암호 · 인증 · 권한관리

기술개요

암호 · 인증 · 권한관리는 정보통신망을 통한 정보의 안전한 전송 및 이용, 정보통신망 상의 상대방에 대한 신원확인, 정보통신망을 통한 불법적인 접근을 통제하기 위한 기반기술로, 암호기술은 정보통신망을 통한 안전한 정보의 송수신을 위한 프리미티브로서 암호 알고리듬, 암호 키 관리기술, 암호 응용기술 등으로 구분되며, 인증기술은 정보통신망에서 상대방의 신원을 확인하기 위한 기술로서 PKI, 익명인증기술, 디바이스 인증기술로 분류되며, 권한관리기술은 정보통신망을 통해 정보를 이용하고자 하는 자가 적절한 권한을 가지고 있는지를 판단하기 위한 것으로서 PMI, 하드웨어 기반의 접근제어 등으로 구분

표준화의 필요성

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

표준화의 비전 및 목표

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

1단계('08~'10)
선도가능분야를 선별하여
국제표준화 우선 추진

2단계('10~'15)
기 개발된 국내표준을 토대로 국제표준화 추진
– 암호분야별 1건, 인증권한관리 분야 5건

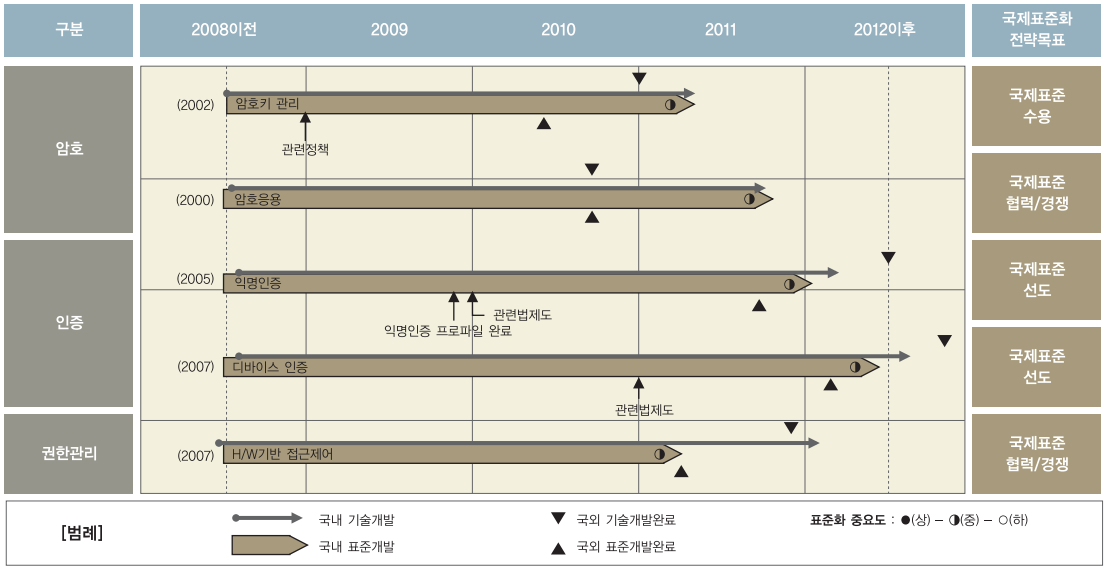
표준화 대상항목

* 0 (매우 낮음) 〈 "전략적 중요도 및 기술적 파급효과" 〈 1 (매우 높음)

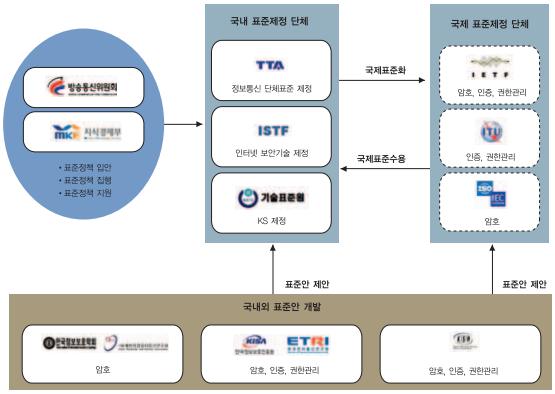
표준화 대상항목 (중점 표준화항목)		정의	전략적 중요도	기술적 파급효과	대응 표준화기구	국내 참여 기관/업체	국내 개발주체	
							표준개발	기술개발
암호	암호 알고리듬	블럭 암호 알고리듬, 스트림 암호 알고리듬, 공개키 암호알고리듬, 키분배 알고리듬, 해쉬 알고리듬, 전자서명 알고리듬, 난수발생기 및 양자 암호알고리듬 등으로 분류	0.50	0.45	IETF ISO/IEC JTC1 ITU-T	KISA ETRI KIISC TTA	TTA 기술 표준원	산업체 연구소 학계
	암호 키 관리	개인키 암호화 기술, 패스워드 기반의 암호화 기술, 비밀정보 교환기술, 보안토큰내의 비밀정보 저장기술, 암호 키 복구 기술 등 암호 키를 안전하게 생성 · 분배 · 복구 · 폐기하는 기술	0.61	0.66				
	암호 응용 기술	암호메시지 전송기술, 암호토큰 인터페이스 기술, 암호기반 다중 인증기술 등 응용서비스에서 암호 기능에 대한 공통 플랫폼을 제공하는 기술. 또한 기존 암호기술을 기반으로 유비쿼터스 환경에 적용 가능하도록 경량화 시키는 기술	0.65	0.72				
인증	PKI(Public Key Infrastructure)	인증서 프로파일, 인증서 관리 프로토콜, 인증서 운영프로토콜, 인증서 검증 프로토콜, 사용자 인터페이스 기술, 전자서명 키 보호기술 등을 이용하여 전자거래에서 부인방지, 무결성, 인증 등의 정보보호 서비스를 제공하기 위한 기술	0.43	0.49	IETF ITU-T	KISA ETRI TTA	TTA	
	익명 인증(Anonymous Authentication)	웹사이트 가입, 성인인증 등 개인의 실명이 필요 없는 곳에서 프라이버시 보장을 위해 가명 또는 익명을 사용할 수 있도록 보장하면서 익명성 남용을 방지하기 위한 기술로서 익명인증체계, 익명인증서 프로파일, 익명인증 프로토콜, 익명인증서 검증기술, 익명에 대한 추적기술 등으로 분류	0.71	0.67				

표준화 대상항목 (중점 표준화항목)		정의	전략적 중요도	기술적 파급효과	대응 표준화기구	국내 참여 기관/업체	국내 개발주체	
							표준개발	기술개발
	디바이스인증(Device Authentication)	CCTV, 휴대단말기, 지능형 가전 등 네트워크에 참여하는 디바이스에 대한 신뢰된 인증서비스를 제공하기 위한 기술로써, 디바이스인증체계, 디바이스인증서 프로파일, 디바이스환경에서의 인증서 관리 및 검증 기술, 전자서명 키 보호기술 등으로 구분	0.75	0.76				산업체 연구소 학계
권한관리	PMI(Privilege Management Infrastructure)	속성인증서 프로파일, 속성인증서 관리프로토콜, 속성인증서 운영프로토콜, 속성인증서 검증프로토콜, 사용자 인터페이스 기술 등 속성인증서를 이용하여 사용자에 대한 권한을 관리하기 위한 기술	0.41	0.42	IETF ITU-T	KISA ETRI TTA	TTA	
	H/W 기반 접근제어	OTP, 스마트카드, RFID, USB토큰 등 하드웨어를 기반으로 권한관리 프로토콜, 권한관리 API, 관한관리 운영지침 등으로 분류	0.68	0.71				

중점 표준화항목별 중기(3개년) 표준화로드맵

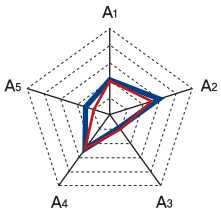
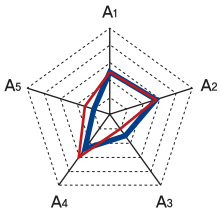
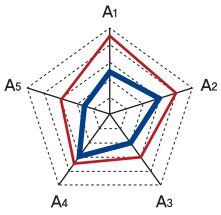
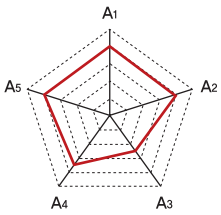


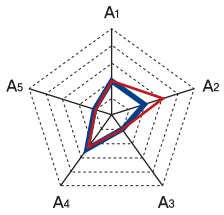
표준화 추진체계



중점 표준화항목별 세부전략(안)

* A_1: 국외대비 국내 표준화 수준, A_2: 국외대비 국내 기술개발 수준, A_3: IPR 확보 가능성, A_4: 국내 표준화 인프라 수준, A_5: 국제표준화 기여도

중점 표준화항목	현황분석 (파란색: Ver.2008, 빨간색: Ver.2009)	세부전략(안)
암호키관리		국제표준화 전략목표: 국제표준 수용/적용(Ver.2008) → 국제표준 수용/적용(Ver.2009) – 국제적으로 암호키 관리 기술에 대한 연구 및 표준화는 진행이 되었으나 서비스는 활성화 되지 않는 것으로 판단되기 때문에, 암호키 관리 서비스 분야에 대한 표준화 아이템을 발굴하여 IETF KeyProv 워킹그룹 등에서 국제 표준화 추진 – 암호키 관리 관련 국내 표준화 인프라는 국외에 비해 많이 부족하다고 판단되며, 국내 독자 표준 개발이 어려운 암호알고리듬 및 응용기술에 대한 표준화 인프라 확보를 위한 정부 및 산 · 학 · 연 전문가들의 적극적인 참여가 요구되며, 암호키 관리 서비스 분야에서의 IPR 확보는 가능 IPR확보가능분야 | ECC실현 기술분야, 패스워드기반 인증 및 키 교환
암호 응용기술		국제표준화 전략목표: 국제표준 협력/경쟁(Ver.2008) → 국제표준 협력/경쟁(Ver.2009) – 암호토큰 인터페이스 등과 같은 고전적 암호응용기술은 이미 국내외 적으로 표준화 추진이 완료되었기 때문에, OTP, RFID 등에 활용되는 암호응용기술에 대해 국제 경쟁력 있는 표준안을 TTA에서 선행 개발하고 이를 기반으로 IETF, ITU-T 등에서 국제 표준화 선도 – 암호 메시지 전송, 암호토큰 인터페이스 등과 같이 국제 표준화가 완료된 분야에 대해서는 필요한 표준을 국내에 수용하여 표준화 추진 – 하지만, 국제적으로 경쟁력이 있는 암호응용기술에 대해서는 적극적인 국제 표준화 추진을 통해 해당 기술에 대한 국제적 선도 기반 마련 IPR확보가능분야 | Decoy상태에 대한 양자 암호 원천기술 및 각종 상용화를 위한 요소기술분야
익명 인증		국제표준화 전략목표: 국제표준 협력/경쟁(Ver.2008) → 국제표준 선도(Ver.2009) – 국내에서 독자 개발한 익명인증 기술에 대한 국내 TTA 표준화 및 IETF 보안그룹 PKIX 워킹그룹에서 국제 표준화 추진이 필요함 – 익명인증서 프로파일, 익명인증 프로토콜 등 익명인증에 필요한 기술에 대한 국내외 표준화 추진 중 IPR확보가능분야 | 익명인증 프로토콜 및 서비스 분야
디바이스인증		국제표준화 전략목표: 국제표준 선도 – ITU-T SG17 등에서 홈네트워크 에서의 디바이스 인증 관련 표준이 추진되고 있으며, 향후 디바이스 인증에 대한 표준화 활성화 예상 – 홈 네트워크 디바이스 인증, CCTV 등 다양한 기기에 대한 인증기술에 대해 ITU-T 등을 통해 국제 표준화 추진 – 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 판단 IPR확보가능분야 | CCTV, URC 로봇, RFID 다양한 디바이스 및 서비스분야

중점 표준화항목	현황분석 (파란색: Ver.2008, 빨간색: Ver.2009)	세부전략(안)
H/W 기반 접근제어		국제표준화 전략목표: 국제표준 수용/적용(Ver.2008) → 국제표준 협력/경쟁(Ver.2009) – ITU-T, IETF 등에서 하드웨어 기반 접근제어 관련 표준화를 추진 중에 있기 때문에 관련 표준화 기구를 통해 국내 기술에 대한 표준화 추진 – 전적인 하드웨어 접근제어 기술 뿐 아니라 OTP, 바이오인식 등을 이용한 하드웨어 접근제어 기술에 대한 표준안 개발 필요 – 바이오 인식 기술의 경우 ITU-T, TTA 등 국내외 표준화 기구를 중심으로 활발히 표준화가 진행 중에 있으며, OTP 관련 기술은 '09년부터 국내를 중심으로 개발 예정이며 해당 기술에 대한 산 · 학 · 연 전문가 검토를 통해 국제 표준화 추진 IPR확보가능분야 | 이동성을 고려한 ID-LOC 맵핑시스템