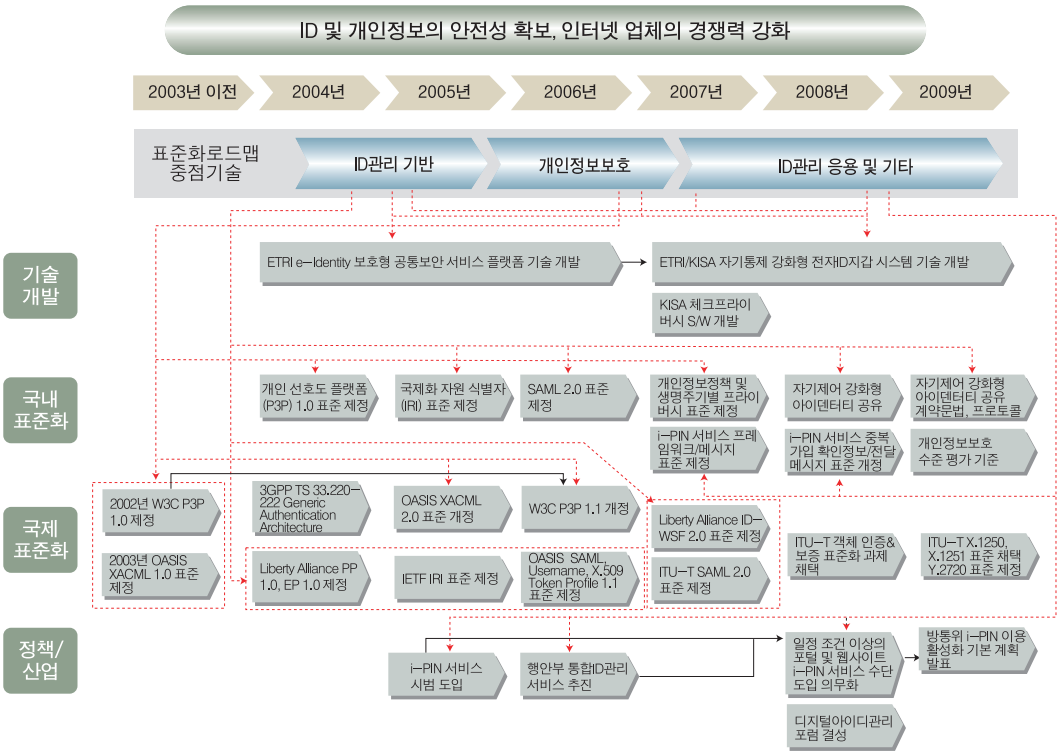
■ 표준화의 필요성

• 인터넷 활용이 커져가면서 ID관리의 불편함과 개인정보 오·남용으로 인한 피해가 증가하고 있으며, NGN/BcN 통신망에 인터넷 기술의 특성을 추가하고 있어 사용자가 임의의 접속점을 통해 망에 접속하는 것이 가능하여, 사용자 로그인 및 인증절차가 요구되며, 관련 ID들을 적절하고 안전하게 관리하는 표준화된 방법을 정의하는 것이 NGN/BcN의 상용화 도입을 위해 필수적임

■ 표준화의 비전 및 기대효과



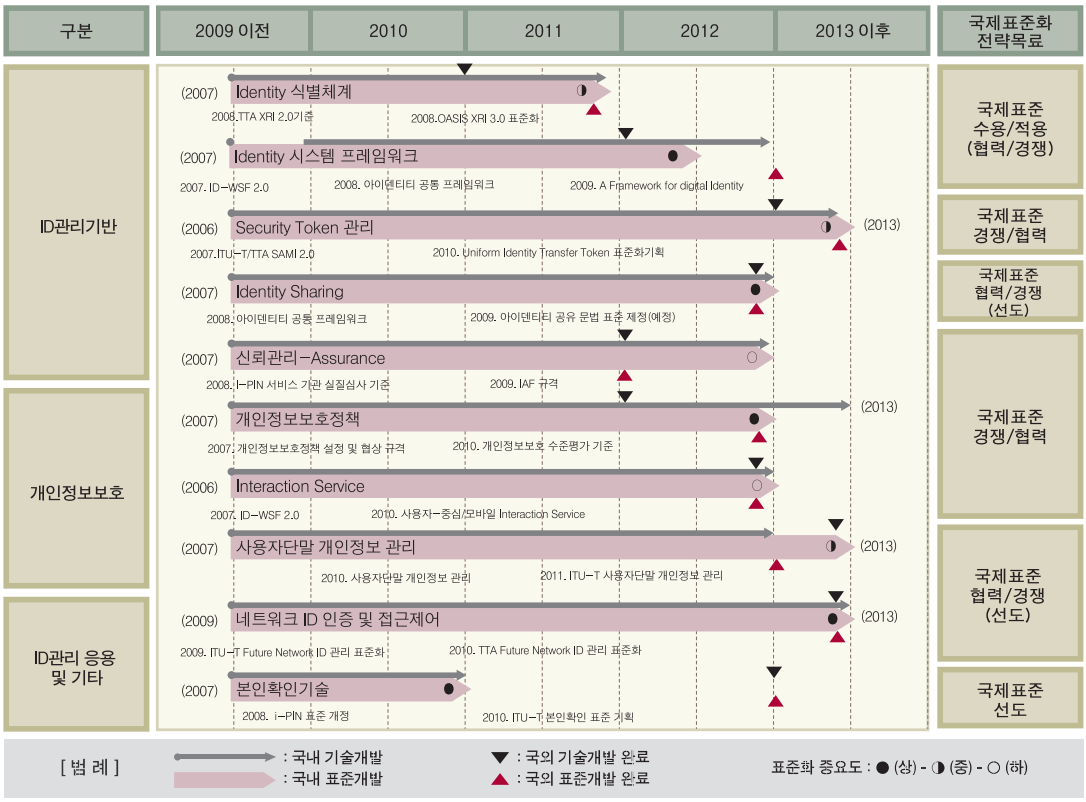
■ 연도별 주요현황 및 이슈



■ 표준화 대상항목

표준화 대상항목 (중점 표준화항목)		표준화 내용	대응 표준화기구	국내참여 기관/업체	표준화수준	
					국내	국외
ID 관리 기반	Identity 식별자 체계	멀티도메인에서 식별 가능한 식별자의 정의 및 생성?관리 규격	ITU-T SG17, OASIS, Liberty Alliance	TTA, ETRI, KISA 등	개발검토	제/개정
	Identity 시스템 공통 프레임워크	유무선 환경에서 ID 생성, 저장, 유통, 관리 서비스를 위한 공통 프레임워크 규격			항목승인	최종검토
	Security Token 관리	인증, 권한 및 속성, 익명 정보를 포함한 보안토큰의 생성 및 검증 규격			개발검토	최종검토
	Identity 서비스 디스커버리	ID 서비스 발견 메커니즘과 메타데이터의 질의 및 응답 프로토콜 규격			기획	제/개정
	Identity Ontology	시스템 간 자동화된 정보의 교환과 이용이 가능하도록 정의된 ID의 개념과 관계			기획	개발검토
	Identity Sharing	ID 정보 공유를 위한 메시지 형식과 프로토콜 규격			개발검토	최종검토
	신뢰관리-Assurance	통신 당사자 간의 협상을 통한 신뢰구축 메커니즘, 보안토큰 메시지 및 전송 규격, 보안 토큰의 보증 수준 및 서비스 및 크리덴셜 평가 기준			개발검토	최종검토
개인 정보보호	개인정보보호 정책	개인정보 획득에 따른 의무와 이용범위 등에 대한 정책 생성, 공개, 검토를 위한 형식	ISO, OASIS, Liberty Alliance	ETRI, TTA, KISA	개발검토	최종검토
	Interaction Service	개인정보 이용과 제공을 위해 사용자 또는 대리인의 동의를 받기 위한 상호작용 서비스 프로파일			항목 승인	개발검토
	개인정보 DB 보안	개인정보의 최종 저장소인 데이터베이스에 대한 사전 접근통제, 데이터 암호화, 감사 등의 다양한 보안기술			기획	기획
	사용자단말 개인정보 관리	사용자 단말에서 입력되는 다양한 정보 보호 기술, 저장되는 정보에 대한 보호 기술 그리고 정보를 안전하게 표시하는 기술 및 규격			기획	기획
ID관리 응용 및 기타	네트워크 ID 인증 및 접근제어	안전한 네트워크 서비스를 위해 네트워크 접속자의 Identity를 바탕으로 인증하고 접근 제어하는 기술	ITU-T, OASIS, Liberty Alliance, GSI/SG3/SG11, 3GPP, ETSI	TTA, ETRI, KISA, KT, Xener	기획	기획
	본인확인 기술	온라인 상에서 서비스 사용자가 실제 해당 사용자 본임임을 확인할 수 있도록 해 주는 기술			제/개정	항목승인

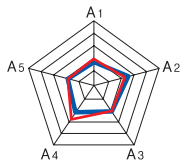
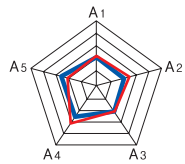
■ 중점 표준화항목별 중기(3개년) 표준화로드맵



■ 중점 표준화항목별 세부전략(안)

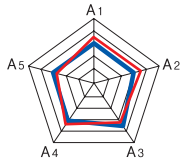
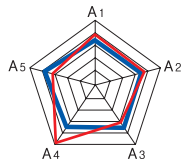
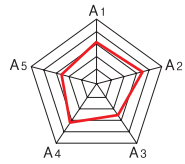
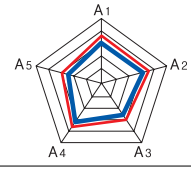
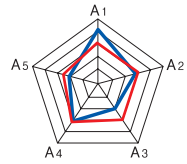
* A1: 국외대비 국내 표준화 수준, A2: 국외대비 국내 기술개발 수준, A3: IPR 확보 가능성, A4: 국내 표준화 인프라 수준, A5: 국제표준화 기여도

* 파란색: Ver.2009, 빨간색: Ver.2010

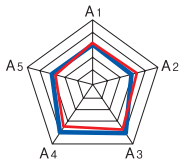
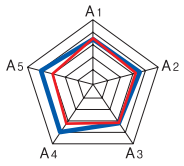
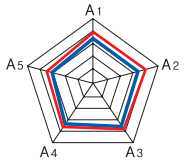
중점 표준화항목	세부전략(안)
Identity 식별자 체계	* **국제표준화 전략목표** : 국제표준 협력/경쟁(수용/적용)(Ver.2009) → 국제표준 수용/적용(협력/경쟁)(Ver.2010)
	• IETF 1738 URL(Uniform Resource Locators)과 IETF 3987 IRI (Internationalized Resource Identifiers) 표준 및 Identity 자원에 대한 추상화된 식별자인 OASIS의 XRI 2.0이 TTA에서 국내 표준으로 수용된 상태임 • URL, IRI 식별자는 인터넷의 근간을 이루며 인터넷 서비스에서 활용되고 있으며, XRI의 경우 이미 국내에서 OpenID 서비스에 사용하는 기술로 국내외 기술 격차가 없는 상태로, 식별자 기술은 모든 서비스의 기반 기술이기 때문에, 산업체에서 신뢰성 있고 신속한 제품과 서비스를 제공할 수 있도록, 국제 표준을 국내에 빠르게 수용하는 것이 필요 • 식별자 기술에 대한 IPR의 확보는 매우 미흡한 상태로, 국제적으로 통용될 수 있는 식별자 기술에 대한 국내 표준을 개발하고 산업계에서 적용 검증함으로써 IPR 확보하고 해당 표준을 국제 표준화하는 것이 필요 • 학계와 연구기관을 중심으로 표준을 개발하고 표준 개발과 동시에 IPR 항목을 도출하며, 표준 개발이 완료되면 산업계를 중심으로 표준에 대한 산업기술을 개발하여 표준의 적용성 및 응용성을 확보함
선행표준	* IPR확보가능분야 : –
Identity 시스템 공통 프레임워크	* **국제표준화 전략목표** : 국제표준 협력/경쟁(수용/적용)(Ver.2009) → 국제표준 수용/적용(협력/경쟁)(Ver.2010)
	• ITU-T SG17에서 2007년 ID관리 기술 Focus 그룹을 운용하여 ID관리 프레임워크 표준화에 대한 선행 작업을 수행 및 ISO SC27에서 ID관리 기술에 대한 프레임워크 표준화를 제정 및 Liberty Alliance에서 ID 프레임워크로 개발한 ID-WSF 2.0을 산업계 표준을 제정한 상태임 – 국내의 경우, ID관리 시스템들 간의 상호운용성을 제공하는 기틀을 마련하기 위해, ITU-T SG17 Q.6에서 진행하고 있는 'Global Interoperable Identity Management 기술' 표준을 수용하여 '공통 아이덴터티 데이터 모델'과 '상호호환성 및 신뢰를 위한 글로벌 ID관리 시스템 요구사항'에 대한 국내표준화를 완료하였음. Liberty Alliance의 ID-WSF와 ISO, ITU-T 표준화 진행을 참고하고 ID-WSF 개발 경험을 토대로 국내 환경에 적합한 ID관리 프레임워크 표준을 제정하는 것이 필요하며, ITU-T 표준화 작업에 적극적인 참여를 통해 국제 표준화를 주도하려는 노력이 필요함 • ID관리 프레임워크 기술에 대한 국내외 IPR은 거의 없는 상태로, 국제적으로 활용될 수 있는 프레임워크 기술에 대한 국내 표준을 개발하고 이를 국제 표준화함으로써 IPR을 확보하는 노력이 필요
선행표준	* IPR확보가능분야 : 시스템 프레임워크

* A1: 국외대비 국내 표준화 수준, A2: 국외대비 국내 기술개발 수준, A3: IPR 확보 가능성, A4: 국내 표준화 인프라 수준, A5: 국제표준화 기여도

* 파란색: Ver.2009, 빨간색: Ver.2010

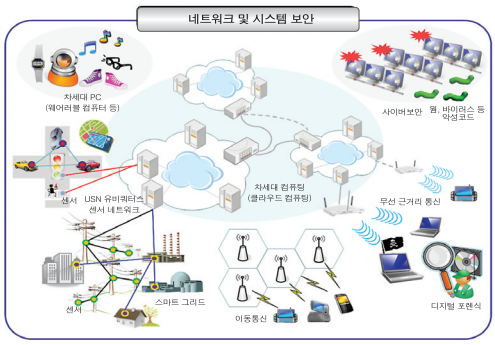
중점 표준화항목	세부전략(안)
Security Token 관리	* 표국제준화 전략목표 : 국제표준 협력/경쟁(Ver.2009) → 국제표준 협력/경쟁(Ver.2010)
	• OASIS에서는 X.509 Token, SAML Token, Kerberos Token 등에 대한 프로파일 표준을 제정, SAML 2.0 Metadata, SAML 2.0 Authentication Context와 SAML 2.0 Conformance Requirements와 Privacy Considerations 부분이 2007년 TTA 표준으로 제정된 상태로, 국내 표준화가 진전되었기 때문에, ITU-T 등과 같은 국제 표준화 단체에 국제 표준을 기고하려는 노력이 필요 • 다양한 ID관리 프레임워크에 공통적으로 사용될 수 있는 Uniform Identity Transfer Token과 서로 다른 Security Token을 해석하여 교환할 수 있는 Token Transformation 기술 및 표준을 개발하여 국제 표준화를 진행하는 것이 필요함 • 보안 토큰 분야에서는 ID관리의 다른 기술 분야에 비해 상대적으로 많은 IPR이 확보되어 있는 상태로 새로운 IPR 확보가 쉽지는 않은 상황임. 그러나 다양한 ID관리 프레임워크에 공통적으로 사용될 수 있는 Uniform Identity Transfer Token과 서로 다른 Security Token을 해석하여 교환할 수 있는 Token Transformation 기술을 개발하여 국제 표준화함으로써 IPR을 확보하는 것이 필요함
동시표준	* IPR확보가능분야 : –
Identity Sharing	* 국제표준화 전략목표 : 국제표준 협력/경쟁(선도)(Ver.2009) → 국제표준 협력/경쟁(선도)(Ver.2010)
	• ITU-T SG17에서 2007년 ID관리 기술 Focus 그룹을 운용하여 ID 공유 표준화에 대한 선행 작업을 수행하였으며, 현재 ITU-T SG17 Q.6에서 ID 공유 기능 요구사항 표준작업을 진행 중이며, ETRI는 X.idif라는 표준과제로 채택되었고 현재 ITU-T에서 표준화 작업을 진행하고 있으며 국내에서는 2008년 TTA에서 '자기 제어 강화형 디지털 아이덴터티 공유 프레임워크' 로 표준화가 완료되었음 – 산업체에서 개발된 주요 ID관리 시스템인 Microsoft CardSpace의 ID 교환 프로토콜, OpenID의 Attribute Exchange 프로토콜 특성을 고려하여 ID 공유 요구사항, 관련 프로토콜 표준을 개발하여 국제 표준을 선도하는 것이 필요함 • Identity Sharing 분야에 대한 IPR은 아직 많이 축적되지 않은 상태이므로 국제적으로 활용성이 높은 IPR 확보 가능성은 상대적으로 높은 편이므로 Identity Sharing 기술에 대한 국내 표준을 개발하고 국제표준으로 상정함으로써 IPR을 확보하는 것이 필요
동시표준	* IPR확보가능분야 : Infra ENUM 구현방법 및 요구사항
신뢰관리-Assurance	* 국제표준화 전략목표 : (신규) 국제표준 협력/경쟁(Ver.2010)
	• liberty Alliance, ITU-T SG17, ISO/IEC JTC/SC27등을 표준화 활동이 진행 중 • 전자서명 인증관리체계, i-PIN 서비스 등에서 해당 서비스를 제공하기 위한 기관 설립 조건, 신원확인 방법 등을 명시하는 기준은 있음. 또한, 이러한 기준에는 각 항목별 평가방법 등 세부적인 사항까지 포함되어 있음 • 국제 표준화 중인 보증 수준 관련 표준에 국내 기준의 일부를 반영하는 형태로 국제 표준화 추진이 가능하며, 국내 기준의 세부적인 평가 방법을 사례 형태로 함께 제시할 필요가 있음 • 전자서명인증관리체계, i-PIN 서비스 체계 만족 등과 같이 Assurance를 만족시키기 위한 국내 기술수준도 상당히 높은 편이기 때문에, 국내 기술 요소를 반영하여 국제 표준화를 추진하는 것이 필요함 • Assurance 등은 국가별로 정책적인 요인에 따라 결정되는 부분이 많기 때문에 Assurance 기술 자체에 대한 IPR 확보보다는 Assurance 기술을 위한 요소 기술들로부터 IPR을 확보하는 것이 필요
선행표준	* IPR확보가능분야 : –
개인정보보호 정책	* 국제표준화 전략목표 : 국제표준 협력/경쟁(Ver.2008) → 국제표준 협력/경쟁(Ver.2009)
	• W3C, OASIS XACML TC에서 표준화 활동이 진행 중이며, 국내 RFID 프라이버시보호 가이드라인을 기반으로 하여 RFID 응용에서의 개인정보보호를 위한 가이드라인(X.rfpg)의 ITU-T 표준화를 추진하는 것이 필요함 • ID관리 분야에서의 개인정보보호 수준에 대한 평가기준(X.priva) 등에 대한 지속적인 ITU-T 표준화 활동을 통해 개인정보보호 분야에서의 국제 표준과 협력/경쟁하는 것이 필요함 • 개인정보보호정책 표준 자체의 IPR이 아닌 표준에서 요구되는 개인정보보호기술을 추가적으로 개발하고 표준화하여 IPR을 확보하는 것이 필요함
선행표준	* IPR확보가능분야 : 신규식별체계
Interaction Service	* 국제표준화 전략목표 : 국제표준 협력/경쟁(Ver.2009) → 국제표준 협력/경쟁(Ver.2010)
	• Liberty Alliance에서 제정된 ID-WSF 2.0 스펙의 일부분으로서 Interaction Service가 제정되어 있는 반면 국내의 표준화 현황은 매우 미비한 상태로, 국내 산업계에서 기술 개발에 적극 활용할 수 있도록 국제 표준을 국내 환경에 맞게 수용하려는 노력이 필요함 • 사용자 중심 ID관리와 개인정보의 자기통제권 확보 등을 위한 새로운 지침 및 표준 개발이 요구됨에 따라 기존에 표준화되어 있지 않은 Interaction Service와 최근 급속히 성장하는 모바일 컴퓨팅 환경에 적합한 Interaction Service에 대한 국내 표준을 제정하여 이를 국제 표준화하려는 노력이 필요함 • 표준 기술의 실용적 적용을 위한 관련 기술 분야의 IPR을 확보하기 위한 좋은 시기로, 다양한 Interaction 단말 환경과의 Interaction Service 모델 개발과 비즈니스 모델 개발 등 분야에서 국제 표준화를 진행하여 IPR 확보하려는 노력이 필요
후행표준	* IPR확보가능분야 : Interaction 단말 환경, 모델개발, 비즈니스 모델 개발분야

* A1: 국외대비 국내 표준화 수준, A2: 국외대비 국내 기술개발 수준, A3: IPR 확보 가능성, A4: 국내 표준화 인프라 수준, A5: 국제표준화 기여도　　* 파란색: Ver.2009, 빨간색: Ver.2010

중점 표준화항목	세부전략(안)
사용자단말 개인정보 관리	*** 국제표준화 전략목표 : 국제표준 협력/경쟁(선도)(Ver.2009) → 국제표준 협력/경쟁(선도)(Ver.2010)**
	• 국내에서는 PKCS#11 프로파일 표준이, 국제적으로는 RSA의 de-factor 표준인 PKCS 시리즈 표준이 제정된 상태로, ETRI는 X.msec-5라는 신규 표준과제로 승인을 받아 현재 표준화가 진행중임 • 국내외적으로 아직 활발히 진행되고 있지 않은 분야이므로 국내에서 표준화 기술 항목 도출하고 이를 통해 국제 표준을 선도하는 것이 필요하며, 금융권과 공공분야에서의 필요성에 의하여 빠른 속도로 추격을 하고 있으며, 모바일 단말기의 개인정보 관리 기술은 국제적인 수준임 • 모바일 단말의 개인정보 관리 기술은 국제적인 경쟁력을 가지고 있기 때문에, 국내 표준화를 선행하고 이를 국제 표준화하려는 노력이 필요 • 사용자단말은 인터넷 보안의 최전방에 위치하는 기술이기 때문에 IPR의 확보시 그 파급력은 매우 클 것으로 예상됨. • 기존 산업체 선도기술의 장점을 반영하고 단점을 해결될 수 있는 방향으로 표준을 개발하고 기존 기술의 문제점을 해결할 수 있는 IPR 항목을 도출하며, 표준 진행과 동시에 산업체의 제품에 표준기술을 적용하여 표준의 적용성 및 응용성을 확보
후행표준	* IPR확보가능분야 : -
네트워크 ID 인증 및 접근제어	*** 국제표준화 전략목표 : 국제표준 협력/경쟁(선도)(Ver.2009) → 국제표준 협력/경쟁(선도)(Ver.2010)**
	• 2009년부터 개편된 ITU-T SG13은 mobile과 NGN을 포함하는 미래 네트워크 기술에 대한 표준을 담당하고 있으며, Q16에서 네트워크 ID에 대한 인증 및 접근제어 기능에 대한 표준 연구를 시작한 단계로, 3GPP가 추진 중인 M2M 접속 인증을 위한 신뢰성 확보 절차기술에 대해 참여하고, 이를 응용한 NGN 표준 개발을 추진하는 것이 필요 • 3GPP의 표준안들을 기반으로 모바일 환경에서의 클라이언트와 서버간의 상호인증 문제들을 해결하는 국내 표준안을 개발하는 것이 필요하며, 이를 바탕으로 국제 표준을 선도하는 것이 필요함 • 네트워크 ID 인증 및 접근제어 기술에 대한 IPR은 매우 미흡한 실정이며 또한 ITU-T SG13을 한국이 주도하는 등 IPR을 확보하기에 적절한 시기임
동시표준	* IPR확보가능분야 : 번들 인증 등 NGN에 대한 신규 기능 설계
본인확인 기술	*** 국제표준화 전략목표 : 국제표준 협력/경쟁(선도)(Ver.2009) → 국제표준 선도(Ver.2010)**
	• i-PIN의 서비스 프레임워크, 서비스 전달 메시지 형식에 대한 표준 제정 및 공공 i-PIN과 민간 i-PIN간의 상호연동 등을 위해 i-PIN 서비스 전달 메시지 형식 및 중복가입 확인정보에 대한 표준계정 • ITU-T, ISO/IEC 등에서 ID Proofing 과정에서 사용자 인증의 하나로 본인확인에 대해 언급하고 있으나, 세부적인 기술은 포함하고 있지 않아, 표준화가 아직은 초기 단계로 서비스 프레임워크 전반에 걸쳐 국내 본인확인기술의 적용 가능성을 사전에 검토해 국제 표준화를 선도할 필요가 있음 – 실세계의 단일 식별자 체계를 대체하는 기술로 국제 환경에 맞는 i-PIN 규격을 개발하여 ITU-T에 기고하여 국제 표준화를 선도하는 것이 필요함 • 본인확인기술에 대한 국내 IPR은 보유하고 있지 않은 상황이므로, 빠른 시일 내에 국제 환경에 맞는 i-PIN 규격을 개발하여 국제 표준화를 진행하며 IPR을 확보하는 것이 필요함
동시표준	* IPR확보가능분야 : 본인확인기술

네트워크/시스템보안

기술개요



- 개방형 네트워크 환경에서 전달되는 정보의 위조, 변조, 유출, 무단침입 등을 비롯한 불법 행위로부터 정보를 보호하는 네트워크 보안과, 정보통신 시스템의 안전성과 가용성을 향상시키는데 필요한 정보보호 기술 및 디지털 증거 제공을 위한 기술을 포함한 시스템 보안으로 구성
- 네트워크 및 시스템 보안 분야는 유비쿼터스 센서 네트워크(USN) 보안, 이동통신 및 휴대인터넷 보안, 무선근거리통신망 보안, BcN 보안, 미래인터넷 보안, LED 통신 보안, 차세대 컴퓨팅 보안, 차세대 PC보안, 디지털 포렌식, 스마트 그리드 보안, 사이버 공격 역추적/보안관리 및 봇넷 대응 등으로 구분

표준화의 필요성

- 차세대 서비스 플랫폼 및 단말설 네트워크의 등장, 그린 IT를 지원하고 국내 정보보호 기술의 경쟁력 강화 및 표준화 선도를 위하여 네트워크 및 시스템 보안 분야의 신규 핵심 기술에 대한 표준 개발이 필요

표준화의 비전 및 기대효과

비전및목표

새로운 환경에서의 네트워크 및 시스템 보안 기반 조기 마련

1단계('10)	2단계('15)	3단계('15 ~)
클라우드 컴퓨팅 등 새로운 서비스 구축을 위한 기술 개발 및 IPR 확보	신규 서비스 및 인프라 보안 기술 표준화 주도	보안 표준기술의 상용화 및 실제 서비스 적용

기대효과

경제적 효과	기술적 효과	사회적 효과
• 보안 제품 세계 시장 확대 • 신규 보안 시장 창출	• 차세대 보안기술확보 • 관련규격 및 표준화 선도 • 상호운영성이 지원되는 정보보호 제품 개발	• 유비쿼터스 환경에 적합한 정보 보호 체계 구축

표준역량 4P 강화

Product	People	Partnership	Promotion
• 수요자 중심 표준 • 핵심 IPR, 특허개발 • 표준기술의 경제적 파급효과 분석	• 정보보호 표준 전문 인력조성 • 선진기관과 인력교류	• 한중일 공동으로 국제 표준 추진 • 한중일 공동 워크샵 추진	• 연구개발 및 시범 서비스 사업과 정보보호 표준기술 연계 추진

R&D 및 표준화

신규 네트워크 보안 기술 확보

- USN 보안 프레임워크
- USN 미들웨어 보안 가이드라인
- WSN 보안 라우팅 기법
- 센서 네트워크 키관리 모델
- LBS 서비스 인터페이스 보안 가이드라인
- 이동통신망 보호를 위한 보안 관제 프레임워크
- 휴대인터넷 서비스를 위한 보안 가이드라인
- 휴대 인터넷 Endpoint 보안 가이드라인
- 무선근거리 통신망 보안 요구사항
- 고속 무선랜 상에서의 보안 프레임워크 및 절차
- 분산 시스템 및 AP 협동하에서 인증 /보안통신절차
- BcN 보안 구조 및 요구사항
- Mobility Security 보안 구조 및 절차
- Mobility payment 보안 구조 및 절차
- Security Risk 보안 구조 및 절차
- 가상 환경에서의 보안 프레임워크
- 클라우드 컴퓨팅 환경에서의 암호/인증기법
- 클라우드 컴퓨팅 환경에서의 보안관제

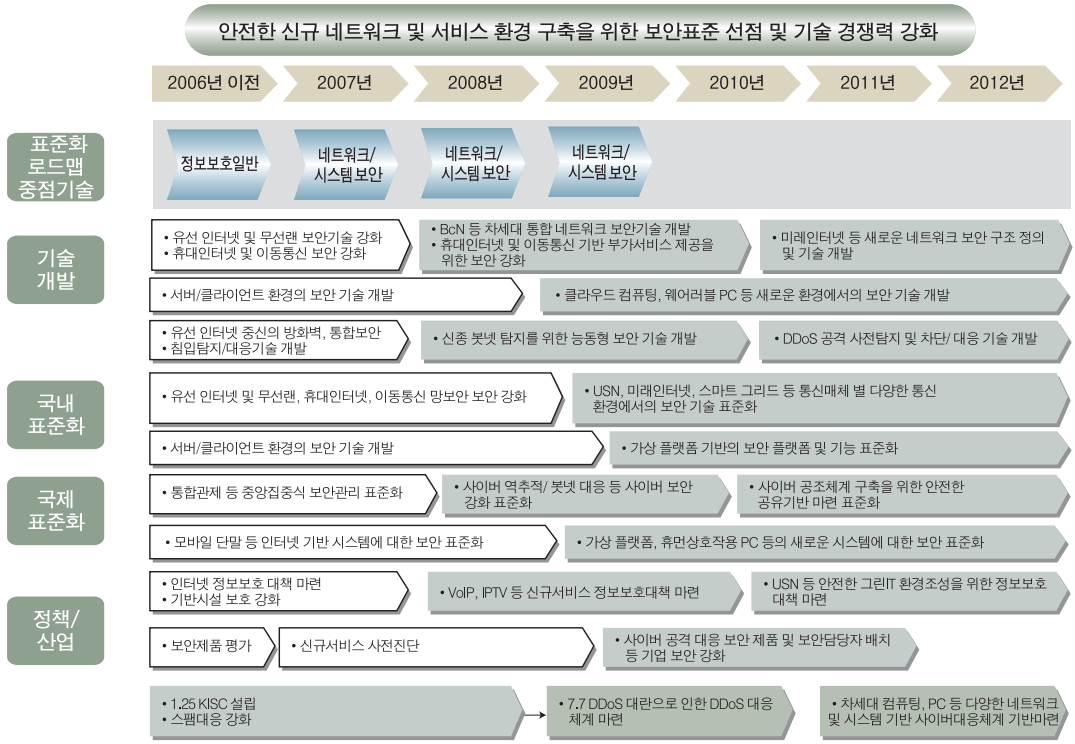
차세대 시스템 보안 기술 주도

- 차세대 PC 프레임워크
- 차세대 PC 통신 보안 기술
- 차세대 PC 사용자 인증 기술
- 차세대 PC 정보 유출 방지 기술
- 스마트 그리드 정보보안 관리 프레임워크
- 스마트 그리드 제어망 보안
- 스마트 미터 보안 가이드라인

사이버 보안 능력 강화

- 컴퓨터 포렌식을 위한 디지털 증거 분석도구 검증 이미지
- e-discovery 프레임워크, e-discovery 증거자료 표현
- e-discovery 가이드, 사이버 공격 추적이벤트 교환포맷
- 역추적 기술의 Use cases 및 capabilities
- 역추적 프레임워크 및 메커니즘, 봇넷 탐지 대응 프레임워크
- 봇넷을 이용해 발송되는 스팸 대응기술
- 보안 정보 교환 프레임워크 요구사항

■ 연도별 주요현황 및 이슈



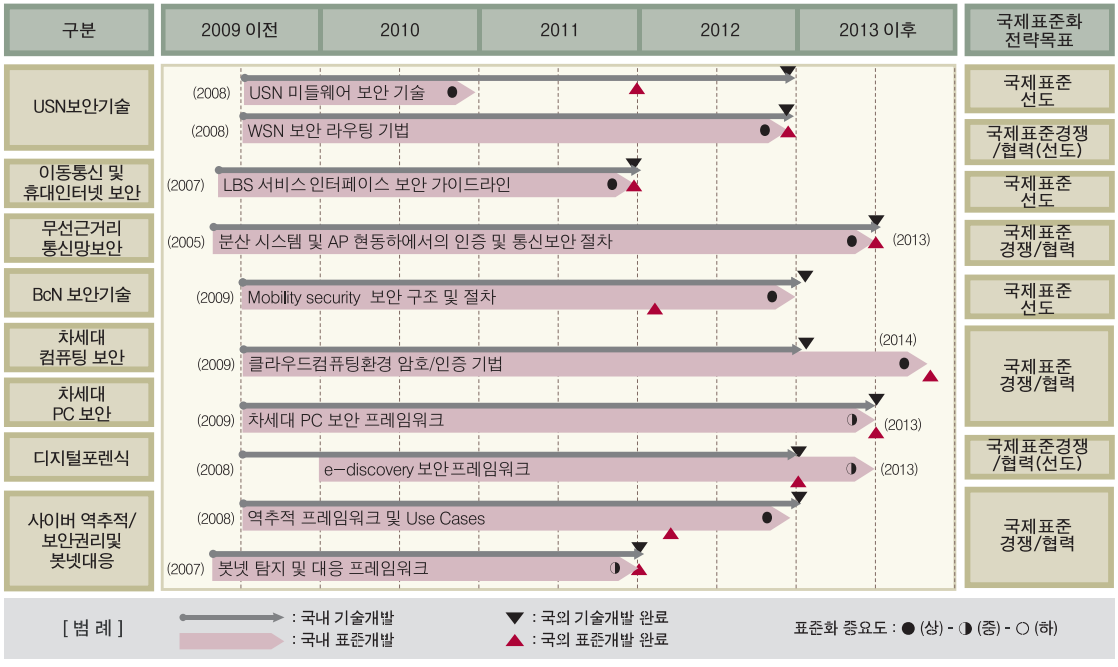
■ 표준화 대상항목

표준화 대상항목 (중점 표준화항목)		표준화 내용	대응 표준화기구	국내참여 기관/업체	표준화수준	
					국내	국제
USN 보안	USN 보안 프레임워크	– USN 서비스 전반에 걸친 보안 이슈를 제공. USN 환경에서 발생할 수 있는 보안 위협과 보안 위협 대응을 위한 보안 고려사항을 제공하며, 신뢰성 있는 USN 서비스를 제공하기 위해 USN 환경에서 적용할 수 있는 보안 메커니즘을 제공	ITU-T SG17, ISO/IEC JTC1 SC6	KISA ETRI	개발 검토	개발 검토
	USN 미들웨어 보안 가이드라인	– 개방형 센서 네트워크를 이용하는 USN 서비스 환경에서 USN 미들웨어 설계 및 구축 시 USN 미들웨어를 위협하는 다양한 요소로부터 안전한 USN 미들웨어를 설계하고 구축할 수 있도록 하는 USN 보안 기능 및 보안 모델 제공	ITU-T SG17, IEEE 802.15		개발 검토	개발 검토
	WSN 보안 라우팅 기법	– 무선 센서 네트워크 라우팅에서 발생할 수 있는 다양한 보안 위협으로부터 안전한 라우팅 구성을 위한 보안 메커니즘 제공			기획	개발 검토
	센서 네트워크 키관리 모델	– 센서 네트워크에서 규모, 환경, 보안위협 등을 고려한 키관리 모델 제공	ITU-T SG17		제/ 개정	기획
이동통신 및 휴대 인터넷 보안	LBS 서비스 인터페이스 보안 가이드라인	– Mobile 단말과 Location Server사이의 데이터 교환을 위한 인터페이스를 대상으로 하는 보안 가이드라인 제공 – 특히 개인정보와 관련된 데이터의 보안을 위한 암호화/인증을 포함하여 데이터 전송을 위한 보안 메커니즘이 필요함	3GPP, 3GPP2, ITU-R, IETF	KISA, ETRI, SK, KT, LGT	항목 승인	제/ 개정
	이동통신망 보호를 위한 보안 관제 프레임워크	– 단말의 다양화와 타 네트워크와의 다양한 인터페이스로 인해서 향후 이동통신망을 대상으로 하는 새로운 유형의 공격이 발생할 수 있는 여지가 충분함 – 이동통신망(LTE, WiMax, Wi-Fi, W-CDMA 등)의 보호를 보안 관제 기술 도출 및 관제 프레임워크에 대한 표준화가 필요			제/ 개정	제/ 개정
	휴대 인터넷 서비스를 위한 보안 가이드라인	– 휴대 인터넷 서비스의 상용화/활성화에 앞서서 서비스 정보의 보호를 위한 인증/암호화, 휴대 서비스 이용자의 개인정보 보호, 서비스 자체의 보호를 위한 보안 지침 등의 보안 가이드라인에 대한 표준화가 필요	IEEE 802.16, ITU			
	휴대 인터넷 Endpoint 보안 가이드라인	– Privacy, 무결성, 인증, 부인방지, 보안 통신 등의 보안 기능을 포함한 휴대 인터넷 Endpoint용 보안 가이드라인에 대한 표준화가 필요				

표준화 대상항목 (중점 표준화항목)		표준화 내용	대응 표준화기구	국내참여 기관/업체	표준화수준	
					국내	국제
무선 근거리 통신망 보안	무선 근거리 통신망 보안 요구사항 (802.11)	– 최신 무선 근거리 망 (차량통신네트워크, 메쉬 네트워크) 상에서의 통신 규약에 따른 통신보안 절차를 정의하고, 주요 보안요소로써 개인정보 보호방안을 제안	IEEE	ETRI	개발 검토	개발 검토
	고속 무선랜 상에서의 보안 프레임워크 및 절차					
	분산 시스템 및 AP 협동하에서의 인증 및 통신보안 절차				기획	기획
	최신 무선 근거리 망에서의 개인정보보호 방안				개발 검토	개발 검토
BcN 보안 기술	BcN 보안 구조 및 요구사항	– BcN 네트워크에서 사용자 인증을 위한 보안 요구사항을 제시하고 이를 위한 보안 구조 및 절차 표준 개발. 이종 사업자 또는 다른 네트워크 간의 mobility 보안을 위한 구조 및 절차 표준화 추진. 또한 BcN 네트워크에서 안전한 서비스 제공을 보안 risk 프레임워크 등의 국제 표준화 활동이 요구됨	ITU-T, IETF, ISO/IEC	KISA ETRI	최종 검토	제정
	Mobility Security 보안 구조 및 절차				항목 승인	항목 승인
	Mobile payment 보안 구조 및 절차				기획	항목 승인
	Security Risk 보안 구조 및 절차				기획	기획
차세대 컴퓨팅 보안	가상화 환경에서의 보안 프레임워크	– 클라우드 컴퓨팅의 기반 기술이 되는 가상화 환경의 보안 프레임워크에 대해 표준 개발의 필요성이 있으며, 클라우드 컴퓨팅에서 사용될 암호/인증 기술에 대한 기본적 정의가 시급 – 클라우드 컴퓨팅 환경이 도래 했을 시 나타날 침해사고에 대한 대응을 위해 관제 시스템 및 인프라의 표준 도출이 필요	CCC(Open Cloud Consortium) WG on Information Sharing, Security and Clouds	삼성SDS, LG CNS, TTA 등	기획	기획
	클라우드 컴퓨팅 환경의 암호/인증 기법					
	클라우드 컴퓨팅 환경의 보안관제					
차세대 PC보안	차세대 PC 보안 프레임워크	– 차세대 PC는 언제 어디서나 다양한 정보를 사용자 중심에서 서비스해주며 사용 목적에 따라 특화된 기능을 가지게 되므로 현재의 PC보다 경량화된 구조가 요구되므로 차세대 PC 프레임워크에 대한 표준화가 필요함	ISO, OMA, MIPI	ETRI, 각산업체	기획	기획
	차세대 PC 통신 보안 기술	– 차세대 PC는 소형 단말기 형태나 신체에 부착가능한 형태로 발전해 나갈 것이며 이에 따라 차세대 PC 사이의 통신을 필요로 하게 되며 이에 사용되는 통신 프로토콜과 그 보안 기술 표준화가 필요함	ISO, IEEE 802, Wi-Fi			
	차세대 PC 사용자 인증 기술	– 차세대 PC는 사용자에 특화되어 소형화됨에 따라 사용자를 인식하고 불법적인 사용을 막기 위하여 생체인식 등의 사용자 인증 과정이 필요하므로 이에 대한 표준화가 요구됨	OMA, ISO			
	차세대 PC 정보유출 방지 기술	– 차세대 PC에서 사용되는 개인정보를 수집하고 관리하며 특화된 서비스를 제공하는데, 저장 정보가 유출될 경우 프라이버시 문제가 발생하므로 차세대 PC의 개인정보 저장 형식과 정보유출 방지를 위한 기술 표준화가 필요함	ISO, IETF			
스마트 그리드 보안	스마트그리드 정보보안 관리 프레임워크	– 다양한 규격으로 사용되고 있는 스마트 그리드 정보 보안관리규격(권한관리, 접근제어, 암호화 규칙, 정보저장규칙, 정보)에 대한 표준, 보안참조모델 개발	IEEE/ IEC/NIST	ETRI, KISA	기획	기획
	스마트 그리드 제어망 보안	– 스마트 그리드 제어망의 신뢰성 보장을 위한 인증, 접근제어, 암호화, 키 분배/관리, DDoS대응, 침입탐지/대응 구조 등에 대한 표준, DCS, PCS 시스템 보안 규격, 제어 프로토콜, 메커니즘 및 표현에 대한 표준				
	스마트 미터 보안 가이드 라인	– 스마트 미터 데이터의 무결성 보장, 미터링 데이터의 보안 전송, 디바이스 상호인증 등에 대한 표준				
디지털 포렌식	컴퓨터 포렌식을 위한 디지털 증거 분석도구 검증 이미지	– 컴퓨터 포렌식 증거분석 도구의 검증을 위한 시험 데이터	ITU-T, NIST, ISO	ETRI, KISA, TTA	기획	기획
	e-discovery 보안 프레임워크	– e-discovery 프로세스 정의 – e-discovery 관련 표준들의 연관 관계				
	e-discovery 증거자료 표현	– 증거자료 교환용 컨터이너 구조 – 각 응용프로그램별 증거자료 표현 형식				
	e-discovery 가이드	– e-discovery 증거 수집 – e-discovery 증거 분석 – e-discovery 증거 보존				

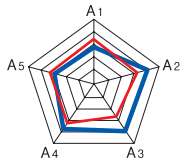
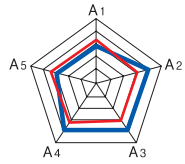
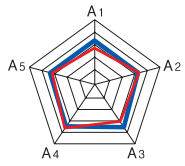
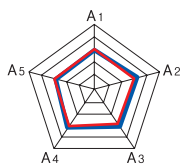
표준화 대상항목 (중점 표준화항목)		표준화 내용	대응 표준화기구	국내참여 기관/업체	표준화수준	
					국내	국제
사이버 역추적/ 보안관리 및 봇넷 대응	사이버공격 추적이벤트 교환 포맷 (TEEF)	– 사용자 및 기능 요구사항 – TEEF 데이터 교환 모델 – TEEF 데이터 클래스 정의 – TEEF 스키마	ITU-T, IETF, ISO	ETRI, 이글루시큐리티, 인젠, KISA	제 / 개정	제 / 개정
	역추적 기술의 Use Cases 및 Capabilities	– 네트워크 기반 Use Cases – 위협 기반 Use Cases – 관리 Capabilities – 기능 Capabilities			개발 검토	개발 검토
	역추적 프레임워크 및 메커니즘	– 다중도메인 협업기반 추적 모델 – 프레임워크 구조 및 구성요소 – 추적 메커니즘			개발 검토	기획
	봇넷 탐지 및 대응 프레임워크	– DDoS, 스팸 발송, 개인 정보 유출 등의 사이버 보안 위협의 수단이 되는 봇넷 대응을 위한 정보 공유 및 공조에 기반한 봇넷 탐지 및 대응 프레임워크 제공	ITU-T	KISA	개발 검토	개발 검토
	봇넷을 이용해 발송되는 스팸 대응 기술	– 봇넷을 통해 대량으로 발송되는 이메일 스팸 대응을 위한 봇넷을 이용한 스팸 발송 대응 기능 및 인터페이스 정의				항목 승인
	보안 정보 교환 프레임워크 요구사항	– 위협, 공격, 침해 혹은 다른 악의적인 행위 식별에 관한 보안 정보 공유 프레임워크 제공		ETRI		개발 검토

■ 중점 표준화항목별 중기(3개년) 표준화로드맵

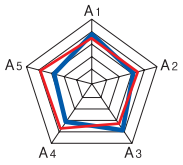
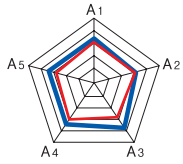
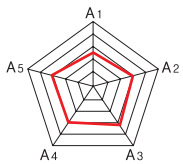
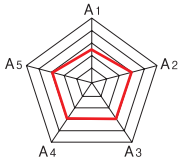


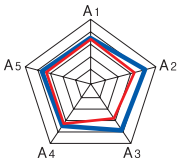
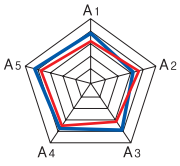
■ 중점 표준화항목별 세부전략(안)

* A1: 국외대비 국내 표준화 수준, A2: 국외대비 국내 기술개발 수준, A3: IPR 확보 가능성, A4: 국내 표준화 인프라 수준, A5: 국제표준화 기여도 * 파란색: Ver.2009, 빨간색: Ver.2010

중점 표준화항목	세부전략(안)
USN 미들웨어 보안 가이드라인	* 국제표준화 전략목표 : 국제표준 협력/경쟁(선도)(Ver.2009) → 국제표준 선도(Ver.2010)
	• 국제 표준화의 지속적인 노력으로 USN 보안 표준화를 주도 하고 있으므로, 지속적인 선도 • 국외대비 국내기술개발 수준의 격차가 다소 줄어듬에 따라 시범서비스 환경 조기 구축 등을 통해 기술개발을 촉진해야 할 것이며, USN 핵심 기술에 대한 특허가 다수 발생함에 따라, 실제 USN 서비스를 위해 필요한 보안기술에 대한 IPR 확보에 주력해야 할 것임 • 국내 표준화 인프라 수준이 다소 줄어듬에 따라, 기술개발 병행 활성화를 통한 표준화 인프라 확대 노력 • USN 보안 분야의 국제 표준화 기여도는 선도적 위치에 있음에 따라 지속적인 주도권 확보를 위한 해당 분야 표준화 전문 인력 양성 확대 필요 • USN 미들웨어에서 준수해야 할 보안 사항을 정의하고 표준화하여, 미들웨어 플랫폼 개발시 반영할 수 있도록 하며, 기술개발과 함께, 미들웨어 보안 핵심 기술에 대한 IPR 확보를 병행하여 추진
동시표준	* IPR확보가능분야 : USN 보안 미들웨어
WSN 보안 라우팅 기법	* 국제표준화 전략목표 : 국제표준 협력/경쟁(선도) (Ver.2009) → 국제표준 협력/경쟁(선도) (Ver.2010)
	• 국제 표준화의 지속적인 노력으로 USN 보안 표준화를 주도 하고 있으므로, 지속적인 선도 • 국내 대비 국외에서 다양한 라우팅 보안 기법을 연구함에 따라 경쟁적 측면에 있으므로, USN 응용서비스 특성에 따라 보안 고려사항 등을 중점적으로 라우팅 보안 연구 필요 • USN 핵심 기술에 대한 특허가 다수 발생함에 따라, 실제 USN 서비스를 위해 필요한 보안기술에 대한 IPR 확보에 주력해야 할 것임 • 국내 표준화 인프라 수준이 다소 줄어듬에 따라, 기술개발 병행 활성화를 통한 표준화 인프라 확대 노력 • USN 보안 분야의 국제 표준화 기여도를 높이기 위해 적극적이고 다양한 보안 라우팅 관련 표준화 추진 필요 • 기존에 제안되어온 WSN 라우팅 기법을 분석하여 정보보호 이슈를 도출하여 표준화하여, 보안 라우팅 기술이 개발/상용화 될 수 있도록 추진하며, 핵심 보안 기술에 대한 IPR 확보에 중점을 둠
동시표준	* IPR확보가능분야 : 안전한 Ad-Hoc 보안 라우팅
LBS 서비스 인터페이스 보안 가이드라인	* 표국제준화 전략목표 : 국제표준 협력/경쟁(Ver.2009) → 국제표준 선도(Ver.2010)
	• 이통통신망을 기반으로 하는 부가 서비스는 한국이 앞서 있으므로, 선도적으로 보안을 위한 가이드라인을 제시해야 함 • 안정된 이동통신망 및 휴대인터넷 기술을 기반으로 보다 빠르게 보안 부분을 추가할 수 있음 • LBS 기반 서비스에 따른 정보보호 기술 기준을 제시하여 선도적으로 IPR 확보 가능할 것임 • 안정화된 서비스 인프라를 기준으로 바로 적용가능한 실용적인 보안 기준을 만들어야 함 • LBS 관련 서비스 보안을 위해 주도적인 표준화에 앞장서야 할 것임 • 상용에서 테스트된 LBS 보안 기술을 개발하여 IPR을 먼저 확보할 수 있을 것이며, 실제 서비스에서의 보안 효율성을 중시해야 할 것임 • 현재 제공되고 있는 LBS 부가 서비스 형태를 분석하여 형태별로 정보보호 대상을 분류하여 보안 제공방안을 도출할 수 있으며, 상용기술 개발 및 적용에 중점을 둠
후행표준	* IPR확보가능분야 : -
분산시스템 AP협동 하에서의 인증 및 통신보안 절차	* 국제표준화 전략목표 : 국제표준 선도(협력/경쟁)(Ver.2009) → 국제표준 협력/경쟁((Ver.2010)
	• 무선근거리통신망의 향상된 인증 및 보안관련 기술표준화가 진행된 후 관련 프로토콜의 표준화 작업, 유무선 통합기술 표준화 및 향상된 속도 및 대용량 데이터 처리 관련 기술에 대한 표준화가 예상됨 • 무선근거리통신망의 로그AP 방지기술과 분산 시스템 및 AP협동 하에서의 인증 및 통신보안 절차에 대한 표준화를 중점적으로 추진하여, 국제표준과 협력하며 경쟁력을 갖출 필요가 있음 • 기존 무선랜 서비스 시장이 외국 선진업체에 의해 선점되어 왔으며, 초고속 무선랜 분야의 기술 개발 및 서비스 모델 개발이 필요 • ITU등의 국제기구에 많은 국내기업체와 ETRI등이 회원으로 가입하여 범세계적 표준화 작업을 추진하고 있음 • 무선근거리통신망에서의 전송용량의 광대역화, 고속 이동성, 글로벌 로밍, 콘텐츠를 재가공하지 않고 자유롭게 이용할 수 있는 유무선 통합서비스 부분에 대한 지적재산권 확보를 시도할 필요 있음 • Giga bit 무선 시스템분야는 802.11n의 후속 표준으로 진행될 것으로 전망되고 있으므로 구현기술 확보 및 IPR의 확보가 필요함 • 정부, 산업체, 학계의 유기적인 협동으로 서비스, 콘텐츠 개발 및 장비개발 분야에서의 지적재산권 확보를 검토할 필요 있음 • 서비스망, 단말장치 등 각종 정보시스템의 유무선 통신망 연결을 고려하여 범국가적 연관 IPR의 획득, 비용절감, 기기 간 상호 운용성, 이식성 등을 고려하고 서비스의 안정 및 신뢰성 확보를 위한 표준 및 기술개발이 필요함
동시표준	* IPR확보가능분야 : 다수 AP들간의 인증 및 통신보안 및 절차분야

* A1: 국외대비 국내 표준화 수준, A2: 국외대비 국내 기술개발 수준, A3: IPR 확보 가능성, A4: 국내 표준화 인프라 수준, A5: 국제표준화 기여도　　* 파란색: Ver.2009, 빨간색: Ver.2010

중점 표준화항목	세부전략(안)
Mobility security 보안구조 및 절차	* 국제표준화 전략목표 : 국제표준 협력/경쟁(선도)(Ver.2009) → 국제표준 선도(Ver.2010)
	• 국제 표준화의 지속적인 활동으로 BcN 보안 표준화를 주도하고 있으므로, 지속적인 선도 • 국외에서 다양한 mobility security 기법을 연구함에 따라 경쟁적 측면에 있으므로, BcN 특성에 따른 보안 구조 및 절차 연구 필요 • BcN 핵심 기술에 대한 특허가 다수 발생함에 따라, BcN 서비스를 위해 필요한 보안기술에 대한 IPR 확보에 주력해야 할 것임 • 국내 표준화 인프라 수준이 다소 줄어듬에 따라, 기술개발 병행 활성화를 통한 표준화 인프라 확대 노력 • BcN 보안 분야의 국제 표준화 기여도를 높이기 위한 security risk 관련 표준화 추진 필요 • 국내에 네트워크 인증 기술을 바탕으로 BcN 보안 제품을 개발하고 동시에 이에 해당하는 표준화를 추진하며, BcN 포럼을 통하여 BcN 보안 기능을 추가하고 이를 바탕으로 특허 획득을 추진함
선행표준	* IPR확보가능분야 : 이종망간 Mobility 보안기술
e-discovery 보안 프레임워크	* 국제표준화 전략목표 : 국제표준 협력/경쟁(선도)(Ver.2009) → 국제표준 협력/경쟁(선도)(Ver.2010)
	• ISO/IEC JTC2/SC27에서 추진중인 Forensic Investigation 분야에 적극적인 참여 필요하며, ITU-T SG17에서 국내주도로 추진중인 포렌식 관련 표준 채택에 노력하고, 향후 주도적인 표준안 제안을 통해 국제 표준을 선도해 나가는 것이 필요함 • 한-미 및 한-EU FTA 체결과 국내 민간분야 디스커버리제도 도입이 예상됨에 따라, e-Discovery 관련 표준개발이 필요함 • e-Discovery의 기술개발은 국외에서 앞서 있으나, 국내에서 강점으로 내세울 수 있는 자료 분석 분야에 대한 IPR을 확보하는 방향으로 표준개발이 필요함 • 포렌식 분야는 전통적으로 국가 수사기관에서 출발한 관계로 표준화에 대한 인식이 없었으나, 수사의 공정성 및 민간분야로의 확대로 인식 수준이 높아지고 있는 단계임. 따라서 전문기술 표준보다는 가이드와 프레임웍등 민간분에서 인식의 수위를 높일 수 있는 표준을 우선 추진할 필요가 있음 • 포렌식에 대한 국제표준은 초보단계로 국내에서 선도하고 있는 만큼, e-Discovery 분야에서도 선도를 유지할 수 있도록 추진 필요함
후행표준	* IPR확보가능분야 : 증거자료 분석
클라우딩 컴퓨팅 환경의 암호/인증 기법	* 국제표준화 전략목표 : (신규) 국제표준 협력/경쟁(Ver.2010)
	• 국외 표준의 경우 몇몇 기관을 통해 정립이 되어가고 있는 상황이며, 이러한 기관과 국내의 표준 추진 기관이 협력/경쟁 할 경우 좋은 결과를 얻을 수 있을 것으로 사려됨. 기존에 가지고 있는 국내 암호화 표준 및 인증 기술에 대한 표준과 클라우드 컴퓨팅의 특성을 반영하여 클라우트 컴퓨팅 환경에서의 암호/인증 기술의 표준을 정립 할 필요가 있음 • 기술 수준으로 볼 때 규모의 경제로 추진하는 미국, 유럽 지역의 기술 성숙도가 상대적으로 높은 실태임. 국내의 연구개발 수준을 고려해서 표준 항목 도출 시 국내 연구개발 수준에 적합한 항목을 도출하여 국외 기관과의 협의를 수행하는 전략적 진행이 필요함. 이미 서비스 제공 단계에 있는 국외 업체 및 기관들의 서비스 분석 및 국내에서 설계중인 기관들과의 연계 개발 필요가 있음. 클라우드 컴퓨팅 환경의 특성을 고려하여 사용자와 제공자 정보 및 데이터에 대한 암호화 기술 및 데이터 접근성을 관리하는 인증 기술에 대한 적합한 기술을 개발할 필요가 있음 • 본 주제와 관련한 국내외 IPR은 찾기 어려운 상태이므로 표준화를 신속히 추진하면서 기술개발 기관과의 협조 체계를 통한 IPR 확보가 필요함. 또한 기존의 암호화 기술 및 인증 기술에 대한 클라우드 컴퓨팅 환경에서 사용 가능한 암호/인증 기술에 대한 IPR확보 전략을 수립할 필요가 있음 • 국내 표준 수준이 낮은 상태이며, 이를 고려하여 빠른 표준 추진을 시도할 필요가 있음. 현재 국내 진행되고 있는 기술 개발과의 협력을 통해 클라우드 컴퓨팅 서비스의 사용자와 서비스 제공자 및 관리 대상인 데이터와 사용자 인증에 대하여 표준화 영역을 정의하고 추진 할 필요가 있음 • 국내의 초고속 인터넷 환경을 기반으로 도출된 표준 및 기술개발 결과를 기반으로 국제 표준을 추진할 필요가 있음. 현재 클라우드 컴퓨팅에서의 암호화 및 인증에 대한 기술의 표준 연구가 국외에서 논의되고 있으며, 이러한 상황을 고려하여 클라우드 컴퓨팅 서비스에서 사용자와 정보 제공자 및 스토리지에서 관리되는 데이터 등의 암호화 및 인증 기술, 인증시 사용되는 키 관리에 대한 국제 표준을 추진할 필요가 있음
후행표준	* IPR확보가능분야 : 스토리지 데이터 암호화 기술, 클라우딩 환경의 적합한 인증기술
차세대 PC 보안 프레임워크	* 국제표준화 전략목표 : (신규) 국제표준 협력/경쟁(Ver.2010)
	• 차세대 PC 보안 분야에 대한 표준의 필요성이 요구되고 있지만 국내외적으로 표준안이 개발되어 있지는 않았으므로 표준화항목을 선정하여 국제적으로 협력경쟁을 할 수 있을 것으로 예상됨 • 국내에서 보안 부분에 대한 의식을 가지고 설계를 하고 있지만 시장형성이 되어 있지 않아 시제품으로 나와 있지 않는 상황이므로 표준화와 기술개발을 동시 추진하는 것이 좋겠음 • 보안 기능에 대한 특허는 많이 나와 있으므로 차세대 PC 환경인 저전력 경량화된 제품에 특화된 보안 기능에 대한 특허가 가능 • 국내에 차세대 PC에 대한 인식은 확산되었으며 그린 IT의 추진으로 차세대 환경에 적합한 제품이 개발되고 있으나 착용형 PC 분야는 아직도 잠잠한 상태이므로 저전력 경량화 제품에 대한 보안 기능부터 표준화를 추진하는 것이 바람직함 • 국내의 차세대 PC에 대한 하드웨어 기술은 국제적으로 뒤지지 않는 만큼 실용적인 가치를 내세우며 국내 기술로 만들어진 제품의 수출을 늘리며 표준화를 추진하는 경우 협력/경쟁 체제를 유지할 수 있으며 국제 표준화에서의 발언권도 높아질 것임 • 차세대 PC와 보안 기능에 대한 각각의 특허는 이미 많이 등록되었으며 이후에도 차세대 PC 하드웨어 제품에 대한 특허가 계속될 것으로 예상되므로, 저전력 경량화된 제품에 보안 기능을 탑재하는 기술에 대한 특허가 가능할 것으로 예상됨
동시표준	* IPR확보가능분야 : 초소형 PC와 착용형 PC의 보안구조

중점 표준화항목	세부전략(안)
역추적 프레임워크 및 Use cases	*** 국제표준화 전략목표 : 국제표준 선도(Ver.2009) → 국제표준 선도(Ver.2010)**
	• 사이버 공격 감시 및 추적기술은 국내 각 정부 및 민간 기관별 침해대응센터의 고도화에 해당되는 것으로서 상호호환성이 절대적으로 필요하며, 국내에서는 추적 메시지에 대한 표준 교환 포맷을 TTA에서 정의하였으며, 향후에 제시될 다양한 방향에 대한 기술 검증과 더불어 실용적인 역추적 Use Case와 추적 메시지 교환 시 안전성 제공을 위한 역추적 프레임워크에 대한 체계적인 국내 고유 표준 개발을 추진 • 사이버공격의 글로벌화로 국제적 상호 호환성 및 세계시장의 단일화로 세계 표준화가 수출 산업화에 핵심 관건이 되고 있음 • 사이버공격 역추적 분야는 국제 기여도가 매우 높으며, 또한 IPR 확보 가능성이 높아야 국제표준 선도 가능성이 높은 관계로, 역추적 Use Case와 추적 메시지 교환 시 안전성 제공을 위한 역추적 프레임워크 등에 대한 국내외 IPR 확보를 적극적 확보 시도 • 약간의 표준 인프라(인력 및 정책 등)만 있어도 충분히 선도가능하며, 현재의 표준 대상의 기술에 대한 검증을 통해 국내표준 시도 추진 • 사이버공격 역추적 분야는 국제 기여도가 매우 높은 상태인 관계이며, 따라서 실용적인 기술 검증과 함께 현재 미흡한 국제표준을 선도하는 상황에 역점을 두어 관련 국제 표준을 선도
선행표준	* IPR확보가능분야 : DDOS 대응형 역추적 프레임워크/메커니즘, 추적이벤트 공유, 역추적 적용 가이드라인, 유무선 환경에서의 역추적기술
봇넷 탐지 및 대응 프레임워크	*** 국제표준화 전략목표 : 국제표준 선도(Ver.2009) → 국제표준 선도(Ver.2010)**
	• ITU-T SG17에서 봇넷 탐지 및 대응 프레임워크에 대한 표준 항목을 제안해 채택된 상태이며, 국내 주도 하에 표준 문서 개발 중이며, 효율적이고 높은 상호 운용성을 제공하기 위해서 다른 나라 유관기관과의 협력이 필요함 • 국내에서는 세계적으로 우수하다고 평가되는 봇넷 대응 체계를 가지고 있지만, 봇넷의 형태가 다양해지고 피해의 정도가 날로 심각해지고 있어, 다양한 변종 및 조기 대응을 위한 기술 개발이 필요함 • 기존의 악성코드 탐지 및 네트워크 공격 시그니처 생성 등의 IPR은 많이 존재하지만, 봇넷의 변종에 대한 능동적 탐지 및 조기 대응의 필요성이 대두됨에 따라 관련 기술 개발 후 해당 기술에 대한 IPR 확보에 주력해야함 • 국내에서 봇넷 대응 체계를 가지고 있기 때문에, 기존의 대응 체계를 활용하여 신기술에 대한 선적용 노력 • 봇넷 탐지 및 대응 분야 국제 표준화를 선도적으로 추진하는 입장에서 미국, 일본 등 주요 국가들과의 의견 조율 필요
동시표준	* IPR확보가능분야 : 신종 본넷 능동형 탐지 및 대응

응용보안/평가인증

■ 기술개요

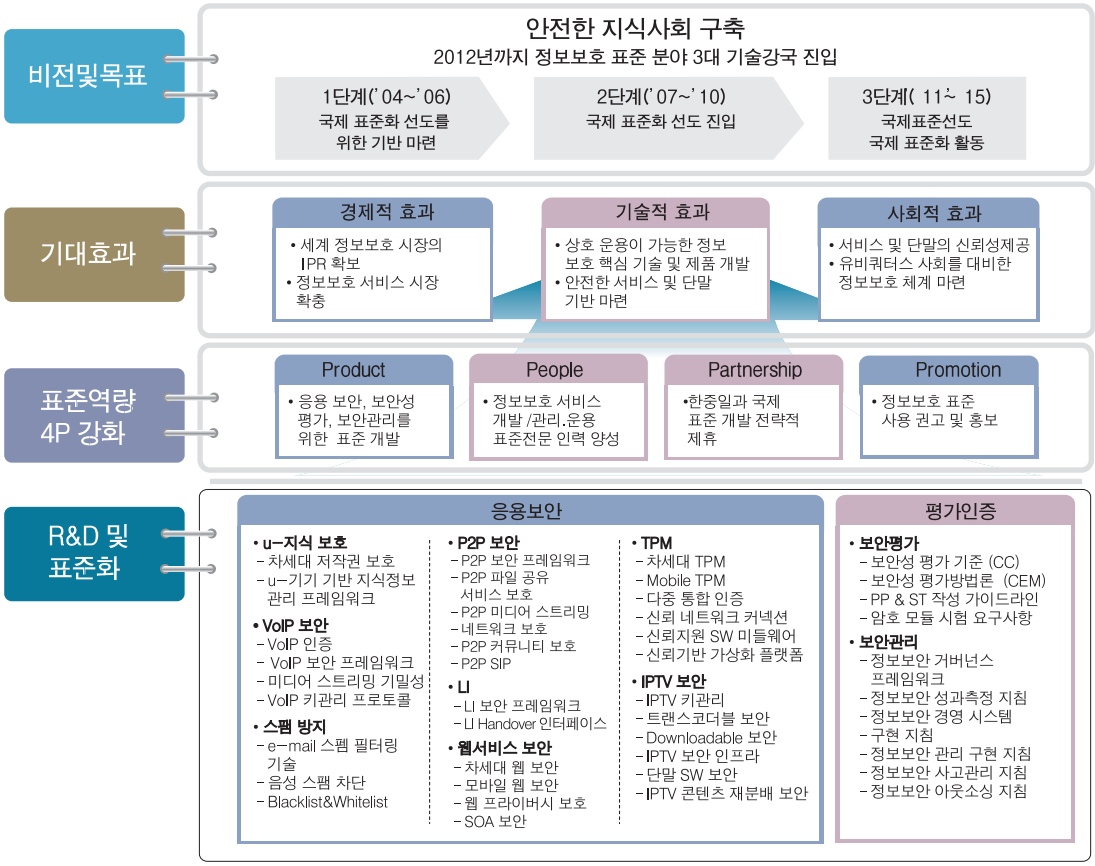
• 응용보안은 정보통신기반의 응용(서비스)의 기밀성, 무결성, 인증, 가용성, 신뢰성 제공을 위한 정보보호로 정의 하며, 평가인증은 정보제품에 대한 정보보안 사고를 사전에 예방하기 위한 보안성 평가와 비즈니스 활동을 지속적으로 지원하는 정보보호 수준을 평가/관리를 정의함

• 응용보안/평가인증은, 유비쿼터스 지식, VoIP 보안, 스팸방지, P2P보안, IPTV보안, TPM(Trusted Platform Module), LI(Lawful Interception), 웹 서비스 보안, 보안평가, 보안관리와 같이 10개의 분야로 세분됨

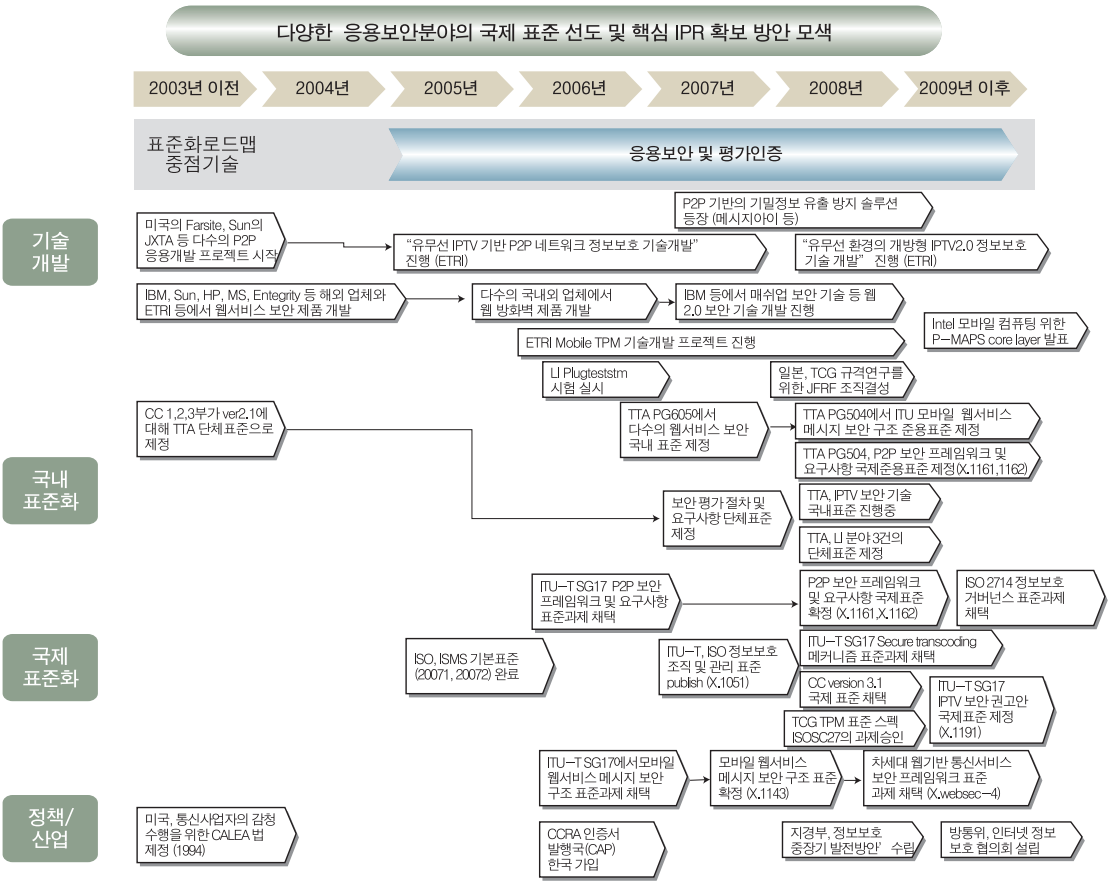
■ 표준화의 필요성

• 최근 정보화의 역기능을 방지하기 위한 정보보호기술의 중요성이 증대됨에 따라 정보보호 제품의 설치가 활발히 진행되고 있으나 상호 운용성을 제고하기 위한 정보보호 제품에 대한 표준이 부재한 상황. 세계 각국은 자신이 개발한 기술을 국제 표준에 반영함으로써, 관련 정보보호 제품에 대한 IPR을 확보하고 관련 제품의 기술경쟁력과 시장지배력을 향상시키고 있는 추세로, 이에 대응하여 IPR이 확보된 국내 기술을 바탕으로 국제 표준화가 필요

■ 표준화의 비전 및 기대효과



■ 연도별 주요현황 및 이슈



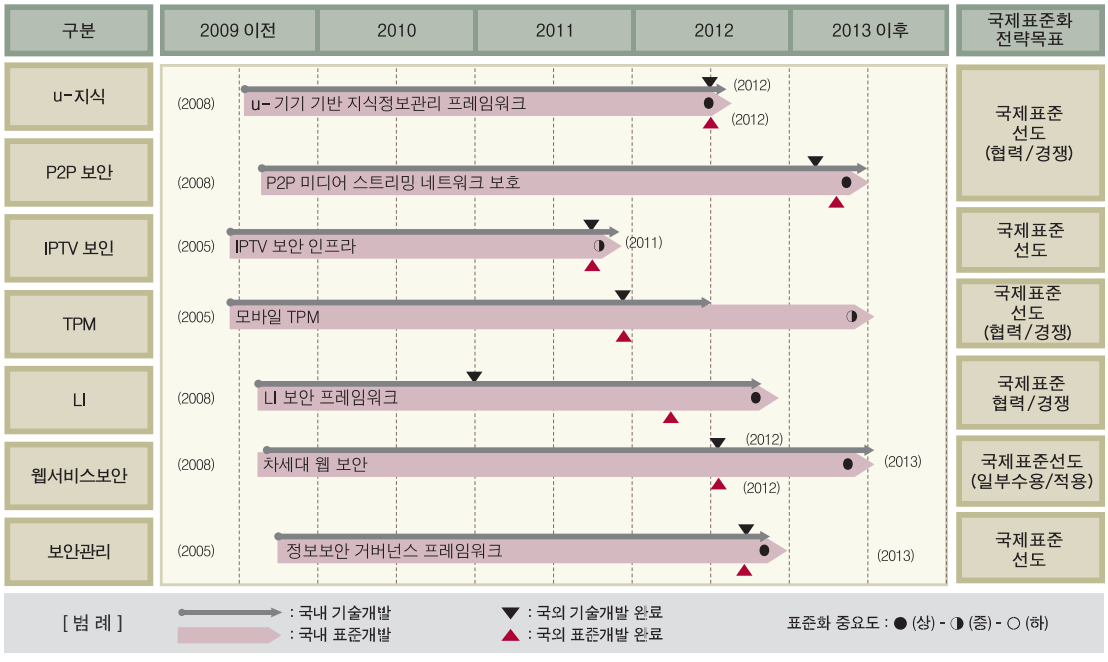
■ 표준화 대상항목

표준화 대상항목 (중점 표준화항목)		표준화 내용	대응 표준화기구	국내참여 기관/업체	표준화수준	
					국내	국제
u-지식	차세대 저작권 보호	- UCC, 복합 콘텐츠 등 차세대 저작권 보호 기술 표준화	MPEG-21, OMA, DVB-CPCM, DHWG, TVAnytime, OpenCableLab	ETRI, 삼성전자, SK텔레콤, KT	기획	항목승인 기획
	u-기기 기반 지식정보 관리 프레임워크	- 유비쿼터스 환경에서 u-기기 기반의 지식정보 관리 및 유통보호 기술 표준화				
VoIP 보안	VoIP 인증	- VoIP 서버, 디바이스, 사용자 등에 대한 인증 기술 표준화	IETF, ITU-T	KISA, ETRI, 숭실대학교	항목승인	개발 검토
	VoIP 보안 프레임워크	- 안전한 VoIP 서비스 제공을 위한 보안 프레임워크 표준화				
	미디어 스트리밍 기밀성	- 스트리밍 되는 미디어의 기밀성 보장을 위한 암호기술 표준화				
	VoIP 키관리 프로토콜	- VoIP 키관리 프로토콜 표준화				
스팸 방지	e-mail 스팸 필터링 기술	- e-mail 기반의 스팸방지 기술 표준화		ETRI KISA	항목승인	개발 검토
	음성 스팸 차단	- 유선/이동 전화, SMS, VoIP 등을 통한 음성스팸의 탐지 및 차단 기술 표준화				
	Blacklist & Whitelist	- Blacklist & Whitelist 관리 및 이를 통한 접근제어 기술의 표준화				
P2P 보안	P2P 보안 프레임워크	- P2P 보안 구조 및 메커니즘에 대한 표준화	ITU-T, IETF	KISA, ETRI, KAIST, 소만사	개발 검토	제/개정
	P2P 파일 공유 서비스 보호	- P2P 기반의 파일 공유 응용서비스 보호를 위한 기술 표준화. 피어인증, 키관리, 보안그룹관리, P2P 유통 불법저작물 필터링 등	ITU-T	ETRI	기획	기획
	P2P 미디어 스트리밍 네트워크 보호	- P2P 기반 미디어 스트리밍 서비스 보호 기술 표준화 - P2P 오버레이 네트워크 구축, dynamic membership 관리, 그룹보안 등에 대한 요구사항 및 보안 프레임워크	ITU-T	KISA, ETRI, KAIST		

표준화 대상항목 (중점 표준화항목)		표준화 내용	대응 표준화기구	국내참여 기관/업체	표준화수준	
					국내	국제
P2P 보안	P2P 커뮤니티 보호	– P2P 협업 등 커뮤니티 기반의 서비스 제공을 위한 커뮤니티 보호 기술 표준화. P2P 그룹 키 관리 기술, 협업을 위한 상호 인증 기술, 아이디 보안 기술 등	ITU-T, IETF	KISA, ETRI	기획	제 / 개정
	P2P SIP	– P2P SIP 프로토콜 보호, 세션 관리, 도청 및 Spoofing 방지 기술 표준화	IETF	KISA, ETRI, 숭실대		
IPTV 보안	IPTV 키관리	– IPTV 키 관리 기술 표준화	DVB	TTA, ETRI, KISA	항목승인	개발검토
	트랜스코더블 보안	– 차세대 IPTV 환경에서 format, resolution, quality, frame-rate 변환시 종단간 보안을 보장하는 기술 표준화. secure transcoding, 키관리, E2E 보안 기술 표준화	ETSI	TTA, ETRI		
	Downloadable 보안	– IPTV 보안 서비스 제공을 위한 보안 모듈의 안전한 다운로드 및 구동을 위한 기술 표준화	CableLabs	TTA, ETRI, Alticast,LGCNS	최종검토	제 / 개정
	IPTV 보안 인프라	– IPTV 인프라 보호 기술 표준화	DVB	TTA, ETRI, KT, 삼성	기획	최종검토
	단말 Software 보안	– IPTV STB, mobile device에 대한 software보안 기술 표준화		TTA	기획	항목승인
	IPTV 콘텐츠 재분배 보안	– 차세대 IPTV 환경에서 IPTV 콘텐츠의 재분배를 위한 보안 기술 표준화. 보안 메커니즘 연동, 키연동, 라이선스 관리 등	DVB, ATIS	TTA, ETRI	개발검토	항목승인
TPM	차세대 신뢰보안 모듈 (Next TPM)	– 신뢰 컴퓨팅 기술 표준화 · 신뢰보안 프레임워크, 신뢰보안 메커니즘 · 디바이스/플랫폼 보호, 악성코드 탑재 방지용 무결성 측정 기술(IMVA: Integrity Measurement and Verification Agent) 등	ISO, 3GPP, OMTP	ETRI, 삼성, SKT	기획	개발 검토
	모바일 TPM	– 모바일 TPM 기술 표준화 · 모바일 TPM 보안 프레임워크, 메커니즘 · 디바이스/플랫폼 보호, 임베디드 장치 보호 등				
	다중통합인증(USIM, Smart, TPM)	– USIM, Smart TPM 기반 다중 통합 인증 기술 표준화				
	신뢰 네트워크 커넥션	– Network Access Protocol(NAP), Network Access Controller(NAC), Trusted Network Connect(TNC)로 유.무선 네트워크에서 신뢰 네트워크 커넥션 표준화				
	신뢰지원 SW 미들웨어	– 하드웨어 씨큐리티 기반인 TPM 및 Mobile TPM을 지원하는 미들웨어 표준				
	신뢰기반 가상화 플랫폼	– 데스크탑 및 모바일 플랫폼의 가상화 기술에서 virtual TPM을 지원하여 물리적인 TPM을 공유하는 표준				
LI	LI 보안 프레임워크	– 유무선 통신 매체를 통해 암호화되어 전송되는 음성, 데이터의 합법적 분석기술 표준화 · 보안 프레임워크, 시스템, 알고리즘, 프로토콜 등	ETSI, ATIS, TIA, 3GPP, IETF	ETRI, CORPA LG, 삼성, SKT, KT, 대우통신, 데이콤, 하나로통신, 머큐리, 현대시스콤	기획	항목 승인
	LI Handover 인터페이스	– 유무선 통신 매체를 통해 암호화되어 전송되는 음성, 데이터의 합법적 분석기술 표준화 · LI Handover interface			항목 승인	제 / 개정
웹 서비스 보안	차세대 웹 보안	– 차세대 웹 환경을 위한 보안 기술에 관한 표준화 · 웹 2.0 보안, 모바일 웹 2.0 보안 기술 · 차세대 웹 기반 융합 서비스 보안, SOA 기반 융합서비스 보안 기술 · 유비쿼터스 웹 보안, 시맨틱 보안 기술 등	ITU-T, W3C, OASIS	ETRI, KISA, TTA	기획	항목 승인
	모바일 웹 보안	– 모바일 웹 어플리케이션 및 단말을 위한 보안 기술 표준화 · 모바일 웹 어플리케이션 데이터 보호 기술 · 모바일 브라우저 보안 기술			항목 승인	항목 승인
	웹 프라이버시 보호	– 웹서비스 환경에서의 프라이버시 보호 기술 표준화 · 웹 프라이버시 정책 협상 기술 · 프라이버시 데이터 접근 제어 기술				
	SOA 보안	– SOA (Service Oriented Architecture)를 위한 보안 기술 · SOA를 위한 인증/인가 기술 · SOA 메시지 보안 기술 · SOA기반 서비스를 위한 보안 정책 기술				
보안 평가	보안성 평가기준(CC)	– CC(Common Criteria) 인증을 위한 보안성 평가기준 및 체계의 표준화	ISO/IEC JTC1 Sc27, ITU-T	KISA, ETRI	개발 검토	개발 검토
	보안성 평가 방법론(CEM)	– 표준 적합성 시험 및 보안성 평가 방법론				
	PP & ST 작성 가이드라인	– 보안평가를 위한 보호 프로파일(PP) 및 보안목표명세서(ST) 작성 가이드라인 표준화				
	암호 모듈 시험 요구사항	– 암호모듈에 대한 구현 적합성 시험 등 암호 모듈 시험 요구사항 표준화. CMVP 평가(암호모듈검증프로그램)				

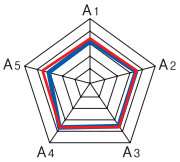
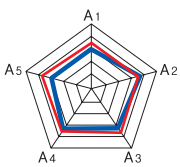
표준화 대상항목 (중점 표준화항목)		표준화 내용	대응 표준화기구	국내참여 기관/업체	표준화수준	
					국내	국제
보안 관리	정보보안 거버넌스 프레임워크	– 조직의 목적 및 전략을 지원하고, 정보자산의 보안 관리를 위한 정보보호의 조직화/제도화 등의 표준화	ISO/IEC JTC1 SC27, ITU-T SG17	KISA, ETRI, 중앙대	기획	항목 승인
	정보보안 성과측정 지침	– 정보보호 성과 측정을 위한 기준, 방법론, 지침 등의 표준			항목 승인	개발 검토
	정보보안 경영 시스템 구현 지침	– 정보보안 경영시스템 구축을 위한 가이드라인 표준				
	정보보안 관리구현 지침	– 정보보호관리체계 계획 수립 및 구현, 운영지원, 감시 및 검토하는 프로세스에 관한 표준화, 지침 및 기법 등				
	정보보안 사고관리 지침	– 정보보안 사고 발생시 체계적인 대응 및 대책 추립을 위한 사고관리 지침 표준				
	정보보안 아웃소싱 지침	– 정보보안 아웃소싱 지침에 대한 표준				

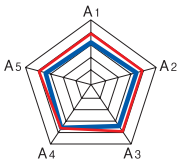
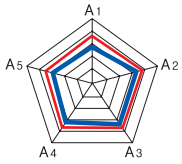
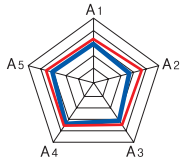
■ 중점 표준화항목별 중기(3개년) 표준화로드맵



■ 중점 표준화항목별 세부전략(안)

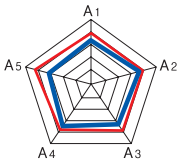
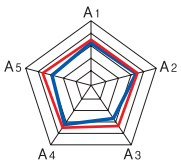
* A1: 국외대비 국내 표준화 수준, A2: 국외대비 국내 기술개발 수준, A3: IPR 확보 가능성, A4: 국내 표준화 인프라 수준, A5: 국제표준화 기여도　　* 파란색: Ver.2009, 빨간색: Ver.2010

중점 표준화항목	세부전략(안)
u-기기기반 지식정보관리 프레임워크	* 국제표준화 전략목표 : 국제표준 선도(Ver.2009) → 국제표준 선도(협력/경쟁)(Ver.2010)
	• MPEG-21, OMA에서는 DRM 표준화를 추진하였고, 국내 표준화를 위해서 TTA에서 DMB-CAS, EXIM 표준화를 추진하며, CAS를 SW 형태로 다운로드하여 단말 트러스트를 제공하는 지식보안 기술 표준화와 관련하여 오픈케이브랩스에서 표준화를 추진중에 있으므로, 국제 표준화에 적극 참여 • 음악 보호 파일에 대한 상호연동을 위해 EXIM을 표준화하였으나, 서비스 사업자간 호환성과 과금 방식에 추가 표준화가 필요한 상태 • CAS와 DRM 등 개별 기술에 대한 표준화는 제정되어 있으나 연동 측면에서의 고려는 부족하기 때문에 transcoding 기법 역시 고려되어 있지 않으므로 CAS와 DRM의 연동을 위한 인터페이스, 콘텐츠 및 정보에 대한 저작권과 리스트에 대한 관리 방안 및 기기 및 서비스, 사용자에 따른 지능적 Transcoding 기술에 대한 표준화 계획 및 제정이 요구됨 • 국내에서는 SW 및 실명ID 기반의 DRM, CAS 등의 지식보호 솔루션을 개발 및 상용화를 진행하고 있으나, 복합지식 보호 및 프라이버시 보호기술 표준화가 요구됨 • 전용 디바이스 단위로 권한관리를 추구하는 음악지식(MP3)에 대한 보호 솔루션은 있으나, 자신 소유의 타 디바이스로 구매 지식의 이동 불가로 사용자 불편을 초래하고 있어, 이에대한 기술 개발과 더불어 표준화가 요구됨 • 사용자 창작/수정/재가공 지식에 대한 지재권보호 및 지분표현 기술 분야 개발이 미약한 수준이므로, 기술개발과 표준화를 동시에 추진함 • DRM과 CAS에 급격한 개발과 연구 이후에 시장이나 연구가 둔화되고 있는 상황에서 기술적 연동은 시장의 확산과 기술적인 확장, 서비스의 개발로 이어질 것이며 이를 위해서는 현재 기술들에 대한 표준과 기술의 기업 간의 상호 연계가 수행되어야 하며 이에 대한 정부에서의 정책적 지원이나 관리가 요구됨 • CAS, DRM에 대한 IPR은 존재하고 활용되고 있으나 기술적인 부재와 연동을 위한 기업 간의 기술 교류의 부족으로 현재 연동을 통한 기술적 요소, Transcoding 기술 등의 연동을 위한 기술 요소에 대한 IPR은 기술 융복합화와 함께 다양한 분야에서 생성이 가능할 것으로 기대됨 • 국내 인터넷 인프라는 세계 최고 수준이므로, 이를 잘 활용하여 새로운 지식 서비스 산업 및 다양한 비즈니스 모델이 발굴될 수 있도록 기술 개발 및 표준화가 요구됨 • 유무선 네트워크 및 지능형 기기, 사용자 정보에 기반한 통합 시스템이 다양하게 발전되어 있는 상태이므로 연동 기술의 개발과 적용을 통해서 충분히 세계 시장과 표준에 적용이 가능한 상태까지 발전이 가능할 것으로 전망되며 따라서 기술의 융합과 적용을 위한 정책적인 지원이 필요함 • MPEG-21, OMA, DVB-CPCM, DHWG, TV-Anytime, OpenCableLab등에서 관련 분야의 표준화가 진행되고 있거나 시작되고 있으며, 향후 상용화를 위한 보다 상세한 규격화가 예상되므로, de factor 기술 분야에 표준화에 적극 참여하여야 함 • TTA에서 국내 표준화를 진행한 후, ITU-T SG17을 통한 국제표준화를 추진하며, CAS나 DRM에 대한 국제 표준의 선도적인 역할을 수행하도록 진행함
동시표준	* IPR확보가능분야 : USN 보안 미들웨어
PP미디어 스트리밍 네트워크 보호	* 국제표준화 전략목표 : 국제표준 협력/경쟁(Ver.2009) → 국제표준 선도(협력/경쟁)(Ver.2010)
	• IM (Instance Message)관련 표준화는 IETF에서, 보안 프레임워크 분야는 ITU-T SG17에서 보안 요구사항, 프레임워크를 중심으로 표준화가 완료되었으므로, P2P 응용 보안 분야에서 신규 표준화 아이템 발굴이 필요함 • Live P2P Television이 등장하는 등 P2P 기반 미디어 스트리밍 네트워크 보호 시장이 점차 확대될 것으로 예상되며, 이에 대응하기 위한 국 제 표준을 제안하여 추진하는 전략이 필요함. • P2P 미디어 스트리밍 네트워크 보호 기술 및 이를 IPTV 등 신규 응용 분야에 적용하기 위한 요구사항 및 프레임워크 표준화 추진이 필요함 • 국외의 경우 PPStream, Livestation, PPLive, YouTube 등 다수의 상용 및 비상용 서비스가 제공되고 있으며 일부 보안 기술이 탑재되고 있으나, 현재까지는 독자적인 스팩을 정의하고 개발하고 있어 이에 대한 표준화가 요구됨 • 국내에서 개방형 IPTV 서비스에 대한 요구가 급증하는 상황에서 P2P 기반의 IPTV 서비스 제공을 위한 표준화 아이템 발굴이 시급함 • 기술개발 수준은 국외에 비해 취약하나 현재 관련 표준화가 미흡한 상황이고, 참조 표준이 될 수 있는 ITU-T의 P2P 보안 프레임워크 표준을 국내에서 개발 완료한 만큼 국제표준을 제안하여 추진하는 것이 충분히 가능함 • 국내 P2P 응용 서비스 이용 규모에 비해 특허 건수는 상대적으로 적은 편이므로, P2P 미디어 스트리밍 네트워크 구축을 위한 동적인 멤버 관리 기술, 오버레이 멀티캐스트 키 관리 기술, 인증 기술 등 신규 분야의 IPR 확보에 집중 • ITU-T 표준화 활동을 주도하고 있지만, IETF 활동은 저조한 상태이므로, 활발한 국내 표준전문가 활용이 필요하며, 또한 기술개발 수준이 국외에 비해 상대적으로 취약하므로 표준화와 함께 관련 기술개발을 병행하는 전략이 필요하며, ITU-T의 표준화에 기여가 매우 높으므로, 국내 표준전문가의 활동을 장려하여 상대적으로 강점이 있는 ITU-T SG17을 통해 신규 표준화를 제안하여 추진
동시표준	* IPR확보가능분야 : 안전한 Ad-Hoc 보안 라우팅

중점 표준화항목	세부전략(안)
IPTV 보안 인프라	★ 표준제준화 전략목표 : 국제표준 선도(Ver.2009) → 국제표준 선도(Ver.2010)
	• TTA 산하 PG504에서 SVC(Scalable Video Coding)영상에 적용 가능한 암/복호화 방식과 가이드라인을 제시하며, SVC 기반의 차세대 IPTV 서비스 구축을 위한 미디어 보안 지침서로 활용이 가능한 "스케일러블 비디오 코딩 암/복호화 가이드라인"의 표준화를 추진하고 있음 • TTA IPTV PG 산하 Mobile IPTV 실무반(WG2193)에서 Seamless 서비스 구조 및 이종망간의 핸드오버 등을 고려하여 SVC 기술의 적용에 대한 표준화 작업방향과 연계하여 스케일러블 정보보호 기술의 국제표준화를 선도하기 위한 적극적인 추진과 정책지원이 필요함 • 디지털 컨버전스의 가속화로 특정 디바이스에 종속된 형태의 현재의 보안기술로는 차세대 IPTV 서비스에서 요구되는 중간 노드에서의 미디어 변환과정과 콘탠츠의 댁내 재사용시에 종단간의 보안을 보장할 수가 없으므로, 전송환경과 디바이스의 특성 및 종류에 따라 중간노드에서 콘텐츠를 안전하게 변환하고 소비자 댁내에서 재사용할 수 있는 안전한 보안기술이 필요함 • 국내 방송사, 학계 및 연구기관에서 공동으로 연구개발 중에 있는 스케일러블 정보보호 기술인 Layered Protection Scheme 기술과 Protection Encoding Scheme기술에 대해 IPR 발굴 및 선행확보를 위한 지속적이고 적극적인 원천기술 개발이 필요 • 국내 IPTV 인프라는 세계 최고 수준이므로, 이를 잘 활용하여 새로운 보안기술을 적용한 다양한 비즈니스 모델이 발굴될 수 있도록 기술 개발 및 표준화가 요구되며, 국내 보안솔루션 업체의 독자적인 D-CAS 개발경험 등 표준화 추진을 위한 기반은 마련되어 있지만 다양한 보안기술에 대한 전문지식을 갖춘 보안 표준전문가의 육성 및 확보가 시급하며, 정부의 적극적인 지원이 절실 • MPEG-21, ITU-T SG17 등에서 관련 분야의 표준화가 진행되고 있거나 검토되고 있으며, 향후 상용화를 위한 보다 상세한 규격화가 예상되므로, de factor 기술 분야의 표준화에 적극적인 참여가 필요 • TTA에서 국내 표준화를 진행한 후, ITU-T SG17을 통한 국제표준화 추진을 위하여 연구소, 방송사 및 보안업체와의 상호협력을 통한 국제표준화 공동대응이 필요
선행표준	* IPR확보가능분야 : -
모바일 TPM	★ 국제표준화 전략목표 : 국제표준 협력/경쟁(Ver.2009) → 국제표준 선도(협력/경쟁)(Ver.2010)
	• 무선인터넷포럼과 TTA를 통하여 2007년부터 표준화를 진행하고 있으며, TCG의 활동 분야 중 TPM와 mobile phone 분야 등의 표준화를 주도하여 국제표준화를 선도 • 국내에서 모바일용 TPM을 개발하고 있고, 타 업체는 아직 검토 단계이므로, 기술개발 시기에 맞추어 표준화를 진행할 필요하며, TCG의 표준화 진행과 업체들의 관련 기술 개발이 동시에 이루어지고 있으므로, 기술개발과 함께 표준화를 추진 • TCG에 다수의 표준문서 존재(TPM, TSS, MTM 등) 하고 있으며, 국내에서는 이미 국내/국제 특허와 논문을 확보하고 있으며, 모바일 TPM 개발에 사용된 다수의 기술들의 IPR 확보에 주력 • 국내에서는 이미 기술개발 경험이 풍부한 전문 인력을 확보하고 있으므로, TCG에서 표준화에 참여 • 관련 표준화는 TCG에서 표준화를 활발히 진행 중이고, 3GPP, OMA, ITU-T와도 liaison을 통한 표준화 추진 예정에 있으나, 국내 표준 전문가의 기여는 매우 저조하다. TTA를 통한 국내 표준화 활성화와 함께 ETRI, 삼성, 스프레드텔레콤, 프롬투 등 국내 산,학,연 공동의 표준화 참여가 요구
동시표준	* IPR확보가능분야 : 다수 AP들간의 인증 및 통신보안 및 절차분야
LI 보안프레임워크	★ 국제표준화 전략목표 : 국제표준 협력/경쟁(Ver.2009) → 국제표준 협력/경쟁(Ver.2010)
	• 기존의 감청 분야에서는 통신망 운용 형태에 따른 감청이 주를 이루었으나, 암호화된 데이터가 네트워크를 통해 전송되는 부분에 대해서는 기술 개발 및 표준화가 전무한 상태이다. 기술 개발과 함께 국제 표준화 단체 (ITU-T)를 통한 표준 제안을 활발히 추진 • 라우터 장비 등에서 감청은 이미 성숙기에 있지만, 암호화된 데이터에 대한 분석은 아직 초기단계에 머무르고 있으므로, 이 분야에서의 표준화 활동에 집중 • ETSI에 관련 표준문서 다수 존재하고 유선망에서의 감청 분야 기술은 포화된 상태이므로, BcN 기반의 신규 서비스망에서 암호화된 데이터에 대한 합법적인 분석 방법 및 구조 분야에서 IPR 확보에 주력 • 인터넷 인프라의 확대와 더불어 국내외적으로 암호화된 정보에 대한 합법적인 분석 기술에 대한 요구가 높으며, 시기 적절한 표준의 제정이 뒤따르지 않으면 상용화 시기의 선점을 위해 해외 선도 업체의 기술을 그대로 도입할 가능성이 높음 • 수 년 전까지 국제표준화의 중요성이 상대적으로 작았던 것이 사실이나 최근 (아시아 권역에서) 국제표준화의 중요성 부각과 함께 국가간 연동이 가능한 표준 개발이 요구되고 있어, 관련 분야의 시장성이 매우 큰 만큼 국내표준화인프라의 양적인 확장뿐만 아니라 질적인 성장이 필요한 시점으로 판단된다. 따라서 국내표준의 선행활동을 활발히 전개 하고 이를 국제표준으로 연계하는 형태로 체제의 전환이 필요 • 이 분야에서의 국제 표준화는 유선망에서의 감청 분야에 중점을 두고 있어 암호화된 정보에 대한 분석 분야의 기술 개발 및 표준화는 상대적으로 활동이 적은 편이다. 이와 더불어 국내 연구 개발 활동도 매우 저조하여 국제 표준화기여도는 매우 낮게 평가되고 있음. 따라서 기술적인 유사성을 근거로 하여 기존 국제 표준을 일부 수용하되, 암호화된 정보 분석을 위한 국제 표준을 선도할 필요가 있음
후행표준	* IPR확보가능분야 : 이종망간 Mobility 보안기술

* A1: 국외대비 국내 표준화 수준, A2: 국외대비 국내 기술개발 수준, A3: IPR 확보 가능성, A4: 국내 표준화 인프라 수준, A5: 국제표준화 기여도

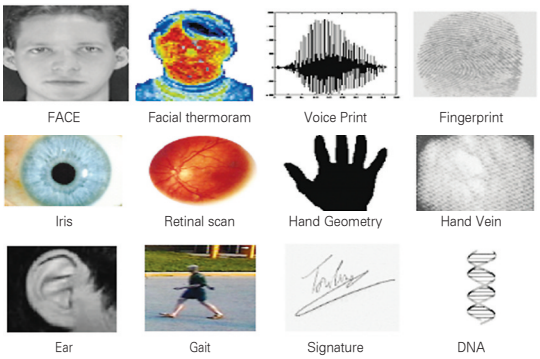
* 파란색: Ver.2009, 빨간색: Ver.2010

중점 표준화항목	세부전략(안)
차세대 웹 보안	*** 국제표준화 전략목표 : 국제표준 선도(Ver.2009) → 국제표준 선도(일부 수용/적용)(Ver.2010)**
	• ITU-T, W3C, OASIS 주도의 표준화 활동이 지속될 것으로 전망됨 • ITU-T에서는 SG17에서 웹서비스 보안 표준화를 담당하고 있으며, 국내에서 개발한 모바일 웹서비스 보안 구조가 표준화가 완료되었고 2008년 하반기부터 차세대 웹기반 융합서비스 보안에 대한 국제 표준 (ITU-T X.websec-4)을 우리나라 주도로 개발하고 있어 차세대 웹 보안 분야 표준화 추진에 유리한 위치에 있음 • ITU-T SG17에서는 2009년부터 시작된 새로운 회기 동안 차세대 웹 보안에 관한 표준 개발이 본격적으로 추진되리라고 전망됨 • 따라서, ITU-T에서 차세대 웹기반 융합서비스 보안 표준에 대한 지속적인 주도적 개발 및 웹 2.0 보안, SOA 기반 융합서비스 보안, 유비쿼터스 웹 보안 등의 차세대 웹 보안 분야에 대한 신규 표준화 항목 추가 발굴 및 적극적인 국제 표준화 추진이 필요함 • 비즈니스 응용에서의 웹서비스 보안 기술 및 웹 방화벽 기술 등은 비교적 기술 개발 결과가 많은 편이나, 차세대 웹 및 SOA 기반 융합서비스 보안 기술, 모바일 웹 2.0 보안 기술, 유비쿼터스 웹 보안 기술, 시맨틱 보안 기술 등은 국내외 적으로 기술 개발 초기 단계이므로, 이러한 분야의 기술개발 및 표준화를 추진 • 국내외적으로 비즈니스 영역에서의 웹 보안 기술은 상당수의 특허가 출원되어 있으나, 웹 2.0 기반 융합서비스, 유비쿼터스 웹, SOA 기반 융합서비스, 시맨틱 웹 분야에서의 보안 관련 특허 건수가 많지 않은 실정임 • 따라서 위의 분야에 대한 보안 기술 개발 및 IPR 확보에 주력 • 국내 기술 개발 및 표준화는 ETRI, KISA, TTA 등에서 이루어지고 있으며, ITU-T를 통해 국제 표준화를 추진하고 있음 • 우리나라는 세계적으로 인터넷 인프라가 발달하였으며, 웹기반 서비스가 널리 활용되고 있지만 그에 비해 웹 보안 분야에 대한 표준화 전문 인력은 아직 많지 않아 향후 산학연 웹 보안 전문가의 더욱 활발한 표준화 참여가 필요함 • 웹 보안, SOA 보안 핵심 기술들은 W3C 및 OASIS, ITU-T 등에서 활발히 표준화가 진행되어 이미 다수의 표준이 승인된 상태임 • 하지만 세계적으로 웹 2.0 보안, 차세대 웹기반 융합서비스 보안, SOA 기반 융합 서비스 보안, 유비쿼터스 웹 보안, 시맨틱 보안 기술 등 차세대 웹 보안 관련 기술은 표준화 초기 단계에 있기 때문에 ITU-T, W3C, OASIS 등에서 보다 적극적으로 표준화에 참여하여 국제 표준화를 추진하는 전략이 필요함 • 특히 국내에서 주도적으로 개발하고 있는 차세대 웹기반 융합서비스 보안 표준에 대한 지속적인 주도적 개발 및 신규 표준화 항목 추가 발굴 필요
동시표준	* IPR확보가능분야 : 증거자료 분석
정보보안 거버넌스 프레임워크	*** 국제표준화 전략목표 : 국제표준 협력/경쟁(Ver.2009) → 국제표준 선도(Ver.2010)**
	• 최근 기업 거버넌스, IT 거버넌스에 대한 요구사항이 높아지고 있으며 기업의 사회적 책임이 강조되는 현실에서 정보보호 거버넌스에 대한 수요도 점차 점증되고 있음 • 현재 미국과 일본은 정보보호 거버넌스 지침을 발표했거나 2009년 하반기에 발표할 예정 • 국내도 보유 기술을 기반으로 보안관리 업체들과 협력체계를 구축하고, 기술의 시장 적용을 통한 상용화 추진 및 표준화 요구사항 도출. ISO, ITU의 보안관리 분야에 대한 국제표준 개발의 집중화 필요 • 현재 정보보호 거버넌스에 대한 초기 연구가 진행되었으나 거버넌스 구현을 위한 구체적인 연구가 필요하며 이의 현실 적용가능성을 실증 분석할 필요가 있음 • 이를 기반으로 정보보호 컨설팅 업계와 협력하여 현실적인 정보보호 거버넌스 구현 방법론을 개발할 필요가 있으며, 사례 연구를 통해 거버넌스의 확산을 위한 노력을 기울일 필요가 있음 • 현재 관련 IPR은 없으며, 학계에서 일부 논문을 발표하고 있음 • 전략적으로 국내 관련기술의 IPR을 확보할 수 있도록 산?학?연?관의 긴밀한 협력 및 체계적인 연구 및 개발의 접근이 필요 • 정보보호 거버넌스의 중요성을 전문가들은 인식하고 있으나, 실무에서는 그 필요성을 충분히 인식하지 못하고 있으므로, 국제 표준화 동향의 소개 및 미국, 일본의 관련 지침 등을 배포하는 것이 필요 장기적으로 관련 법/제도의 정비를 통해 최고경영층에 대한 정보보호의 역할과 책임을 강조할 필요 있음 • 정보보호 거버넌스 구현을 위한 구체적 지침을 수립하여 국내/국제 표준화에 실질적인 선도적 역할 추진 • KISA, 관련 산업체 및 단체에서 국제표준화의 적극적인 참여와 건설적인 협조 • 정보보호 거버넌스의 인식 확대 및 전문가의 결집을 위해 정보보호 거버넌스 포럼 설립 고려
동시표준	* IPR확보가능분야 : 스토리지 데이터 암호화 기술, 클라우딩 환경의 적합한 인증기술

바이오인식

■ 기술개요

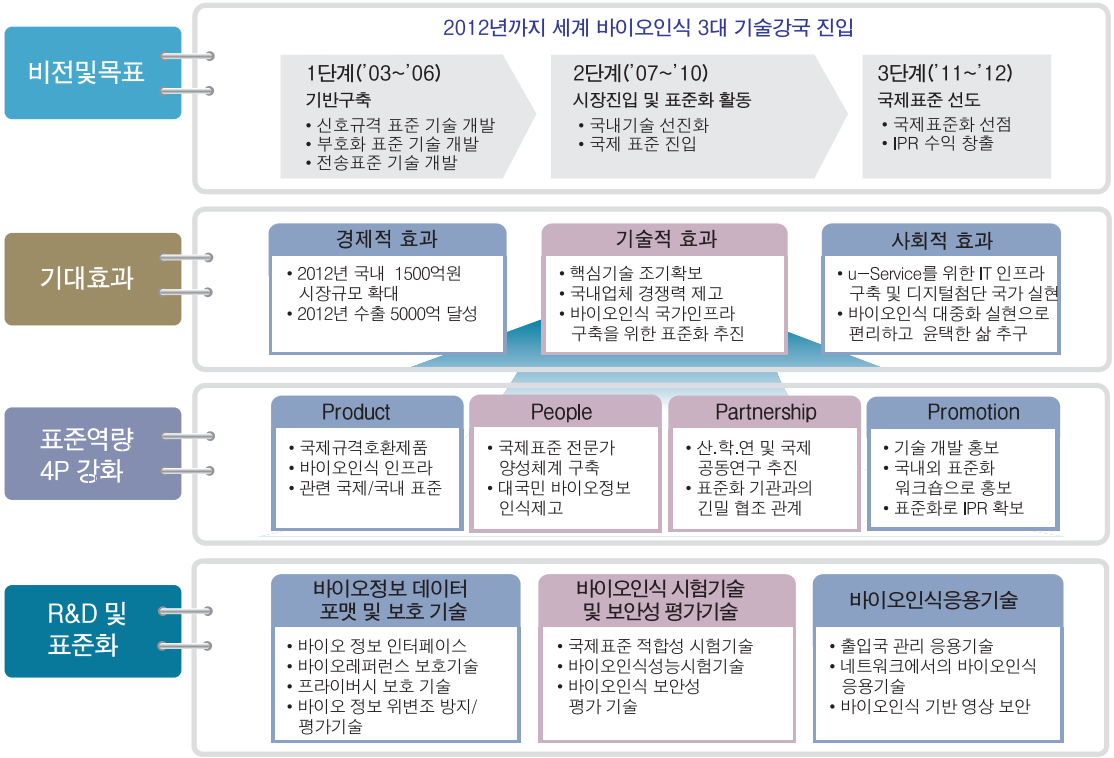
- 개개인으로부터 평생불변과 만인부동의 특성을 갖는 특징을 찾아 이를 자동화된 수단으로 등록 · 저장하여 제시한 바이오정보와 비교 · 판단하는 기술
- 지문 · 얼굴 · 홍채 · 망막 · 정맥 등의 신체적 특성을 이용한 방법과 서명 · 음성 · 걸음걸이 등의 행동학적 특성을 이용하는 방법 등이 상용화 됨



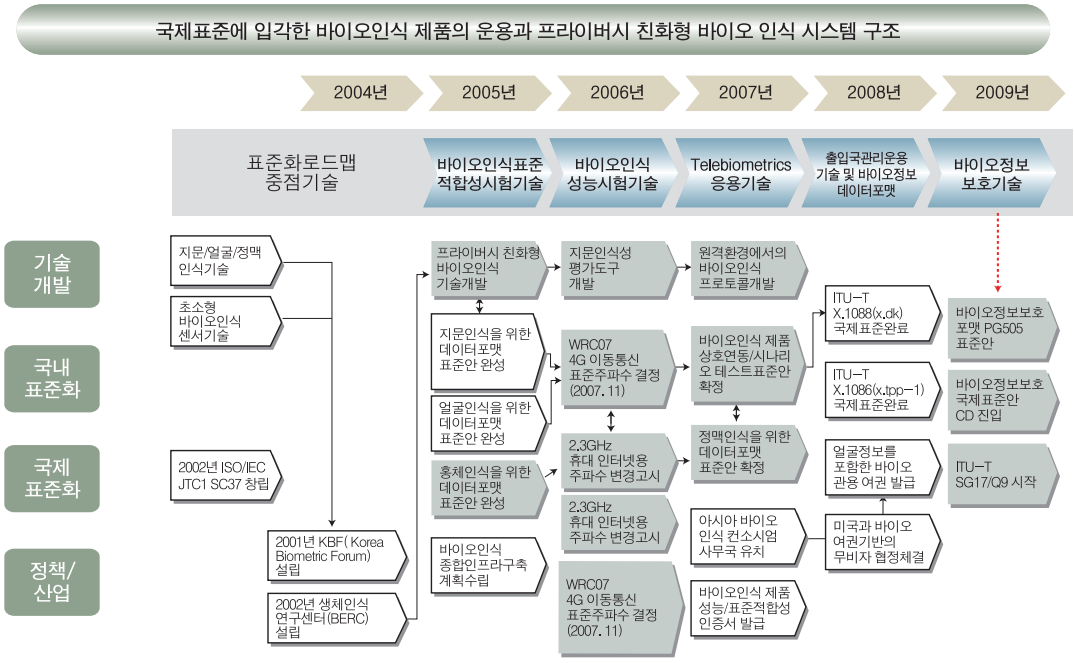
■ 표준화의 필요성

- UN 산하 국제민간항공기구(ICAO), 국제노동기구(ILO), 국제표준화기구(ISO, ITU) 등 전세계적으로 국제공항, 항만, 육로상의 출입국심사에 신원확인 핵심기술로서 바이오인식이 세계적으로 널리 확산되고 국내외 바이오인식 시장규모가 현저히 증가(국외 10%, 국내 15%)하는 추세이며 미국, 영국, 일본 등 주요 선진국에서 바이오인식 세계 시장선점을 위하여 앞다투어 국제표준화를 추진함에 따라, 바이오인식 관련 국내외 표준개발 및 보급이 시급히 필요

■ 표준화의 비전 및 기대효과



■ 연도별 주요현황 및 이슈

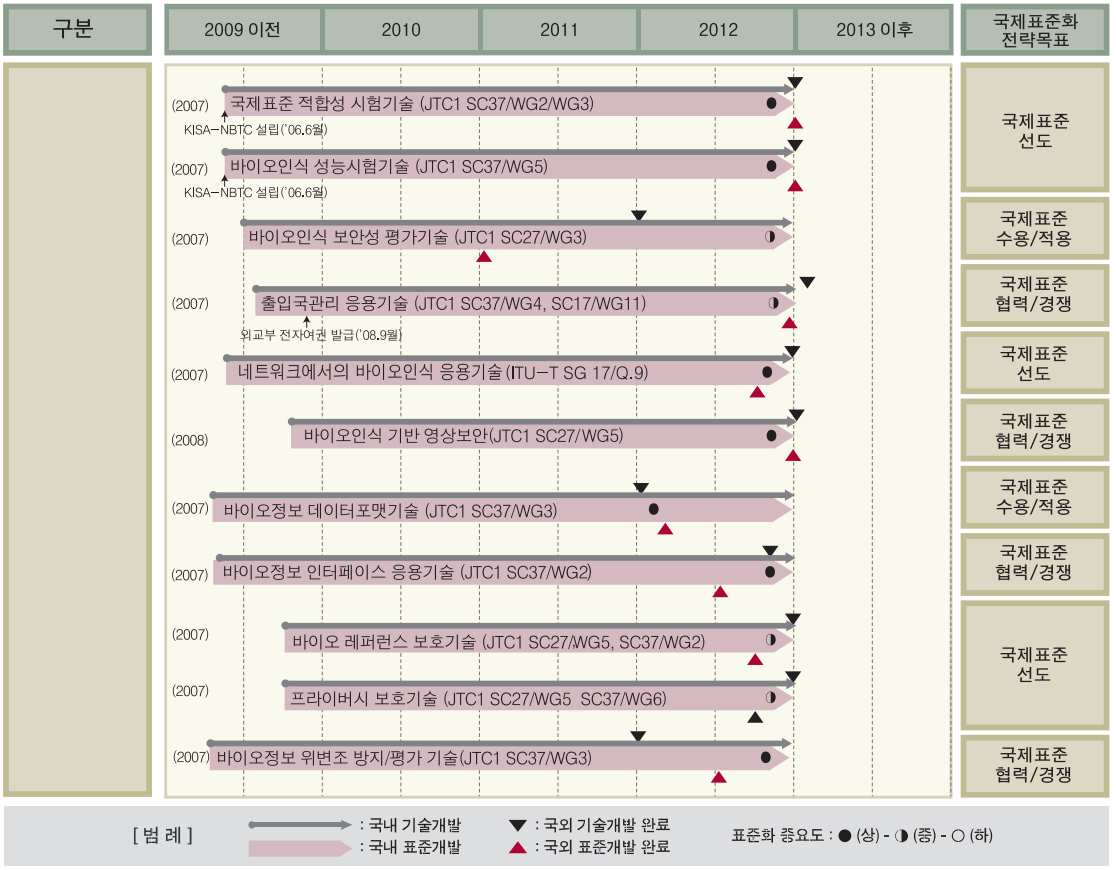


■ 표준화 대상항목

표준화 대상항목 (중점 표준화항목)		표준화 내용	대응 표준화기구	국내참여 기관/업체	표준화수준	
					국내	국제
바이오 인식 시험 기술 및 보안성 평가기술	시험 · 인증절차, 시험기준	– 바이오인식시스템 시험·인증절차, 시험기준 및 평가방법론	ANSI, NIST JTC1 SC27/37	KISA,인하대, KBA회원사	개발/ 검토	개발/ 검토
	국제표준 적합성 시험기술	– BioAPI, CBEFF, 바이오인식 데이터포맷 등 국제규격에 대한 적합성 시험방법 · 절차, 시험명세서(DNA,정맥)	ANSI,BSI,BioAPI Consortium, DoD BMO, NIST, NPL, JTC1 SC37	KISA,인하대,IC카드 연구센터,KBA회원사 일부 기업체,BERC	개발/ 검토	개발/ 검토
	바이오인식 성능시험기술	– 입력장치, 인식알고리즘, 제품, 운영환경 시험방법 및 시험결과 표준포맷				
	바이오정보 상호연동 시험기술	– 지문, 얼굴, 홍채 등 각 데이터 상호연동	ANSI, NIST JTC1 37	KISA, 인하대	개발/ 검토	개발/ 검토
	바이오인식 보안성 평가기술	– 신원확인 보안관리(SC27/WG5) 바이오정보기반 신원확인 보안관리 프레임워크 – 보안성 평가기술(SC27/WG3) CC(Common Criteria)기반 보안성 평가방법?절차	DoD BMO, NIST,NPL,TUViT,IPA,JTC1 SC27	KISA, 국보연	개발/ 검토	개발/ 검토
바이오 인식 응용기술	출입국관리 응용기술	– 출입국관리용 응용프로파일(SC37/WG4) – 바이오인식기반 선원 신원 검증 및 식별 – 공항직원용 바이오인식 출입통제 키오스크 (KIOSK)시스템 운영관리 지침(SC17/WG4)	ANSI, BSI, NIST, DoD BMO, NPL, TUViT, JTC1 SC17/27/37, ITU-T SG17	KISA,ETRI, KBA회원사, ISP/SI 사업자, IC카드 연구센터, 인하대	표준 기획 및 일부 항목 승인	개발/ 검토
	네트워크에서의 바이오인식 응용기술	– 텔리바이오정보 기반 전자서명(X.tdk) – 텔리바이오정보 보안대책 가이드라인(X.tpp1-2) – 바이오정보 통신보안 프로토콜(X.tsm1-2) – PKI기반 바이오정보 보안인프라(X.tai) – One-time 템플릿 기반의 바이오 인증 프레임워크(X.ott) – 바이오인식 기반 원격의료 통합 프레임워크(X.tif)-응용				
	바이오인식 기반 영상 보안	– 물리보안과 결합한 바이오인식 융합기술 표준 – CCTV				
	스마트카드를 이용한 바이오인식 응용기술	– 국제통용 ID카드 응용기술(SC17/WG11) – 공무원증, 전자여권, 전자주민증, 의료정보, 국제운전면허증 (conformance test), 금융 IC카드(보안 적합성, 표준 적합성)	JTC1 SC17/37	KISA IC카드연구센터, KBA회원사 일부 기업체	개발/ 검토	개발/ 검토

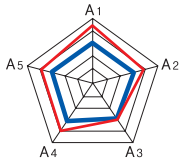
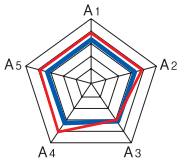
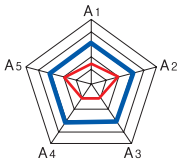
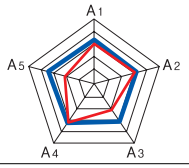
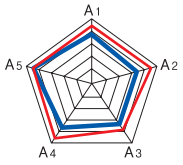
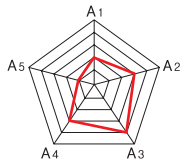
표준화 대상항목 (중점 표준화항목)		표준화 내용	대응 표준화기구	국내참여 기관/업체	표준화수준	
					국내	국제
바이오 정보 데이터 포맷 및 보호 기술	바이오인식 용어 표준	– JTC1 SC17, 27, 37 등 바이오인식 표준용어	JTC1 SC17/27/37	KISA KBA 회원사	표준기획및 일부 항목 승인	개발/검토
	다중 바이오인식기술	– 다중 바이오인식기술 정합기술	ANSI, BioAPI Consortium, NIST, JTC1 37	KISA,인하대,충북대,KBA회원사 일부 기업체,BERC	개발/검토	개발/검토
	바이오정보 데이터 포맷기술	– 지문 · 얼굴 · 홍채 · 서명 · 정맥 · 손모양 · 음성 · DNA 등 바이오인식 데이터에 대한 호환규격	ANSI, BSI, JTC1 SC37	ETRI, BERC, 인하대, 충북대, KBA 회원업체	개발/검토	개발/검토
	바이오정보 인터페이스 응용기술	– BioAPI 인터페이스 응용기술 – BioAPI Lite – BIP(BioAPI Interworking Protocol) – BioAPI를 이용한 10指 指紋 채취방법 – CBEFF 데이터 공통전송 포맷 – CBEFF Patron 포맷				
	바이오 레퍼런스 보호기술	– CBEFF 보안블럿 포맷(SC37/WG2) – 바이오인식 템플릿 보호기술(SC27/WG5)	ANSI, BSI, NIST, IBIA, UK–BWG, JTC SC27/SC37, ITU–T SG17	KISA, ETRI, KBA 회원사 일부기업체, BERC	개발/검토	개발/검토
	프라이버시 보호기술	– 상용 바이오인식 응용제품에서 개인정보 보호 등 프라이버시 침해 예방을 위한 고려사항				
	바이오정보 위변조 방지/평가기술	– 위조 지문/얼굴/홍채 검출 성능 평가기술 – 위조 지문/얼굴/홍채 취약성 평가기술				

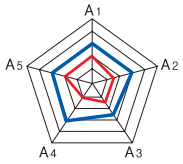
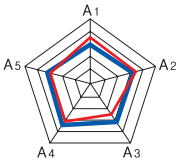
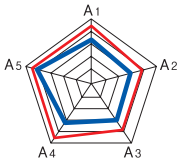
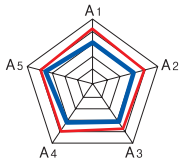
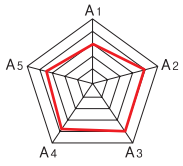
■ 중점 표준화항목별 중기(3개년) 표준화로드맵



■ 중점 표준화항목별 세부전략(안)

* A1: 국외대비 국내 표준화 수준, A2: 국외대비 국내 기술개발 수준, A3: IPR 확보 가능성, A4: 국내 표준화 인프라 수준, A5: 국제표준화 기여도　　* 파란색: Ver.2009, 빨간색: Ver.2010

중점 표준화항목	세부전략(안)
국제표준 적합성 시험기술	*** 국제표준화 전략목표 : 국제표준 선도(Ver.2009) → 국제표준 선도(Ver.2010)**
	• KISA 바이오인식정보시험센터(K-NBTC)에서 CBEFF 표준적합성, 바이오인식 데이터 포맷 적합성 시험기술을 주요 선진 연구기관과 공동으로 개발하여, ISO/IEC JTC1 SC37 국제표준화를 선도하도록 집중하고 이를 선도적인 국제표준을 국내 실정에 적합한 국내표준으로 수용할 필요성이 절대적임 • 또한, 적용기술의 IPR 확보와 함께 국내제품에 적극 적용이 요구됨
선행표준	IPR 확보가능분야 : 표준적합성/성능/상호연동시험분야
바이오인식 성능시험기술	*** 국제표준화 전략목표 : 국제표준 협력/경쟁(부분선도)(Ver.2009) → 국제표준 선도(Ver.2010)**
	• KISA 바이오인식정보시험센터(K-NBTC)를 통하여 시나리오기반 제품 성능시험과 운영환경기반 바이오인식시스템 성능 시험기술을 주요 선진 연구기관과 공동으로 개발하여, ISO/IEC JTC1 SC37 국제표준화를 적극 추진할 필요가 있음
선행표준	IPR 확보가능분야 : 표준적합성/성능/상호연동시험분야
바이오인식 보안성 평가기술	*** 국제표준화 전략목표 : 국제표준 협력/경쟁(Ver.2009) → 국제표준 수용/적용(Ver.2010)**
	• JTC1 SC27을 통하여 바이오인식 보안성 평가기술 국제표준이 독일 중심으로 개발중에 있으며, 이를 국내표준으로 수용하여 CC기반의 바이오인식 국산제품에 대한 보안성 평가를 추진할 계획임 • 국내 적용가능한 얼굴 · 홍채의 보호프로파일(Protection Profile)을 인증기관과 협의할 필요가 있음
선행표준	IPR 확보가능분야 : 보안성 평가방법
출입국관리 응용기술	*** 국제표준화 전략목표 : 국제표준 협력/경쟁(Ver.2009) → 국제표준 협력/경쟁(Ver.2010)**
	• 선진국과의 국제 협력을 통한 전자여권, 출입국관리서비스 등 정부 시범사업에서의 국제표준 호환성 및 정확성 보장을 추구 • 관련 국내 SI 사업자와의 산학연관 협업체계 구축을 통한 국내/외 표준화 추진
선행표준	IPR 확보가능분야 : 전자여권단말기
네트워크에서의 바이오인식 응용기술	*** 국제표준화 전략목표 : 국제표준 선도(Ver.2009) → 국제표준 선도(Ver.2010)**
	• 원격의료, CCTV등 수요가 급증하고 있는 도메인의 바이오인식기반 네트워크 환경을 면밀히 분석하여, 특정 네트워크 기반 바이오정보 보호에 대한 지속적인 연구를 통하여 국제표준화와 연계할 필요가 있음. • Telebiometric 원격의료 기술 표준 제정과 ITU-T SG17 Q.9(Telebiometrics) 국제표준화를 선도하는데 집중하여 Telebiometrics 응용기술 국제표준을 적용한 상용 국산제품 개발로 유도하여 신규 시장창출에 박차를 가할 필요가 있음.
선행표준	IPR 확보가능분야 : 원거리바이오인식
바이오인식 기반 영상 보안	*** 국제표준화 전략목표 : 국제표준 협력/경쟁(Ver.2010)**
	• 국내표준화 수준 및 국제표준화 기여도가 낮은 상황을 극복하기 위한 표준화 인력 강화 및 국제적인 표준화 활동을 강화 전략이 필요 • IPR 확보 가능성이 높은 분야이므로, 주요 기술의 경우에는 IPR 확보와 국내/외 표준화 추진을 병행 • ETRI에서 연구중인 바이오인식,영상보안기술등의 결과물을 적극 활용하여 국내/외 표준화를 추진
선행표준	IPR 확보가능분야 : 원거리바이오인식

중점 표준화항목	세부전략(안)
바이오정보 데이터 포맷기술	***국제표준화 전략목표** : 국제표준 협력/경쟁(Ver.2009) → 국제표준 수용/적용(Ver.2010)
	• JTC SC37을 통한 바이오인식 데이터 포맷기술의 국제표준화 추진과 더불어 국립과학수사연구소 및 해당업체, 학계가 데이터 포맷 등과 관련된 유기적이며 지속적인 연구를 통하여 국제표준화와 연계할 필요가 있음
선행표준	IPR 확보가능분야 : 알고리즘융합기술분야
바이오정보 인터페이스 응용기술	***국제표준화 전략목표** : 국제표준 협력/경쟁(Ver.2009) → 국제표준 협력/경쟁(Ver.2010)
	• BioAPI, CBEFF 등 주요 인터페이스 규격은 이미 JTC1 SC37 국제표준으로 제정되었으나 BioAPI Lite, 10指 指紋 채취방법, 유무선 이동기기 및 Telebiometrics용 인터페이스 등과 같은 응용기술에 대하여 KBA, SC37-Korea 전문위원회에서 국내 연구가 필요한 실정이다. • 간결성이나 적용의 용이성 측면에서 실용적인 Framework free BioAPI에 대한 연구가 필요하다. • 실질적인 바이오인식 기능 제공을 제공하는 Biometric Function Provider와 관련한 연구가 필요하다.
선행표준	IPR 확보가능분야 : 알고리즘융합기술분야
바이오 레퍼런스 보호기술	***국제표준화 전략목표** : 국제표준 협력/경쟁(Ver.2009) → 국제표준 선도(Ver.2010)
	• JTC1 SC27을 통한 템플릿 보호기술의 국제표준화 추진과 더불어 BERC, ETRI, KBA를 통한 바이오정보 레퍼런스 데이터 보호에 대한 지속적인 연구를 통하여 국제표준화와 연계할 필요가 있음. • 바이오전자 여권발급 사업의 본격 시행으로 이를 시행하는 업체의 바이오인식 레퍼런스 보호 기술을 국내외 표준안에 적극 반영할 필요가 있음
선행표준	IPR 확보가능분야 : 템플릿보호, 보안대책기술
프라이버시 보호기술	***국제표준화 전략목표** : 국제표준 협력/경쟁(Ver.2009) → 국제표준 선도(Ver.2010)
	• 바이오정보보호 가이드라인 개정안, 바이오정보 프라이버시 보호대책 등에 국내 보급은 있었으나 관계부처와 함께 프라이버시 보호를 위한 국가 전반에 걸친 보안대책에 법제도 정립이 필요한 실정임. 바이오정보를 포함한 전자여권 발급 사업 등을 통해 얻어진 운영 know-how 등을 국내외 표준안으로 개발해 나가야 함
선행표준	IPR 확보가능분야 : 템플릿보호, 보안대책기술
바이오정보 위변조 방지/평가기술	***국제표준화 전략목표** : 국제표준 협력/경쟁(Ver.2010)
	• BERC, 인하대와 관련기업들이 개발한 바이오정보 위변조 탐지 기술에 대해 K-NBTC (KISA)에서 성능평가를 수행하고, 국가 전자여권사업 및 출입국간소화사업에 활용할 수 있도록 함 • 활용 결과를 바탕으로 국내 기술표준으로 개발한 후, ISO/IEC JTC1/SC37 및 ITU-T/SG17 WP2/Q.9에 국제표준으로 제안함
선행표준	IPR 확보가능분야 : 템플릿보호, 보안대책기술