ID관리 / 개인정보보호

1. 개요

1.1. 중점기술개요

1.1.1. 중점기술 및 표준화 대상항목의 정의

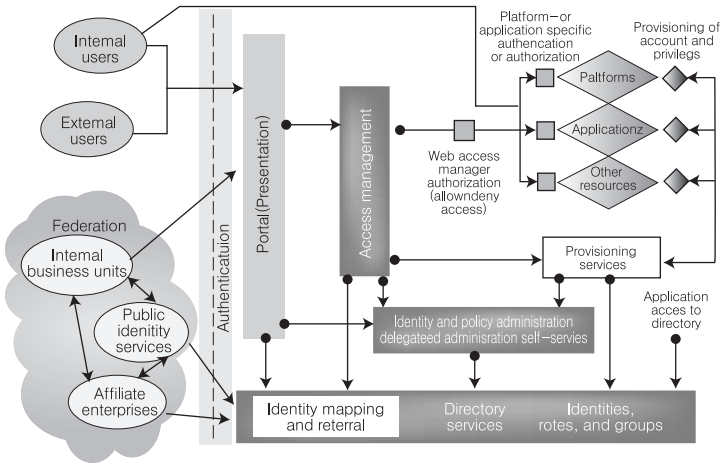
• 중점기술의 정의

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 정책으로 요약할 수 있음. ID관리 및 개인정보보호 기술은 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 기술임

- ID1)는 사이버스페이스 상에서 개인식별을 가능하게 함으로써 개인의 안녕과 이해관계에 영향을 미치는 모든 정보로서 식별자(Identifier, id)와 속성들(Attributes)로 구성되며, '공공기관의개인정보보호에관한법률' 제2조 2항에 정의된 개인정보2)와 유사한 의미로 쓰일 수 있음. 또한 ID를 ITU-T에서는 엔티티를 설명하고 인식하기 위한 속성 또는 엔티티에 대해 알려진 속성들로 정의하고 있으며, Liberty Alliance와 OASIS(Organization for the Advancement of Structured Information Standards)의 SAML(Security Assertion Markup Language)에서는 엔티티가 지닌 속성들로 설명되는 엔티티의 본질로 정의하며, OpenGroup에서는 지역, 기업, 국가, 글로벌 같은 지정된 콘텍스트 내에서 객체를 유일하게 식별할 수 있는 기본 개념으로 정의하고 있음
- ID관리 기반 기술은 ID관리의 기반이 되는 기술로, Identity를 식별할 수 있는 식별자, ID 생성과 유통, 저장, 관리를 위한 공통 프레임워크, 인증, 권한, 속성 정보를 표현하는 보안 토큰, ID 서비스를 발견하는데 사용되는 서비스 디스커버리, ID의 개념과 관계를 정의하는 Identity Ontology, ID 공유를 위한 ID 공유 기술, 통신 당사자들 간의 신뢰관리 및 보안 토큰의 보증 수준을 평가하는 Identity Assurance 기술 등으로 구성됨
- 개인정보보호 기술은 사용자의 개인정보를 보호하기 위한 기술 및 정책으로, 개인정보 획득에 따른 의무와 이용범위 등에 대한 개인정보보호 정책, 개인정보 이용과 제공을 위한 사용자 동의를 받기 위한 상호작용 기술, 사용자 개인정보 DB 보안 기술, 사용자단말 개인정보 관리 기술 등으로 구성됨
- ID관리 응용 및 기타 기술은 ID관리 기반 기술과 개인정보보호 기술에 대한 응용 기술로서, 네트워크상에서의 ID 인증 및 접근제어, 사용자가 본임임을 확인하는 본인확인 기술 등으로 구성됨
- ID관리 시스템은 ID관리 기반 기술, 개인정보보호 기술 및 ID관리 응용 및 기타 기술이 통합적으로 운용되는 시스템으로 〈그림 1〉은 Burton Group에서 제시한 ID관리 시스템의 구조도임

1) ID는 Identity의 약어로 본 문서에서는 문맥에 따라 병행하여 사용함

2) '개인정보' 라 함은 생존하는 개인에 관한 정보로서 당해 정보에 포함되어 있는 성명 · 주민등록번호 등의 사항에 의하여 당해 개인을 식별할 수 있는 정보(당해 정보만으로는 특정개인을 식별할 수 없더라도 다른 정보와 용이하게 결합하여 식별할 수 있는 것을 포함한다)를 말함



〈그림 1〉 ID 관리 시스템 구조도

• 표준화 대상항목의 정의

구 분	정 의	표준화 대상항목	표준화 내용
ID관리 기반	ID 정보의 식별자, 의미, 형식, 공유, 서비스 디스커버리 와 공통 프레임워크 및 신뢰관리 기술과 같이 ID관리의 기반이 되는 표준	Identity 식별자 체계	멀티도메인에서 식별 가능한 식별자의 정의 및 생성 · 관리 규격
		Identity 시스템 공통 프레임워크	유무선 환경에서 ID 생성, 저장, 유통, 관리 서비스를 위한 공통 프레임워크 규격
		Security Token 관리	인증, 권한 및 속성, 익명 정보를 포함한 보안토큰의 생성 및 검증 규격
		Identity 서비스 디스커버리	ID 서비스 발견 메커니즘과 메타데이터의 질의 및 응답 프로토콜 규격
		Identity Ontology	시스템 간 자동화된 정보의 교환과 이용이 가능하도록 정의된 ID의 개념과 관계
		Identity Sharing	ID 정보 공유를 위한 메시지 형식과 프로토콜 규격
		신뢰관리-Assurance	통신 당사자 간의 협상을 통한 신뢰구축 메커니즘, 보안토큰 메시지 및 전송 규격, 보안 토큰의 보증 수준 및 서비스 및 크리덴셜 평가 기준
개인정보보호	개인정보보호 정책, 상호작용 서비스, 개인정보 DB 보안, 사용자단말 개인정보 관리와 같이 사용자 개인정보의 보호를 위한 표준	개인정보보호 정책	개인정보 획득에 따른 의무와 이용범위 등에 대한 정책 생성, 공개, 검토를 위한 형식
		Interaction Service	개인정보 이용과 제공을 위해 사용자 또는 대리인의 동의를 받기 위한 상호작용 서비스 프로파일
		개인정보 DB 보안	개인정보의 최종 저장소인 데이터베이스에 대한 사전 접근통제, 데이터 암호화, 감사 등의 다양한 보안기술
		사용자단말 개인정보 관리	사용자 단말에서 입력되는 다양한 정보 보호 기술, 저장되는 정보에 대한 보호 기술 그리고 정보를 안전하게 표시하는 기술 및 규격
ID관리 응용 및 기타	네트워크 상에서의 인증, 접속제어, 본인확인 기술과 같이 ID관리 응용과 관련된 표준	네트워크 ID 인증 및 접근제어	안전한 네트워크 서비스를 위해 네트워크 접속자의 Identity를 바탕으로 인증하고 접근 제어하는 기술
		본인확인 기술	온라인 상에서 서비스 사용자가 실제 해당 사용자 본임임을 확인할 수 있도록 해 주는 기술

- ID 식별자 체계 표준화는 서로 다른 도메인 간에서도 사용자의 ID를 유일하게 구분· 확인할 수 있는 식별자의 생성, 분석, 관리를 위한 규칙 등을 정의하며, URI(Uniform Resource Identifier), IRI(Internationalized Resource Identifier), XRI(eXtensible Resource Identifier), OpenID 등의 최근 인터넷 표준 식별체계 기술들을 참조함. URI, IRI는 IETF(Internet Engineering Task Force)와 W3C에 의해 제정된 웹 주소 표준으로 인터넷 자원들의 구체적 주소를 표현하는 URL(Uniform Resource Locator)과 지속성을 보장하기 위한 추상적 주소를 표현할 수 있는 URN(Uniform Resource Name)으로 구성됨. OASIS에서 표준화를 진행 중인 XRI는 추상화되고 구조화된 식별체계를 가지며 도메인, 위치, 응용 분야, 통신 프로토콜 등에 무관한 고유 식별자를 정의할 수 있는 방법을 제공하나 URI와 달리 인터넷에 추가적인 식별 시스템

들을 구축해야 하는 어려움이 있음. OpenID는 하나의 URI로 인터넷 사용자를 유일하게 식별해주는 기술로 Web 2.0 환경에 적합한 기술로 보급이 확산되고 있음

- 프레임워크 표준화는 ID의 생성, 저장, 유통, 폐기와 같은 생명주기 관리 서비스를 위한 공통의 프레임워크 규격을 정의하여, 이를 바탕으로 ID 응용 간 상호운용성 문제를 해결하고 ID 응용기술 개발과 이용을 촉진함. 프레임워크 표준화는 ID 관련 용어 표준, 다양한 연관 표준 수용과 상호운영을 위한 아키텍처 그리고 공통 API를 포함하며, 높은 보안과 프라이버시를 위한 운영 시나리오, 프로파일 등을 포함함

- 보안토큰은 서비스요청 주체(subject)가 서비스제공 주체의 서비스 이용을 지원하기 위해, ID관리 주체가 서비스요청 주체에게 발급하고 서비스제공 주체에게 전달하는 주장정보(인증, 권한, 기타속성 정보)를 통칭하며, SAML, Kerberos, X.509 등의 기술들을 통해 생성됨. 보안토큰은 주로 단일인증 및 권한관리 기술의 일부로 사용되어 왔으나 ID관리 기술의 발전과 새로운 요구사항이 대두되면서 사용자의 ID 정보를 전달하는 매개체로 이용되는 추세임. 예를 들어, Microsoft의 CardSpace와 같은 ID관리 기술은 SAML 보안토큰을 기반으로 사용자의 속성정보를 전달함. 보안토큰 표준화는 OASIS의 SAML 2.0, W3C의 WS-Security(Web Service Security), OASIS의 WS-Trust 등 기존 표준과의 상호운영성을 고려한 보안토큰의 생성, 전달, 검증, 이용에 관한 표준과 ID 공유기술 등과 같은 새로운 기술들에 대응할 수 있는 다양한 프로파일 규격을 포함함

- 서비스 디스커버리는 ID 열람권한을 획득한 주체(주로 서비스제공자 시스템)가 사용자 ID를 획득하기 위해, 사용자가 제공한 ID 식별자에 기반하여 ID 정보제공자의 ID 관련 서비스 위치와 사용되는 프로토콜, 보안 메커니즘 등을 확인하는 기술임. ID 열람 서비스를 제공하는 ID관리 주체는 외부에서 접근할 수 있는 서비스 인터페이스와 정책을 메타데이터 형태로 공개하고, 필요한 경우 서비스 요청 주체와의 협상을 통한 서비스가 가능하도록 함. 서비스 디스커버리 표준화는 서비스 위치, 프로토콜, 보안 메커니즘 등에 대한 메타데이터의 교환 프로토콜 및 메시지 포맷 등을 정의하며, YADIS, SXIP, Liberty Alliance 등의 기술을 사용하여 제공되는 디스커버리 서비스들 간의 상호운영성을 위한 프로파일을 정의함

- Identity Ontology는 시스템 간 자동화된 정보의 교환과 이용이 가능하도록 ID의 개념과 ID간 관계를 정의하고 관리하여 컴퓨터가 ID 관련 정보를 스스로 해석하고 처리할 수 있도록 하는 기술로, 특정 응용 도메인 또는 글로벌 도메인에서 교환되는 ID의 공통 사전·스키마에 대한 표준이 필요함. 또한 ID 정보 분석과 판단의 정확성을 높이기 위해 상황인식 정보(Context-Awareness) 등과의 연계를 위한 관련 표준화가 필요함

- ID 공유 표준화 항목은 동일 도메인 내에서 또는 연계된 도메인들 내에서 사용자의 정보를 주고받는 사업자 중심의 공유 기술과 사용자 정보가 해당 사용자를 거쳐 확인되어 전달되는 사용자 중심의 공유 기술을 다룸. ID 공유는 개인정보를 연계하는 매쉬업 서비스 등을 제공하거나 다양한 도메인 내에 분산화된 사용자 정보의 동기화에 필수적인 기술로, ID 공유 과정에서 발생할 수 있는 프라이버시 및 보안 위험 등을 분석하고 상호운영성 문제 등을 해결하기 위한 사전 연구가 필요함. 현재 개발되어 서비스 중이거나 개발 중인 공유 기술은 Liberty Alliance의 ID-WSF(IDentity Web Services Framework), CardSpace, XDI(XRI Data Interchange) 등이 있으나, 좀 더 발전된 형태의 서비스들이 계속적으로 등장할 것으로 예상됨

- 신뢰관리-Assurance는 통신 당사자 간의 협상을 통한 신뢰구축 방법과 보안토큰의 발급 요청·응답 프로토콜에 관한 것으로, 통신에 참여하는 참여자가 메시지를 교환하기 이전에 보안토큰의 종류, 보안 알고리즘, 키 정보, 메시지 포맷 등의 메타데이터를 교환하여 신뢰관계를 구축하는 메커니즘 등을 다룸. 또한 제출된 Credential에 대한 보증 정도와 서비스 및 Credential에 대한 평가 기준 등을 다루는 Identity Assurance를 포함함. 이와 관련된 기술은 WS-Trust, Liberty Alliance의 Identity Assurance Framework 등이 있으며, Microsoft의 CardSpace와 같은 ID 서비스는 이 기술에 기반을 둠

- 개인정보보호 정책 표준화 항목은 개인정보 획득에 따른 의무와 이용범위 등에 대한 정책 생성, 공개, 검토를 위한 형식을 마련하며 개인정보 공유에 대한 법규의 기반이 됨. 개인정보보호정책은 개인정보보호 관련 법률과 권고안에서 정한 범위를 준용하면서도 개인정보 취득자의 다양한 비즈니스 상황을 고려해 준비되어야 함. 개인정보보호정책 공개는 P3P와 같은 표준화된 기술을 사용하여 개인정보 제공자가 자기정보 제공시에 취득자의 의무와 이용범위 등을 폭 넓게 인식하고 제공여부를 결

정할 수 있는 방법이 제공되어야 하며, 이를 위해 개인정보제공자의 시스템에서 개인정보제공자를 대신하여 공개 정책을 분석하고 평가하여 사용자에게 보고할 수 있는 에이전트의 기능과 사용자 상호작용 메커니즘 등을 정의하여야 함

- 상호작용 서비스(IS, Interaction Service)는 개인정보획득자(서비스제공자)가 개인정보의 이용과 제공에 대한 사용자 선호도를 사용자 별로 수집 · 관리하거나 사용자의 사전 선호도 조사로 결정될 수 없는 범위에서는 개인정보 이용과 제공 시마다 사용자와의 상호작용으로 사용자 동의를 획득하기 위한 서비스임. 예를 들어 Liberty Alliance의 ID-WSF IS(Interaction Service)와 같은 명세는 웹서비스 제공자가 웹서비스 소비자에게 서비스 제공에 필수적인 소비자 정보를 해당 소비자의 ID관리 서비스로부터 획득하는 방법 및 ID관리 서비스가 요청된 정보를 전달하기에 앞서 소비자에게 동의를 얻는 메커니즘을 설명하고 있음. 상호작용 서비스 표준화는 상호작용 서비스를 제공하기 위해 필요한 공통의 스키마와 프로파일 등을 정의함

- 개인정보를 기반으로 사용자에게 허용되거나 커스터마이즈된 서비스를 제공하는 대부분의 공공기관 또는 기업들은 대용량 개인정보를 효과적으로 검색, 저장, 관리하기 위해 데이터베이스를 활용하고 있음. 개인정보 DB 보안 표준화는 개인정보를 최종적으로 저장, 관리하고 있는 데이터베이스에 대한 사전 접근통제, 중요 개인정보에 대한 암호화 및 개인정보 사용내역에 대한 사후감사 등 다양한 데이터베이스 보안기술에 대한 표준 및 가이드라인 개발을 포함하고 있음

- 사용자단말 개인정보 관리는 최근 그 활용도가 크게 증가하고 있는 스마트폰과 같은 다양한 사용자 단말 환경에서 ID 인증을 위한 입력정보를 비롯하여 ID 인증 자체를 보호하기 위한 다양한 정보 보호 기술, 개인이 작성하거나 전달받은 정보를 안전하게 저장하는 보호 기술 그리고 보유 정보 및 전달받은 정보를 안전하게 표시하는 기술 및 규격 등을 정의함

- 네트워크 ID 인증 및 접근제어 표준화는 3GPP(3rd Generation Partnership Project), 클라우드 컴퓨팅과 같은 네트워크 환경에서 ID 인증 및 접근제어 기술에 대한 표준화를 다룸. 3GPP에서는 GAA(Generic Authentication Architecture)와 GBA(Generic Bootstrapping Architecture) 표준을 정의하여 모바일환경에서의 클라이언트와 서버간의 상호인증을 수행함. GAA는 공유키 또는 인증서를 기반으로 상호인증을 수행할 수 있는 공통 아키텍처이며, 특히 GBA는 공유키를 생성하여 단말과 서버 간에 이를 공유하고, 이후 인증용도로 공유키를 사용할 수 있는 응용 독립적인 메커니즘을 규정함. 최근 연구개발이 활발히 진행되는 클라우드 컴퓨팅의 활성화를 위해서는 클라우드 컴퓨팅에 적합한 ID 인증 및 접근제어 기술이 필수적일 것으로 예상됨

- 본인확인기술은 웹사이트에 주민등록번호 대신 이용할 수 있는 개인식별번호로서 인터넷 상에서 주민등록번호가 무단으로 유출되어 도용되는 부작용을 막기 위한 서비스이며, 현재 국내 인터넷 서비스 환경에서 실명확인 또는 연령확인(성인인증)시에 입력되는 주민등록번호의 과도한 사용을 줄이기 위해 정부주도 하에 개발된 기술임. 현재 국내에서는 i-PIN(Internet Personal Identification Number)이 표준화되어 있고 국외에서는 ID-Proofing에 대한 연구가 활발히 진행되고 있음

• 표준화 대상항목의 그린 ICT 연관성

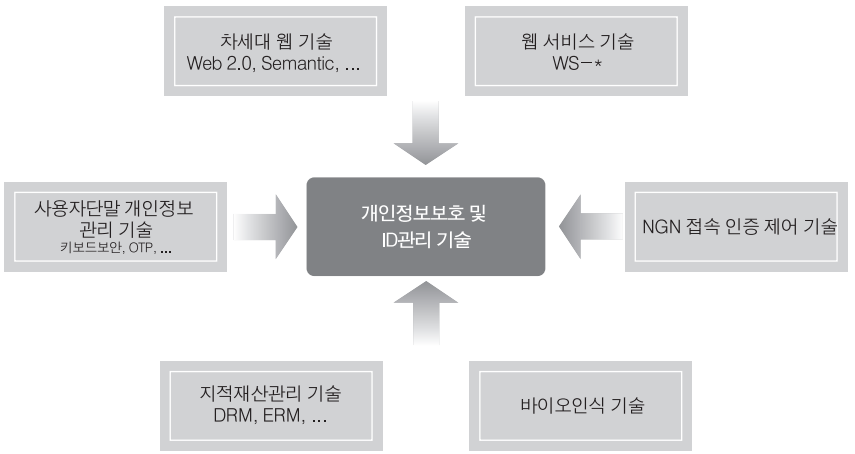
표준화 대상항목 (음영:중점표준화항목)	물건의 소비감소	전력 · 에너지 소비감소	인간의 이동 감소	물류의 이동 감소	공간 효율화	폐기물 감소	고 효율화 (업무 효율화)	비 고
identity 식별체계	-	-	-	-	-	-	-	-
Identity 시스템 프레임워크	-	-	-	-	-	-	◐	- 표준화된 시스템 프레임워크를 사용할 경우, 이기종 ID관리 시스템간에 발생하는 프로토콜 및 데이터 변환 과정을 거치지 않아도 되기 때문에 시스템 효율을 높일 수 있음
Security Token 관리	-	-	-	-	-	◐	-	- 다중으로 발급받는 토큰의 수를 줄임으로써 토큰의 사용종료 시 발생되는 폐기물을 감소시킬 수 있음
Identity 서비스 디스커버리								
Identity Ontology								
Identity Sharing	-	-	-	-	-	-	○	- 인터넷 서비스 등에 필요한 사용자 정보를 공유함으로써, 인터넷 서비스 제공 업체가 사용자 정보를 수집하고 관리하는데 소요되는 시간과 비용을 줄임으로써 업무의 고효율화를 달성할 수 있음
개인정보보호정책	-	-	-	-	-	-	-	-
신뢰관리-assurance	-	-	-	-	-	-	-	-
Interaction Service	-	-	-	-	-	-	-	-
개인정보보 DB보안								
사용자단말 개인정보 관리	-	-	-	-	-	-	-	-
네트워크 ID인증 및 접근제어	-	-	-	-	-	-	-	-
본인확인기술	-	-	○	-	-	-	○	- 인터넷을 통한 본인확인서비스를 통해 기존에 본인확인을 위해 필요한 신분증과 서류를 발급받기 위한 사용자의 이동을 감소시킬 수 있음 - 인터넷을 통한 본인확인서비스를 통해 기존 본인확인업무를 표준화된 방식으로 처리할 수 있기 때문에 중복되는 업무를 감소시켜 업무의 효율을 높일 수 있음

〈범례〉 -(관련없음) ○(소) ◐(중) ●(대)

1.1.2. 연관기술 분석

• 연관기술 관계도

- ID관리 및 개인정보보호 기술은 개인의 ID에 기반을 둔 모든 기술들과 연관될 수 있으나, 직접적 관계로 표현될 수 있는 기술들은 차세대 웹 기술, 웹서비스 기술, 지적재산관리 기술, 바이오 인식 기술 등이 있음



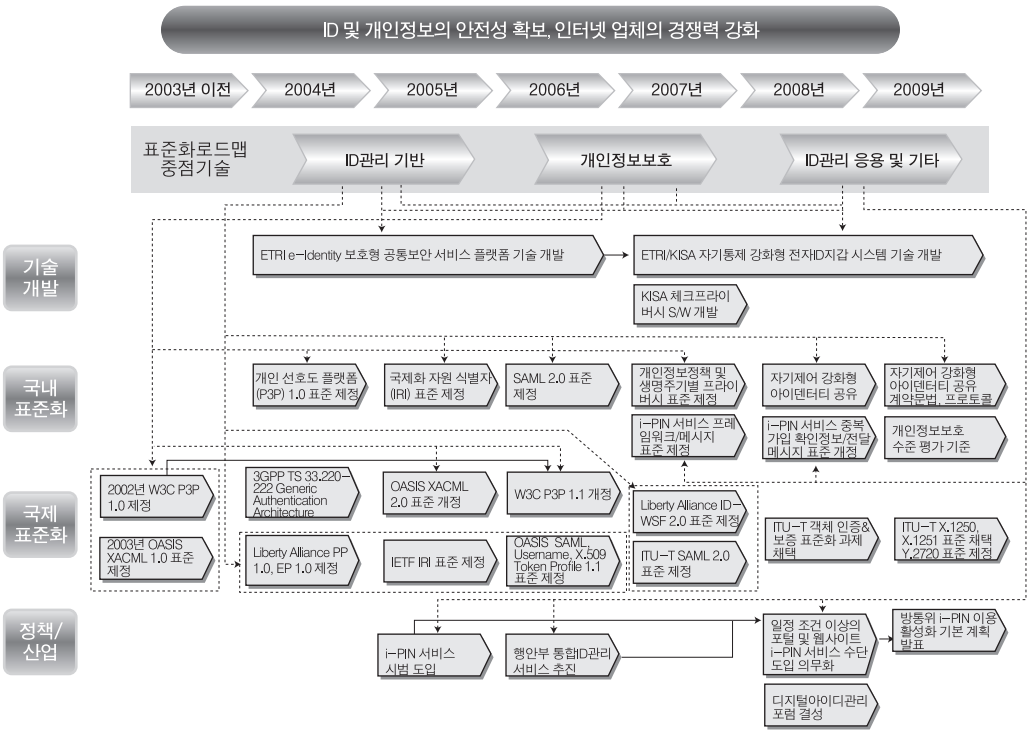
〈그림 2〉 ID관리기술의 연관기술 관계도

• 연관기술 분석표

연관기술	내 용	표준화기구/단체		표준화수준		기술개발수준	
		국내	국외	국내	국외	국내	국외
차세대 웹 기술 (Web 2.0, Semantic Web, etc.)	웹에 저장된 수많은 데이터에 컴퓨터가 처리 가능한 의미를 부여하여 높은 활용성을 제공하고, 현재의 웹보다 더 넓은 범위의 개방성, 이동성, 연결성 등을 제공하고자 하는 기술로, 차세대 웹에 좀 더 높은 신뢰성을 부여하고자 하는 노력으로 다양한 ID관리 기술이 적용되고 있음	TTA	W3C, OASIS	표준안 개발/검토	표준안 개발/검토	상용화	상용화
웹 서비스 기술 (WS-*)	서로 다른 종류의 컴퓨터들 간에 유연하고 확장적인 방법으로 상호작용할 수 있는 서비스 지향 분산 컴퓨팅 기술로서, 서비스 요청응답 주체의 확인, 상호인증, 서비스 제어, 안전한 메시지 전송 등을 위해서 ID관리 기술을 활용함	TTA, ECIF[3]	W3C, OASIS	표준안 개발/검토	표준화 완료	상용화	상용화
지적재산관리 기술 (DRM, ERM, etc.)	디지털화된 비디오, 오디오, 문서 등의 콘텐츠의 저작권자(개인, 조직, 정부)를 보호하고 안전하게 유통관리하기 위한 기술로서, 유통과정에서 발생할 수 있는 문제들을 해결하기 위해서 ID관리 기술을 채택함	TTA, DRM 포럼	IETF, MPEG, OMA, W3C 등	표준안 개발/검토	표준안 개발/검토	상용화	상용화
사용자단말 개인정보 관리 기술	접근 권한, 개인 인증 정보, 개인의 주요 정보 등을 안전하게 저장하고 전달하며 표시하는 역할을 담당하여 전자상거래를 비롯한 다양한 개인정보 유통을 보호하는데 사용됨	TTA/ ECIF	ISO/IEC JTC1 SC17	표준안 개발/검토	표준안 개발/검토	상용화	상용화
바이오인식 기술	사람의 평생불변 · 만인부동의 특성을 갖는 정보를 획득하여 등록 · 저장하고 이후 제시된 정보와 비교하여 본인인지 여부를 판단하는 기술로서, ID관리 기술에서 본인여부를 강하게 확인해야 하는 경우에 사용됨	TTA, KBA	SO/IEC IITU-T OASIS	표준안 개발/검토	표준안 개발/검토	상용화	상용화
NGN 접속 인증 제어 기술	NGN의 엑세스단에 접속 시도하는 단말을 식별, 인증하고 권한을 확인하여 망서비스에 접속하도록 configuration 하며, 접속을 위한 사용자 ID를 관리하는 기능을 포함함	TTA	ITU-T SG11, SG13	표준안 개발다수/ 계속 진행중	표준안 개발다수/ 계속 진행중	개발단계	시제품/ 프로토타입

3) ECIF : 전자상거래 표준화 통합 포럼

1.2. 중점기술의 연도별 주요현황 및 이슈



• 기술 개발
- 2004년 ~ 2006년 ETRI에서 e-Identity 보호형 공통보안 서비스 플랫폼 기술 개발
- 2007년 ~ 2008년 ETRI와 KISA에서 자기통제 강화형 전자ID지갑 시스템 기술 개발
- 2007년 KISA에서 체크프라이버시 S/W 개발

• 국제 표준화
- 2002년 W3C, P3P 1.0 표준 제정
- 2003년 OASIS XACML 1.0 표준 제정
- 2004년 3GPP Generic Authentication Architecture 기술 규격 제정
- 2005년 IETF, IRI 표준 제정
- 2006년 W3C에서 P3P 1.1 표준 제정
- 2006년 OASIS에서 SAML, Username, X.509 Token Profile 1.1 표준 제정
- 2007년 ITU-T, SAML 2.0 표준 제정
- 2008년 ITU-T, 객체 인증&보증 표준화 과제 채택

• 국내 표준화
- 2004년 개인 선호도 플랫폼(P3P) 1.0 표준 제정
- 2005년 국제화 자원 식별자(IRI) 표준 제정
- 2006년 SAML 2.0 표준 제정
- 2007년 i-PIN 서비스 프레임워크/메시지 표준 제정

- 2008년 자기 제어 강화형 아이덴터티 공유 프레임워크 표준 제정
- 2008년 i-PIN 서비스 중복가입 확인정보/전달 메시지 표준 제정

• 정책/산업
- 2005년 i-PIN 서비스 시범 도입
- 2006년 행안부 통합ID관리 서비스 추진
- 2008년 일정 조건 이상의 포털 및 웹사이트 i-PIN 서비스 수단 도입 의무화
- 2008년 디지털아이디관리포럼 결성

1.3. 추진경과 및 중점 추진방향

• 추진경과
- Ver.2007에서는 개인정보보호 및 ID 기술 분야는 정보보호(일반)의 표준화 대상항목으로 기술되었음
- Ver.2008에서는 국 · 내외적으로 ID 도용에 따른 피해액이 급증하고, 국내의 경우 ID 도용이 사회적인 문제가 되고 시장에서 산업적인 요구사항이 증가하고, ID관리 기술 및 개인정보보호가 정보화/지식 사회의 필수 요소로 인식되고 국 · 내외적으로 ID관리 및 개인정보보호 핵심 기술의 개발이 활발히 진행되고 이들 핵심 기술에 대한 표준화 작업이 ITU-T, ISO 등과 같은 국제 표준화 단체에서 활발히 진행됨에 따라, ID관리 및 개인정보보호 분야에 대한 중장기 표준화로드맵을 수립하게 되었음
- Ver.2009에서는 표준화 네트워크 중심 ID 인증 및 접근제어 표준화 항목을 추가하였으며, Ver.2008에서의 데이터보호 및 감사를 개인정보 DB 보안으로, i-PIN을 본인확인 기술로 확대하여 변경 기술하였으며, 국내외 IPR 보유현황 및 확보 가능 분야를 추가 기술하였음
- Ver.2010의 추진계획은 TTA 표준화본부를 중심으로 관련부처와 전문가 Pool을 통해 추진되었으며, 2009년 1월부터 3월까지 기본계획 수립 및 사전 조사 분석이 진행되었으며, 3월에서 4월까지 민간 수요조사를 수행하였으며, 4월에 37대 중점기술 선정 및 중점 추진방향이 수립되었음

• 버전별 중점기술의 변천

구 분	Ver.2007	Ver.2008	Ver.2009	Ver.2010
ID관리기반	- ID관리 프레임워크 - 보안 정보/생성 분배	- 식별체계 - 보안토큰 생성 · 분배 - 디스커버리 - 온톨로지 - 공유 - 프레임워크 - 신뢰 관리	- Identity 식별자 체계 - Identity 시스템 공통 프레임워크 - 보안 토근 관리 - Identity 서비스 디스커버리 - Identity 온톨로지 - Identity 공유 - 신뢰 관리	- Identity 식별자 체계 - Identity 시스템 공통 프레임워크 - Security Token 관리 - Identity Sharing - 신뢰관리-Assurance
개인 정보보호		- 개인정보보호 정책 - 상호작용 서비스 - 데이터보호 및 감사 - IC카드 이용 사용자 보호 기술	- 개인정보보호 정책 - Interaction Service - 개인정보 DB 보안 - 사용자단말 개인정보 관리	- 개인정보보호 정책 - Interaction Service - 사용자단말 개인정보 관리
ID관리 응용 및 기타	- ID관리 응용(SSO, EAM, IAM)	- i-PIN - 네트워크 중심 ID관리 - XML 전자서명 및 암호화	- 네트워크 중심의 ID관리 모델 - 네트워크 ID 인증 및 접근제어 - 본인확인 기술	- 네트워크 ID 인증 및 접근제어 - 본인확인 기술

- Ver.2007에서는 정보보호(일반) 표준화로드맵의 표준화 대상항목으로 3가지 중점기술이 선정됨
- Ver.2008에서는 ID관리 및 개인정보보호 분야가 독립적인 표준화로드맵을 구성함에 따라 중점기술의 세분화 작업에 따라

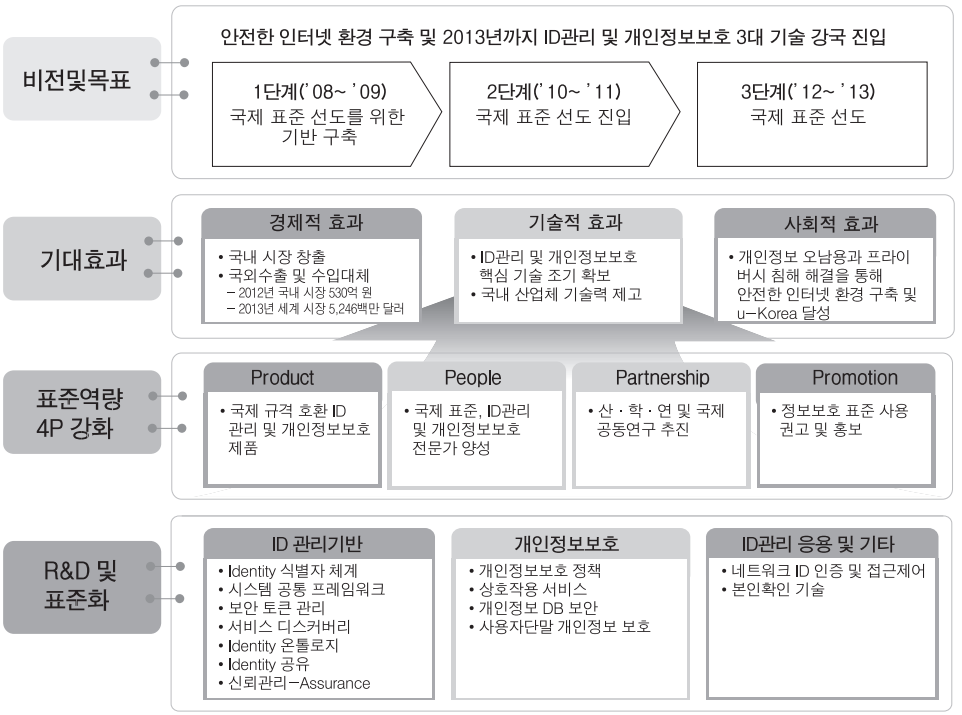
14개 중점기술이 선정됨

- Ver.2009에서는 시스템 상호 운용을 위한 Identity 시스템 공통 프레임워크 기술, SAML 등을일괄적으로 표현하는 보안 토큰 관리 기술이 추가되었음. 이전 버전의 네트워크 중심 ID관리는 네트워크 중심 ID관리 모델과 ID 인증 및 접근제어로 세분화됨. 상호작용 서비스는 Interaction Service로, ID카드 이용 사용자 보호 기술은 사용자단말 개인정보 관리로 명칭이 변경되었으며, I-Pin은 본인확인 기술로 확대되었음. XML 전자서명 및 암호화는 표준화 작업의 종료로 인해 중점기술에서 삭제됨
- Ver.2010에서는 보안 토큰 관리가 Security Token 관리로, 신뢰 관리는 ID 관리에 대한 regulation 강화 추세를 반영하여 신뢰관리-Assurance로 변경됨. 네트워크 중심 ID관리 모델은 Identity 시스템 공통 프레임워크로 통합함

• 중점 추진방향

- ID관리 및 개인정보보호 분야의 기술과 표준화 필요성에 대한 이해 제고를 위해 기술 개요, 국내외 시장 현황 및 전망, 국내외 기술개발 현황 및 전망, 국내외 표준화 현황 및 전망을 기술
- 정부의 정책 추진 의지, 산업체의 요구사항, 적시성, 시장파급성, 국제경쟁력, 상용화 가능성과 같은 전략적 중요도와 타 기술에 대한 파급효과, 산업적 파급효과, 미래 영향력 등과 같은 기술적 파급효과를 고려하여 ID관리 및 개인정보보호 분야의 중점 표준화 항목을 선정
- 국 · 내외 기술/시장/표준화 동향을 고려하여 중점 표준화 대상 항목의 세부전략을 수립하고 중장기 표준화 로드맵을 작성

1.4. 표준화의 Vision 및 기대효과



〈그림 3〉 ID관리 및 개인정보보호 기술 표준화 비전 및 기대효과

• ID관리 및 개인정보보호 기술의 경제적 효과

- 국내의 경우, ID관리 및 접근제어 시장이 2008년 346억 원 규모에서 연평균 11.5%의 성장을 보이며 2012년 530억 원 규모의 시장으로 성장할 것으로 전망하고 있음
  ▫ 한국IDC, "Korea Security Software 2008-2012 Forecast and Analysis: 1H 2008 Update," 2009.1.30
- 전 세계적으로 ID관리 및 접근제어 시장 규모를 2008년 3,504백만 달러에서 연평균 8.4%의 성장을 보이며 2013년에 5,246백만 달러에 이를 것으로 전망하고 있음
  ▫ DC, "Worldwide Identity and Access Management 2009-2013 Forecast : The Initial View," 2009.03
- 2007년도 KISA 조사에 의하면, 국내의 경우 인터넷 이용자들이 느끼는 연간 개인정보보호에 대한 총 가치는 약 1조 2,982억 원에 달하고 있음
  ▫ KISA, "개인정보의 경제적 가치 연간 약 1조 3천억원에 달해," 2007.1
- 2007년 11월 미국 FTC에 의하면 신원도용 피해를 입은 미국인이 약 8천 3백만 명에 이르며, 그 피해규모는 156억 달러에 이를 것으로 보고하고 있음
  ▫ FTC, "Federal Trade Commission - 2006 Identity Theft Survey Report," 2007.11

1.4.1. 표준화의 필요성

• 인터넷의 활용이 커지면서 사용자는 수많은 사이트에 ID를 등록하게 되고 자신의 개인정보를 여러 곳에 방치하게 됨으로써 ID관리의 불편함뿐만 아니라 개인정보 오 · 남용 및 유출로 인한 피해가 증가하고 있음

- 일반 인터넷 이용자들이 느끼는 연간 개인정보보호에 대한 총 가치는 약 1조 2,982억 원에 달하고, 개인정보 중에서 특히 금융정보 유출을 가장 우려하고 있는 것으로 나타났음
  ▫ KISA, "개인정보의 경제적 가치 연간 약 1조 3천억원에 달해," 2007.1
- 2008년 국내 최대 인터넷 쇼핑몰 중 한 곳에서 1,000만 여명의 회원 정보가 해커에 의해 유출되어 회원의 개인정보와 금융정보가 노출된 후 스팸 및 보이스 피싱 등 2차 공격에 악용된 사고나 유명 통신업체에서 600만 명의 회원 정보가 불법 거래되는 사건이 발생하였음

• 웹 기술의 보편화와 함께 웹 정보 시스템을 통한 정부 또는 기업의 대국민, 대고객 서비스가 확산되고 있으며, 개인들은 자신의 개인정보와 선호정보(preference)를 웹 정보 시스템이 활용하도록 함으로써 다른 사용자와는 차별화된 개인화된 서비스를 이용할 수 있게 되었음. 현재 각 정부기관 및 기업들은 서비스 제공자 관점에서 서비스 제공에 필요한 고객의 개인정보를 각각 수집, 저장, 활용하고 있는 실정임

• 개인정보 소유자 관점에서 평가할 때 개인정보를 관리하는 현재 정보시스템 체계에서 자신의 개인정보는 각 정부기관 및 기업의 정보 시스템간 상호운용성 부재로 중복, 저장되어 있고 개인정보 활용시 개인정보 소유자에 대한 사전고지 및 동의 절차 미비 등으로 인해 개인정보의 유출 위험성과 오 · 남용으로 인한 경제적, 사회적 비용발생 문제점을 안고 있음. 이러한 문제들의 근본적인 원인은 개인정보를 수집, 저장, 공유, 관리, 활용, 폐기 서비스를 수행하는 ID관리 시스템에 대한 기능 요구사항, 프레임워크, 시스템 구현을 위한 메커니즘 개발 및 이를 지원하는 제반 법률 및 제도적 장치가 존재하지 않는데 있음

• NGN/BcN 통신망에서 사용자 로그인 및 인증절차가 필수적으로 요구되며, 특히 최근 차세대 컴퓨팅 환경으로 연구 · 개발이 활발히 진행되고 있는 클라우드 컴퓨팅이 확장가능성과 보안성을 확보하기 위해서는 ID관리 기능이 필수적임
  ▫ Gartner, "Identity Services (in) the Cloud," 2008.5

• 이와 같은 문제를 해결하기 위해 ID관리 및 개인정보보호 핵심 기술에 대한 연구 및 개발이 국내에서도 활발히 진행되고 있

으며 일부 기능이 탑재된 제품이 출시되고 있는 상황임. 그러나 제품의 기술 경쟁력을 확보하고 국제 경쟁력을 제고시키기 위해서는 국내 및 국제 표준의 준용이 매우 중요한 요인이 되고 있음

- 특히 세계 각국은 자신이 개발한 기술을 국제 표준에 반영함으로써, 관련 제품에 대한 IPR(Intellectual Property Rights)을 확보하고 관련 제품의 기술 경쟁력과 시장지배력을 향상시키고 있는 추세임

- 따라서 ID관리 및 개인정보보호 제품의 기술 경쟁력과 시장 지배력을 향상시키며, 인터넷 사용자들의 개인정보 오 · 남용과 프라이버시 보호 및 시스템간의 상호운용성을 확보하기 위해서는 ID관리 및 개인정보보호 분야의 표준화가 필요함

1.4.2. 표준화의 목표

- 2009년까지 1단계로 ID 공유, 본인확인기술 표준 등 국내표준을 개발하여 국제 표준화 기반 구축
- 2011년까지 2단계로 ID관리 및 개인정보보호 핵심 기술을 개발하고 ITU-T, ISO 등 국제표준화 단체 기고를 통해 ID 관련 국제 표준화 선도 진입
- 2013년까지 3단계로 개발된 핵심 기술의 국내 표준화 및 우수기술에 대한 국제표준화 진행으로 국제표준화 선도

- 2009년까지 ID 공유, ID 관련 용어 및 i-PIN의 국내 표준화 완료 및 ITU-T, ISO/IEC, 3GPP 등 ID관리 및 개인정보보호 관련 국제 표준화 단체에 적극적으로 참여함으로써 국제 표준화 기반을 구축함

- 2011년까지 ID관리 및 개인정보보호 핵심 기술을 개발하고, ITU-T/SG2, SG11, SG13, SG17, ISO/IEC JCT1/SC17, SC27 등 국제 표준화 단체에 개발된 핵심 기술에 대한 표준을 기고함으로써 ID관리 및 개인정보보호 분야의 국제 표준화를 선도할 수 있는 상태에 진입함

- 2013년까지 국제표준화 선도를 위하여 ITU-T/SG2, SG11, SG13, SG17, ISO/IEC JTC1/SC17, SC27 등 국제표준화 기구에서 ID관리 프레임워크, ID관리 및 개인정보보호 응용과 기타 분야의 핵심 기술들에 관한 국제표준(안) 개발을 적극적으로 주도하며 관련 IPR을 다수 획득함

- 지금까지 개발된 대부분의 ID관리 시스템들은 사용자 중심, 응용 중심, 네트워크 중심 등 특정 응용분야에 한정된 제한적 기능만을 제공하고 있고 ID관리 시스템간 서비스 발견, ID 체계 및 ID 공유 프로토콜을 위한 표준 부재로 인해 상호운용이 어렵다는 문제를 안고 있음. 따라서 이러한 문제들을 극복하기 위해 특정 응용분야에 국한되지 않는 포괄적인 ID관리 시스템 요구사항을 정리하고 현재 사용 중인 유 · 무선 통신망뿐만 아니라 클라우드 컴퓨팅, 미래 유비쿼터스 통신망에도 적용가능하고 다른 ID관리 시스템과 상호운용이 가능한 ID관리 시스템 기반 기술을 개발하고 표준화함

- 또한 인터넷의 고도화, 웹 2.0, 유비쿼터스 사회로의 진입에 따라, 온라인 및 오프라인 상에서의 개인정보에 대한 누출 및 오 · 남용으로 인한 피해가 기하급수적으로 증가할 것으로 예상됨. 이와 같은 문제를 해결하기 위해 국내 법률 및 제도적 장치의 정비 등을 포함하여 개인정보정책, 사용자의 서비스 사용 동의 방식, 온 · 오프라인 상에서 사용자 본인 확인 기술 등을 개발하고 이를 표준화함

- 국내에서는 디지털아이디관리포럼, 통합번호체계포럼, TTA PG 204(NGN), 및 PG502(개인정보보호 및 ID관리) 등에 참여하며, SG2, SG11, SG13 분과위원회의 협력과 지원을 받아 국제 표준화에 참여함

1.4.3. Vision 및 기대효과

• 2013년까지 국내 ID관리 및 개인정보보호 기술력이 세계 3대 기술 강국으로 진입하는 것을 목표로 국제표준화를 추진함으로써,
- 국내 우수기술의 국제표준화 선점 및 국내산업 기술경쟁력 강화
- ID관리 및 개인정보보호 분야의 시장 창출, 국외수출 및 수입대체를 통한 ID관리 및 개인정보보호 산업 진흥
- 개인정보 오 · 남용과 프라이버시 침해 해결을 통해 안전한 인터넷 환경구축 및 u-Korea 달성

• ID관리 기반, ID관리 및 개인정보보호 응용 등에서 ID관리 및 개인정보보호 분야의 핵심 기술을 개발하고 이들 기술에 대한 국내표준을 개발하고, 우수기술에 대해 ITU-T와 ISO/IEC JTC1 등 국제표준화 단체의 표준으로 채택되도록 함으로써,
- ID 도용으로 발생하는 막대한 경제적 피해와 피싱 등과 같은 개인정보보호 유출 문제를 방지할 것을 기대하며,
- 시스템적 시각에 의한 빅브라더 가능성에 대해 사용자 개개인이 스스로 자신의 정보를 지킬 수 있는 기반 제공을 기대하며,
- 국제 표준화된 우수 기술을 탑재한 국내 ID관리 및 개인정보보호 관련 제품의 출시를 통해, 국내 관련 분야의 시장을 창출하고, 해외수출 및 수입대체 효과를 기대하며,
- 활발한 국제 표준화 활동을 통해, 관련 기술에 대한 다수의 IPR 확보를 기대하며,
- 일반 인터넷 사용자의 개인정보 오 · 남용에 대한 우려를 해결하고, 편리한 ID관리 기술을 제공함으로써, 안전한 인터넷 환경을 구축하여 u-Korea 구축의 초석을 다질 것을 기대

• 개방과 공유를 특징으로 하는 웹 2.0 환경 및 서비스 확대에 따라 지금까지 개인정보의 활용과 관리를 정부기관이나 기업에 맡겼던 개인정보 소유자들이 ID관리 시스템간 상호운용을 통해 개인정보 중복성 최소화 및 자기정보 통제권 실행을 통해 다양한 통신환경에서 개인화된 서비스 활용이 가능할 것임

2. 국내 · 외 현황분석

2.1. 시장 현황 및 전망

2.1.1. 국내 시장 현황 및 전망

• 한국IDC의 2009년 조사에 따르면, 국내 ID관리 및 접근제어 시장이 2008년 346억 원 규모에서 연평균 11.5%의 성장을 보이며 2012년 530억 원 규모의 시장으로 성장할 것으로 전망하고 있음

〈표 1〉 ID관리 및 접근제어 국내 시장 규모, 한국IDC, 2009

(단위, 백만 원)

구 분	2008년	2009년	2010년	2011년	2012년	08-12 성장률
ID관리 및 접근제어	34,607	38,550	42,517	47,406	53,000	11.5%

• KISA의 '2008 국내 정보보호 시장 및 동향보고서'에 의하면 DB보안 및 DB암호화를 합친 DB보안시장은 2007년에 165억 원, 2008년 174억 원에서 연평균 6.4% 성장하여 2013년에는 224억 원에 이를 것으로 전망하고 있음. 국내 DB 보안 분야는 2008년 통신사, 쇼핑몰 등의 개인정보유출 사고 발생으로 필수적인 기능으로 자리매김을 하고 있으며, 2009년도 DB보안 시장은 경기 불황에도 불구하고 IT 컴플라이언스 강화로 더욱 활성화 될 것으로 예상됨

• 한국HP는 통합ID관리 솔루션 분야의 선두 업체인 트러스트제닉스를 인수한 후 통합ID관리 솔루션 라인업을 강화하고 있음. 한국HP는 트러스트제닉스의 솔루션을 HP의 IT 자원관리 솔루션인 '오픈뷰' 포트폴리오에 통합하여 이를 기반으로 '셀렉트 아이덴티티', '셀렉트 액세스', '셀렉트 페더레이션', '셀렉트 오딧' 등 총 4가지 계정관리 솔루션을 보유, 기업의 보안프레임워크를 구현하는 핵심기반으로 활용한다는 전략임

• 한국IBM은 통합 권한 관리 프레임워크인 'IBM 티볼리 액세스 매니저 포 e비즈니스', 전사 통합 계정 관리 솔루션 'IBM 티볼리 아이덴터티 매니저', 서비스지향아키텍처(SOA) 및 페더레이션 환경 고객을 위한 'IBM 티볼리 페더레이션 아이덴터티 매니저' 등의 제품을 보유하고 있으며, 2008년에는 가상화-유비쿼터스 환경 및 다양한 인증기술의 다중인증 방식을 제공하는 '티볼리 엑세스 매니저 포 엔터프라이즈 싱글 사인 온 V8.0'을 발표하였음

• 한국BMC는 접근 및 컴플라이언스 관리 등을 지원하는 '통합 계정관리 스위트'를 출시하고 본격적인 마케팅 활동을 벌이고 있음. BMC의 이 솔루션은 디렉토리 관리, 액세스 관리, 프로비저닝, 패스워드 관리, 감사 및 법규준수 관리 등으로 구성돼 있어, 프로세스와 시스템, 비즈니스 서비스에 연결된 상태에서 기업 내외부의 모든 사용자에게 액세스 권한을 할당하고 관리할 수 있는 것이 특징임

• 한국Oracle은 최근 계정관리 솔루션 '오라클 아이덴티티 매니지먼트 10g 릴리즈3'을 발표하며 본격적인 계정관리 공략을 선언한 한국오라클은 최근 오블릭스, 옷텟스트링, 쏘어테크놀로지스 등 이 분야 전문벤더들을 인수한 이후, 기존 SSO나 EAM을 구축한 기업이 데이터차원의 진정한 통합을 이뤄내지 못한 것을 감안해 이 시장에 대한 공략에 집중할 전략을 가지고 있음

• 한국CA는 2008년 ID관리 및 접근제어 솔루션의 새로운 버전인 'CA IAM r12'를 출시하였음. 이 제품은 일반적인 환경은 물론 SOA 및 웹 서비스 환경에서도 IT 조직이 보다 효율적으로 데이터 및 애플리케이션에 대해 접근토록 하며, 인텔리전트 접근제어 및 종합적 리포팅을 통해 리스크 감소와 용이한 규정 준수 규제 컴플라이언스가 가능하도록 하며, ID 생명주기 라이프사이클 관리, 접근 관리, 업무흐름 자동화, 위임 관리, 리포팅, 통합 등의 기능을 제공함

• 소프트포럼은 ID관리 솔루션으로 'SafeIdentity' 제품군을 보유하고 있음. 멀티도메인 간, 다양한 어플리케이션 간의 통합인증(SSO) 제공, 역할기반접근제어(RBAC, Role-based Access Control) 시스템 제공, 정책기반의 관리 기능 제공, 고도의 사용자 개인화를 통해 자동 사용자 요청 및 승인 프로세스 지원, 감사 보고 기능을 제공함

- 소프트포럼의 'XecureDB' 보안제품은 DB에 공개키 기반의 강력한 암호화 및 전자서명 기능을 제공함으로써 DB에 저장되어 있는 주요 데이터에 불법적인 방법을 취하여 접근하였다 하더라도 인가자 이외에는 알 수 없는 형태인 암호문으로 저장되어 있어 내용의 기밀성을 유지되고, 전자서명 등을 통하여 데이터 무결성이 보장되도록 하는 DB 솔루션임. 이 솔루션은 응용과 연동한 DB 암 · 복호화 및 검증, DBMS 저장 및 추출 데이터에 대한 암/복호 기능, 관리자가 설정한 규칙에 따라 컬럼별 선택적 암호 및 다이제이트 계산, RSA(1024비트)/3DES(128비트)/SEED(128비트) 등 암호 알고리즘 및 SHA 해시 알고리즘을 지원함
- 이니텍은 'INISAFE Nexess'를 통해 기업의 분산된 자원과 사용자를 통합하고 일관된 체계를 구축하는 EAM 솔루션을 제공함. Id(Identifier)/PW, PKI, 지문인식, OTP, MOTP(Mobile One-Time Password), Smart Card 등 다양한 인증 방식뿐만 아니라 Multi-Domain에서의 안전한 SSO가 가능함. 또한 RBAC 기반의 권한 관리, 중앙집중적 통합 관리와 관리자 위임 기능을 통한 분산적 관리 기능을 제공함
- 이니텍의 'SafeDB'는 데이터베이스에 저장된 데이터를 암호화하고 데이터베이스에 대한 접근을 제어함으로써 중요한 데이터를 보호할 수 있는 데이터베이스 보안 솔루션으로서, 기존 어플리케이션의 수정이나 별도의 개발 과정 없이 데이터베이스에 추가 설치하는 과정만으로 중요 데이터를 암호화하고 간편하게 보안정책을 적용할 수 있음. 또한 컬럼 단위의 암호화 기능을 지원하며, 허가된 사용자 이외에는 암호화된 정보에 접근할 수 없도록 함으로써 보안을 강화하였고, 데이터베이스 관리자도 보안 관리자의 승인 없이는 암호화된 정보를 조회하거나 수정, 삭제할 수 없어 내부자에 의한 정보 유출을 방지하는 기능을 제공함
- 드림시큐리티는 id/pw, 인증서, 생체인식, cd-key 등과 같은 다양한 인증방식을 지원하며 인증 단계에 따른 권한을 선택적으로 부여하는 SSO 솔루션인 'Magic SSO & EAM v3.0' 제품을 제공함. 사용자인증 및 ACL 발급을 담당하는 인증서버(Policy Server)와 사용자 PC에 설치되고 사용자인증 후 세션을 관리하는 클라이언트 에이전트(Client Agent), 사용자 및 권한관리가 필요한 어플리케이션을 등록하고 권한을 관리하는 인터페이스인 관리자 어드민(Policy Server Admin)으로 구성되어 있음
- 티맥스소프트는 인터넷 상에서 SSO 기능을 제공하는 'SysKeeper SSO'와 기업 EAM 기능을 제공하는 'SysKeeper EAM' 제품을 제공함. SysKeeper SSO는 SSO, 암호, 감사 및 통제 기능 등을 제공함. SysKeeper EAM은 다양한 인증, RBAC 등의 기능을 제공함
- 펜타시큐리티시스템의 'ISign'은 SSO 기능을 기본적으로 제공하면서 통합 권한 관리 기능을 제공하는 EAM 솔루션임. SSO 기능은 전자정부 및 공인인증기관의 PKI 인증서를 지원하며, 속성 인증서(Attribute Certificate)를 이용한 사용자 권한 제어와 RBAC 기반의 권한 설정 정책을 제공함. 또한 ISign의 Roaming 기능은 사용자에게 키 로밍을 통한 사용자 인증과 접근제어를 다양한 환경에서 보장하여 사용자의 이동성을 증가시킴. 또한 사용자 측면에서는 단 한번의 로그인으로 편리하고 안전하게 업무시스템에 접근할 수 있고, 관리자 측면에서는 효율적으로 계정을 관리할 수 있게 해주는 SSO 솔루션인 'eGSign'을 제공함
- 펜터시큐리티의 'D'Amo'는 통합 DB보안 솔루션으로 데이터 암호화, 접근제어 및 감사를 통해 기업 내 중요 데이터 보호서비스를 제공함. 이 제품의 특징은 기존 응용 프로그램의 수정 없이 컬럼단위로 암호화를 수행하며 컬럼 단위 작업내역을 기록/보관할 수 있으며 인가된 사용자 및 응용프로그램 등에 대해서만 데이터베이스 접근을 허용하고 있음. 또한 DB관리와 보안관리 기능의 분리로 전문적인 DB 보안관리가 가능하며 작업내역 추적 기능을 이용하여 외부 및 내부 공격자에 의한 불법 정보유출에 대응할 수 있는 기능을 제공함
- 알툴즈(ALTools) 사의 '알패스'는 회원제로 운영되는 많은 웹사이트의 아이디와 비밀번호를 관리할 수 있는 프로그램으로, 2009년 6월 25일 현재 버전 3.08이 배포되었음. 알패스는 클라이언트와 서버로 구성되어 있으며, 클라이언트는 사전에 id/pw 데이터를 서버에 등록하고 암호화된 랜덤키를 저장하고 있다가 특정 사이트에 로그인할 때 해당 랜덤키로 사이트에 로그인하는 방식을 사용함. 로그인 정보 자동 채움 기능을 제공하며 부가적으로 USB 연동, 온라인에 데이터를 저장함으로써

데이터 손실 회피, 개인정보 노출 방지가 가능함

- 워너다임사의 'Privacy Scanner'는 홈페이지 개인정보 노출 차단 및 점검 기능을 제공하는 소프트웨어로 개인정보 노출 점검 솔루션인 ' Privacy Scnner Manager'와 개인정보 노출 차단 솔루션인 'Privacy Scanner Filter'로 구성되어 있음. 또한 국내의 개인정보보호 법적 의무사항을 만족하는 개인정보보호정책을 손쉽게 생성 및 관리할 수 있는 한국형 P3P 개인정보보호 정책 생성기 솔루션인 'WD-P3P'를 출시하고 있음
- SafeFolder의 LogoutCleaner는 PC를 종료하거나 로그아웃할 때, 시스템의 임시파일들과 윈도우 사용기록들을 자동으로 삭제하는 프로그램임. 웹브라우저에 저장되는 쿠키, 암호, 방문기록, 캐시 정보들을 자동으로 삭제하여 이용자의 개인정보가 타인에게 노출되는 것을 방지함
- SecuTronix의 '이지패스'는 웹에서의 로그인뿐만 아니라 각종 메신저 및 응용 프로그램의 로그인까지 지원하는 제품으로, 2009년 6월 2일 현재 2.0.6 베타 버전이 출시되었음. MSN, Nate-On과 같은 메신저에서의 로그인과, Melon, JukeOn 등의 응용프로그램에서의 로그인을 지원함. 추가적으로 USB에 탑재하여 사용할 수 있으며, 한 사이트에 여러 계정을 보유한 경우 또한 지원함. 이지패스 솔루션은 id/pw 방식의 로그인을 기반으로 하며, 지문인식기가 제공된 경우 지문인증으로 로그인이 가능함
- 이글로벌시스템의 'CubeOne' 제품은 ARIA, AES, SEED, DES, 3DES 암호화 알고리즘을 이용하여 데이터베이스 컬럼을 암호화하며 암호화된 컬럼에 대한 인덱스 검색을 지원하는 DB 암호화 솔루션임. 이 제품은 기존 응용 프로그램의 수정 없이 적용될 수 있으며 컬럼별로 접근통제 및 고유 암 · 복호 키를 생성하고, 사용자/IP/응용별 접근통제, DB관리자와 보안 관리자의 권한 분리, 보안정책 설정에 대한 보안감사, 암호화된 컬럼에 대한 보안감사 기능 등을 지원함. 현재 이 제품은 Oracle 8.1.6부터 Oracle 10g R2 버전에 적용될 수 있음
- 국내의 OpenID 시장은 2007년부터 시작되었으며, 현재 NC소프트(http://myid.net), 안철수연구소(http://idtail.com), Daum(http://openid.daum.net)이 OpenID 제공자로 동작하고 있음. OpenID 소비자로는 NC 소프트의 스프링노트(www.springnote.com), 미투데이(me2day.net), 라이프팟(www.lifepod.co.kr), 아이두(www.idoo.net)가 있음. 최근 대형 포털 및 인터넷 사업자들도 OpenID 적용에 관심을 보이고 있으며, Paran과 Egloos 등은 자사의 URL을 OpenID로 사용할 수 있는 기능을 제공함

〈표 2〉 국내 ID관리 및 접근제어 솔루션 개발 현황

구 분	기 관	내 용
EAM	드림시큐리티	- MagicSSO, MagicAccess - PKI 기반의 인증서 이용 SSO 지원 - 서버별 사용자 접근 권한 부여 및 확인
	소프트포럼	- SafeSignOn - PKI 기반의 인증서 이용 SSO 지원 - 통합적 권한 관리 - SAP, IBM 등 솔루션업체와의 제휴 및 연동 - 웹 환경과 C/S 환경 지원
Federated ID	소프트포럼	- SafeIdentity - 멀티 도메인간, 다양한 어플리케이션 간의 SSO 제공 - 정책 기반 관리 - Self-Profile 관리 모듈을 통해 사용자 프로파일 수정과 자동 사용자 요청, 승인 프로세스 지원 - 로그 데이터를 기반으로 한 보안 감사 및 통계 리포팅 작업 지원, 감사 데이터 백업 및 삭제 기능
User-Centric ID	다음	- openid.daum.net - 2007년 하반기부터 OpenID 서비스를 제공 - 블로그 주소를 OpenID로 사용 가능
	OpenMaru	- myid.net - NCSoft 계열사 - OpenID 서버를 제공하는 국내 최초의 서비스 - URL을 식별자로 하여 OpenID를 지원하는 사이트에서는 OpenID를 사용하여 SSO를 제공함
	IDtail	- Ahn. Lab 계열사 - OpenID 서버를 제공 - URL을 식별자로 하여 OpenID를 지원하는 사이트에서는 OpenID를 사용하여 SSO를 제공함

2.1.2. 국외 시장 현황 및 전망

• IDC의 2009년 3월 조사에 따르면, 전 세계적으로 ID관리 및 접근제어 시장 규모를 2008년 3,504백만 달러에서 연평균 8.4%의 성장을 보이며 2013년에 5,246백만 달러에 이를 것으로 전망하고 있음

〈표 3〉 ID관리 및 접근제어 세계 시장 규모, IDC, 2009

(단위, 백만 달러)

구 분	2008년	2009년	2010년	2011년	2012년	2013년	08-13 성장률
ID관리 및 접근제어	3,504	3,773	4,086	4,458	4,836	5,246	8.4%

• ID관리 시장은 ID관리 종합지원 솔루션과 Provisioning, 인증, 연계형 ID 솔루션으로 구분되며 최근 사용자중심 ID관리 솔루션이 새롭게 제공되고 있음

• ID관리 종합지원 솔루션은 조직 내의 인증, 인가, 계정관리, 감사를 모두 수행하는 솔루션으로서 실시간으로 리소스 접근을 제어하기 위한 인증, 인가와 이를 위해 사전에 설정되고 관리되는 계정정보, 이러한 과정들이 사전에 설정된 정책에 위배되는지 감사하는 감사기능을 포함함. ID관리 종합 지원 솔루션 벤더로는 CA, IBM, Microsoft, Novell, Oracle, Siemens, Sun microsystem 등이 있음

• Provisioning은 ID관리에 초점을 맞춘 것으로 조직 내에 신규 등록되는 사용자의 인입과 변동되는 ID 정보 등의 관리를 수행함. Provisioning 솔루션 벤더로는 Beta System, BMC, Courion, MaXware, Thor 등이 있음

• 인증은 PKI, 생체, OTP 등 다양한 기술로 인증 강도를 높이고 사용자 편의성을 제공하는 솔루션에 초점이 맞추어 있고 해당 벤더로는 Entrust, CA, Oblix, RSA Security(EMC에 합병)가 있음

• 연계형 ID관리는 조직 간에 연계된 서비스를 제공하기 위해 ID를 서로 연계하고, 이를 통해 인증, 접근제어 관리 등을 수행하는 솔루션임. 관련 벤더로는 HP, Ping Identity, M-Tech, HP 등이 있음

• Sun은 사용자 Provisioning, 패스워드 관리, 역할 관리, 접근 제어, 웹 SSO, 연계 SSO, 디렉토리 서비스 및 가상 디렉토리 기능을 제공하는 'Sun Java System Identity Management Suite'을 제공함. 이 Suite은 웹과 자바 응용에서 연계 환경까지 ID 및 접근 제어 기능을 제공하는 Sun Java System Access Manager, 사용자 provisioning, identity 감사 및 compliance 기능을 제공하는 Sun Java System Identity Manager와 파트너사와의 안전한 연결 기능을 제공하는 Sun Java System Federation Manager를 포함함

• IBM은 TIM(Tivoli Identity Manager), TAM(Tivoli Access Manager), RACF(Resource Access Control Facility)으로 구성된 기업 고객용 ID 제품군을 보유하고 있음. IBM은 2006, 2007년 연속으로 ID관리 및 접근제어 시장의 선두주자임

• CA는 웹에서부터 메인프레임에 이르기까지 IAM(Identity and Access Management) 솔루션을 제공하기 위해 다양한 IAM 제품군을 제공함. CA Identity Manager를 비롯하여 CA SiteMinder, CA Single Sign-On, CA Directory 등과 같이 다양한 IAM 솔루션을 제공함

• 스토리지 부분의 업계선두인 EMC는 RSA Security를 합병하였음. OTP 토큰 제품인 SecurID와 다양한 PKI 개발 역사를 가지고 있는 RSA는 다양한 IAM 제품을 보유하고 있음. RSA FIM(Federated Identity Manager)는 XML, SOAP, SAML 2.0 등의 최신 웹 서비스 표준을 준용하여 다른 시스템들과의 호환성을 확보하고 있으며, RSA Access Manager는 웹 SSO를 제공함

• Verisign은 사용자의 디지털 ID를 강화하고 보호하는 VIP(VeriSign Identity Protection)을 제공하고 있음. VIP suite는 two-factor 인증 솔루션인 VIP Authentication Service와 risk-based 인증 솔루션인 VIP FDS(Fraud Detection Service)로 구성됨

- Oracle은 기업을 위한 end-to-end Identity 플랫폼을 제공하며 Oracle Access Management Suite, Oracle Identity Manager, Oracle Role Manager, Oracle Enterprise SSO Suite, Oracle Identity Federation, Oracle Web Services Manager 등 Directory, Oracle Virtual Directory, Oracle Identity and Access Management Suite 등의 제품을 제공함
- Novell은 조직 내의 identity 통합을 위한 기반과 룰-기반으로 자동화된 provisioning 능력을 제공하는 Identity Manager, 웹 SSO 기능을 제공하는 Novell Access Manager, 기업 SSO 기능을 제공하는 Novell SecureLogin, identity 기반 물리/빌딩 보안 기능을 제공하는 Novell Identity Assurance Solution 제품을 제공함
- Microsoft는 IAM 시장의 중추적인 벤더로 인식되고 있음. ILM(Identity Lifecycle Manager) 2007은 메타디렉토리, 인증서 및 스마트카드 관리, 사용자 provisioning 기능을 제공함. 최근 출시된 ILM 2는 사용자의 편의성을 강화한 것으로 정책 관리, 크리덴셜 관리, 사용자 관리, 그룹 관리 기능을 제공함. 또한 Microsoft는 기존의 .net Passport에서의 독점적인 중앙 관리에서 벗어나 여러 ID 제공자의 다양한 ID 기술들을 상호 운용하는 ID 메타시스템 개념을 제안하고, 이 개념을 윈도우 Vista에 CardSpace로 구현하였음
- i-name은 NETSTAR, Cordance, xdi.org가 인프라를 담당하고 있는 사이트로 OASIS의 XRI 표준의 한 형태로 사용자들이 기억하고 사용하기 쉽도록 고안되었음. 전 세계적으로 XRI 주소를 해석해주는 역할을 수행하고 있으며, 개인용 i-name과 비즈니스용 i-name을 발급하고 있음. i-name 서비스 제공자는 GSS(Global Services Specifications)에 따라 서비스를 구축하며, GSS는 법적, 관리상의 정책, GRS(Global Registry Service)의 운영 · 등록 · 주소해석 정책 등을 명시함
- OpenID는 사용자가 쉽게 기억하고 간단한 URL 형태의 식별자를 이용하여 사이트에 로그인할 수 있도록 해주는 기술로 SNS(Social Network Service) 사이트를 통해 광범위하게 확대되고 있음. 2008년 Yahoo와 MySpace가 OpenID를 지원하기 시작하였으며, Microsoft와 Google에서도 OpenID를 지원하고 있으며, 2009년 3월 현재 OpenID를 적용한 사이트 수가 3만 6천여 개에 달하고 있으며 사용자는 5억여 명에 이르고 있음
- SAML 2.0은 많은 ID관리 및 접근제어 솔루션에 채택이 되어 있음. Google, NTT, 미국의 GSA E-Authentication 솔루션에 채택되고 있음. Google은 Google 고객들이 Google Apps에 인증할 때, SAML 2.0을 사용하고 있으며, NTT는 SAML 2.0을 이용하여 사용자들이 PC에서 SSO를 수행하고 모바일 폰의 강력한 인증 기능을 활용할 수 있도록 해 주는 개인 ID 제공자인 SASSO를 개발하였음
- Ping Identity는 사이트 간의 Federated SSO를 제공하며, Identity-enabled 웹 서비스를 쉽게 제공하며, 인터넷 사용자의 계정 관리를 자동화시키는 기능을 제공하는 PingFederate 6.0을 출시하였음
- Sxipper는 Firefox 브라우저의 확장 기능을 이용한 패스워드 관리 어플리케이션으로, WebWare에서 선정한 2007년 100대 웹 소프트웨어로 현재 'Sxipper 2.2.2'가 출시되었음. 개인 데이터는 암호화하여 안전하게 유지하며, 자동 Form Filling 기능을 제공함. OpenID 표준을 준용하여 OpenID를 이용한 로그인과 속성 정보 교환, 인증 레벨 정책에 따른 인증 기술을 제공하는 PAPE(Provider Authentication Policy Extension) 스펙 또한 제공함
- CPLab은 보안상 중요한 패스워드를 안전하게 저장 관리하는 어플리케이션인 'Password Manager XP'를 제공하고 있음. 현재 version 2.3.470이 출시되었으며 저장 관리 대상으로 모든 로그인 id, 패스워드, PIN 코드, 신용카드 번호, 접근 코드, 파일, 기타 중요 정보 등을 포함함. Blowfish, 3DES, Rijndael, Tea, Cast128, RC4, Serpent, Twofish 등의 암호화 알고리즘이 지원되어 원하는 암호화 방식을 사용할 수 있으며, 패스워드 생성 기능, 여러 컴퓨터에서 네트워크를 통해 여러 데이터베이스에 접근할 수 있는 기능, 패스워드 데이터베이스를 USB 플래시 드라이브와 같은 착탈식 장치에 저장할 수 있는 기능, 패스워드 데이터베이스의 백업 및 복원기능 등이 제공됨
- P3P는 해당 웹사이트를 방문하지 않고 검색 프로그램을 이용하여, 해당 웹사이트와 자신의 프라이버시 선호 수준을 입력을 하면 정책 선호도 및 해당 웹사이트의 정책 원문을 확인할 수 있는 에이전트의 새로운 대안 프로그램으로 2003년에 AT&T

개발을 시작으로 IBM 등에서 구현되고 있음. 사업자용 P3P는 IBM Tivoli Privacy Manager, 알파웍스, JRC P3P APPEL Privacy Preference Editor 등이 있고, 이용자용 P3P로는 Netscape, AT&T Privacy Bird, IE 등이 개발되어 보급되고 있음

- Oracle, Sybase, MS SQL Server DB2 등 주요 상용 DBMS들은 DB에 저장, 관리되는 정보를 보호하기 위해 사용자/IP/응용/접근시간대별 접근통제, 암호 및 보안감사로깅 기능을 제공하고 있으며 기존 DBMS에서 암호화 기능은 소프트웨어 방식을 적용한 이유로 운용 시 DB 서버의 성능을 상당히 떨어뜨리는 문제가 있어 이를 해결하기 위한 하드웨어 기반의 DB 암호화 솔루션이 개발되고 있음
- DB보안 전문솔루션은 DB 보안기능 수행에 따른 DBMS의 성능저하 문제를 해결하기 위해 개발되었으며, 접근제어 방식과 암호화 방식으로 구분됨. 접근제어 방식의 대표적 DB 보안솔루션으로는 Application Security사의 AppRadar, IPLocks사의 IPLocks 등이 있고 암호화 방식의 DB 보안솔루션으로는 Ingrian Network사의 Ingrian, Protegrity사의 Defiance Data Protection System 등이 있음
- Protegrity는 소프트웨어 에이전트 방식의 데이터베이스 암호화 업체 중에서 국외 시장 평가 1위인 업체로서 키 관리 기능은 별도의 하드웨어 제품으로 보완하고 있음. 특히 키 관리 기능은 DB 암호화에 적용할 때, 컬럼별 적용, 사용자별 적용과 같이 고려해야 할 요소가 많기 때문에 복잡도가 높아질 수밖에 없고, Protegrity는 이를 별도의 하드웨어 제품으로 해결하고 있음. DB 암호화 제품 적용 시 언급되는 난제 중 또 하나는 암호화된 컬럼에 대한 검색 속도 개선 문제가 있음
- Application Security에서 출시한 AppRadar는 실시간 모니터링 및 감사 기능과 기업용 데이터베이스 보안을 결합한 실시간 데이터베이스 활동 감시 솔루션임. 일반적인 네트워크 또는 운영체제 로그 시스템과 달리, AppRadar는 데이터베이스에 특화된 감사와 위협 감시를 수행하기 때문에 실시간으로 보안 이벤트들을 경고할 뿐만 아니라 또한 사용자 활동에 대해 정의된 감사기록 정보를 제공함
- JERICOA에서 출시한 iVault for iPhone(http://www.ivault.mobi)은 애플사의 iPhone이 대중화 되면서 AppStore에 출시된 제품으로, iPhone에 저장되는 개인정보를 암호화하여 안전하게 보관하는 기능을 제공함

〈표 4〉 국외 ID관리 및 접근제어 솔루션 개발 현황

구 분	기 관	내 용
User-centric ID	Microsoft	- CardSpace - 안전하고 신뢰된 방법으로 자신의 디지털 ID를 온라인 서비스에 제공하는 클라이언트 소프트웨어 - 다양한 ID 표준 지원 - 일관된 사용자 컨트롤 지원 - 패스워드 기반의 웹 로그인을 대체하는 토큰 기반의 보안 포맷 제공 - MS의 차세대 OS인 Vista에 탑재되어 제공
	Intel	- personal server - 전통적인 입출력 기능 없이 무선 인터넷을 이용하여 개인정보를 접근할 수 있음 - 인텔의 XScale 마이크로 아키텍처를 기반으로 저전력을 요구하면서 고성능의 연산이 가능함 - Apache 웹서버를 통해 무선으로 웹서비스를 지원하며, 파일 공유, 원격 기기제어 기능을 제공함
	SXIP	- OpenID - URL을 식별자로 사용하는 범용 인증 프로토콜을 제안 - LID, SXIP, SXIP, XRI/i-names 프로토콜을 포함하고 있음 - 지적재산권으로 보호받지만, 누구나 자유롭게 사용할 수 있는 정책임
	NetMesh	- SXIP, lid - LID는 URL을 식별자로 사용하는 인증 프로토콜로 SSO, 프로파일 데이터 교환, 소셜 네트워킹, 인증된 메시징과 블로깅을 제공할 수 있음
	NeuStar	- i-names - 도메인 네임과 유사하게 사람이 읽을 수 있는 식별자지만, 더 간단하고 사용하기 쉬움 - 조직의 경우 '@', 개인의 경우 '=' 가 접두사로 붙는 식별자 정책사용 - 식별자 뒤에 '+' 로 개인정보를 추가하여 공유할 수 있음 - 2006년 6월에 한국을 비롯하여 전세계에 서비스를 런칭하였음

구 분	기 관	내 용
Federated ID	Microsoft	- Active Directory Federation Service - Microsoft 제품 기반에서의 연동으로 시작되었으나, Unix, Linux 플랫폼으로 확장 - 중앙 집중 방식으로 ID관리 및 SSO 제공 - 특정 표준에 국한되지 않고 다양한 ID 기술을 적용한 플랫폼 기술인 ID 메타시스템 개념을 적용함
	Liberty Alliance	- Amex, AOL, GM, HP, Nokia, Sony, Sun 등 약 150 여개 업체로 구성 - 웹 서비스 지원을 위한 표준 제공 - 네트워크 ID 정보에 대한 보안과 개인정보 보호 제공 - 제3의 신뢰 기관 없이 고객 관리 및 연계 가능 - 분산된 인증, 인가를 통한 SSO 제공
IAM	IBM	- Tivoli Identity Manager - 웹기반의 셀프서비스 인터페이스 - 사용자 요청의 제출 및 승인과정을 자동화해주는 워크플로우 - 관리 작업의 적용을 자동화해주는 프로비저닝 엔진 - 관리자 권한 위임을 위한 Role 기반의 관리 모델
	SUN	- Java System Identity Manager - 빠르고 정확한 자동화 프로비저닝과 동기화 서비스 제공 - 간단한 정책 설정을 통해 규제 감시와 예방 기능 처리 - 수천 개의 id 생성과 업데이트를 수분 이내에 제공 - 99.9%의 가용성 보장
	Netegrity	- SiteMinder, IdentityMinder - 다양한 환경에서 중앙집중적인 정책기반 인증, 인가 관리 - 웹 서비스를 지원하는 정책기반 솔루션 - Role 기반의 권한 제어 기술과 위임 기술 - 웹 어플리케이션 및 기업 시스템에 대한 ID 기반 관리
	Oblix	- NetPoint with COREid, IDLink - SSO를 통한 편리한 웹 접근 관리 방법 제공 - End-to-End 프로비저닝 - 도메인간의 안전한 Federation 제공 - Seamless Enterprise Integration 제공 - 감사 및 리포팅 기능 제공
Privacy	IBM	- Tivoli Privacy Manager - 진보된 P3P 인터페이스 - Privacy 정책관리를 위한 언어 제공 - 개인정보 접근에 대한 모니터링 및 로그 기능 - 자동 리포팅 기능
	Zero Knowledge	- Enterprise Privacy Manager - Privacy 정책 표현을 위한 EPML(Enterprise Privacy Markup Language) - 기존 시스템으로부터 Privacy 정보 추출 방법 - Privacy 정책 분석 기능 제공 - 정책 리포팅 기능

2.2. 기술개발 현황 및 전망

2.2.1. 국내 기술개발 현황 및 전망

• 정부정책

- 방송통신위원회가 추진하고 있는 i-PIN은 대면 확인이 불가능한 인터넷 상에서 주민등록번호를 대신하여 본인임을 확인받을 수 있는 개인식별 정보임. i-PIN은 13자리 숫자나 영문자로 구성되며, 13자리 번호 자체에는 주민번호와 달리 생년월일, 출생지, 성별 등의 개인정보를 포함하지 않음. i-PIN 발급을 위한 신원확인 방법으로는 대면확인, 공인인증서, 신용카드 정보, 휴대폰 SMS 등이 이용되고 있음

  ▫ i-PIN은 2005년 10월부터 시범적으로 도입된 이후로 2009년 4월 256개 민간 웹사이트와 공공 웹사이트 681개(중앙부처 417, 지자체 245, 학교 등 19)가 도입하여 운영 중이며, 발급된 i-PIN은 민간 875,559건, 공공 90,799건임. 대표적인 i-PIN 도입 사이트로 MSN(Microsoft Network) 코리아는 2007년 7월 네티즌 의견 달기 과정에서의 본인확인 방법으로 i-PIN 을

채택했으며, 국내 대형 포털인 Daum과 Naver는 2007년 9월 및 10월에 i-PIN을 도입하여 서비스를 제공하고 있음

▫ 특히, 2008년 6월 개정되어 2009년 1월 시행령이 공표된 정보통신망법에서 일평균 이용자 수가 5만 명이 넘는 포털 사이트, 1만 명이 넘는 일반 웹사이트에 대해서는 주민등록번호를 이용하지 않고 회원에 가입할 수 있는 수단을 의무적으로 제공해야 함을 규정함에 따라, i-PIN 도입 사이트의 수는 향후 급속히 증가할 것으로 예상됨

▫ 방송통신위원회는 2007년 i-PIN 적용 사례집과 i-PIN 도입 매뉴얼 등도 배포하여 i-PIN 도입을 고려하는 웹사이트의 도입 절차 및 활용의 이해를 돕도록 하고 있으며, 2008년에는 KISA, 주요 포털업체와 공동으로 『i-PIN과 함께하는 개인정보 클린 캠페인』을 개최하였음. 이와 함께 인터넷 사업자를 대상으로 설명회를 지속적으로 개최하며, i-PIN 도입 업체에게는 'ePrivacy 마크' 인증 심사 시, 가산점을 부여하는 방식의 회유책을 병행하는 등 i-PIN 도입 확대를 위한 노력을 지속적으로 추진하고 있음

▫ 특히, i-PIN 보급의 저해요소로 거론되고 있는 제휴 서비스와의 연계 및 본인확인기관 기억의 어려움 등을 해결하기 위해 방송통신위원회는 2009년 3월 i-PIN 서비스의 편의성 향상을 위한 i-PIN 2.0 구현 계획과 i-PIN에 대한 인식제고 방안, 법제도 정비 계획 등을 포함한 『인터넷상 주민등록번호 대체수단(i-PIN) 이용 활성화 기본 계획(안)』을 발표하였음

▫ 방송통신위원회와 KISA는 2009년 6월1일부터 30일까지 i-PIN 홈페이지(http://www.i-pin.kr)에서 '2009 자기정보보호 캠페인 '을 개최하며, ID/PW 변경과 i-PIN의 한글이름 공모를 통해 i-PIN에 대한 인식을 제고하고 있음

- 방송통신위원회는 2008년 6월 '정보통신망 이용촉진 및 정보보호 등에 관한 법률(정보통신망법)' 의 제23조의2를 다음과 같이 신설하여 주민등록번호만으로 웹사이트 회원가입에 사용하는 경우 개인정보의 침해가능성을 해소하고자 함

① 정보통신서비스 제공자로서 제공하는 정보통신서비스의 유형별 일일 평균 이용자 수가 대통령령으로 정하는 기준에 해당하는 자는 이용자가 정보통신마을을 통하여 회원으로 가입하는 경우에 주민등록번호를 사용하지 아니하고도 회원으로 가입할 수 있는 방법을 제공하여야 함

② 제1항에 해당하는 정보통신서비스 제공자는 주민등록번호를 사용하는 회원가입 방법을 따로 제공하여 이용자가 회원가입 방법을 선택할 수 있음

▫ 개정 정보통신망법에 대한 시행령에서 정보통신서비스의 유형별 일일 평균 이용자수에 대한 기준을 포털 사이트의 경우 5만 명, 일반 웹사이트의 경우 1만 명으로 정의하고 있어 대상이 되는 웹사이트는 주민등록번호를 사용하지 않고도 회원 가입할 수 있는 방법을 제공해야 함에 따라, i-PIN 도입이 활성화될 수 있을 것으로 기대됨

- 행정안전부는 공공기관에서의 개인정보보호를 위한 ID관리 체계 구축을 핵심으로 한 통합ID관리 서비스를 추진하였음. 통합ID관리 서비스는 정부부처 및 지방자치단체, 공공기관 등의 사이트에 다양하게 산재되어 있는 회원들의 개인정보를 안전하게 보호, 관리하는 서비스로서, 행정안전부는 2007년에 중앙행정기관 및 지방자치단체 300여 기관에 서비스를 도입하는 것을 시작으로 2008년에는 각급 교육기관 및 기타 행정기관 1만 3000여 곳, 2009년에는 서비스 이용을 희망하는 공공기관으로 서비스를 확대한다는 3단계 추진 계획을 마련하였음

▫ 통합ID관리 서비스는 g-PIN으로 명칭을 변경하였으며, 2008년 7월부터 행정안전부는 g-PIN 센터(http://g-pin.go.kr)를 구축하여 시범적용 테스트를 진행중임. 행정안전부는 2010년까지 g-PIN을 전국적으로 도입할 계획이었으나, 2008년 7월 방송통신위원회와 합의에 따라 g-PIN을 공공 i-PIN으로 명명하고 정부 · 공공 기관은 g-PIN 센터와 시스템을 연계하도록 하고, 공공 i-PIN은 공인 PKI 인증서, 주민등록확인시스템, 읍면동 주민센터를 이용한 대면확인으로 본인임을 증명함

▫ 2008년 8월부터 중앙행정기관, 지방자치단체 대표 홈페이지부터 공공 i-PIN을 보급하고 있으며, 2009년 5월에 약 700여 개, 2009년 내에 중앙행정기관 · 지방자치단체 소속기관, 공사 · 공단, 교육기관, 학교 등 약 2,000여개 공공기관 홈페이지에 추가로 공공 i-PIN을 확대 보급하고 장애인과 고령자가 공공 i-PIN을 편리하게 이용 할 수 있도록 관련 소프트웨어(SW)를 개선할 계획임

- i-PIN 서비스는 민간분야의 4개 본인확인기관에서 제공되는 가상주민번호(한국신용평가정보), OnePASS(한국정보인증), 나이스아이핀(한국신용정보), Siren24아이핀(서울신용평가정보)가 제공되고 있으며, 공공분야는 행정안전부에서 공공

i-PIN 서비스를 제공하고 있음. 특히, 2008년 8월 서비스 개시한 공공 i-PIN은 현재 민간 i-PIN과의 연계가 가능해 i-PIN 이용자는 하나의 i-PIN으로 공공 · 민간 웹사이트를 모두 이용할 수 있음

▫ 행정안전부는 방송통신위원회, 교육과학기술부, 외교통상부와 함께 재외국민 및 초중고학생의 인터넷 이용 편의를 위한 '공공 아이핀 서비스 활성화 방안' 을 마련하고 관련 시스템을 개발하여 2009년 9월부터 서비스할 계획임

- 행정안전부는 2010년까지 우리나라 정보보호 순위를 세계 5위 수준으로 끌어올리는 계획을 추진하기 위해 금년 하반기 개인정보보호법을 제정하여 개인정보에 수집 · 이용 · 제공 등을 엄격히 통제하고, 법률에 근거하거나 개인의 동의에 의해서만 개인정보를 수집할 수 있도록 함으로써 공공 · 민간의 웹사이트 상의 주민번호 수집률이 현재 69%에서 2012년에는 30% 이내로 축소를 목표로 함

▫ 이를 위해 주민등록번호에 대한 사회적 관행을 개선하기 위해 주민등록번호와 같이 개인을 식별할 수 있는 고유정보의 수집 · 저장 · 유통을 통제하고, 주민등록번호 은행계좌번호 등 주요 정보는 반드시 암호화 하도록 함으로서 무분별한 개인정보 이용에 대한 사회적 관행과 개인정보 오남용을 개선할 예정임

▫ 또한, 정보가 유출되었을 때 피해가 큰 주민번호, 은행계좌번호, id와 패스워드 등 주요정보는 반드시 암호화하여 저장 · 유통하도록 의무화되며, 정보의 주체자(해당 개인)는 공공기관의 자기정보 열람 · 제공 내역을 언제든지 확인할 수 있어 개인정보의 자기통제권이 강화됨에 따라 개인정보의 무분별한 오 · 남용을 방지할 계획임

▫ 2008년 중국발 해킹 시도가 9,000만 여 건으로 2007년보다 2배 이상 급증하고 개인정보 유출로 인한 개인정보 침해사고 신고도 전년보다 53% 증가함에 따라, 2009년 4월 21일 행정안전부는 지식경제부, 방송통신위원회, 국가정보원 등과 함께 정보해킹 및 개인정보 유출 실태를 국무회의에 보고하고, 이를 막기 위해 i-PIN의 확대 보급이 포함된 8개 역점 추진과제를 선정하였음

- 방송통신위원회는 인터넷 이용환경의 안전성 제고 및 인터넷 경제의 신뢰기반 조성을 목표로 하는 인터넷 정보보호 종합대책을 발표하였음. 동 종합대책은 침해사고 예방 및 대응능력 제고, 개인정보 관리 및 피해구제 체계 정비, 건전한 인터넷 이용질서 확립, 정보보호 기반조성 등 4개 전략을 달성하기 위한 50개 세부 대책으로 구성되어 있음

▫ 이 중 개인정보 관리 및 피해구제 체계 정비 전략에는 주민등록번호 등 개인식별번호는 법령으로 규정한 경우 외에는 수집 · 저장 · 유통 등 처리를 금지하고 사업자의 인터넷 상 개인정보 수집을 최소화 하도록 규제화할 예정임

▫ 또한 개인정보 유출 시 추가적인 활용이 불가능하도록 계좌번호 등 중요 개인정보는 암호화하여 저장하도록 의무화할 계획임

▫ 이 밖에도 인터넷상 개인정보 유출을 실시간 탐지 · 대응할 수 있는 시스템 구축, 개인정보 대량 유 · 노출 사이트에 대한 접속 차단제 실시, 개인정보보호 인증제도 도입 등 개인정보 유출방지 대응체계를 강화할 예정임

• 기술개발

- ETRI는 Microsoft, KISA와 공동으로 2007년부터 2009년까지 수행하는 '자기통제 강화형 전자ID지갑 시스템 기술개발' 과제에서 Information Card 솔루션인 전자ID지갑을 개발하였음. 전자ID지갑은 사용자 본인이 개인정보와 인증정보(id/pw, 인증서 등)를 안전하게 관리하고 있다가, 언제 어디서나 자신을 인증하고 개인정보를 자신의 통제 하에 선택하여 이용할 수 있는 시스템임

▫ 1차년도인 2007년에 개발된 프로토타입은 IETF 표준인 SASL(Simple Authentication Security Layer)을 활용한 범용인증 서비스, Identity 정보 공유 및 Link Contract, Identity 동기화 기능을 제공하는 Identity 공유 서비스, 전자ID지갑을 이용한 사이트 가입 및 인증 기능을 구현하였음

▫ 2차년도인 2008년에는 1차년도의 프로토타입을 상용 수준으로 개발하고 i-PIN, OpenID, CardSpace 등의 관련 표준들과 호환되며, 오픈소스 환경뿐만 아니라 모바일 환경에서도 동작하도록 진행하였음

▫ 3차년도(2009년)는 i-PIN에 최적화되어 동작할 수 있는 lightweight 버전의 전자ID지갑을 개발하였으며 KISA와 i-PIN 기관들이 참여하는 시범서비스를 추진하고 있음. 또한 스마트폰과 같은 모바일 단말에서 동작하는 모바일 전자ID지갑의

개발을 진행하고 있음.

- 공공 i-PIN의 경우 민간 부문에서 사용되는 i-PIN과 역할이 중복되지만, 실제로 사용되는 기술이 다르기 때문에 호환이 불가능하다는 점이 지적되었음. 이를 해결하기 위해 2008년 6월, ETRI는 'PIN 연계 기술'을 개발하여 i-PIN의 상호운용 메시지를 해석하여 SAML 메시지로 변환하는 기능, SAML 메시지를 해석하여 i-PIN 상호운용 메시지로 변환하는 기능을 제공함. 이 기술은 통해 i-PIN을 보유한 사용자가 공공 i-PIN을 만들 필요 없이 자유롭게 서비스를 이용할 수 있게 됨

- 2008년 5월, KISA는 i-PIN 본인확인기관간 키 분배 서비스를 정의하였음. 키 분배 프로토콜로는 RFC 2412인 OAKLEY Key Determination Protocol을 준용하였음. 이 프로토콜은 각 분기별로 본인확인기관별로 i-PIN 상호운용 메시지에 사용할 마스터키를 생성하고, 업체 간에 이 키를 각각 분배하는 절차를 수행함

- OAuth는 단순하고 표준화된 방식으로 안전한 API 인증이 가능하도록 하는 공개 인가 프로토콜임. 현재 국내에서는 NC소프트의 자회사인 오픈마루가 OpenAPI 인증을 총괄하는 API 센터에서 스프링노트(http://www.springnote.com/)와 귓속말(http://blog.openmaru.com/216) 서비스의 OpenAPI를 사용하기 위한 인증 방식으로 OAuth를 지원한다고 발표하였음. 또한 2008년 6월 이후로는 OAuth 인증 방식을 사용하는 OpenAPI 서비스만 신규 지원하고 있음

- 현재 국내의 OpenID 프로바이더는 1.1 버전의 인증 체계를 사용하고 있음. 국내의 특수한 상황을 고려하여, NC소프트의 자회사인 오픈마루에서는 OpenID 프로바이더인 myID를 확장하여 제한적 본인확인제 사이트에 OpenID 로그인을 지원하였음. 사이트의 Id 인증과 회원 계정을 분리하여, OpenID를 로그인 방법으로 하나 더 지원하는 개념을 채용하였음. 따라서 OpenID 프로바이더 자체는 본인확인을 기본적으로 수행할 부담 없이, 본인확인제 사이트에 접근하는 OpenID 사용자에게만 한 번 실명확인을 거치게 됨

- P3P 1.0 버전을 기반으로 국내 개인정보보호법제 사항을 반영한 P3P스펙과 정책생성기, 민간업체 KT는 P3P 이용자 에이전트를 개발하였고, 2007년 개인정보취급방침의 전자적 표시방법 고시안의 제정과 함께 KISA는 체크프라이버시 S/W를 개발하여 보급을 하고 있으며 TTA에서 개인정보보호 정책 설정 및 협상 규격표준을 표준으로 제정하였음
  - PAgent는 사이트 정책 충돌 여부 등을 판단하여 신뢰도를 5등급으로 나누어 결과 값을 5가지 색으로 표시하고 경고음, 팝업창 등을 통해 결과를 구현하고 각각의 정책에 대한 수준을 설정하고 해당 정보에 대한 접근수준, 수집 · 이용 목적 항목을 설정할 수 있으며, 방문사이트의 이력관리, 신뢰사이트 등록 등을 지원함

- DB보안기술은 크게 접근제어 방식과 암호 방식으로 구분되며, 접근제어 방식의 DB 보안솔루션은 웨어밸리, 피앤피시큐어, 바넷정보기술, 소만사, 모니터랩, STG시큐리티 사 등에 의해 개발되었고, 암호 방식의 DB 보안제품은 펜타시큐리티, 이글로벌시스템, 소프트포럼, 이니텍 사에 의해 지원되고 있음

- 사용자 단말에서의 개인정보 보호 기술은 스마트카드 방식과 소프트웨어에 의한 자체 암호화 방식 등이 이용되고 있음. 스마트카드 방식은 가장 안전한 기술로 여겨지고 있으며, 이미 신용카드, 직불카드 등에서 이용되고 있으나 PC와 스마트폰 등에서 활발히 이용되고 있지는 못함. 스마트폰 운영체제로 가장 많이 사용되는 Windows Mobile OS는 id/password를 저장할 수 있는 Credential Manager API를 제공하고 있음. 그러나 대부분의 스마트폰 어플리케이션들은 이러한 기능을 사용하지 않고 직접 관리가 쉬운 저장 영역에 id/password를 포함한 개인정보들을 저장하는 방식을 이용함. 필요에 따라서는 암호화 되어 있으나, 암호 기술에 대한 인식 부족으로 취약성이 매우 높음

- 국내의 모바일 플랫폼 표준인 WIPI는 개인정보보호 기능이 거의 전무함. 따라서 대부분의 WIPI 어플리케이션은 개인정보를 파일시스템에 저장하고 암호화가 필요한 경우 자체적으로 수행함. WIPI 기반의 대표적인 웹브라우저인 인프라웨어의 폴라리스의 경우에도 자체 암호방식을 이용해서 id/password 등을 파일시스템의 특정 공간에 저장함

2.2.2. 국외 기술개발 현황 및 전망

• 정부정책

- 미국은 지난 2003년 id/pw, PKI, 바이오정보 등을 통한 사용자 인증 프레임워크를 제공하기 위하여 크리덴셜의 안정성 기준과 발급기관의 신뢰성 평가 등을 포함한 e-Authentication 정책을 수립하여 추진 중임. NIST(National Institute of Standards and Technology)는 크리덴셜 기술표준 개발, 크리덴셜 발급기관의 신뢰성 평가, 크리덴셜 발급 및 검증 솔루션에 대한 상호운용성 테스트를 수행함. e-Authentication 이니셔티브는 온라인 환경에서의 새로운 인증관련 비즈니스 모델을 개발하는 '전자인증 파트너십(Electronic Authentication Partnership)'을 추진하고 있으며, 미 연방정부의 전자인증 프레임워크를 지원하는 Relying Party의 수는 2007년 2분기의 46개에서 2008년 1분기의 97개(정부기관 21곳, 웹사이트 76곳)에 달하며 IdP 역할을 수행하는 CSP(Credential Service Providers)는 8개가 존재함(E-Authentication Solutions, DOE Information Management Conference, 2008/3/19)

- 2007년 5월에 발간된 'e-Authentication의 기술 아키텍처 가이드라인 v2.0'에 따르면 연계된 ID공유 스킴으로 OASIS의 SAML 표준을 지원한다고 명시되어 있으며 자세한 적용 방안을 설명하고 있음. 이 문서에서에 따르면 e-Authentication에 구축되는 제품들은 2007년 내에 SAML 2.0 SSO 프로파일을 적용해야 함. 이에 따라 e-Authentication 상호운용성 연구실에서 SAML 표준을 준용한 제품들의 상호운용성을 시험하고 있으며, 이미 CA, HP, IBM, Novell, Oracle, RSA, Sun 등의 기업 제품이 테스트를 통과하였음. 2008년 7월 30일자로, SAML 2.0 테스트를 통과한 e-Authentication 참여 기업은 CA, Ping Identity, Entrust, HP, IBM, Sun임(U.S. E-Authentication Identity Federation Approved Product List(APL), 2008/7/30).

- 유럽연합(EU)은 'i2010 전자정부 실행계획'에 따라 2010년까지 상호인정 및 연동 가능한 디지털 ID관리 프레임워크 구축을 목표로, 2007년에는 상호운용 가능한 디지털ID관리 기술의 공통사항 합의, 2008년에는 대규모 시험 프로젝트의 운용 및 관찰을 거쳐 2010년까지 범 유럽 차원에서 운용할 수 있는 디지털 ID관리 시스템 구축을 추진 중임. 대표적인 관련 기술연구 프로젝트로는 FIDIS(Future of Identity in the Information Society), GUIDE, MordinisIDM, PRIME(Privacy and Identity Management for Europe), adapID(advanced applications for electronic Identity cards in Flanders) 등이 있음
  - EU는 2006년부터 여권 없이 국경 통과가 가능하며, 운전면허증 기능을 통합한 EUID라는 유럽 공통 ID카드 개발을 추진하고 있음

- 오스트레일리아는 정부 부서의 관할 하에 빅토리아 주 정부의 프로젝트인 VBMK(Victorian Business Master Key) 프로젝트를 통해 정부의 중요 정보를 비즈니스에 쉽게 사용할 수 있도록 하였음. 사업자들은 SSO 기능을 통하여 한 번의 로그인으로 여러 정부 부처가 제공하는 정보를 사용할 수 있게 되었음. 이 프로젝트는 2006년 2월부터 SAML 2.0 기술을 적용하여 SSO 기능을 제공 중임. VBMK 프로젝트는 3년 동안 6백만 호주 달러(약 48억 원)로 운영되고 있으며, 현재 VBMK는 매년 65,000 명의 비즈니스 가입자를 신규로 받고 있음
  - 오스트레일리아 중앙 정부는 2005년부터 AGAF(Australian Government e-Authentication Framework)를 지원하며, 업계에 인증 솔루션을 제공하는 VANGuard 프로그램을 2006/2007년도에 신설하였음
  - VANGuard가 현재 제공하는 기능은 사용자 인증, 고객이 서명한 전자문서의 검증, 브라우저 기반 거래에서 서명을 통한 부인 봉쇄 등임. 향후에는 정부기관, 공장 간에 안전한 거래를 보장하는 보안토큰 및 상호인증을 통한 SSO 기능을 제공할 예정임

- 일본은 신뢰기관을 통한 사용자 인증기반을 마련하여 사용자의 개인정보를 보호하기 위해 차세대 전자인증 프로젝트를 진행중임. 크리덴셜 서비스제공자 및 서비스 제공자가 적절한 인증수단을 선택할 수 있도록 가이드라인을 제시하고, SAML과 같은 표준 명세에 기반하여 상호운용성이 보장된 인증서비스가 제공될 수 있도록 기반을 마련함
  - 세부 내용으로는 차세대 인증 적용 시 관련되는 참여자를 식별하고 크리덴셜 발급과 관련하여 필요한 시나리오 개발을 위

해 전자인증 업무 모델 체계를 수립함. 또한 인증프레임워크, 보증레벨을 결정하는 절차, 운영 및 기술기준으로 구성된 인증가이드라인을 개발하고, 사용자와 인증서비스 제공자간 계약 시 참조될 수 있는 합의서 등의 템플릿을 제공할 예정임

▫ 일본에서는 2006년 4월부터 전 국민을 대상으로 전자주민증을 보급하고 있으며, 미국입국을 위한 전자여권 개발에서 앞장서 전자여권을 현재 시험발급하고 있음

- 웹사이트 이용자들의 효과적인 개인정보보호방침 확인을 위해 요약 방침, 다단계 고지 방법 등의 채택을 권고하는 국제적 움직임이 있으며, APEC, OECD 등 주요 국제기구 연구반에서 방침에 대한 고지를 개인정보보호 분야 주요 현안으로 다루고 있고 기업뿐만 아니라 호주, 뉴질랜드, 온타리오와 같은 다양한 정부들이 다단계 고지를 적극적으로 활용하고 채택하였음

▫ 캐나다의 경우 BC와 온타리오에서 Healthcare 분야에서 다단계 고지를 도입하였음

▫ 호주의 경우 프라이버시법에서 간략한 프라이버시 고지를 활용할 것을 장려하고 정부 분야에서는 세계에서 처음으로 2005년 7월부터 다단계 고지를 웹사이트에 게시하였음

▫ 미국의 경우 US Postal service가 웹사이트에 다단계 고지를 도입하였음

• **기술개발**

- Bandit 프로젝트는 2006년 6월에 시작된 이후, ID 인프라를 구성할 수 있는 공개 시스템을 구성하기 위해 상호운용성과 통합 관점에서 관련 기술을 개발하고 공개적으로 표준화하였음 따라서 Bandit 을 적용한 제품은 ID저장소의 위치에 무관하며, 다양한 인증 방법을 지원하고 쉽게 기존 시스템에 적용할 수 있음

▫ Bandit은 2007년에 CardSpace와 Liberty Alliance의 스펙을 지원하였음. 2008년 상반기에 Bandit은 DigitalME의 핵심 기능을 개선하고 OpenID를 지원하는 등의 작업을 수행하는 버전 2.0 개발을 진행중임. 2008년 3월부터 Bandit 2.0과 Higgins 1.0을 개발하기 시작하였으며, 6월에는 DigitalME를 개발하기 시작하였으며 2008년 10월에 Bandit 2.0을 완성하였음

- Higgins 프로젝트는 2004년 Eclipse 재단에서 'Eclipse Trust Framework' 라는 이름으로 시작되었으며, 2006년부터 IBM, Novell, Google, Microsoft 등이 지원하는 프로젝트임. Higgins는 다양한 사이트, 애플리케이션, 디바이스에 흩어져 있는 ID/프로파일/소셜 관계 정보를 통합 제공하는 인터넷 ID 프레임워크를 지향함. 특정 프로토콜이 아닌 소프트웨어 아키텍처로서, 기존의 모든 ID 프로토콜을 지원하면서도 일관된 사용자 경험을 제공함. 이를 통해 사용자가 웹사이트에 가입할 때 정보를 제공하는 작업, 커뮤니티 간에 데이터를 교환하는 작업, 소셜 네트워킹 프로그램들과 정보를 공유하는 작업, 자신만의 애플리케이션을 구축하는 작업 등을 쉽게 처리할 수 있음

▫ Higgins 아키텍처의 설계 철학은 모든 컴포넌트를 플러그인(plug-in) 방식으로 제공하는 것임. 이에 따라 데이터 저장소, 보안 토큰 타입, 보안 프로토콜, 데이터 카드 타입, 토큰 서비스를 플러그인 방식으로 자유롭게 추가/제거하게 됨

▫ 2008년 2월에 1.0 버전을 릴리즈했고, 2009년 3사분기에 1.1 버전을 개발 완료할 예정임. 향후 id/pw 카드와 relationship 카드 타입을 지원하고 모바일 단말까지 확장할 예정임

- Information Cards는 Microsoft의 ID Metasystem에 따라 CardSpace와 같은 IS(Identity Selector)의 상호운용성을 제공하기 위한 스펙 및 기술을 총칭함. 관련 스펙은 2007년 1.0 버전에서 2008년 7월 1.5 버전으로 확장되었음. OASIS의 IMI(Identity Metasystem Interoperability) TC는 1.0 드래프트 버전을 2009년 2월 작성하였고 6월에 표준화할 예정임

- OSIS(Open Source Information System)는 2006년에 만들어진 단체로 사용자 중심의 ID관리 기술들의 상호운용성을 목표로 함. 이 목표에 따라 OSIS는 Microsoft의 CardSpace 표준인 ISIP(Identity Selector Interoperability Profile)를 기준으로 타 Information Card 프로젝트들의 호환성을 주도하였음. 지금까지 5차례의 상호운용성 시험을 수행하였으며, RSA 2009에서 열린 최근의 상호운용성 시험에는 17개의 IDP, 35개의 RP, 5개의 IS, 19개의 OP, 15개의 OpenID RP가 참여하였음

- Liberty Alliance는 2005년에 Liberty ID-FF(IDentity Federation Framework), ID-WSF(IDentity Web Services Framework), ID-SIS(IDentity Services Interface Specification)를 만들었으며, 해당 내용을 SAML 표준에 반영시켰음. 이후에는 여러 도메인 간의 정책이나 프라이버시 보호 정책을 반영한 표준화된 프레임워크를 개발하고 있으며, 구체적인 결과물로 IAF(Identity Assurance Framework)와 IGF(Identity Governance Framework)라는 프레임워크를 개발 중임. 이들 프레임워크를 통해 상호운용성, 보안 정책 기반의 ID 솔루션 시장 확대, 사용자를 ID 도용이나 침해로부터 보호하며 기업들의 규제 요구사항을 만족시킬 수 있음
  - IAF(Identity Assurance Framework)는 Liberty Alliance의 IAEG(Identity Assurance Expert Group)가 관리하며, 2008년 6월 1.1 버전 스펙을 공개하였음. 이 스펙은 미국의 e-Authentication 전략 프레임워크를 기반으로 Common Organization 서비스 평가, Identity Proofing 서비스 평가, Credential Management 서비스 평가 항목을 4단계 보증 레벨에 따라 구분하였음. 또한 IAF의 구축단계에서 조직의 순응도, identity proofing 서비스, 인증서 강도, 인증서 관리 서비스 등을 평가하는 체계를 다룬 Service Assessment Criteria(SAC) 드래프트 버전을 2009년 6월 릴리즈하였음
  - IGF(Identity Governance Framework)는 기업 내 시스템 간의 ID 정보 교환 체계를 두어, ID 정보를 효과적으로 처리하기 위한 목적으로 2006년 11월에 발족한 프로젝트임. Liberty Alliance의 TEG(Technology Expert Group)가 관리하며, OpenLiberty.org에서 오픈 소스로 구현 중임. IGF는 산업계의 주도로 만든 첫 번째 정책 프레임워크로, 규제 정책(유럽의 데이터 보호 이니셔티브, Gramm-Leach-Bliley 법, PCI 보안 표준, Sarbanes-Oxley)을 준수하여 조직 내의 identity 흐름을 관리함. 2008년 6월에 IGF의 스펙과 스키마, 프라이버시 제약사항을 명시한 1.0 드래프트 문서를 릴리즈하였음
  - Concordia 프로젝트는 기존의 ID관리 프로토콜이 해결하지 못하는 문제나 시나리오에 대처하기 위한 방안을 고안하는 프로젝트로, 2007년 4월부터 Liberty Alliance의 주관으로 운영 중임. Concordia는 상호연동성과 프라이버시 보호 기능을 제공하는 ID 계층을 개발함으로써 개발 및 구축 과정에서 더 높은 성공률과 생산성을 보장하려는 목적을 가짐
  - Kantara 이니셔티브는 2009년 6월 Concordia, DataPortability Project, Information Card Foundation, Internet Society, Liberty Alliance, OpenLiberty.org, XDI.org의 7개 단체와 ID관리 기업 45 곳이 참여하며, 상호운용이 가능한 ID관리 솔루션을 전세계에 보급시키는 것을 목적으로 함. 공개 표준에 근거하여 사용자의 편의성, 보안, 프라이버시 보호에 초점을 맞추며, 이를 통해 IAF, ID-WSF, Information Card, OAuth, OpenID, SAML 2.0, WS-*, XACML, XDI 등의 표준을 조합한 솔루션이 개발될 예정임

- OAuth 토론그룹은 2007년 4월에 구성되었으며, OAuth의 드래프트 문서 작성과 실제 구현을 담당하였음. 2007년 7월에 초기 스펙이 완성되었으며, 2007년 10월에 OAuth Core 1.0 최종 드래프트 문서가 완성되었음. 스펙은 업데이트 되지 않았으나, 2008년 6월 26일에 개최된 OAuth Summit 2008에서는 OAuth 프로토콜, 확장성, OAuth 구현 사례를 공유하면서 특히 OAuth Core 1.0 스펙에 추가되는 여러 요구사항이 언급되었음
  - OAuth는 최근 여러 서비스의 인가 기능으로 활발하게 도입되었으나, 2009년 4월에 프로토콜 상의 문제점이 노출되어 전면적으로 사용이 중단된 상태임. OAuth 측은 경고 문구를 서비스 중간에 삽입할 것을 권고하였으며, 수정된 프로토콜을 차후 공개할 예정임

- Shibboleth 프로젝트는 American Chemical Society를 비롯한 20개 기관이 Information Provider로 동작하며, GridShip과 Napster를 비롯한 25개 시스템과 연동됨. Condor-Shib, Grid-Shib, Project Sentinel Collaboratory와 같이 미국 내에서의 연동 프로젝트뿐만 아니라, SAML을 기반으로 노르웨이의 교육센터에 federated ID관리를 제공하는 FEIDE(Federated Electronic Identity), 덴마크의 고등 교육기관의 리소스 관리를 위한 DK-AAI 프로젝트, 스웨덴의 교육기관을 대상으로 SAML기반의 federated ID 서비스를 제공하는 SWAMID(SWedish ACadeMic IDentity), 스위스의 SWITCH(Swiss Education and Research Network) 인증 인가 인프라(Authentication and Authorization Infrastructure(AAI)), Shibboleth를 테스트한 영국의 SDSS(Shibboleth Development and Support Services)과 실제로 제품화를 시작한 영국의 Access Management Federation for Education and Research 프로젝트, 영국의 JISC Core Middleware Initiative, 오스트레일리아의 고등 교육기관을 위한 연계된 IAM 인프라를 구축하는 MAMS(Meta-Access Management System), 프랑스의

고등 교육 기관을 대상으로 국가적인 federation을 구축하는 목적으로 2006년 10월에 제품화를 시작한 CRU 프로젝트, 핀란드 대학간의 ID Federation을 통한 SSO를 제공하는 Haka 등의 국제적 프로젝트가 있음

▫ Shibboleth는 2007년 8월 1.3 버전이 출시되었으며, OpenSAML 2.0 이 정식으로 출시된 이후 2008년 3월 Shibboleth 2.0이 완료되었음

▫ 2008년 8월 11일, Shibboleth는 2.0 버전의 다양한 버그를 해결하고 일부 기능을 개선한 2.1 버전의 SP(Service Provider)를 공개하였음

▫ 2009년 6월에 공개한 2.2 버전의 로드맵에 따르면, IDP에 JAAS와 X.509 인증을 지원하며, SAML ECP를 지원함. 또한 ADFS(Active Directory Federation Server) v1을 지원하며, Information Card를 IDP와 SP에서 사용하도록 하며 OpenID 2.0을 지원함

- OpenID는 2007년 12월, 인증 스펙 2.0 버전과 속성 교환(Attribute Exchange) 1.0 버전을 완성하였음. 이미 여러 번의 드래프트 작업으로 스펙은 완성되어 있었는데, OpenID 표준에 대한 지적재산권을 보유한 SXIP사가 Non-Assertion Agreement 에 서명하면서 18개월간의 스펙 작업이 완료되었음

  ▫ 현재 진행 중인 드래프트 문서로 Data Transport Protocol v1.0, Simple Registration Extension v1.1, Provider Authentication Policy Extension v1.0이 존재함

- OpenID SReg(Simple Registration) Extension 1.0에는 개인정보 구성요소를 9개(nickname, email, fullname, date of birth, gender, postcode, country, language, timezone)로 정의하였으나 OpenID Attribute Exchange 1.0에서는 Simple Registration에서 정의된 기본 정보 외에 Name, Work, Date of Birth, Telephone, Address, Email, Instant Messaging, Web Sites, Audio/Vide Greetings, Images 그리고 기타 Preferences를 정의함으로써 개인정보를 보다 상세히 정의하고 있음

- 인터넷을 위한 개방형 ID, 연관성 개발을 목적으로 하는 Identity Commons에서는 ID 스키마 개발을 위해 FOAF, VCard, MS Outlook CSV Export, Google Contact API와 Contact Kind, Google OpenSocial Data API, LDAP/DSML, OpenID SReg, OpenID AX, ID-SIS Personal Profile Service, ID-SIS Employee Profile Service 등에서 개발된 ID 관련 스키마를 참조하고 있음

- P3P는 해당 웹사이트를 방문하지 않고 검색 프로그램을 이용하여, 해당 웹사이트와 자신의 프라이버시 선호 수준을 입력을 하면 정책 선호도 및 해당 웹사이트의 정책 원문을 확인할 수 있는 에이전트의 새로운 대안 프로그램으로 2003년에 AT&T 개발을 시작으로 IBM 등에서 개발되었음

  ▫ 또한, P3P 관련 S/W는 크게 에이전트와 정책생성기, 사업자용과 이용자용으로 나누어 개발되며, 대부분의 S/W는 무료로 보급되고 있으나 정책 생성기는 일부 유료로 제공하며, 2006년 7월말 기준으로 P3P채택을 신고한 사이트가 약 870여 개로 실제로 적용하고 있는 업체를 포함하면 훨씬 많은 사이트가 채택한 것으로 추정됨

  ▫ 사업자용 P3P는 IBM Tivoli Privacy Manager, 알파웍스, JRC P3P APPEL Privacy Preference Editor 등이 있고, 이용자용 P3P로는 Netscape 7.0, AT&T Privacy Bird, IE 6.0 등이 개발되어 보급되고 있음

- ID관리 분야는 SAML, Liberty Alliance와 같은 기업 위주의 ID관리 기술과, CardSpace, OpenID 등의 사용자 중심의 ID관리 기술로 양분되어 진행되고 있음. 기업 위주의 ID관리 기술은 법률이나 규제를 만족하면서 조직 내 · 외부의 ID 정보를 안전하게 공유하는 방법을 다루고 있으며, 개별 기술보다는 실제 적용을 고려한 프레임워크 관점을 지향하고 있음. 이에 따라 SAML을 기반으로 하는 Liberty Alliance의 IAF, IGF, e-Authentication 전략 등이 업계를 중심으로 개발 및 적용될 전망임. 사용자 중심의 ID관리 기술은 급격하게 진행되고 있으며, 관련 표준 및 사용자들의 증가 추세가 뚜렷함. OpenID의 경우, 초기에는 신뢰를 고려하지 않은 블로그 수준의 인증에만 사용될 것으로 예상되어 파급력이 미미했으나 최근에는 whiltelist나 PAPE 같은 신뢰 기반의 연결을 고려하고 있음. 또한 google, yahoo, microsoft, myspace, facebook, daum 등의 메이저 업체가 OpenID를 지원하고 있으며 OpenID 수는 5억여 개에 달함. 마지막으로 CardSpace의 경우, Identity

Selector를 개발하는 여러 프로젝트들의 상호호환성을 만족하는 기준으로 ISIP(Identity Selector Interoperability Profile)가 사용되고 있으며, 여러 기업들이 ISIP를 준용하는 솔루션을 개발하고 상호운용성 시험을 통과함. 현재는 CardSpace의 도입이 지체되고 있지만, 향후 id/pw 기반의 인증 체계를 근본적으로 변화시키는 대안이 될 것임

- 모바일 디바이스에서의 개인정보 보호는 SIM/USIM을 중심으로 이루어짐. SIM/USIM은 가장 안전한 저장매체로 여겨지는 스마트카드의 모바일 디바이스용 인터페이스임. USIM은 자체 저장장소를 제공하며, Network Provider 가입자 정보뿐만 아니라 SMS, 주소록 등의 개인정보도 안전하게 저장할 수 있음. 그러나 SIM 카드 내부의 데이터 저장 공간의 한계 등으로 대부분의 모바일 디바이스 어플리케이션들은 SIM 대신에 파일시스템 저장장치를 선호하는 경향이 높음. 따라서 디바이스를 분실했을 때, 개인의 SMS 내용, 주소록, 인터넷 접속 기록 등의 개인정보는 타인에게 바로 노출된다고 볼 수 있음

- iPhone의 대중화로 촉발된 모바일 환경에서의 인터넷 이용은 모바일 디바이스에 더욱 더 많은 개인정보를 저장하게 만들었음. PC 환경에서는 보통 저장하지 않는 웹사이트 로그인 비밀번호도 iPhone 등의 모바일 디바이스에서는 이용상의 불편함 때문에 비밀번호 저장기능을 이용하는 경향이 높아짐. 이를 보완하기 위해서 최근 일부 제품들이 출시되고 있으나, 아직은 그 기능이 많이 부족한 상태로 모바일 ID관리 및 보안이 필요한 상태임

2.2.3. 국내외 IPR 보유현황 및 확보 가능분야

가) 주요 기술 IPR 현황

• 시스템 공통 프레임워크
- ID 생성, 저장, 유통 및 관리 서비스를 위한 공통 프레임워크 규격에 대한 특허는 국내외적으로 많지 않은 상태임
- 미국의 경우 Networked Identity 프레임워크에 대한 특허 등 3건이 조사됨

• Security Token 관리
- Security Token 관리와 관련된 특허는 다른 기술에 비해 상대적으로 많은 특허가 조사됨
- 국내의 경우 보안 토큰을 이용한 전자거래 방법에 관련된 특허 등 4건이 조사됨
- 미국의 경우 출력가능한 클레임을 포함하는 보안 토큰에 대한 특허 등 14건이 조사됨
- 유럽의 경우 사용자 인증을 위한 보안 토큰과 방식 등 3건이 조사됨
- 일본의 경우 인증기관간 상호 인증에 사용되는 포터블 보안 토큰에 대한 특허가 출원됨

• Identity 서비스 디스커버리
- Identity 서비스 디스커버리에 대한 특허는 많지 않은 상태임
- 국내의 경우 Identity 연계를 이용하여 다중 도메인에서 서비스를 검색하는 방식에 대한 특허 등 2건이 조사됨
- 미국의 경우 다른 사용자의 개인 웹 서비스를 발견하고 호출할 수 있는 방식에 대한 특허 등 2건이 조사됨
- 유럽의 경우 1건이 조사됨

• Identity Sharing
- 최근에 연구가 많이 진행되고 있는 Identity 공유에 대한 특허는 많지 않은 상태임
- 국내의 경우 자기통제 강화형 디지털 아이덴터티 공유 장치 및 그 방법 등 5건이 조사됨
- 미국의 경우 contacting identity sharing 등 3건이 조사됨
- 유럽의 경우 3건이 조사됨

• 개인정보보호 정책
- 인터넷 상의 프라이버시 보호는 가장 중요한 문제로 많은 연구가 이루어진 분야이기 때문에 다른 분야에 비해 상대적으로 많은 특허가 조사됨
- 국내의 경우 프라이버시 도메인 간 개인 정보 유통의 제어를 위한 방법 등 3건이 조사됨

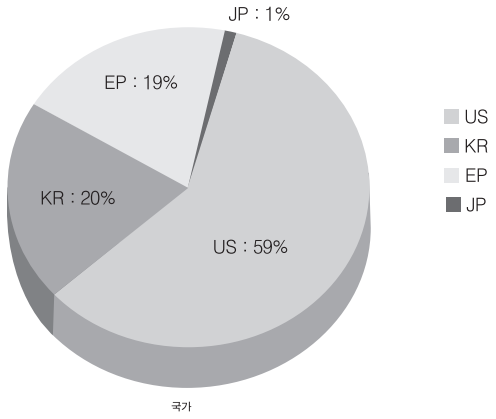
- 미국의 경우 기업, 개인 등에 대한 프라이버시 보호 관련 특허가 24건 조사됨
- 유럽의 경우 프라이버시 보호 시스템 등 5건의 특허가 조사됨

• **개인정보 DB 보안**
- 개인정보 DB 보안은 주로 데이터베이스 암호화, 접근제어 등에 대한 특허가 많이 조사됨
- 국내의 경우 공개키 기반구조 기술 기반의 키 프로파일 기법을 이용한 데이터베이스 보안 기술 등 3건이 조사됨
- 미국의 경우 데이터베이스 보안 제공 방법에 대한 특허 등 8건이 조사됨
- 유럽의 경우 6건이 조사됨

• **네트워크 ID 인증 및 접근제어**
- 네트워크 ID 인증 및 접근제어에 대한 특허는 아직 많지 않은 상태임
- 국내의 경우 1건이 조사됨
- 미국의 경우 분산 컴퓨터 시스템에서 시스템 자원에 대한 접근 제어를 촉진시키는 방법과 시스템에 대한 특허 등 6건이 조사됨
- 유럽의 경우 2건이 조사됨

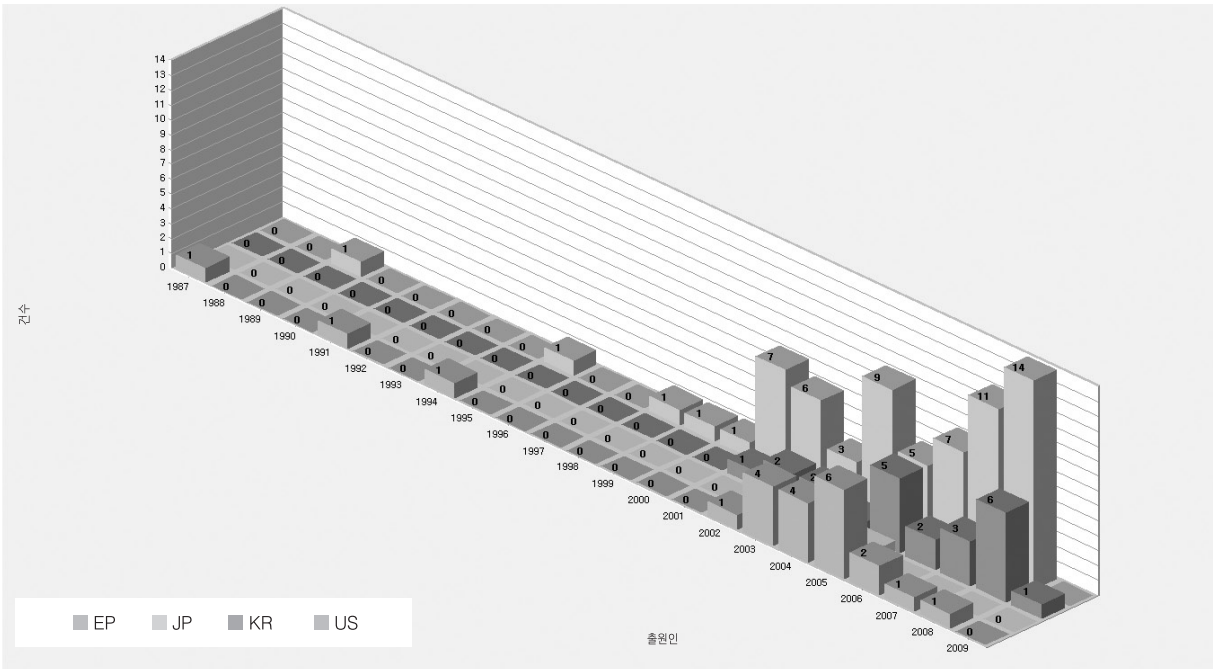
• **본인확인기술**
- 본인확인기술에 대한 특허는 국내 특허가 상대적으로 많은 상태임
- 국내의 경우 본인확인 시스템 및 그 방법 등 5건이 조사됨
- 미국의 경우 인증 기관을 이용한 ID proofing을 위한 방법과 시스템 등 3건이 조사됨

나) IPR 현황 분석 및 전망
- ID관리 및 개인정보보호 분야와 관련되어 조사된 특허는 총 113건으로, 1987년부터 2009년에 걸쳐 출원이 되었음
- 〈그림 4〉는 조사된 특허의 국가별 특허 출원 점유율로 미국이 67건으로 59%의 점유율을 보이며, 한국이 23건으로 20%, 유럽이 19% 그리고 일본이 1%의 점유율을 가지고 있음을 보임



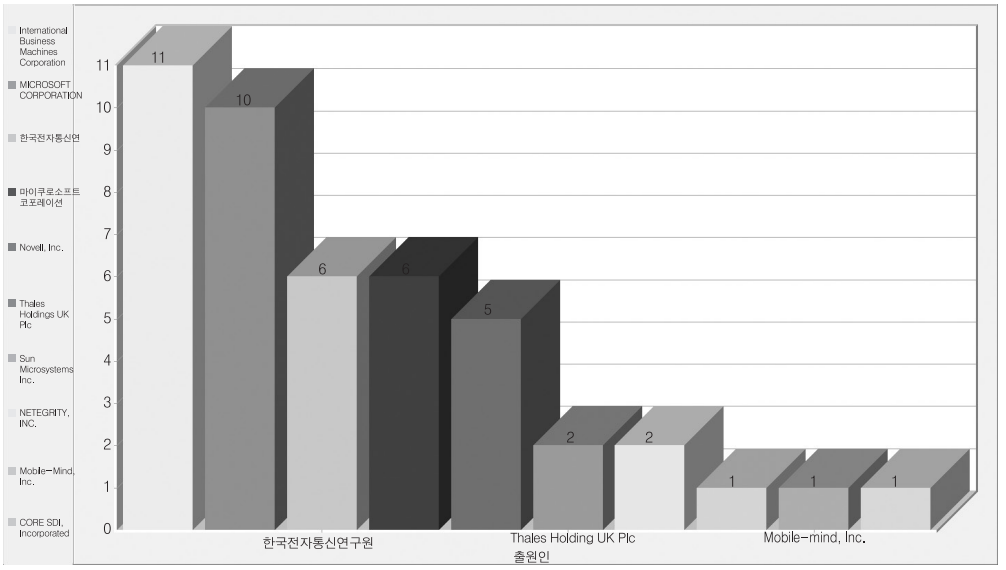
〈그림 4〉 국가별 점유율 분석

- 〈그림 5〉는 조사된 특허의 국가별 시계열 분석으로, 1987년부터 특허가 출원되기 시작하여, 2008년에 가장 많은 특허가 출원되었음을 보임. 2009년에 출원된 특허는 아직 공개되지 않은 것이 많기 때문에 〈그림 5〉에서 매우 적은 것으로 보이나 2010년에 공개가 되면 2008년 정도의 수준이 될 것으로 예상됨



〈그림 5〉 국가별 시계열 분석

- 〈그림 6〉은 조사된 특허의 출원인을 분석한 것으로, IBM과 마이크로소프트가 가장 많은 특허를 보유하고 있으며, 국내의 경우 한국전자통신연구원이 가장 많은 특허를 보유하고 있음을 보임



〈그림 6〉 출원인 랭킹 분석

- ID관리 및 개인정보보호 기술에서 많은 부분이 최근에 연구가 시작되는 분야이기 때문에, 국내외적으로 IPR이 많이 축적되어 있지 않은 상태임. 국외의 경우 국내에 비해 상대적으로 많은 IPR이 축적되어 있으며, 국내에서도 일부 분야의 경우 IPR이 축적된 상황임

- ID관리 기술 분야에서는 IPR이 축적되지 않은 ID관리 프레임워크, ID 공유 기술에 IPR 확보 역량을 집중시킬 필요가 있음
- 또한 국내에서 인터넷 상에서 주민번호 오 · 남용을 방지하기 위해, 기존의 주민번호를 통하지 않고도 본인임을 확인할 수 있는 본인확인 기술에 대한 IPR을 확보하고, 이 기술이 국제적으로 활용할 수 있도록 하는 노력이 필요함

2.3. 표준화 현황 및 전망

- 인터넷 환경에서 제공되는 정보보호는 시스템간의 연동과 확장성을 위해 반드시 표준을 준용하여야 함. ID관리 기술에 대한 표준화는 국제적으로 활발히 진행되고 있으나 개인정보 공유 및 보호 기술에 대한 표준화는 아직 초기 단계
- ID관리와 관련하여, OASIS는 SAML, XACML, SPML, XRI, XDI 등의 표준을 제정하고 있으며, Sun을 중심으로 150여 개 업체가 연합한 Liberty Alliance와 IBM과 Microsoft를 중심으로 여러 업체가 연합한 WS-I에서 표준화를 진행하고 있음
- 개인정보 보호와 관련하여, W3C의 P3P와 APPEL, OASIS의 XACML, IBM의 EPAL 등의 규격이 제정되고 있음
- 2005년 3월 OASIS는 기존의 ID관리 표준들을 통합 적용한 SAML 버전 2.0을 공표한 뒤 상호운용성 시험(2005.7)을 개최하여 ETRI를 포함한 8개 기업이 호환성 인증을 받았고, ITU-T가 OASIS와 협의를 통해 SG17 WP2 Q.6에서 수행하는 SAML과 XACML의 표준화 작업에 국 · 내외 전문가들이 참여하였음
- ID관리와 관련하여, ITU-T는 SG17에서는 다양한 형태의 ID관리 시스템 간 신뢰구축 및 상호연동을 위한 시스템 요구사항 및 데이터 모델 등에 대한 표준화를 진행하고 있으며, ISO는 SC17에서 IC카드의 자체 및 응용 분야 기술에 대한 표준을 제정하고 있고 SC27 WG5에서는 ID관리와 프라이버시 분야의 표준 및 가이드라인 개발을 위한 요구사항과 개발 내용을 도출하는 단계임
- 국내의 경우, KISA, ETRI와 한국정보통신기술협회(TTA)가 ID관리 및 개인정보보호 기술에 대한 표준화를 추진 중에 있음

2.3.1. 국내 표준화 현황 및 전망

- 국내 정보보호 일반표준은 디지털 ID관리 포럼과 TTA에서 추진하고 있음. 표준화는 두 가지 방식으로 추진되고 있음. 첫 번째 방식은 사실표준화단체가 표준초안을 개발하고, TTA에서 정보통신 단체표준으로 개발하는 방법이고, 다른 방식은 TTA에서 표준 초안이 개발되고 관련 PG(Project Group)를 통하여 최종 표준을 확정하는 것임
- KISA(http://www.kisa.or.kr)는 국가인터넷주소자원 관리기관으로 전 분야에 걸친 이슈를 담당하고 있음. 최근 KISA는 인터넷 관련 국제기구들과의 협력을 통해 최신 정보를 공유하고 동향 파악에 힘을 기울이는 한편, 내부 연구역량 강화에 특히 주안점을 두고 있음. 차세대 인터넷 식별자의 표준화와 관련된 핵심 기술인 '보편적자원식별자(URI, URL과 URN을 포함하는 개념)' 표준화에 적극 나서고 있음
- 디지털아이디관리포럼(http://www.didm.or.kr)은 인터넷 기반 ID 서비스 사용자 편의성을 고려하고 자신의 개인정보 통제권을 강화한 ID관리 서비스 모델 및 ID관리 기술 표준을 개발하고 관련 정책 방안을 마련하여 국내 ID관리 서비스 활성화에 기여할 목적으로 2008년에 설립되어 ID관리 및 개인정보보호에 대한 표준을 개발하고 있음
- TTA 개인정보보호 및 ID관리 프로젝트 그룹(PG502)
  - TTA에서 개인정보보호 관련 표준화는 TC1 PG101 정보보호기반 프로젝트 그룹에서 주로 관리하였으나, 더 구체적이고 다양한 ID관리 분야의 국내 표준개발을 위해 2008년에 TC5(정보보호 기술위원회) PG502 개인정보보호 및 ID관리 프로젝트 그룹으로 편성되어 표준화를 진행하고 있음

▫ 2006년 SAML 2.0 주장과 프로토콜, 바인딩, 프로파일에 대한 국내 표준화를 완료하였으며, 2007년 SAML 2.0 메타데이터와 인증 문맥에 대해 표준을 제정하였음

▫ 2007년에 P3Pv1.1을 기반으로 국내 개인정보 관련 법규를 반영한 개인정보보호 정책 설정 및 협상 규격, 서비스 이용자의 개인정보 수집·저장·이용·파기 등의 생명주기를 고려한 개인정보 생명주기별 관리모델 등의 표준이 제정되었음

▫ 2008년에 인터넷 식별자 체계인 확장형 자원 식별자(XRI) 문법 V2.0, 본인확인기술인 i-PIN 중복가입 확인정보 및 서비스 전달 메시지 형식, 사용자중심 아이덴터티 시스템의 공유 프레임워크 등의 표준이 제정되었음

▫ 2009년에 현재 공통 아이덴터티 데이터 모델, 개인정보보호에 대한 수준 평가 기준 및 DB 보안 감사 로그, 사용자중심 ID 관리 서비스의 안전성 검증 기준, HTTP를 위한 상호 인증 프로토콜 및 자기제어 강화형 디지털 아이덴터티 시스템에서 인증 프로토콜, 공유 계약 문법 및 공유 프로토콜에 대한 표준화를 진행하고 있음

- TTA에 제정되거나 또는 추진 중인 ID관리 및 개인정보보호 관련 표준은 다음과 같음

관련분야	표준번호	표준내용	제정년도	제정현황
ID관리 및 개인 정보보호	TTAS.IT-X1141_1	SAML 2.0 주장과 프로토콜	2006	제정
	TTAS.IT-X1141_2	SAML 2.0 바인딩	2006	제정
	TTAS.IT-X1141_3	SAML 2.0 프로파일	2006	제정
	TTAS.KO-06.0111	RFID 프라이버시 보호 가이드라인	2006	제정
	TTAS.IT-X1141_4	SAML 2.0 메타데이터	2007	제정
	TTAS.IT-X1141_5	SAML 2.0 인증문맥	2007	제정
	TTAS.IT-X1141_6	SAML v2.0 - 호환성 요구사항과 보안 및 프라이버시 고려사항	2007	제정
	TTAS.KO-06.0146	모바일RFID 프라이버시 보호 프레임워크	2007	제정
	TTAS.KO-12.0051	개인정보보호정책 설정 및 협상 규격	2007	제정
	TTAS.KO-12.0053	개인정보 생명주기별 프라이버시 관리 모델	2007	제정
	TTAS.KO-12.0054	i-PIN 서비스 프레임워크	2007	제정
	TTAS.KO-12.0055	i-PIN 서비스 전달 메시지 형식	2007	제정
	TTAE.OT-12.0007	확장형 자원 식별자(XRI) 문법 V2.0	2008	제정
	TTAI.IT-X1250	상호호환성 및 신뢰를 위한 글로벌 ID 관리 시스템 요구사항	2008	제정
	TTAI.OT-10.0040/R2	확장성 접근제어 생성언어 3.0	2008	개정
	TTAK.KO-12.0038/R1	i-PIN 서비스 중복가입 확인정보	2008	개정
	TTAK.KO-12.0055/R1	i-PIN 서비스 전달 메시지 형식	2008	개정
	TTAK.KO-12.0072	개인정보 DB 관리 기술의 보안요구사항	2008	제정
	TTAK.KO-12.0073	프라이버시 강화형 역할기반 접근통제 정책언어	2008	제정
	TTAK.KO-12.0074	자기제어 강화형 디지털 아이덴터티 공유 프레임워크	2008	제정
	2008-668	공통 아이덴터티 데이터 모델	2009	진행중
	2009-075	개인정보보호 수준 평가 기준	2009	진행중
	2009-076	사용자중심 ID관리 서비스의 안전성 검증 기준	2009	진행중
	2009-077	개인정보보호를 위한 DB 보안감사 로그	2009	진행중
	2009-829	HTTP를 위한 상호 인증 프로토콜	2009	진행중
	2009-830	자기제어 강화형 디지털 아이덴터티 공유 프로토콜	2009	진행중
	2009-831	자기제어 강화형 디지털 아이덴터티 공유 계약 문법	2009	진행중
	2009-832	자기제어 강화형 디지털 아이덴터티 인증 프로토콜	2009	진행중

2.3.2. 국외 표준화 현황 및 전망

- 2006년 12월에 결성된 ITU-T SG17 Focus Group on IdM(Identity Management)에서는 포괄적인 IdM 프레임워크 개발을 촉진하고 분산 환경에서 자율적인 Identity 발견, Identity 연계 및 구현 수단 개발을 진행하였음. FG IdM 외에도 ITU-T에는 Identity 관리와 관련된 Study Group들이 있는데 Q.15/13(NGN Security)에서는 NGN(Next Generation Network)

환경에서 보안 요구사항 권고안을 확정하였고 인증, AAA, 보안 메커니즘, NGN 인증서, IdM 보안 등에 관한 권고 초안을 개발 중에 있음. 그리고 A.6/17(Cybersecurity)에서 작성 중인 X.IdM (IdM Security)에 관한 권고안이 Identity 관리 시스템과 관련이 깊고 중요함

- 2006년 12월부터 2007년 9월까지 진행된 FG IdM에서는 IdM과 관련된 활동 중인 표준화 기구, 포럼 및 컨소시엄 목록을 정리하고 일반적인 IdM 프레임워크 요구사항 도출을 위한 사용 사례 시나리오를 작성하였음. 또한 IdM 요구사항 및 기능에 관한 포괄적인 분석 보고서와 함께 아직 미완성인 IdM 프레임워크 개발 문서를 보고서로 제출하였음. 다음은 FG IdM이 제출한 6개의 보고서들임
  - SG17 WP2 TD 0292: Report on Activities Completed and Proposed
  - SG17 WP2 TD 0293: Overview of Deliverables
  - SG17 WP2 TD 0294: Report on Identity Management Ecosystem and Lexicon
  - SG17 WP2 TD 0295: Report on Identity Management Use Cases and Gap Analysis
  - SG17 WP2 TD 0296: Report on Requirements for Global Interoperable IdM
  - SG17 WP2 TD 0297: Report on Global Interoperable IdM Framework
- 2007년 8월 ITU-T SG17 총회에서는 Ad Hoc Group on FG IdM Future라는 주제로 FG IdM의 Focus Group 활동 연장 문제에 대한 토의와 향후 ID관리 표준화의 방향에 대한 포괄적인 문제를 다루기 위해 여러 시간에 걸쳐 회의를 진행하였음. 여러 나라에서 제출한 기고문과 회의에서의 의견을 종합하여 JCA(Joint Coordination Activities)와 GSI(Global Standards Initiative) IdM을 결성하여 진행하는 것으로 결정하고 2007년 12월에 TSAG(Telecommunication Standardization Advisory Group) 승인을 얻어 2008년 1월에 서울에서 처음 회의를 진행하였음
- ISO/IEC JTC1 SC27 WG5에서는 ID관리 프레임워크 국제표준 개발을 진행중에 있으며, ID관리 프레임워크 개발을 위한 선행되어야 할 작업으로 ID 온톨로지 정의를 들고 있음. ID 온톨로지는 실제적인 ID관리에 필요한 용어와 개념 공유를 위해 필수적이며, ID관리 프레임워크 이용자에게 ID관리와 관련된 일관성 시각을 제공하는 한편 서로 상이하거나 연관된 목적을 가진 다른 사용자와의 협력을 가능하게 하는 중요한 역할을 담당하고 있음. 또한, ITU-T와 함께 ID관리 과정에서 요구되는 객체에 대한 인증 및 보증을 위한 프레임워크와 인증에 영향을 미칠 수 있는 요소들에 대한 기준, 위협 등을 정의하는 'Entity Authentication and Assurance' 표준을 개발하고 있음
- 현재 GSI는 ITU-T 내의 다양한 표준화 단체들이 IdM의 표준화 개발에 참여하여 의견을 개진할 수 있는 기회를 제공하며 Trusted Service Provider Identity 기술 관련하여 표준화를 진행하고 있음. JCA는 ITU-T외에 ISO와 같은 다양한 표준단체들이 모여 상호운용 가능한 IdM을 주제로 정보를 교환하고 다양한 의견이 토의될 수 있는 자리를 만들어 보다 폭 넓고 심도 있는 IdM 관련 표준 결과물을 생성하는 것을 목적으로 운영되고 있음
- ITU-T SG17내에서 ID관리의 표준 개발을 직접적으로 담당하고 있는 곳은 Q10/17임. FG IdM의 결과물 중 IdM 상호운용성 요구사항은 'X.1250: Baseline capabilities for enhanced global identity management trust and interoperability'라는 제목으로 표준화를 진행하여 2008년 4월 SG17회의에서 표준으로 결정되어 현재 승인절차를 밟고 있음. 또한 IdM 시스템들 간의 아이덴터티 정보의 표현을 위한 아이덴터티 데이터의 공통 데이터 모델을 개발하는 표준으로 'X.idm-dm: Common Identity Data Model'의 표준화 작업을 진행중에 있음
- ETRI는 ID관리 기술인 '자기 통제 강화형 디지털 아이덴티티 공유 프레임워크'에 관한 기고문을 발표하여 X.idif - A framework for user control of digital 라는 표준과제로 채택되었고 1명의 에디터가 선정되어 2007년 9월부터 ITU-T SG17에서 국제 표준화 작업을 진행하고 있음. 2009년 9월 SG17 총회에서 ITU-T X.1251 국제 표준으로 승인되었음
- ETRI에서 제안한 Digital Identity 공유 프레임워크는 사이버스페이스에서의 사용자 중심의 자기통제권이 강화된 전자ID지갑을 통하여 다양한 객체들이 서로 사용자의 Identity 정보를 자유롭게 공유할 수 있는 ID 공유 프레임워크에 관한 내용을

담고 있음. 현재 Q6에서 X.idif는 ID관리 분야 표준에 중추적이고 핵심적인 표준으로 자리를 잡을 것으로 예상되며 SG17에서 IdM의 표준화 중요성이 부각되어 2009년 새로운 회기부터는 ID관리 분야의 표준과제를 전담하는 새로운 Question이 Q10으로 만들어 졌음

- SG17 외에도 ITU-T에는 ID관리와 관련된 SG들이 있는데 FG IdM에서 미완성으로 중단된 IdM 프레임워크는 Q.15/13(NGN Security)에서 다음과 같이 진행되고 있으며, SG13에서 Y.idmFramework이 Y.2720 – NGN Identity management framework 로 표준이 제정되었음
  - Y.ngnIdMuse: NGN identity management use cases – NGN에서 IdM을 사용하는 시나리오를 설명
  - Y.ngnIdMreq: NGN identity management requirements – NGN에서 IdM의 요구사항에 대한 표준
  - Y.idmFramework: NGN identity management framework – NGN에서 IdM들 간의 상호운용에 대한 프레임워크 표준
- ISO에서 ID관리와 연관된 표준화 활동들로는 인터넷 기반 PKI에 대한 ISO 9594-8(X.509 PKI 인증서 및 인증서 취소 목록, IETF RFC 3280과 관련), 전자 거래(electronic transaction)에서 활용되는 전자 ID에 대한 명세 ISO/IEC 15944-1(Information technology – Business agreement semantic descriptive techniques – Part 1: Operational aspects of Open-Electronic Data Interchange(EDI)), 생체인식정보 교환 표준형식을 개발하는 ISO/IEC 19794, ID관리 프레임워크를 연구하는 ISO/IEC JTC1 SC27(Information Technology – Security Techniques – A Framework for Identity Management) 등이 있음. SC27 WG5에서는 ID 개념, ID, 식별(identification) 및 식별자(identifier), ID 생명주기, ID 인증, 정보사회에서 ID관리, 정보기술과 ID관리, 정보보안과 ID관리 등 포괄적인 ID관리에 대한 표준 개발을 진행하고 있음. 또한 전자여권과 관련하여 ISO/IEC JTC1 SC17 WG3, 전자운전면허증과 관련하여 ISO/IEC JTC1 SC17 WG10, 바이오 카드와 관련하여 ISO/IEC JTC1 SC17 WG11 등이 표준 개발을 진행하고 있음
- IETF에서 개발된 표준 중 ID관리와 연관된 RFC들로는 자원이나 개체 식별을 위한 RFC3986(Uniform Resource Identifier), URI를 포함하는 식별자에 대한 표준들인 RFC3987(Internationalized Resource Identifier), RFC2822(Internet Message Format), RFC2141(Uniform Resource Name), RFC4122(Universally Unique Identifier(UUID) URN Namespace), RFC4474(Enhancements for Authenticated Identity Management in the Session Initiation Protocol), RFC4484(Trait-Based Authorization Requirements for the Session Initiation Protocol) 등이 있음
- OASIS에서 제정한 ID 관련 표준들로는 SAML, XACML, SPML, XRI, WS-Security(Web Service Security) 등이 있음. SAML 표준에서는 주체에 대해 발행된 assertion 구조 및 assertion 처리를 위한 관련 프로토콜들에 대해 정의하고 있으며 XACML은 정보시스템에 의해 관리되는 자원에 대한 접근허용여부를 정의하는 XML 언어 기반 보안정책 기술언어 표준임. SPML은 사용자, 자원, 서비스 프로비저닝 정보교환을 위한 XML 기반 프레임워크를 정의하고 있으며 XRI는 위치, 응용, 전송 프로토콜과 독립적인 URI와 호환성있는 추상적 식별자와 결정(resolution) 프로토콜에 대한 표준을 정의하고 있음. WS-Security 표준에서는 웹 서비스 메시징에 적용되는 무결성 및 비밀성 지원을 위한 프로토콜을 정의하고 있음. OASIS의 SAML 표준은 ITU-T에 제안되어 X.1141로 표준화가 되었음
- OMA(Open Mobile Alliance)는 멀티벤더 환경에서 응용과 서비스를 효과적이고 안정적으로 구축, 설치, 관리하도록 하는 공개형 표준기반 프레임워크를 개발하여 가입자에게 시장, 사업자, 그리고 모바일 단말기 등에 결쳐 상호운용 가능한 모바일 서비스를 제공함을 목표로 하고 있음. OMA에 의해 개발된 IdM 관련 명세로는 ID Management Framework Requirement(OMA-RD-Identity_Management_Framework-V1_0-20050202-C)가 있음. 이 명세의 목적은 모든 OMA enabler들에 의해 공통적으로 사용될 수 있는 단일 IdM enabler를 만드는 데 있으며 이 명세에는 모든 OMA 기술 WG들의 요구사항들과 단일 IdM enabler가 제공해야 하는 ID관리 관련 모든 기능들을 포함되어 있음
- Liberty Alliance project는 연계 ID관리를 위한 가이드라인과 실례 그리고 공개 표준을 개발할 목적으로 2001년에 결성되었

고, 웹 서비스의 소비자들이 ID 정보에 대한 프라이버시와 보안을 유지하면서 온라인 업무를 어디에서든지 더 쉽게 할 수 있게 하는 것을 목표로 하고 있음. ID들이 연계되고, 공유함으로써 사용자에게 SSO, Single Logout 등의 편리함을 제공함. Liberty Alliance project는 크게 세 개의 모듈로 구성되어 있음. 여러 사이트의 사용자 계정을 연결하는 ID의 연계를 다루는 ID-FF, ID서비스의 생성, 검색, 사용을 위한 프레임워크를 제공하는 ID-WSF와 ID-WSF 위에서 일정, 주소록, 달력, 위치 추적, 사용자 상태나 경고등을 위한 ID 기반의 서비스를 다루는 ID-SIS로 구성되어 있음. ID-FF는 OASIS의 SAML 2.0으로 표준화되었음

- Liberty Alliance project는 기본적인 프레임워크인 FF나 WSF외에도 Identity 서비스를 평가하고 검증할 수 있는 Identity Assurance Framework를 개발하였고 엔티티들간의 Identity 정보의 원활한 교환과 프라이버시 제한을 정책으로 설정할 수 있는 Identity Governance Framework 표준안도 현재 개발되어 발표되었음. 또한 ID-SIS PP(Personal Profile), EP(Employee Profile)에서는 사용자 및 고용자에 대한 개인정보 구성요소를 규정하고 있으며 필요에 따라 개인정보 스키마를 확장할 수 있는 기능을 제공하고 있음

- OASIS는 E-business와 웹 서비스의 공통 표준들을 개발하는 것이 목표로 진행하고 있음. OASIS의 기술적 영역은 웹서비스, 전자상거래, 보안, 법률과 정부, 컴퓨터 관리 등임. OASIS에서 명세한 표준으로는 CAP(Common Alerting Protocol), CIQ(Customer Information Quality), DocBook, DITA(Darwin Information Typing Architecture), OpenDocument(OASIS Open Document Format for Office Application), SAML, SPML, UBL(Universal Business Language), WSDM(Web Services Distributed Management), XRI, XDI 등이 있음. 이중 XRI는 인터넷 규모의 URI 기반 추상화된 ID를 정의하는 명세와 XRI 데이터 공유를 위한 조율 프로토콜, 도메인 상호간에 자원 공유 등을 명세하고 있음. 또한 XDI는 XRI에 기반을 둔 dataweb 구축을 목표로 인터넷 규모의 멀티 도메인들 간에 XRI와 XDI 기본 스키마에 기반을 둔 XML 도큐먼트를 상호간에 서로 공유하고 링킹, 동기화하는 표준화를 제안하고 있음

- ID관리 및 개인정보보호 관련 국제 표준은 다음과 같음

표준화기관	표준식별자	제 목
Liberty Alliance	liberty-idwsf-disco-svc	Liberty ID-WSF Discovery Service Specification V2.0
	liberty-idwsf-soap-binding	Liberty ID-WSF SOAP Binding Specification V2.0
	liberty-idwsf-security-mechanisms	Liberty ID-WSF Security Mechanisms Specification V2.0
	liberty-idwsf-interaction-svc	Liberty ID-WSF Interaction Service Specification V2.0
	liberty-idwsf-client-profiles	Liberty ID-WSF Client Profiles Specification V2.0
	liberty-idwsf-dst	Liberty ID-WSF Data Service Template Specification V2.0
	liberty-idwsf-authn-svc	Liberty ID-WSF Authentication Service Specification V2.0
	liberty-idwsf-people-service	Liberty ID-WSF People Service Specification V1.0
	liberty-idwsf-subs	Liberty ID-WSF Subscription and Notification Specification V1.0
	liberty-idsis-pp	Liberty ID-SIS Personal Profile Service Specification V1.1
	liberty-idsis-ep	Liberty ID-SIS Employee Profile Service Specification V1.1
	liberty-idsis-sis-cb	Liberty ID-SIS Contact Book Service Specification V1.0
	liberty-idsis-sis-gl	Liberty ID-SIS Geolocation Service Specification V1.0
	liberty-idsis-sis-presence	Liberty ID-SIS Presence Service Specification V1.0
OASIS	sstc-saml-core-2.0-os	Assertions and Protocol for the OASIS Security Assertion Markup Language (SAML) V2.0
	sstc-saml-bindings-2.0-os	Bindings for the OASIS Security Assertion Markup Language (SAML) V2.0
	sstc-saml-profiles-2.0-os	Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0
	sstc-saml-metadata-2.0-os	Metadata for the OASIS Security Assertion Markup Language (SAML) V2.0
	sstc-saml-authn-context-2.0-os	Authentication Context for the OASIS Security Assertion Markup Language (SAML) V2.0
	oasis-access_control-xacml-2.0-core-spec-os	eXtensible Access Control Markup Language(XACML) Version 2.0
	access_control-xacml-2.0-rbac-profile1-spec-os	Core and hierarchical role based access control (RBAC) profile of XACML v2.0

표준화기관	표준식별자	제 목
OASIS	access_control-xacml-2.0-hier-profile-spec-os	Hierarchical resource profile of XACML v2.0
	access_control-xacml-2.0-privacy_profile-spec-os	Privacy policy profile of XACML v2.0
	access_control-xacml-2.0-saml-profile-spec-o	SAML 2.0 profile of XACML v2.0
	os-pstc-spml2-dsml-profile-os	OASIS Service Provisioning Markup Language (SPML) Version 2
	pstc-spml2-xsd-profile-os	OASIS Service Provisioning Markup 3 Language (SPML) v2 - XSD Profile
	pstc-spml2-dsml-profile-os	OASIS Service Provisioning Markup Language (SPML) v2 - DSML v2 Profile
	xri-syntax-V2.0-cs	Extensible Resource Identifier (XRI) Syntax V2.0
	xri-resolution-v2.0-cs	Extensible Resource Identifier (XRI) Resolution Version 2.0
	xri-metadata-v2.0-cd-01	XRI Metadata V2.0 Committee Draft 01
W3C	P3P 1.1	The Platform for Privacy Preferences 1.1 (P3P1.1) Specification
	APPEL1.0	A P3P Preference Exchange Language 1.0 (APPEL1.0)
	EPAL 1.2	Enterprise Privacy Authorization Language (EPAL 1.2)
ITU-T	X.1141	Security Assertion Markup Language (SAML)
	Y.2720	NGN Identity management framework
IETF	RFC3986	Uniform Resource Identifier (URI): Generic Syntax
	RFC3987	Internationalized Resource Identifiers (IRIs)
	RFC4122	A Universally Unique IDentifier (UUID) URN Namespace
	RFC4474	Enhancements for Authenticated Identity Management in the Session Initiation Protocol(SIP)

2.4. 표준화 대상항목별 현황 분석

구 분		ID관리 기반	개인정보보호
표준화 대상항목		Identity 식별자 체계, Identity 시스템 공통 프레임워크, Security Token 관리, Identity 서비스 디스커버리, Identity Ontology, Identity Sharing, 신뢰관리-Assurance	개인정보보호 정책, Interaction Service, 개인정보 DB 보안, 사용자단말 개인정보 관리
시장현황 및 전망	국 내	- 한국IDC의 2009년 조사에 따르면, 국내 ID관리 및 접근제어 시장이 2008년 346억 원 규모에서 연평균 11.5%의 성장을 보이며 2012년 530억 원 규모의 시장으로 성장할 것으로 전망하고 있음	
	국 외	- IDC의 2009년 3월 조사에 따르면, 전 세계적으로 ID관리 및 접근제어 시장 규모를 2008년 3,504백만 달러에서 연평균 8.4%의 성장을 보이며 2013년에 5,246백만 달러에 이를 것으로 전망하고 있음	
기술개발 현황 및 전망	국 내	- ETRI에서 보안토큰 생성 · 분배, 디스커버리, ID 연계 기술 개발 - SSO, EAM 시스템 제품군 출시 - OpenID, XRI 식별체계를 지원하는 제품군 출시 - ID 공유 기술 개발 - PKI, 메타데이터를 통한 시스템간의 신뢰관리기술 보유	- 개인정보보호 정책 기술인 P3P 기술 개발 - ETRI에서 XACML 기술과 Interaction Service 기술 개발 - 개인정보 DB 암 · 복호화 및 전자서명 기술을 포함하는 제품이 출시됨 - 키보드보안, 일회용패스워드 등 사용자단말 보안기술이 개발되어 적용되고 있음
	국 외	- 식별체계, 보안토큰 생성·분배, 디스커버리, ID 연계 등 핵심 기술이 다수 개발된 상태임 - SSO, EAM 등 개별 기능 제품군에서 ID를 종합적으로 관리하는 IAM 제품군이 다수 출시됨 - 최근 사용자 중심 ID 제품군이 출시되고 있음 - PKI, 메타데이터를 통한 시스템간의 신뢰관리기술	- 개인정보보호 정책 기술인 P3P 기술 개발 - Liberty Alliance에서 Interaction Service 기술 개발 - Oracle, Sybase 등 주요 DBMS 개발사들이 데이터베이스에 대한 암 · 복호화, 전자서명, 접근제어 기능을 제공하고 있음 - 키보드보안, 일회용패스워드 등 사용자단말 보안기술이 개발되어 적용되고 있음
기술 개발 수준	국 내	- Identity 식별자 체계 : 시제품/프로토타입 - Identity 시스템 공통 프레임워크 : 구현 - Security Token 관리 : 구현 - Identity 서비스 디스커버리 : 구현 - Identity Ontology : 구현 - Identity Sharing : 구현	- 신뢰관리-Assurance : 구현 - 개인정보보호 정책 : 설계 - Interaction Service : 구현 - 개인정보 DB 보안 : 구현 - 사용자단말 개인정보 관리 : 구현
	국 외	- Identity 식별자 체계 : 시제품/프로토타입 - Identity 시스템 공통 프레임워크 : 구현 - Security Token 관리 : 구현 - Identity 서비스 디스커버리 : 시제품/프로토타입 - Identity Ontology : 시제품/프로토타입 - Identity Sharing : 구현 - 신뢰관리-Assurance : 구현	- 개인정보보호 정책 : 구현 - Interaction Service : 구현 - 개인정보 DB 보안 : 시제품/프로토타입 - 사용자단말 개인정보 관리 : 구현
	기술격차	-1년	-1년
	관련제품	PKI, EAM, IAM	PKI, EAM, IAM, 정보보호 제품 전반, Portal
IPR 보유현황	국 내	Security Token, 디스커버리, ID 공유 등에서 IPR 확보	개인정보보호정책, 개인정보 DB 보안 분야에서 IPR 확보
	국 외	프레임워크, Security Token, 디스커버리, ID 공유 등에서 IPR 다수 확보	개인정보보호정책, Interaction Service, 개인정보 DB 보안 분야에서 IPR 확보
IPR확보 가능분야		프레임워크, ID Sharing, ID Ontology	Interaction Service
IPR확보 가능성		높음	보통

표준화 현황 및 전망	개 요	- 국내의 경우, Security Token, 식별자에 대한 국내 표준이 제정되었으며, 프레임워크 및 ID Sharing에 대한 표준화가 진행되고 있음 - 국외의 경우, Security Token, 식별자, 디스커버리에 대한 표준을 제정하였으며, ID 핵심 기술에 대한 표준화가 진행되고 있음	- 국내의 경우, 개인정보보호정책, 프라이버시 관리 모델에 대한 표준이 개발되었음 - 국외의 경우, Liberty Alliance에서 Interaction Service에 대한 표준이 개발되었으며, OASIS에서 개인정보보호정책에 대한 표준이 제정되었음 - 개인정보 DB 보안과, 사용자단말 개인정보 관리의 경우, 국 · 내외적으로 표준화가 아직 미비한 상황임
	국 내	- Identity 식별자 체계 : 개발/검토 - Identity 시스템 공통 프레임워크 : 항목승인 - Security Token 관리 : 개발/검토 - Identity 서비스 디스커버리 : 기획 - Identity Ontology : 기획 - Identity Sharing : 개발/검토 - 신뢰관리-Assurance : 개발/검토	- 개인정보보호 정책 : 개발/검토 - Interaction Service : 항목승인 - 개인정보 DB 보안 : 기획 - 사용자단말 개인정보 관리 : 기획
	국 제	- Identity 식별자 체계 : 제/개정 - Identity 시스템 공통 프레임워크 : 최종검토 - Security Token 관리 : 최종검토 - Identity 서비스 디스커버리 : 제/개정 - Identity Ontology : 개발/검토 - Identity Sharing : 최종검토 - 신뢰관리-Assurance : 최종검토	- 개인정보보호 정책 : 최종검토 - Interaction Service : 개발/검토 - 개인정보 DB 보안 : 기획 - 사용자단말 개인정보 관리 : 기획
	표준화격차	-1년	-1년
표준화 기구/ 단체	국 내	TTA, 디지털아이디관리포럼	TTA
	국 제	ITU-T SG17, OASIS, Liberty Alliance	ISO, OASIS, Liberty Alliance
	국내참여 업체/기관	TTA, ETRI, KISA 등	TTA, ETRI, KISA 등
	국내기여도	높음	높음
국내표준화 인프라수준		높음	높음
개발 주체	표준개발	TTA, 디지털아이디관리포럼	TTA
	기술개발	산업체, 연구소	산업체, 연구소

구 분		ID관리 응용 및 기타
표준화 대상항목		네트워크 ID 인증 및 접근 제어, 본인확인기술
시장현황 및 전망	국 내	- 한국IDC의 2009년 조사에 따르면, 국내 ID관리 및 접근제어 시장이 2008년 346억 원 규모에서 연평균 11.5%의 성장을 보이며 2012년 530억 원 규모의 시장으로 성장할 것으로 전망하고 있음
	국 외	- IDC의 2009년 3월 조사에 따르면, 전 세계적으로 ID관리 및 접근제어 시장 규모를 2008년 3,504백만 달러에서 연평균 8.4%의 성장을 보이며 2013년에 5,246백만 달러에 이를 것으로 전망하고 있음
기술개발 현황 및 전망	국 내	- 네트워크 중심 ID 인증 및 접근제어 기술 연구 중 - KISA에서 주민번호대체 기술인 i-PIN을 이용한 본인확인 기술을 개발
	국 외	- 유럽에서는 ETSI 회원국들을 중심으로 NASS 표준기술을 적용, 유선 통신사업자의 IP 망 구축을 지원 - 관련 식별, 접속, 인증에 대한 다양한 solution 이 제안되고 있음 - i-PIN과 같은 본인확인 기술은 미개발된 상태임
기술개발 수준	국 내	- 네트워크 ID 인증 및 접근 제어 : 기술기획 - 본인확인기술 : 상용화
	국 외	- 네트워크 ID 인증 및 접근 제어 : 기술기획 - 본인확인기술 : 설계
	기술격차	부분적으로 선도
	관련제품	BcN/NGN 인증 및 접속제어 제품 전반, 포털
IPR 보유현황	국 내	미흡
	국 외	네트워크 ID관리 관련 IPR 확보
IPR확보 가능분야		번들 인증 등 NGN 에 대한 신규 기능 설계 분야 본인확인기술
IPR확보 가능성		높음
표준화 현황 및 전망	개 요	- NGN 표준개발의 진행이 가속화되고, 이동성과 인증 식별의 문제가 ID관리의 문제로 확대 중 - ITU-T를 중심으로 한 NGN 표준과, 3GPP를 중심으로 한 trusted computing 응용 표준의 시장전망이 확대 중 - 국내의 경우 개인정보보호 정책, 본인확인 기술에 대한 표준이 제정되었으며, i-PIN과 관련된 표준화가 진행되고 있음
	국 내	- 네트워크 ID 인증 및 접근 제어 : 기획 - 본인확인기술 : 제/개정
	국 제	- 네트워크 ID 인증 및 접근 제어 : 기획 - 본인확인기술 : 항목승인
	표준화격차	0년
표준화 기구/ 단체	국 내	TTA
	국 제	ITU-T, OASIS, Liberty Alliance, GSI/SG3/SG11, 3GPP, ETSI
	국내참여 업체/기관	TTA, ETRI, KISA, KT, Xener 등
	국내기여도	높음
국내표준화 인프라수준		높음
개발 주체	표준개발	TTA, 디지털아이디관리포럼
	기술개발	산업체, 연구소

3. 중점 표준화항목의 표준화 추진전략

3.1. 중점기술의 표준화 환경분석

3.1.1. 표준화 추진상의 문제점 및 현안사항

- 인터넷 상에서의 ID 도용 및 개인정보유출 문제는 이전부터 존재해 왔으나, 최근 사용자 정보의 대량 유출과 같은 사건의 발생에 따라 문제의 심각성이 일반인에게 알려지며 사회적인 문제로 인지되고 있는 상황임. 또한, 인터넷이 웹 2.0, 유비쿼터스 환경으로 진화할수록 ID 도용 및 개인정보유출 문제는 더욱 심각해 질 것으로 예상됨

- 현재 국제적으로도 ID관리 및 개인정보보호 기술에 대한 표준화는 최근에야 진행되고 있으며, 대표적인 국제 표준화 단체로는 ITU-T SG17과 ISO/IEC JCT1/SC27이 있음. 따라서 ID관리 및 개인정보보호 기술에 대한 핵심 기술을 개발하고 우수 핵심 기술을 국제 표준화 단체의 표준으로 채택하도록 하며 IPR을 확보하기에는 현재가 적기임

- 국내의 경우 ID관리 및 개인정보보호 기술에 대한 표준화는 주로 TTA의 개인정보보호 및 ID관리 프로젝트 그룹인 PG502에서 진행되어 왔음. TTA의 표준화는 주로 ETRI, KISA 등과 같은 연구기관과 학계를 통해 이루어지고 있으며 산업체의 참여가 상대적으로 저조한 문제가 있었음. 이러한 문제를 해결하기 위해, 통신사 및 주요 포털을 포함하는 산업계의 요구가 수렴될 수 있는 디지털아이디관리 포럼이 2008년에 결성되어 국내 표준화에 산업계의 다양한 의견이 반영될 수 있는 토대가 마련된 상황임

- 개인정보보호를 위한 기술들은 국가별, 지역별, 환경별로 각기 다른 정책이나 법률, 지침 등이 적용 가능해야하며 변경이 자유로워야 하는 특성을 갖고 있어 설정된 수준을 객관적으로 판단할 수 있는 일반화된 기준을 규정하기 어렵고, 공통적으로 적용할 수 있는 기술을 개발하거나 표준화하는데 어려움이 있음. 특히, 정책적 사항을 포함하는 개인정보보호 기술은 일반적인 정보보호 기술을 활용한 형태가 대부분으로 원천 기술에 대한 IPR 확보가 어려운 것이 사실임. 다만, 기존 기술을 모바일, 클라우드 컴퓨팅 등 신규 서비스에 적용하기 위한 형태로 재조합하거나 개인정보보호 관련 표준에서 요구하는 신규 기술을 추가적으로 개발하여 표준화 및 IPR을 확보할 필요가 있음

3.1.2. SWOT 분석 및 표준화 추진방향

국내역량요인 / 국외환경요인			강점 요인 (S)	약점 요인 (W)
		시장	- 정보통신 인프라구축이 잘 되어 있고, 새로운 기술 수용이 매우 빠름 - 방송통신위원회 민간 i-PIN, 행정안전부 공공 i-PIN 등 ID관리에 대한 국가 인프라 구축 의지가 높음 - 개인정보보호 필요성에 대한 높은 인식	시장 - 세계 시장 대비 ID 관리 시장 규모의 상대적 협소 - ID 관리 및 개인정보보호 산업체의 영세성, 브랜드 인지도 부족으로 경제성 형성의 한계 - 구축에 많은 비용이 소요되나 투자 대비 회수 비용의 산정이 매우 어려움
		기술	- 기존 정보보호 산업에 대해 물리보안, 융합보안을 확장한 지식정보보안 산업 육성에 대한 정부의 정책에 따라 새로운 정보보호 서비스와 새로운 정보보호 장치 개발의 필요성 대두 - ETRI를 통한 선도 기술개발을 통한 핵심 기술 확보 가능	기술 - ID 관리 기술개발 고급 인력 부족 - ID 관리 기술 전반을 포괄하는 플랫폼 기술이 매우 미흡하며, 응용 위주의 제품 생산
		표준	- 국제표준화 단체에서의 활발한 참여 및 대응 - 국제표준전문가 양성에 대한 정부의 강력한 의지	표준 - ID 관리 및 개인정보보호 표준 전문가의 부족 - 업체의 표준 추진 의지 미흡 - 행정편의성 증진 등의 사유로 개인정보 보호에 다소 소극적임
기회요인 (O)	시장	- ID 도용과 개인정보 유출 피해 증가에 따른 ID 관리 및 개인정보보호 기술에 대한 관심 고조 - ID관리 분야의 시장 규모가 급속히 증가될 것으로 예상 - 클라우드 컴퓨팅, Green IT 등 새롭게 등장하는 시장에서의 ID 관리 수요 증가 예상 - 국가적 차원 및 국제통용 ID의 발급 추진	**- 현황분석에 의한 우선순위 : 2** - ID관리 및 개인정보보호 분야의 국내 독자 IPR 확보 - ITU-T/SG17, ISO/IEC JTC1/SC27 등 국제 표준화 기구에서의 표준화 활동 강화 - ETRI 등의 국책 연구기관에서 개발된 선도개발기술의 국제 표준화 추진 - ITU-T SG13 의장직, SG17 부의장직 등 확보된 국제 표준 전문가 풀을 활용한 국제 표준화 추진	**- 현황분석에 의한 우선순위 : 1** - 신규 ID 서비스에 대한 시장 창출을 통한 지속적인 정보보호 인력 양성 - 공공 분야의 ID 인프라 구축 및 개인정보보호 제품 확대를 통한 국내 정보보호 시장 확대 - 지속적인 기반 기술 개발과 우수 제품 개발을 통해 국내 정보보호 수준 제고 및 제품 경쟁력 향상 - 디지털아이디관리포럼 등을 통해 국내 산업계의 요구사항을 수렴하고 TTA PG502를 통해 국내 표준화를 수행
	기술	- 웹2.0, 클라우드 컴퓨팅의 등장 등 외부 환경 변화에 따라 ID관리 및 개인정보보호 관련 핵심 기술 개발 필요성 증가		
	표준	- ID관리 관련 국제표준화가 ITU-T와 ISO에서 초기 단계이기 때문에, 국제 표준화 참여 및 선도 가능		
			SO전략 : 공격적 전략(강점사용-기회활용) / WO전략 : 만회전략(약점극복-기회활용) / ST전략 : 다각화 전략(강점사용-위협회피) / WT전략 : 방어적 전략(약점최소화-위협회피)	
위협요인 (T)	시장	- 미국, 유럽 등 ID관리 제품을 제공하는 기업들의 독점 우려 - 개인정보보호의 경우 국가별 정책, 규제 등과 일치시켜야 하는 문제 발생 - 개인정보보호 기술 · 제품에 대한 국내시장 과열	**- 현황분석에 의한 우선순위 : 3** - 개발된 ID관리 및 개인정보보호 기술을 국내의 인터넷 환경에 선적용하여 제품의 인지도와 완성도를 제고하여 해외 시장 경쟁력을 확보 - ID관리 및 개인정보보호 관련 국외 연구기관과 전문가 초청 워크숍을 통한 기술 교류 - TTA PG502와 디지털아이디관리포럼을 통해 국내 표준화를 수행하고 국책연구기관의 표준전문가를 적극 활용하여 국제표준화 추진 - 인터넷 중심의 식별자 기술로 무장된 북미의 ID관리 기술에 대항하여, 한국이 적극적인 ITU-T NGN의 scope를 기반으로 기존 활동의 확대를 추구	**- 현황분석에 의한 우선순위 : 4** - 선도기반 과제를 통한 IPR 획득 및 이를 통한 기술 및 서비스 제공 - 산 · 학 · 연 연계 연구 개발을 통해 지속적인 정보보호 고급 인력을 양성하고 이를 통해 기반 기술 확보 - 투자비 환수의 개념을 탈피하여 ID 도용 및 개인정보 분야의 유출의 피해 예방 개념을 적용한 정책적 지원을 통한 정보보호 제품 구매 확대 정책 시행 - 정보 집중화로 인하여 빅브라더 우려에 대한 개인의 ID 통제권 부여 등 적극적 개인정보 보호 기술 적용 - 북미, 유럽의 유력한 ID관리 기술보유 기관들과 연합 및 협력체계 구축 모색
	기술	- 일부 선진 국가와 회사에서 ID 관리 핵심 원천 기술에 대한 기술적 우위 선점 - 개인정보보호를 위한 특화된 원천 기술 부재		
	표준	- 국가간, 업체간 경쟁이 치열 - 선진국의 경우 국제표준 경험 및 전문 인력 풍부 - 국가주의에 의한 개인정보 보호에 대한 우려		

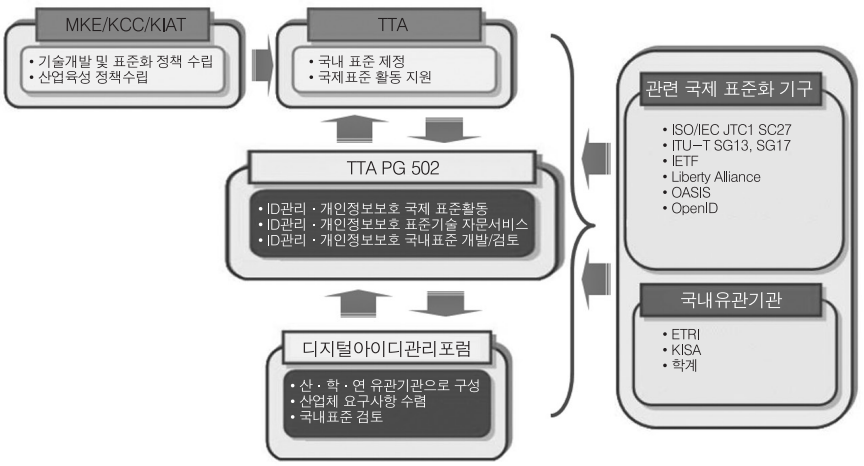
• **현황분석을 통한 우선순위**: WO -› SO -› ST -› WT

- WO전략: 만회 전략(약점극복-기회활용)
  - ▫ ID관리 시장이 협소하다는 약점을 극복하고 최근 ID 도용 및 개인정보 침해 사고 발생으로 인한 관련 기술의 필요성이 급증한다는 기회를 활용하여 공공 분야의 ID 인프라 구축 및 개인 정보보호 제품 확대를 통해 표준화를 추진하는 것이 필요함
- SO전략: 공격적 전략(강점사용-기회활용)
  - ▫ 국내 정보통신 인프라가 잘 구축되어 있고 i-PIN과 같은 시스템 도입이 활발히 이루어지고 있다는 강점과 사회적으로 ID 관리 및 개인정보보호에 대한 요구가 급증하는 기회를 활용하여 관련 IPR을 독자적으로 확보하고 이를 바탕으로 ITU-T, ISO 등의 국제 표준화 단체에서 적극적으로 표준화를 추진하는 것이 필요함
- ST전략: 다각화 전략(강점사용-위험회피)
  - ▫ ID관리 및 개인정보보호 기술에 대한 적극적인 개발 추진의지가 있는 강점과 외국 제품의 독점이 우려되는 위험을 회피하기 위하여 개발된 ID관리 및 개인정보보호 기술의 국내 선적용을 통하여 제품의 인지도와 완성도를 높이고, 이를 기반으로 다양한 국내외 기관의 표준전문가와 교류를 통하여 표준화를 추진하는 것이 필요함
- WT전략: 방어적전략(약점최소화-위험회피)
  - ▫ 시장과 인력이 취약하다는 약점을 최소화하고 외산 제품 독점 위협을 회피하기 위하여 산학연 연계를 통한 선도기반 과제를 통한 기술 획득 및 이를 기반으로 하는 인력 양성 및 표준화 추진이 필요함

• **표준화 추진방향**

- ID관리 및 개인정보보호에 대한 기초 기술은 학계의 연구를 통해 개발하고, 이를 통한 핵심 · 원천 기술은 국책 연구기관에서 개발하며, 이에 대한 시장 적용 기술은 산업체에서 개발함
- 핵심 기술에 대한 표준화는 국내의 경우 TTA PG502에서 추진하며, 관련 산업계와 학계의 구심적 역할을 수행하는 디지털 아이디관리포럼을 통해 산업체의 요구사항을 수렴함
- 국제 표준화는 ITU-T/SG17, ISO/IEC JTC1/SC17, SC27에 참여하여 수행함

3.1.3. 표준화 추진체계



〈그림 7〉 ID관리 및 개인정보보호 기술의 표준화 추진체계

• 국내 표준은 ETRI, KISA 그리고 정보보호 산업체에서 국내 표준 초안을 개발하고 TTA를 통하여 정보통신 단체표준으로 개발함. 정보통신 단체 표준은 TTA TC5 PG502를 통하여 추진함

• ID관리 및 개인정보보호 기술을 집중적으로 다루는 디지털아이디관리포럼을 통해 학계의 기반 기술과 산업계의 요구사항을 수렴하여 표준을 개발함

• ISO/IEC JTC1과 ITU-T에 국내 표준 전문가들이 활발히 참여하여, 국내에서 개발된 ID관리 및 개인정보보호 기술에 대한 국제 표준화를 수행함

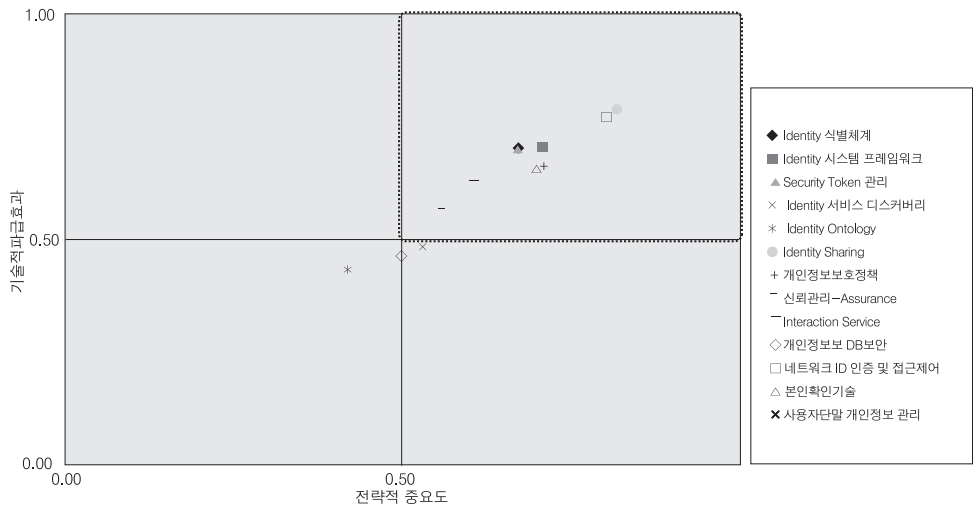
• 네트워크 ID 인증 및 접근제어에 대한 표준화는 국내의 경우 현재 TTA PG 206에서 추진하고 있지만 점차 PG502와 연계하여 표준을 개발하는 방안을 연구하며 국제 표준화는 ITU-T SG13, SG11, SG2를 통해 추진함

3.2. 중점 표준화항목 선정

3.2.1. 중점 표준화항목 선정방법

중점기술 후보별 전략적 중요도 및 기술적 파급효과 분석

평가지표	전략적 중요도(Priority)						기술적 파급효과(Effect)					
	P1 정부 및 산업체 의지(국가 산업전략과의 연관성, 국내 기업의 표준화 참여 및 관심도 등)	P2 공공성(사용자 편리성, 중복 투자 방지 등)	P3 적시성	P4 기술적 선도 가능성(국제표준경쟁력, IPR 확보 등)	P5 국제표준화 이슈정도	PI (Priority Index)	E1 기술적 중요도 (원천성 등)	E2 타 기술에 파급효과(연관성, 활용성 등)	E3 시장파급성 및 상용화 가능성 (구현가능성 등)	E4 산업적 파급효과(산업화로 인한 이득, 국내 관련산업 규모 및 성숙도 등)	E5 미래 영향력 (미래 표준항목에의 적용/응용성)	EI (Effect Index)
표준화 대상항목 \ 평가지표의 중요도	0.22	0.17	0.18	0.21	0.23	-	0.20	0.23	0.17	0.19	0.21	-
Identity 식별체계	3.40	3.63	3.02	3.15	3.60	0.67	3.48	3.15	3.73	3.63	3.65	0.70
Identity 시스템 프레임워크	3.69	3.96	3.46	3.25	3.42	0.71	3.63	3.75	3.08	3.29	3.73	0.70
Security Token 관리	3.46	3.46	3.62	3.32	3.02	0.67	2.96	3.68	3.96	3.76	3.28	0.70
Identity 서비스 디스커버리	2.64	2.75	2.66	2.66	2.57	0.53	2.32	2.36	2.23	2.45	2.68	0.48
Identity Ontology	1.75	1.79	2.04	2.50	2.32	0.42	2.32	2.29	1.89	2.14	2.18	0.44
Identity Sharing	4.19	3.96	4.29	4.06	3.94	0.82	3.81	3.85	3.94	4.31	3.83	0.79
개인정보보호정책	4.09	3.73	3.66	3.23	3.09	0.71	3.14	3.27	3.07	3.27	3.73	0.66
신뢰관리-Assurance	2.79	2.84	2.55	2.82	2.79	0.55	3.00	2.74	2.58	2.89	3.00	0.57
Interaction Service	3.19	3.47	3.00	2.72	2.89	0.61	2.72	2.86	3.33	3.78	3.14	0.63
개인정보보 DB보안	2.84	3.47	2.31	2.38	1.74	0.50	2.51	2.48	2.44	2.20	1.97	0.46
네트워크 ID 인증 및 접근제어	4.11	4.30	4.25	3.91	3.61	0.80	3.75	3.87	3.85	3.96	3.87	0.77
본인확인기술	4.19	4.02	3.71	2.81	2.90	0.70	3.67	3.07	3.48	3.48	2.81	0.66
사용자단말 개인정보 관리	3.35	3.88	3.15	3.10	2.85	0.65	3.60	3.70	3.25	3.38	3.35	0.69



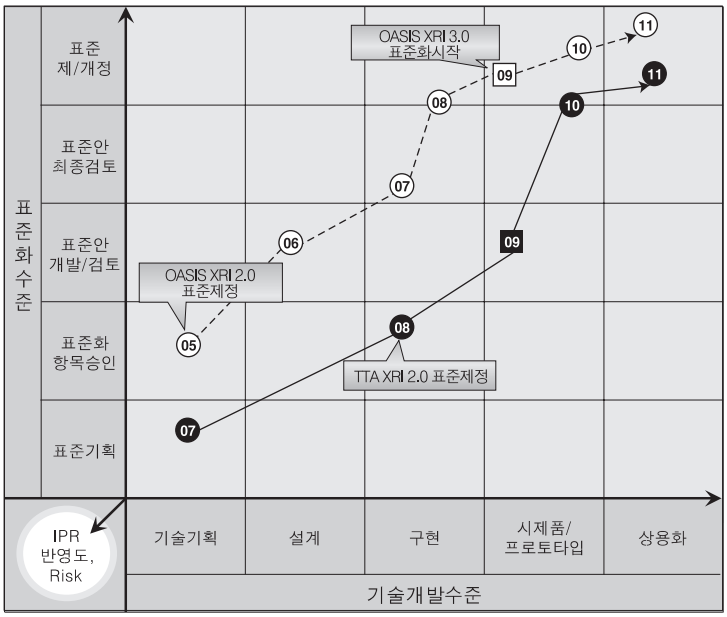
3.2.2. 중점 표준화항목 선정사유

- ID관리와 개인정보보호 분야의 표준화 대상항목 중에서 전략적 중요도와 기술적 파급효과가 모두 0.5보다 큰 10개 항목을 2010년도 ID관리 및 개인정보보호 분야의 중점 표준화 항목을 선정함
- Identity 식별자와 Identity 시스템 프레임워크는 ID관리와 개인정보보호의 기반이 되는 기술로 기술적 파급효과가 매우 큰 분야임
- Identity Sharing, 네트워크 ID 인증 및 접근제어는 사용자의 공유가 핵심인 웹 2.0, 서비스의 개인화가 핵심인 웹 3.0, 사용자의 물리적인 위치에 관계없이 seamless 서비스를 제공받을 수 있는 클라우드 컴퓨팅의 진전에 따라 그 중요성이 더욱 커지고 있음
- Security Token 관리는 인증, 인가 정보 및 Identity 정보 전달을 위한 핵심 기술로 ID관리의 필수 분야임
- 개인정보보호정책과 Interaction Service는 개인정보를 보호하는 정책을 설정하고 판단하며, 개인정보 제공시 사용자의 동의 여부를 확인하고, 개인정보 유출시 책임 소재를 확인할 수 있도록 하는 기능을 제공하는 등 개인정보보호 서비스를 위한 필수 분야임
- 사용자단말 개인정보 관리 기술은 사용자 정보가 모바일 단말기에 집적되고, 모바일 인터넷 뱅킹 서비스 등이 제공되는 등 모바일 컴퓨팅 환경이 급속히 진전됨에 따라 안전한 인터넷 환경 구축의 필수 기술이 되고 있으며 기술규격 완성시 국제 표준으로 추진도 가능한 분야임
- 네트워크 ID 인증 및 접근제어 기술은, NGN 접속제어 기능에 ID관리 기능을 부가하는 것으로, 지난 3년간 ITU-T에서 한국이 주도 해 온 NGN 접속 제어 기능을 확장하는 작업에 해당되며 M2M 접속 인증 제어 등 최근 신기술 표준화가 이루어지고 있는 분야임
- 본인확인기술은 최근 그 중요성이 부각되는 기술로, 국내의 경우 안전한 인터넷 환경과 주민번호 남용 및 도용을 방지하기 위해 정부 정책 의지가 강하게 작용하는 분야임

3.3. 중점 표준화항목별 세부전략(안)

3.3.1. Identity 식별체계

• 표준화-기술개발-IPR 연계분석



표준화 중요도	국내 개발주체		활용도	관련 국제 표준화 기구
고(★★★) 중(★★☆) 저(★☆☆)	표준개발	기술개발		
★★★	TTA 아이디관리 포럼	ETRI KISA	인터넷 서비스 제공자	OASIS IETF

범 례

09 : 중점 표준화항목의 국내상태

09 : 중점 표준화항목의 국제상태

→ : 중점 표준화항목의 국내 표준상태전이

⇢ : 중점 표준화항목의 국제 표준상태전이

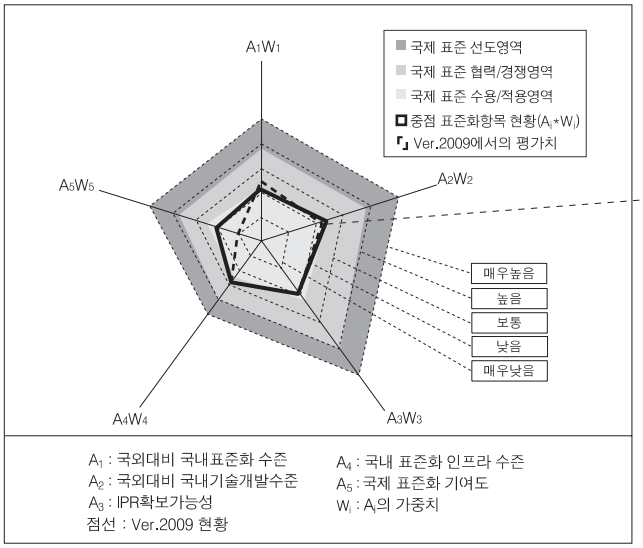
↑ : 선행표준(선 표준화 후 기술개발)

↗ : 동시표준(표준화&기술개발 동시추진)

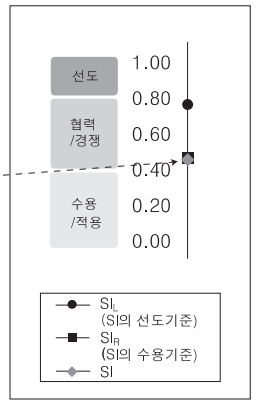
→ : 후행표준(선 기술개발 후 표준화)

표준화 특성	선행표준
표준화-기술개발- IPR 연계방안	선행표준의 특성을 가지고 있기 때문에, 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

• 국제표준화 전략목표 및 세부전략(안)



SI (표준화 전략지수)	
SI_L (SI의 선도기준)	0.77
SI_R (SI의 수용기준)	0.46
SI	0.44



$0 < SI \leq 1$

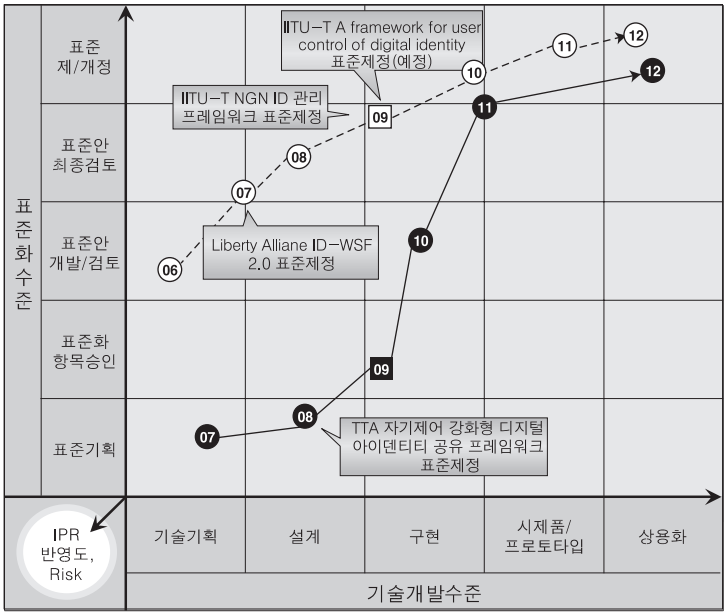
- $SI \geq SI_L$: 선도항목
- $SI_R \leq SI < SI_L$: 협력/경쟁항목
- $SI < SI_L$: 수용/적용항목

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

국제표준화 전략목표	국제표준 협력/경쟁(수용/적용) (Ver.2009) ⟼ 국제표준 수용/적용(협력/경쟁) (Ver.2010)
Trace Tracking (Ver.2009 ⟼Ver.2010)	- 국내에서 XRI에 대한 표준화 완료와 OpenID 서비스의 활성화에 따라 Ver.2010에서는 Ver.2009에 비해 국내표준화수준과 국내기술개발 수준이 상향되었으며 ITU-T, ISO 등 활발한 국제표준화 활동에 따라 국제표준화 기여도도 상향되었음
세부전략(안)	- 국외대비 국내표준화수준 분석에 따른 전략: · 현재 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 · 국제 표준화 작업이 완료되었으며 국내 산업계에서도 활용하고 있는 식별자 관련 표준을 적극적으로 국내에 수용하는 전략이 필요하며, 최근 진행되고 있는 국제 표준화 작업에는 적극적인 참여가 필요함 - 국외대비 국내기술개발수준 분석에 따른 전략: · URL, IRI 식별자는 인터넷의 근간을 이루며 인터넷 서비스에서 활용되고 있으며, XRI의 경우 이미 국내에서 OpenID 서비스에 사용하는 기술로 국내외 기술 격차가 없는 상태임 · 식별자 기술은 모든 서비스의 기반 기술이기 때문에, 산업체에서 신뢰성 있고 신속한 제품과 서비스를 제공할 수 있도록, 국제 표준을 국내에 빠르게 수용하는 것이 필요함 - IPR확보가능성 분석에 따른 전략: · 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 필요함 - 국내표준화인프라수준 분석에 따른 전략: · 2008년 8월 디지털아이디관리포럼이 발족하여 산업체의 다양한 의견이 반영될 수 있는 토대가 마련되었으므로, 디지털아이디관리 포럼을 통해 산업계의 요구를 수렴하고 TTA PG502(개인정보보호 및 ID관리 프로젝트 그룹)를 통하여 국내 산업에 필요한 식별자 기술에 대한 국제 표준을 신속히 수용하는 노력이 필요함 - 국제표준화기여도 분석에 따른 전략: · 식별자 기술에 대한 국제 표준화 기여도는 현재 활발한 국제 표준화 활동으로 인해 점차 상향되고 있으나 활발한 국제 표준 기고를 통해 국제 표준화에 기여도를 높이는 것이 필요함
IPR 확보방안	- 학계와 연구소에서 식별자에 대한 기초 연구 및 IPR 가능 항목을 도출하고 산업계의 서비스 적용을 통한 국제적인 서비스 기반으로의 통용성과 타당성을 검증함으로써 IPR를 확보함

3.3.2. Identity 시스템 프레임워크

• 표준화-기술개발-IPR 연계분석



표준화 중요도	국내 개발주체		활용도	관련 국제 표준화 기구
고(★★★) 중(★★☆) 저(★☆☆)	표준개발	기술개발		
★★★	TTA 아이디관리 포럼	ETRI KISA	포털금융 공공기업	ITU-T SG17 Liberty Alliance

범 례

09 : 중점 표준화항목의 국내상태

09 : 중점 표준화항목의 국제상태

→ : 중점 표준화항목의 국내 표준상태전이

-→ : 중점 표준화항목의 국제 표준상태전이

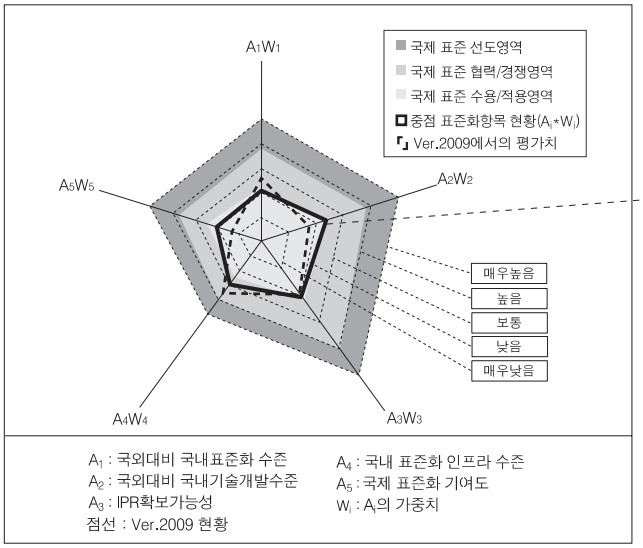
↑ : 선행표준(선 표준화 후 기술개발)

↗ : 동시표준(표준화&기술개발 동시추진)

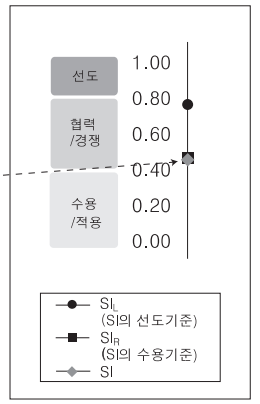
→ : 후행표준(선 기술개발 후 표준화)

표준화 특성	선행표준
표준화-기술개발- IPR 연계방안	선행표준의 특성을 가지고 있기 때문에, 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

• 국제표준화 전략목표 및 세부전략(안)



SI (표준화 전략지수)	
SI_L (SI의 선도기준)	0.77
SI_R (SI의 수용기준)	0.46
SI	0.45



$0 < SI \leq 1$

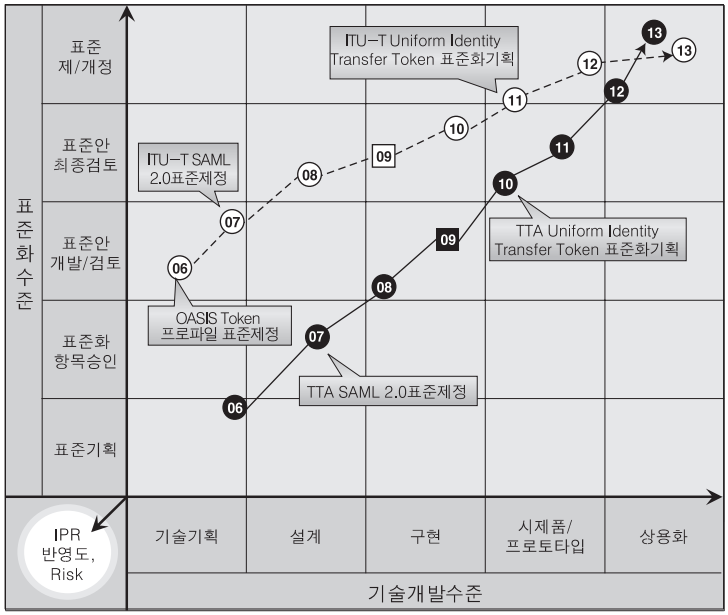
- $SI \geq SI_L$: 선도항목
- $SI_R \leq SI < SI_L$: 협력/경쟁항목
- $SI < SI_L$: 수용/적용항목

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

국제표준화 전략목표	국제표준 협력/경쟁(수용/적용)(Ver.2009) ⟼ 국제표준 수용/적용(협력/경쟁)(Ver.2010)
Trace Tracking (Ver.2009 ⟼Ver.2010)	- 국내에서 출시된 Identity 관리 시스템 제품의 기능 향상에 따라 Ver.2010에서는 Ver.2009에 비해 국내기술개발수준이 상향되었으며, ITU-T, ISO 등 활발한 국제표준화 활동에 따라 국제표준화 기여도도 상향 평가됨
세부전략(안)	- 국외대비 국내표준화수준 분석에 따른 전략: · ITU-T SG17에서 2007년 ID관리 기술 Focus 그룹을 운용하여 ID관리 프레임워크 표준화에 대한 선행 작업을 수행하였음. 현재 SG17 Q.10에서 x.1250 'Baseline capabilities for enhanced global identity management trust and interoperability' 와 x.1251 'A framework for user control of digital identity' 으로 표준이 제정되었음. 또한 SG13에서 Y.idmFramework이 Y.2720 - NGN Identity management framework 로 표준이 제정되었음. 또한 SG17에서는 X.idm-ifa 'Framework architecture for interoperable identity management systems' 에 대한 표준이 진행중임 · ISO SC27에서는 ID관리 기술에 대한 프레임워크 표준화를 제정 중에 있음. 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 · 국내에서는 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 - 국외대비 국내기술개발수준 분석에 따른 전략: · ID관리 프레임워크를 구성하는 세부 기술에 대한 국내외 기술 격차는 거의 없는 상황이나, 세부 기술을 통합하여 제공하는 ID 프레임워크 기술에서는 국내외 기술력의 차이가 존재하는 상태이므로 국내 산업계에서 기술 개발에 적극 활용할 수 있도록 국제 표준을 국내 환경에 맞게 수용하려는 노력이 필요함 - IPR확보가능성 분석에 따른 전략: · 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 필요함 - 국내표준화인프라수준 분석에 따른 전략: · 디지털아이디관리포럼 및 TTA PG502(개인정보보호 및 ID관리 프로젝트 그룹) 등 산업계의 요구사항을 수렴하고 국제 표준화와 연계할 수 있는 국내 표준화 인프라는 잘 갖추어져 있기 때문에 이를 활용한 산학연의 연계 작업을 통해 국내 및 국제 표준화를 진행하는 것이 필요함 - 국제표준화기여도 분석에 따른 전략: · ITU-T SG17 등에서 지속적인 국제 표준화 활동을 통해 국내에서 개발되는 ID 프레임워크 기술이 국제 표준으로 반영되도록 하는 노력이 필요함
IPR 확보방안	- ID관리 프레임워크 기술에 대한 국내외 IPR은 거의 없는 상태로, 국제적으로 활용될 수 있는 IPR 항목을 도출하여 IPR을 확보하고 이를 이용한 국내 표준화와 국제 표준화를 진행하여 확보된 IPR의 가치를 극대화하는 것이 필요함

3.3.3. Security Token 관리

• 표준화-기술개발-IPR 연계분석



표준화 중요도	국내 개발주체		활용도	관련 국제 표준화 기구
고(★★★) 중(★★☆) 저(★☆☆)	표준개발	기술개발		
★★★	TTA 아이디관리 포럼	ETRI KISA	포털금융 공공기업	ITU-T SG17 OASIS

범 례

09 : 중점 표준화항목의 국내상태

09 : 중점 표준화항목의 국제상태

→ : 중점 표준화항목의 국내 표준상태전이

-→ : 중점 표준화항목의 국제 표준상태전이

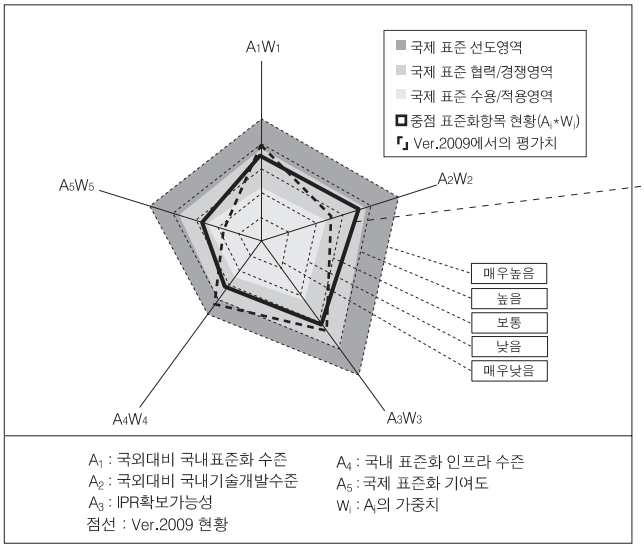
↑ : 선행표준(선 표준화 후 기술개발)

↗ : 동시표준(표준화&기술개발 동시추진)

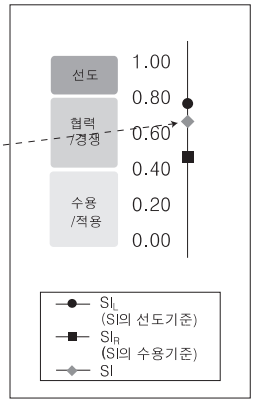
→ : 후행표준(선 기술개발 후 표준화)

표준화 특성	동시표준
표준화-기술개발- IPR 연계방안	동시표준의 특성을 가지고 있기 때문에, 표준 및 산업기술을 동시에 개발하고 표준 개발과 동시에 IPR 항목을 도출하며, 표준이 완료되면 산업체의 제품에 적용하여 표준의 적용성 및 응용성을 확보함

• 국제표준화 전략목표 및 세부전략(안)



SI (표준화 전략지수)	
SI_L (SI의 선도기준)	0.77
SI_R (SI의 수용기준)	0.46
SI	0.65



$0 < SI \leq 1$

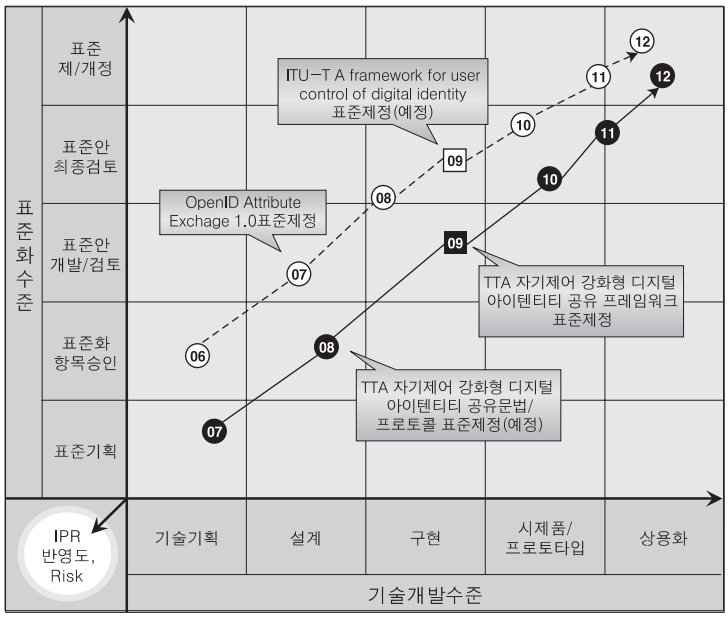
- $SI \geq SI_L$: 선도항목
- $SI_R \leq SI < SI_L$: 협력/경쟁항목
- $SI < SI_L$: 수용/적용항목

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

국제표준화 전략목표	국제표준 협력/경쟁(Ver.2009) ⟼ 국제표준 협력/경쟁(Ver.2010)
Trace Tracking (Ver.2009 ⟼Ver.2010)	- 국내에서 Identity 관리 시스템 제품의 기능 향상에 따라 Ver.2010에서는 Ver.2009에 비해 Security Token에 대한 국내기술개발수준이 상향되었으며, ITU-T, ISO 등 활발한 국제표준화 활동에 따라 국제표준화 기여도도 상향되었음
세부전략(안)	- 국외대비 국내표준화수준 분석에 따른 전략: · OASIS에서는 X.509 Token, SAML Token, Kerberos Token 등에 대한 프로파일 표준을 제정하였음 · TU-T의 X.1141 'Security Assertion Markup Language (SAML 2.0)' 표준은 SAML 2.0 Assertion and Protocol, SAML 2.0 Binding과 SAML 2.0 Profile은 2006년 현재 TTA 표준으로 수용된 상태이고, SAML 2.0 Metadata, SAML 2.0 Authentication Context와 SAML 2.0 Conformance Requirements와 Privacy Considerations 부분이 2007년 TTA 표준으로 제정되었음 · 국내 표준화가 진전되었기 때문에, ITU-T 등과 같은 국제 표준화 단체에 국제 표준을 기고하려는 노력이 필요함 - 국외대비 국내기술개발수준 분석에 따른 전략: · 국외에서 SSO, EAM, IdM 등 다양한 제품군이 출시되고 있으며, 국내에서도 SSO, EAM, IdM 시스템 제품군이 출시되고 있으며, ETRI에서 보안 토큰 생성 분배 관련 기술을 보유한 상태로, 국내외 기술 격차가 크지 않은 상황임 · 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 - IPR확보가능성 분석에 따른 전략: · 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 - 국내표준화인프라수준 분석에 따른 전략: · 기존 국내 표준 제정 인프라는 충분히 확충되어 있으며, 기반 기술인 암호관련 대칭키와 공개키 표준이 이미 제정되어 있으므로, 이들 기반 인력과 기술을 활용하여 국제 표준을 확보하려는 노력이 필요함 - 국제표준화기여도 분석에 따른 전략: · 국내 기술과 국제 기술의 차이가 그리 크지 않기 때문에, Security Token의 국제 표준화에 적극적으로 참여하여 국내기술이 반영된 국제표준을 도출화려는 노력이 필요
IPR 확보방안	- Security Token은 ID관리 시스템의 핵심 기술로 IPR 확보시 그 파급력이 매우 큰 분야이기 때문에, 학계와 연구소에서의 기초연구를 통해 IPR 가능 항목을 도출하고 산업계에서 시스템의 적용성과 타당성을 검증하는 과정을 통해 IPR을 확보함

3.3.4. Identity Sharing

• 표준화-기술개발-IPR 연계분석



표준화 중요도	국내 개발주체		활용도	관련 국제 표준화 기구
고(★★★) 중(★★☆) 저(★☆☆)	표준개발	기술개발		
★★★	TTA 아이디관리 포럼	ETRI KISA	포털금융 공공기업	ITU-T SG17 OpenID

범 례

09 : 중점 표준화항목의 국내상태

09 : 중점 표준화항목의 국제상태

→ : 중점 표준화항목의 국내 표준상태전이

-→ : 중점 표준화항목의 국제 표준상태전이

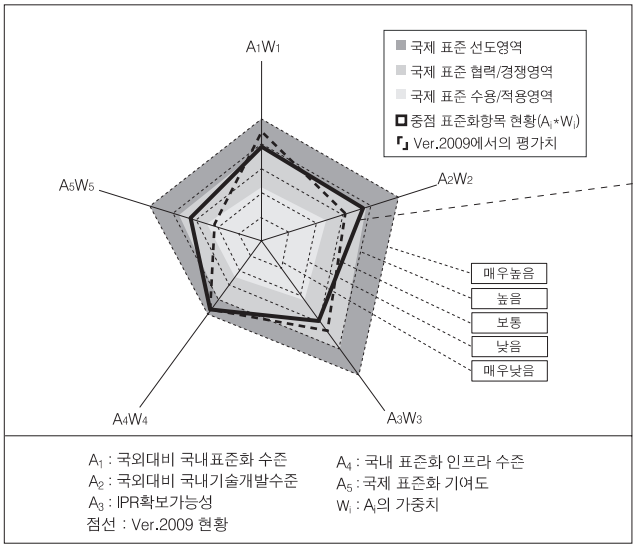
↑ : 선행표준(선 표준화 후 기술개발)

↗ : 동시표준(표준화&기술개발 동시추진)

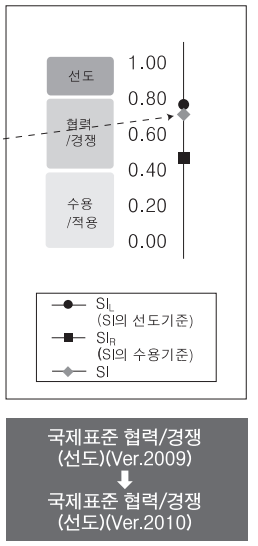
→ : 후행표준(선 기술개발 후 표준화)

표준화 특성	동시표준
표준화-기술개발- IPR 연계방안	동시표준의 특성을 가지고 있기 때문에, 표준 및 산업기술을 동시에 개발하고 표준 개발과 동시에 IPR 항목을 도출하며, 표준이 완료되면 산업체의 제품에 적용하여 표준의 적용성 및 응용성을 확보함

• 국제표준화 전략목표 및 세부전략(안)



SI (표준화 전략지수)	
SI_L (SI의 선도기준)	0.77
SI_R (SI의 수용기준)	0.46
SI	0.72



$0 < SI \leq 1$

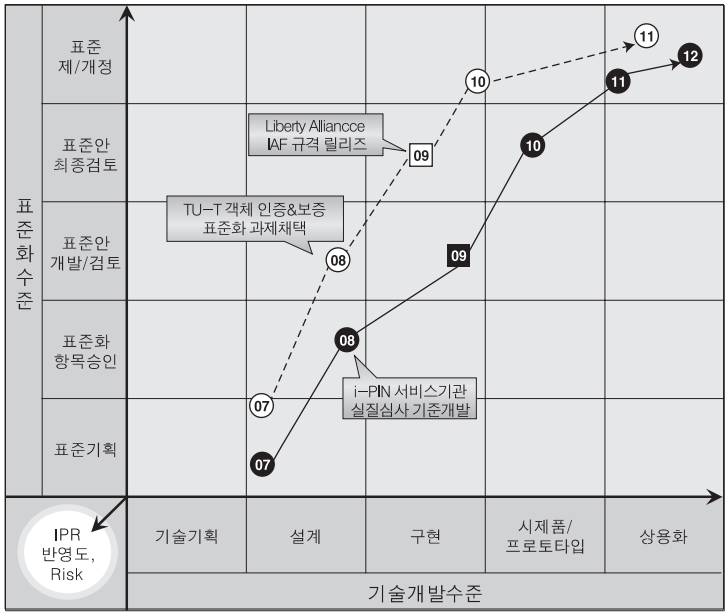
- $SI \geq SI_L$: 선도항목
- $SI_R \leq SI < SI_L$: 협력/경쟁항목
- $SI < SI_L$: 수용/적용항목

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

국제표준화 전략목표	국제표준 협력/경쟁(선도)(Ver.2009) ⟼ 국제표준 협력/경쟁(선도)(Ver.2010)
Trace Tracking (Ver.2009 ⟼Ver.2010)	- 국내에서 사용자 중심 Identity 공유 기술의 개발 진전에 따라 Ver.2010에서는 Ver.2009에 비해 국내기술개발수준이 상향되었으며, ITU-T 등에서의 활발한 국제표준화 활동에 따라 국제표준화 기여도도 상향 평가됨
세부전략(안)	- 국외대비 국내표준화수준 분석에 따른 전략: · 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 진행하고 있음 · ETRI는 ID관리 기술인 'A framework for user control of digital identity' 에 관한 기고문을 ITU-T에 발표하여 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 - 국외대비 국내기술개발수준 분석에 따른 전략: · 국내에서는 ETRI에서 ID-WSF 기반 Identity Sharing 기술을 개발하여 산업체에 기술 이전함으로써 다수 산업체에서 Identity Sharing 기술을 보유하게 되었으며, 2009년 현재 수행 중인 '자기통제 강화형 전자ID지갑 시스템 기술개발' 과제를 통해 사용자 중심 Identity Sharing 기술을 개발하고 있음 · 국외에서는 다수의 ID관리 관련 업체에서 ID-WSF 기반 Identity Sharing 기술을 보유하고 있으며, Microsoft CardSpace와 OpenID에서 ID 교환 프로토콜 및 Attribute Exchange 프로토콜 기술을 보유하고 있음 · 국내외 기술 격차가 거의 없기 때문에, 국내 기술을 바탕으로 국내 표준을 개발하면서 동시에 국제 표준화를 진행하는 것이 필요함 - IPR확보가능성 분석에 따른 전략: · 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 필요함 - 국내표준화인프라수준 분석에 따른 전략: · 디지털아이디관리 ID관리 포럼이 발족하여 Identity Sharing 기술에 대한 국내 주요 표준화기구, 연구기관 및 산업체들의 공동 연구가 가능해지고, TTA PG502를 통해 국내 표준화를 수행할 수 있어 국내 인프라 수준은 높은 수준이므로, 산학연 전문가들과 표준 전문 인력을 활용하여 국제 표준화를 적극적으로 진행하는 것이 필요함 - 국제표준화기여도 분석에 따른 전략: · ITU-T SG17에 지속적으로 참여하며 기고문을 제출하는 등 국제 표준화에 기여도가 높아 국제 표준화 환경이 우수한 분야이기 때문에, 국내에서 개발되는 Identity Sharing 기술의 국제 표준화에 집중할 필요가 있음
IPR 확보방안	- 웹 2.0, 모바일 컴퓨팅 환경 등 다양한 분야에서 현실적으로 필요한 ID 공유 요구를 산업계에서 수렴하고 이를 통해 IPR 항목을 도출하고 IPR을 확보함

3.3.5. 신뢰관리-Assurance

• 표준화-기술개발-IPR 연계분석



표준화 중요도	국내 개발주체		활용도	관련 국제 표준화 기구
고(★★★) 중(★★☆) 저(★☆☆)	표준개발	기술개발		
★	TTA 아이디관리 포럼	ETRI KISA	인터넷 서비스 제공자	ITU-T SG17 Liberty Alliance

범 례

09 : 중점 표준화항목의 국내상태

09 : 중점 표준화항목의 국제상태

→ : 중점 표준화항목의 국내 표준상태전이

-→ : 중점 표준화항목의 국제 표준상태전이

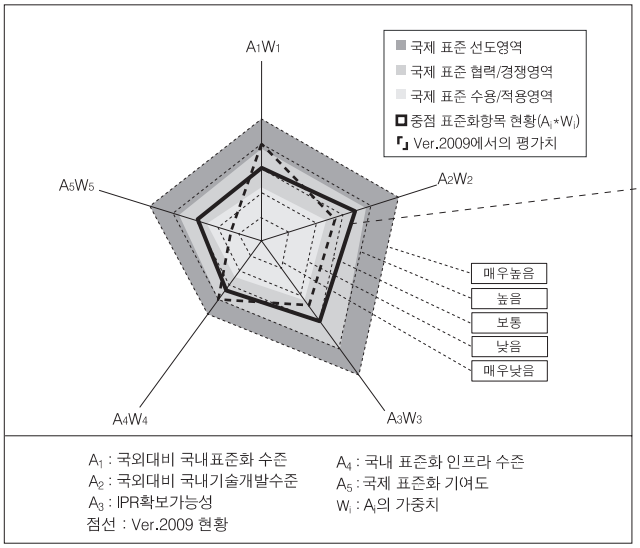
↑ : 선행표준(선 표준화 후 기술개발)

↗ : 동시표준(표준화&기술개발 동시추진)

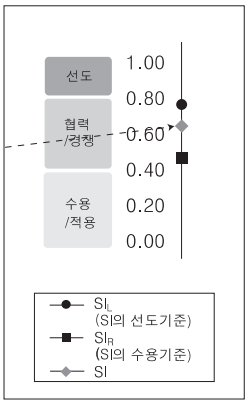
→ : 후행표준(선 기술개발 후 표준화)

표준화 특성	선행표준
표준화-기술개발- IPR 연계방안	선행표준의 특성을 가지고 있기 때문에 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

• 국제표준화 전략목표 및 세부전략(안)



SI (표준화 전략지수)	
SI_L (SI의 선도기준)	0.77
SI_R (SI의 수용기준)	0.46
SI	0.65



$0 < SI \leq 1$

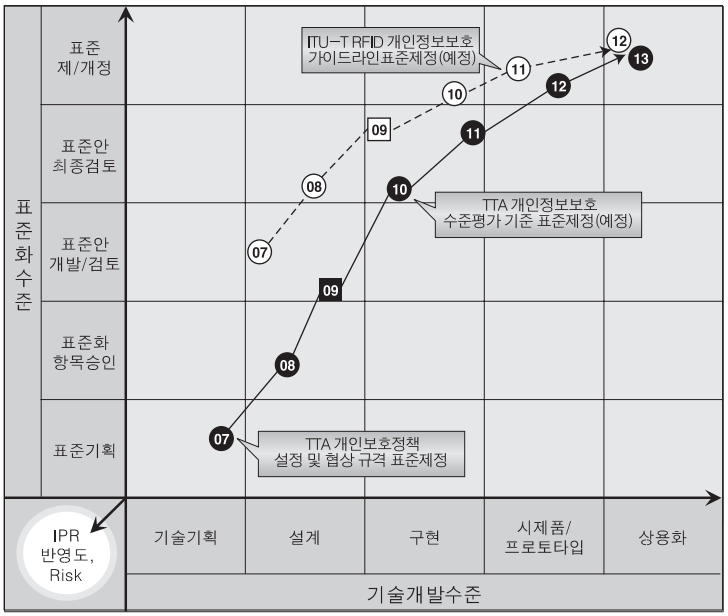
- $SI \geq SI_L$: 선도항목
- $SI_R \leq SI < SI_L$: 협력/경쟁항목
- $SI < SI_L$: 수용/적용항목

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

국제표준화 전략목표	국제표준 협력/경쟁(Ver.2010)
Trace Tracking (Ver.2009 ⊢→Ver. 2010)	- Ver.2009에서는 표준화대상항목으로 선정되지 않았으며, Ver.2010에서는 상대적으로 국외대비 국내 기술개발 수준이 유사한 것으로 평가됨
세부전략(안)	- 국외대비 국내표준화수준 분석에 따른 전략: · Liberty Alliance에서는 미국의 e-Authentication 프레임워크를 기반으로 ID관리 서비스 및 서비스 제공자에 대해 보증(Assurance) 수준별 만족해야 하는 요구조건을 제시하는 IAF(Identity Assurance Framework) v1.1을 2008년 6월 공개하였으며, 2009년 6월 요구조건별 서비스 평가 기준을 제시하는 SAC(Service Assessment Criteria)를 릴리즈하였음 · ITU-T SG17은 ISO/IEC JTC1/SC 27과 함께 미국의 e-Authentication, Liberty Alliance의 IAF, ENISA(European Network And Information Security Agency)의 관련 기준 등을 기반으로 공통된 보증수준에 대한 기준을 제시하는 표준인 "Entity Authentication and Assurance"를 개발 중에 있음 · 국내에서는 공개적으로 인증 및 신뢰 보증수준을 정의하는 기준이나 국내 표준은 없으나, 국내 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 · 현재 국제 표준화 중인 보증 수준 관련 표준에 국내 기준의 일부를 반영하는 형태로 국제 표준화 추진이 가능하며, 표준화 추진 시 국내 기준에서 포함하고 있는 세부적인 평가 방법을 사례 형태로 함께 제시할 필요가 있음 - 국외대비 국내기술개발수준 분석에 따른 전략: · 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 - IPR확보가능성 분석에 따른 전략: · Assurance 등은 국가별로 정책적인 요인에 따라 결정되는 부분이 많기 때문에 Assurance 기술 자체에 대한 IPR 확보보다는 Assurance 기술을 위한 요소 기술들로부터 IPR을 확보하는 것이 필요함 - 국내표준화인프라수준 분석에 따른 전략: · TTA PG502(개인정보보호 및 ID관리 프로젝트 그룹) 및 디지털아이디관리포럼 등을 통해 산업계의 요구사항을 수렴하고 KISA와의 협력을 통해 정책적 수요를 파악하여 산 · 학 · 연 공동으로 국내 환경에 적합한 신뢰관리-Assurance의 국내 표준을 제정하고, 이를 확장하여 국제 환경에 적합한 국제 표준을 도출하려는 노력이 필요함 - 국제표준화기여도 분석에 따른 전략: · ITU-T SG17, ISO/IEC JTC1/SC27 등 신뢰관리-Assurance 표준을 다루고 있는 국제 표준화 기구에서의 활발한 활동이 필요함
IPR 확보방안	- 신뢰관리-Assurance 표준화를 진행함과 동시에 표준에서 요구되는 요소 기술을 추가 개발하여 해당 기술에 대한 IPR을 확보함

3.3.6. 개인정보보호정책

• 표준화-기술개발-IPR 연계분석



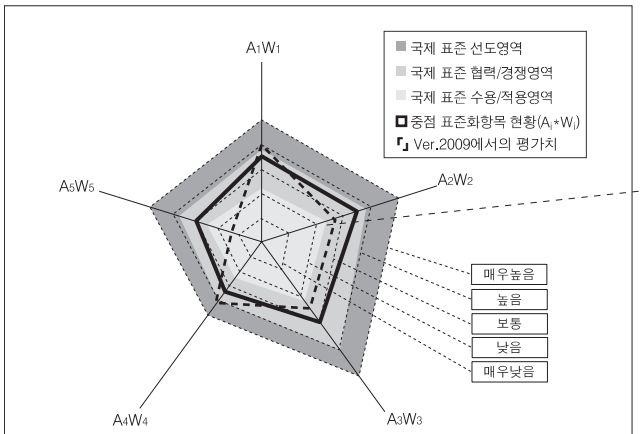
표준화 중요도	국내 개발주체		활용도	관련 국제 표준화 기구
고(★★★) 중(★★☆) 저(★☆☆)	표준개발	기술개발		
★★★	TTA 아이디관리 포럼	ETRI KISA	포털금융 공공기업	IETF OASIS

범 례

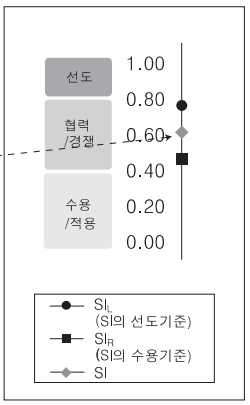
09 : 중점 표준화항목의 국내상태
09 : 중점 표준화항목의 국제상태
→ : 중점 표준화항목의 국내 표준상태전이
⇢ : 중점 표준화항목의 국제 표준상태전이
↑ : 선행표준(선 표준화 후 기술개발)
↗ : 동시표준(표준화&기술개발 동시추진)
→ : 후행표준(선 기술개발 후 표준화)

표준화 특성	선행표준
표준화-기술개발- IPR 연계방안	선행표준의 특성을 가지고 있기 때문에 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

• 국제표준화 전략목표 및 세부전략(안)



SI (표준화 전략지수)	
SI_L (SI의 선도기준)	0.77
SI_R (SI의 수용기준)	0.46
SI	0.65



$0 < SI \leq 1$

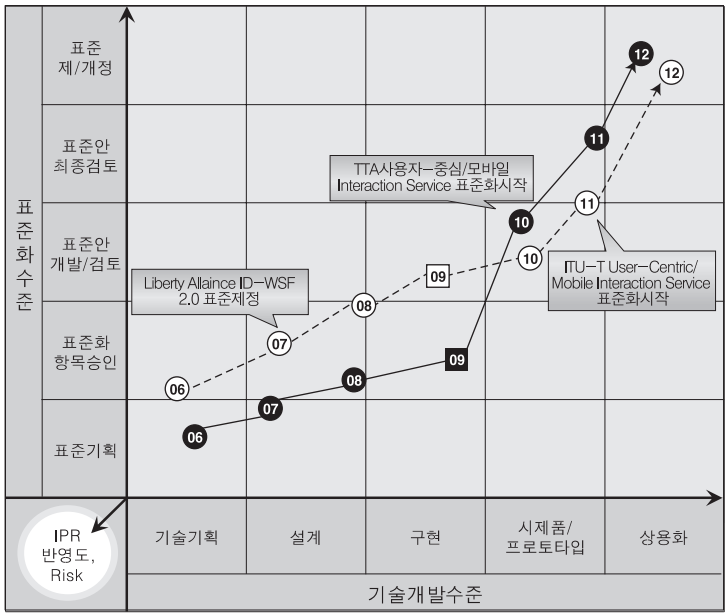
- $SI \geq SI_L$: 선도항목
- $SI_R \leq SI < SI_L$: 협력/경쟁항목
- $SI < SI_L$: 수용/적용항목

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

국제표준화 전략목표	국제표준 협력/경쟁(Ver.2009) ⟼ 국제표준 협력/경쟁(Ver.2010)
Trace Tracking (Ver.2009 ⟼Ver.2010)	- Ver.2009에서는 국외대비 국내 표준화 수준이 "낮음" 으로 분석되었으나, 최근 ITU-T 등에서 국내에서 제안한 개인정보보호 관련 표준화 과제가 신규 채택되는 등으로 인해 Ver.2010에서는 표준화 수준이 상향 평가됨
세부전략(안)	- 국외대비 국내표준화수준 분석에 따른 전략: · W3C에서는 P3P(Platform for Privacy Preferences) 1.0 표준을 2002년도에 제정하였고 2006년도에는 V1.1 표준을 제정한 상태이며, 국내에서는 2007년도에 TTA에서 P3Pv1.1을 기반으로 국내 관련 법규를 반영한 개인정보보호정책 설정 및 협상 규격을 표준으로 제정하였음 · OASIS XACML TC에서는 2005년에는 2.0 버전의 표준을 제정한 상태이며 현재 논의 중인 3.0버전은 올해 표준 제정을 완료할 예정에 있으며, 국내에서는 2005년 XACML 1.0 버전이 국내 표준으로 제정된 상태이며 현재 KISA에서는 XACML 3.0을 기반으로 국내 환경에 적합한 확장성 접근제어 생성언어 3.0 표준을 추진하고 있음 · 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 - 국외대비 국내기술개발수준 분석에 따른 전략: · 웹 브라우저에 내재되어 활용되고 있는 P3P 기술과 ID관리 시스템에서 사용자 접근제어를 수행할 수 있도록 해 주는 개인정보보호정책을 설정하는 XACML 기술은 국내외 모두 보유하고 있음 · ID관리 분야에서의 개인정보보호 수준에 대한 평가기준 등에 대한 국내 표준을 개발하고 ITU-T 등과 같은 표준화 단체에 기고문을 제출하여 국제 표준화를 진행하는 것이 필요함 · 특히, 최근 KISA를 중심으로 개인정보보호 인증체계(PIMS) 구축을 위한 연구·개발이 진행되고 있어, 이를 통한 인증체계에 대한 심사기준 등을 ISO/IEC, ITU-T 등에서 국제 표준화하려는 노력이 필요함 - IPR확보가능성 분석에 따른 전략: · 개인정보보호정책 표준은 특정 기술이 아닌 국가 및 지역에 따라 각기 다르게 적용될 수 있는 정책적 사항을 포함한 것으로 일반적인 기술 개념에서의 IPR 확보는 쉽지 않음 · 따라서 개인정보보호정책 표준 자체의 IPR이 아닌 표준에서 요구되는 개인정보보호기술을 추가적으로 개발하고 표준화하여 IPR을 확보하는 것이 필요함 - 국내표준화인프라수준 분석에 따른 전략: · TTA PG502(개인정보보호 및 ID관리 프로젝트 그룹) 및 디지털아이디관리포럼 등을 통해 산업계의 요구사항을 수렴하고 KISA와의 협력을 통해 정책적 수요를 파악하여 산 · 학 · 연 공동으로 국내 환경에 적합한 개인정보보호 정책의 국내 표준을 제정하고 이를 확장하여 국제 환경에 적합한 국제 표준을 도출하려는 노력이 필요함 - 국제표준화기여도 분석에 따른 전략: · 국내 개인정보보호정책 표준의 국제 표준화를 위해서는 우수 개인정보보호정책 표준의 세부 항목을 보다 일반화하여 국제 표준으로 제안해야 하는데, 이를 위해서는 OECD, ASTAP 등 국제협력 단체 등을 통해 소개되고 있는 각국의 다양한 개인정보보호정책 현황에 대한 사전 파악이 필요함 · 또한, ITU-T SG17 Q10, ISO/IEC JTC 1/SC27 WG3, WG5 등에서 개인정보보호를 다루고 있는 국제 표준화 기구에서의 활발한 활동이 필요함
IPR 확보방안	- 개인정보보호정책 표준화를 진행함과 동시에 표준에서 요구되는 개인정보보호 기술과 모델을 추가 개발하여 해당 기술 및 모델에 대한 IPR을 확보함

3.3.7. Interaction Service

• 표준화-기술개발-IPR 연계분석



표준화 중요도	국내 개발주체		활용도	관련 국제 표준화 기구
고(★★★) 중(★★☆) 저(★☆☆)	표준개발	기술개발		
★	TTA 아이디관리 포럼	ETRI KISA	포털금융 공동기업	ITU-T SG17 Liberty Alliance

범 례

09 : 중점 표준화항목의 국내상태

09 : 중점 표준화항목의 국제상태

→ : 중점 표준화항목의 국내 표준상태전이

-→ : 중점 표준화항목의 국제 표준상태전이

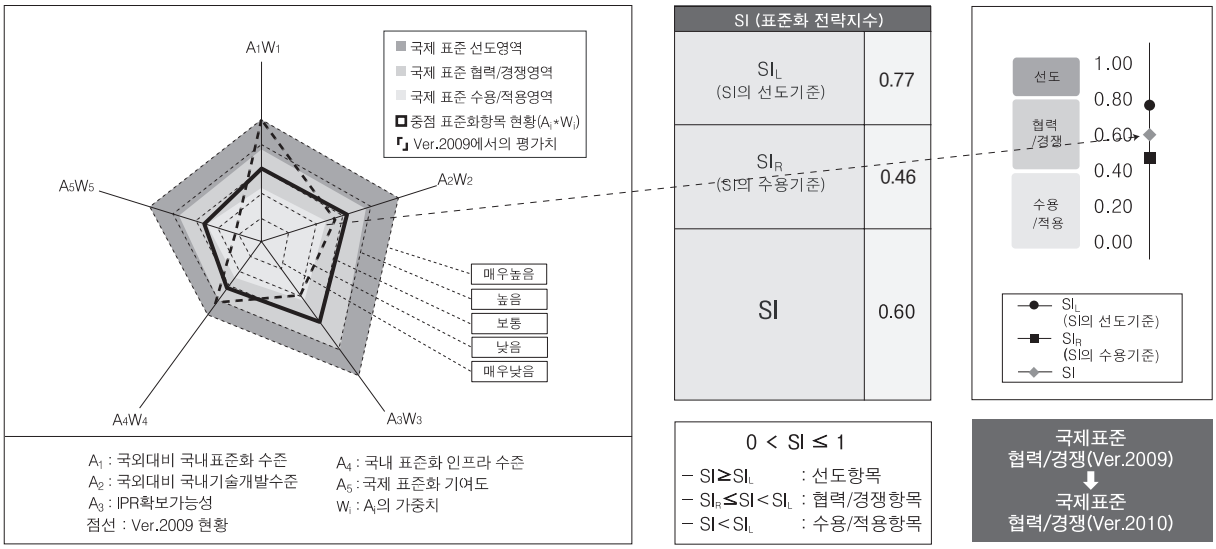
↑ : 선행표준(선 표준화 후 기술개발)

↗ : 동시표준(표준화&기술개발 동시추진)

→ : 후행표준(선 기술개발 후 표준화)

표준화 특성	후행표준
표준화-기술개발- IPR 연계방안	후행표준의 특성을 가지고 있기 때문에, 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 확보함

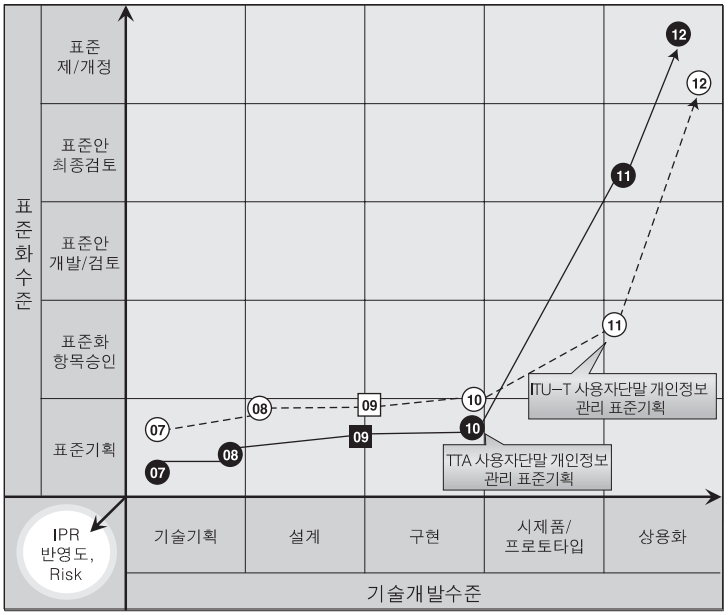
• 국제표준화 전략목표 및 세부전략(안)



국제표준화 전략목표	국제표준 협력/경쟁(Ver.2009) ⟼ 국제표준 협력/경쟁(Ver.2010)
Trace Tracking (Ver.2009 ⟼Ver.2010)	- 국내 모바일 컴퓨팅 환경의 진전에 따라 모바일 디바이스와 사용자간의 Interaction Service 기술이 축적됨에 따라 Ver.2010에서는 Ver.2009에 비해 IPR 확보가능성이 상향되었으며, 2009년 국내 표준화 활동이 다소 미흡함에 따라 국외대비 국내표준화수준은 하향 평가됨
세부전략(안)	- 국외대비 국내표준화수준 분석에 따른 전략: · Liberty Alliance에서 제정된 ID-WSF 2.0 스펙의 일부분으로서 Interaction Service가 제정되어 있는 반면 국내의 표준화 현황은 매우 미비한 상태임 · 국내 산업계에서 기술 개발에 적극 활용할 수 있도록 국제 표준을 국내 환경에 맞게 수용하려는 노력이 필요함 - 국외대비 국내기술개발수준 분석에 따른 전략: · 사용자 중심 ID관리와 개인정보의 자기통제권 확보 등을 위한 새로운 지침 및 표준 개발이 요구됨에 따라 기존에 표준화되어 있지 않은 Interaction Service 표준 제정이 필요한 시기임 · 최근 급속히 발전하고 있는 모바일 컴퓨팅 환경에 적합한 Interaction Service 표준 제정이 필요함 · 사용자 중심 ID관리와 개인정보 자기통제권 확보 기술은 민간 기업에서 여러 모델을 개발하고 있으며, 특히 인터넷 포털 업체를 중심으로 다양한 커뮤니케이션 환경에서의 서비스 모델 개발을 진행하고 있으므로 국내 및 국제 표준기술 확보에 매우 유리함 · 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 국제표준화하려는 노력이 필요함 - IPR확보가능성 분석에 따른 전략: · 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 필요함 - 국내표준화인프라수준 분석에 따른 전략: · 국내 산학연의 표준 전문 인력을 충분히 활용하여 Interaction Service의 국제 표준화를 수행하는 노력이 필요함 - 국제표준화기여도 분석에 따른 전략: · 다양한 커뮤니케이션 단말 환경의 지속적인 혁신이 진행되고 있으므로, 적극적으로 국제 표준화 단체에 참여하여 국내 개발 기술이 국제 표준에 반영되도록 노력하는 것이 필요함
IPR 확보방안	- Interaction Service는 인터넷 포털, 모바일 인터넷 서비스 등에서 특화될 수 있는 기술로 산업체로부터 요구사항을 수렴하여 IPR를 도출하고 확보하는 것이 필요함

3.3.8. 사용자단말 개인정보 관리

• 표준화-기술개발-IPR 연계분석



표준화 중요도	국내 개발주체		활용도	관련 국제 표준화 기구
고(★★★) 중(★★☆) 저(★☆☆)	표준개발	기술개발		
★★	TTA 아이디관리 포럼	ETRI KISA	기업 사용자	ITU-T SG17

범 례

09 : 중점 표준화항목의 국내상태

09 : 중점 표준화항목의 국제상태

→ : 중점 표준화항목의 국내 표준상태전이

-→ : 중점 표준화항목의 국제 표준상태전이

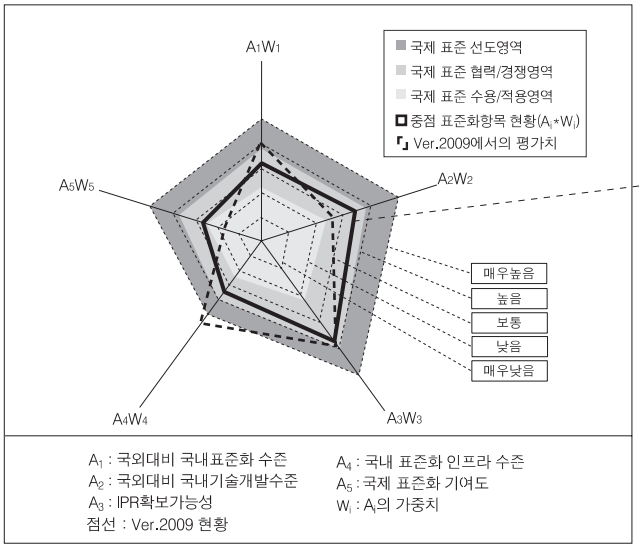
↑ : 선행표준(선 표준화 후 기술개발)

↗ : 동시표준(표준화&기술개발 동시추진)

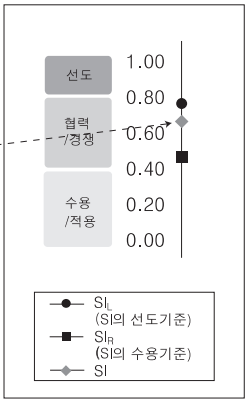
→ : 후행표준(선 기술개발 후 표준화)

표준화 특성	후행표준
표준화-기술개발- IPR 연계방안	후행표준의 특성을 가지고 있기 때문에, 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 확보함

• 국제표준화 전략목표 및 세부전략(안)



SI (표준화 전략지수)	
SI_L (SI의 선도기준)	0.77
SI_R (SI의 수용기준)	0.46
SI	0.67



$0 < SI \leq 1$

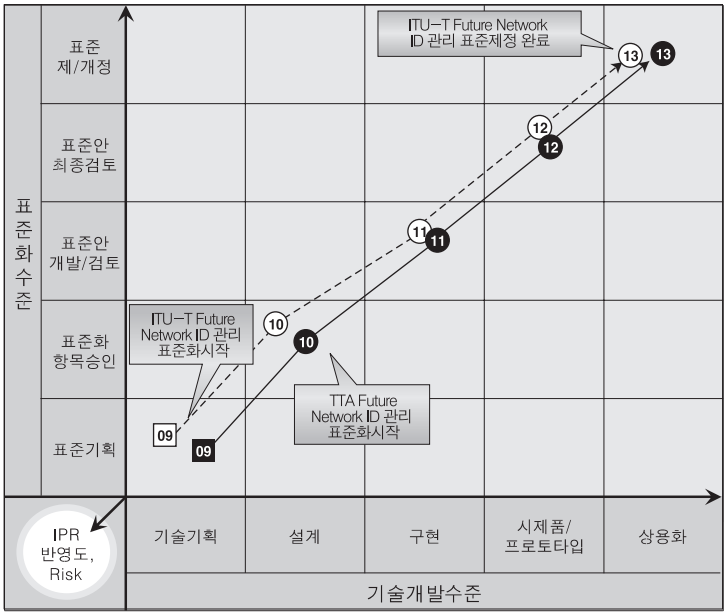
- $SI \geq SI_L$: 선도항목
- $SI_R \leq SI < SI_L$: 협력/경쟁항목
- $SI < SI_L$: 수용/적용항목

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

국제표준화 전략목표	국제표준 협력/경쟁(선도)(Ver.2009) ⟼ 국제표준 협력/경쟁(선도)(Ver.2010)
Trace Tracking (Ver.2009 ⟼Ver.2010)	- 기존 유선 인터넷 뱅킹뿐만 아니라 모바일 단말기를 통해 인터넷 뱅킹 서비스가 제공될 정도로 모바일 인터넷 서비스가 활성화됨에 따라 모바일 단말기의 인증서 등 개인정보 관리 기술이 진전되고 있음. 이에 따라 Ver.2010에서는 Ver.2009에 비해 국내기술개발수준이 상향 평가되었으며, 2009년 국내 표준화 활동이 다소 미흡함에 따라 국외대비 국내표준화 수준은 하향 평가됨
세부전략(안)	- 국외대비 국내표준화수준 분석에 따른 전략: · 국내에서는 인증서를 안전하게 보관하기 위한 표준인 PKCS#11 프로파일 표준이 제정되어 있으며, 국제적으로는 RSA의 de-factor 표준인 PKCS 시리즈 표준이 제정된 상태임 · ETRI는 2008년 9월 ITU-T SG17 Q.9에 'Security requirements and reconfiguration for mobile multi-homed wireless communication'라는 제목으로 모바일 멀티홈드(multi-homed) 장치에서 발생 하는 보안 위협과 보안 요구사항을 정의하고, 이를 위한 보안 서비스 시나리오를 개발하기 위한 표준화 과제를 제안하여 X.msec-5라는 신규 표준과제로 승인을 받아 현재 표준화가 진행중임 · 전반적으로 사용자단말의 개인정보 관리에 대한 표준은 국내외적으로 아직 활발히 진행되고 있지 않은 분야이므로 국내에서 표준화 기술 항목 도출하고 이를 통해 국제 표준을 선도하는 것이 필요함 - 국외대비 국내기술개발수준 분석에 따른 전략: · 기술에 있어서 국내가 많이 뒤쳐져 있었으나 최근 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 필요함 - IPR확보가능성 분석에 따른 전략: · 사용자단말 개인정보 보호에 대한 IPR은 미흡한 상태지만, 사용자단말은 인터넷 보안의 최전방에 위치하는 기술이기 때문에 IPR의 확보시 그 파급력은 매우 클 것으로 예상됨. · 기술적인 격차가 줄어든 지금이 IPR 확보에 적기이며 IPR이 가능한 기술 분야를 도출하고 도출된 분야에 표준화 역량을 집중하는 것이 필요함 - 국내표준화인프라수준 분석에 따른 전략: · 2008년 8월 결성된 디지털아이디관리포럼, TTA PG502(개인정보보호 및 ID관리 프로젝트 그룹) 등 국내 표준화 인프라 수준은 높은 편이며, 이들 기반과 인력을 활용하여 국내 및 국제 표준화를 진행하는 것이 필요함 - 국제표준화기여도 분석에 따른 전략: · 사용자단말 개인정보 보호에 대한 국제 표준화 단체의 활동은 매우 미흡한 실정이기 때문에, 국제 표준화의 필요성을 이해시키고 국내에서 개발된 기술이 국제 표준화 단체의 표준으로 채택되도록 하는 노력이 필요함
IPR 확보방안	- 사용자단말은 키보드보안 등 국내 많은 업체에서 기술 개발이 이루어지고 있는 분야이기 때문에 산업계를 중심으로 IPR 항목을 도출하고 이를 토대로 IPR을 확보하는 것이 필요함

3.3.9. 네트워크 ID 인증 및 접근제어

• 표준화-기술개발-IPR 연계분석



표준화 중요도	국내 개발주체		활용도	관련 국제 표준화 기구
고(★★★) 중(★★☆) 저(★☆☆)	표준개발	기술개발		
★★★	TTA 아이디관리 포럼	ETRI KISA	포털금융 공공기업	ITU-T SG13 3GPP

범 례

09 : 중점 표준화항목의 국내상태

09 : 중점 표준화항목의 국제상태

→ : 중점 표준화항목의 국내 표준상태전이

-→ : 중점 표준화항목의 국제 표준상태전이

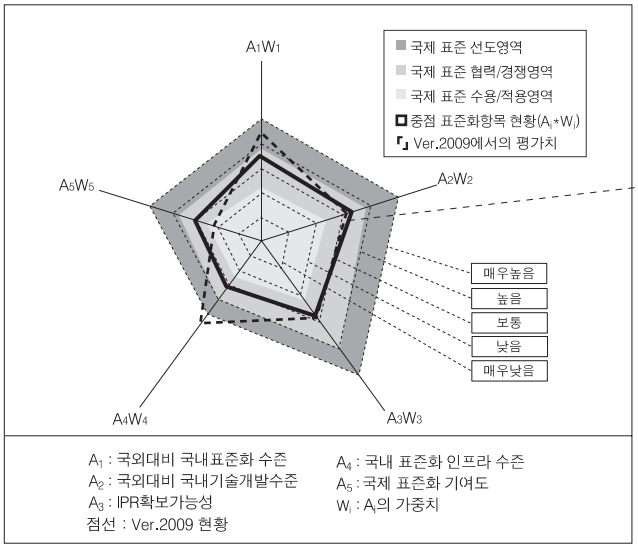
↑ : 선행표준(선 표준화 후 기술개발)

↗ : 동시표준(표준화&기술개발 동시추진)

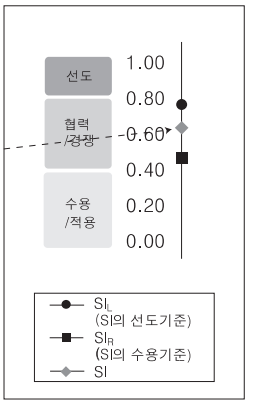
→ : 후행표준(선 기술개발 후 표준화)

표준화 특성	동시표준
표준화-기술개발- IPR 연계방안	동시표준의 특성을 가지고 있기 때문에, 표준 및 산업기술을 동시에 개발하고 표준 개발과 동시에 IPR 항목을 도출하며, 표준이 완료되면 산업체의 제품에 적용하여 표준의 적용성 및 응용성을 확보함

• 국제표준화 전략목표 및 세부전략(안)



SI (표준화 전략지수)	
SI_L (SI의 선도기준)	0.77
SI_R (SI의 수용기준)	0.46
SI	0.63



$0 < SI \leq 1$

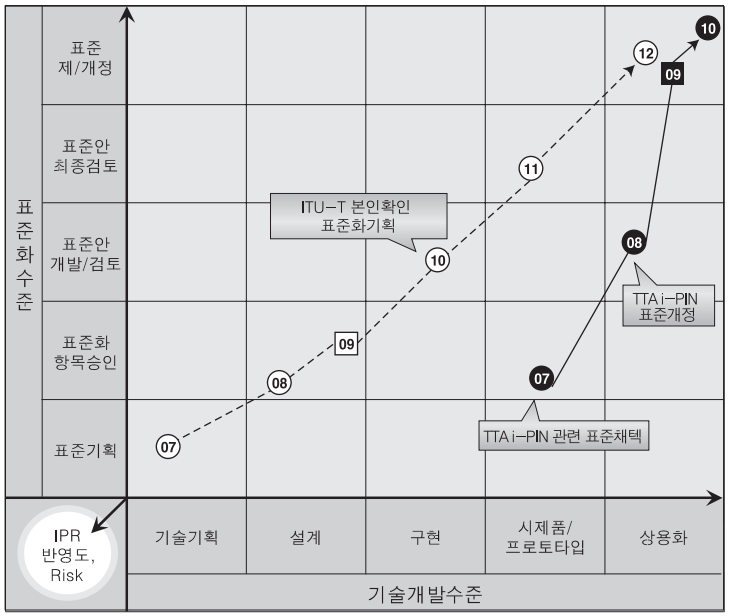
- $SI \geq SI_L$: 선도항목
- $SI_R \leq SI < SI_L$: 협력/경쟁항목
- $SI < SI_L$: 수용/적용항목

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

국제표준화 전략목표	국제표준 협력/경쟁(선도)(Ver.2009) ⟼ 국제표준 협력/경쟁(선도)(Ver.2010)
Trace Tracking (Ver.2009 ⟼Ver.2010)	- ITU-T 등에서의 꾸준한 표준화 활동으로 인해 Ver.2010에서는 Ver.2009에 비해 국제표준화 기여도가 상향 평가되었으며, 2009년 국내 표준화 활동이 다소 미흡함에 따라 국외대비 국내표준화수준은 다소 하향 평가됨
세부전략(안)	- 국외대비 국내표준화수준 분석에 따른 전략: · 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 단계임 · 3GPP가 추진 중인 M2M 접속 인증을 위한 신뢰성 확보 절차기술에 대해 참여하고, 이를 응용한 NGN 표준 개발을 추진하는 것이 필요함 · 3GPP에서는 GAA(Generic Authentication Architecture)와 GBA(Generic Bootstrapping Architecture) 표준을 제정한 상태임. 국내에서는 3GPP의 표준안들을 기반으로 모바일 환경에서의 클라이언트와 서버간의 상호인증 문제들을 해결하는 국내 표준안을 개발하는 것이 필요하며, 이를 바탕으로 국제 표준을 선도하는 것이 필요함 - 국외대비 국내기술개발수준 분석에 따른 전략: · 네트워크 ID 인증 및 접근제어 기술은 국내외적으로 개발이 시작단계인 상황이므로, 네트워크 ID 인증 및 접근제어 표준화를 선도하여 국내외 기술 개발을 선도하는 것이 필요함 - IPR확보가능성 분석에 따른 전략: · 네트워크 ID 인증 및 접근제어 기술에 대한 IPR은 매우 미흡한 실정이며 또한 ITU-T SG13을 한국이 주도하는 등 IPR을 확보하기에 적절한 시기임 - 국내표준화인프라수준 분석에 따른 전략: · 2008년 디지털아이디관리포럼 결성, TTA 개인정보보호 및 ID관리 프로젝트 그룹(PG502) 개편 등 국내 표준화 인프라 수준은 높은 편이며, 이들 기반과 인력을 활용하여 네트워크 ID 인증 및 접근제어 기술을 개발하여 국내 표준화를 진행하고 이와 동시에 국제 표준화를 진행하는 것이 필요함 - 국제표준화기여도 분석에 따른 전략: · ITU-T SG13의 의장을 한국에서 맡고 있을 정도로 국제 표준화에 기여도가 높은 편이며 또한 연구의 시작단계로 국제 표준화를 추진하기에 좋은 시기이므로, 이를 활용하여 네트워크 ID 인증 및 접근제어에 대한 국내 표준화와 동시에 국제 표준화를 진행하는 것이 필요함
IPR 확보방안	- 네트워크 ID 인증 및 접근제어는 기초 기술이면서 동시에 망 서비스의 핵심 기반 기술이기 때문에 산 · 학 · 연 공동으로 IPR 요구사항을 도출하고 이를 토대로 IPR을 확보하는 것이 필요함

3.3.10. 본인확인기술

• 표준화-기술개발-IPR 연계분석



표준화 중요도	국내 개발주체		활용도	관련 국제 표준화 기구
고(★★★) 중(★★☆) 저(★☆☆)	표준개발	기술개발		
★★★	TTA 아이디관리 포럼	ETRI KISA	포털금융 공공기업	ITU-T SG17 ISO-IEC

범 례

09 : 중점 표준화항목의 국내상태

09 : 중점 표준화항목의 국제상태

→ : 중점 표준화항목의 국내 표준상태전이

-→ : 중점 표준화항목의 국제 표준상태전이

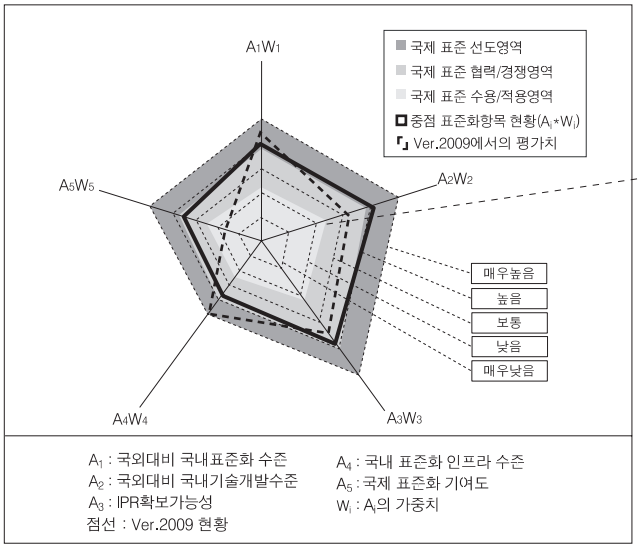
↑ : 선행표준(선 표준화 후 기술개발)

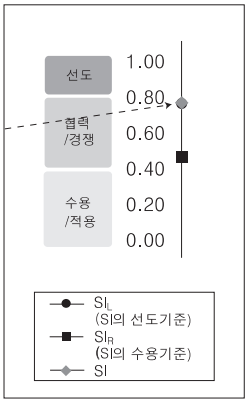
↗ : 동시표준(표준화&기술개발 동시추진)

→ : 후행표준(선 기술개발 후 표준화)

표준화 특성	동시표준
표준화-기술개발- IPR 연계방안	동시표준의 특성을 가지고 있기 때문에, 표준 및 산업기술을 동시에 개발하고 표준 개발과 동시에 IPR 항목을 도출하며, 표준이 완료되면 웹서비스 등에 적용하여 표준의 적용성 및 응용성을 확보함

• 국제표준화 전략목표 및 세부전략(안)





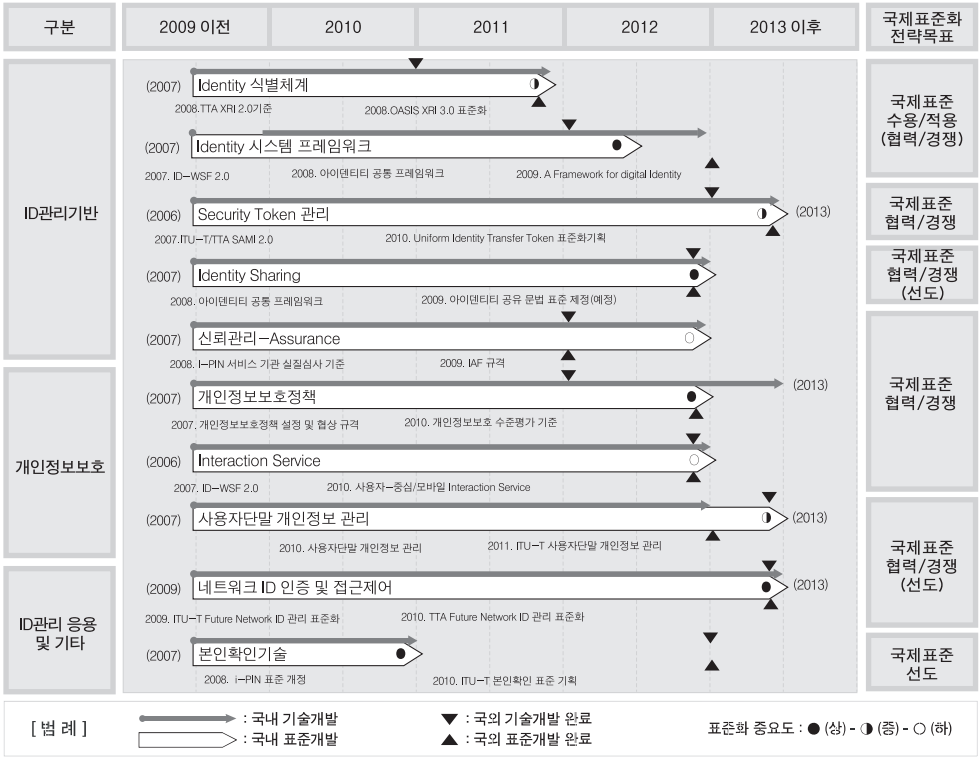
0 < SI ≤ 1
- SI≥SIL : 선도항목
- SIR≤SI<SIL : 협력/경쟁항목
- SI<SIR : 수용/적용항목

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

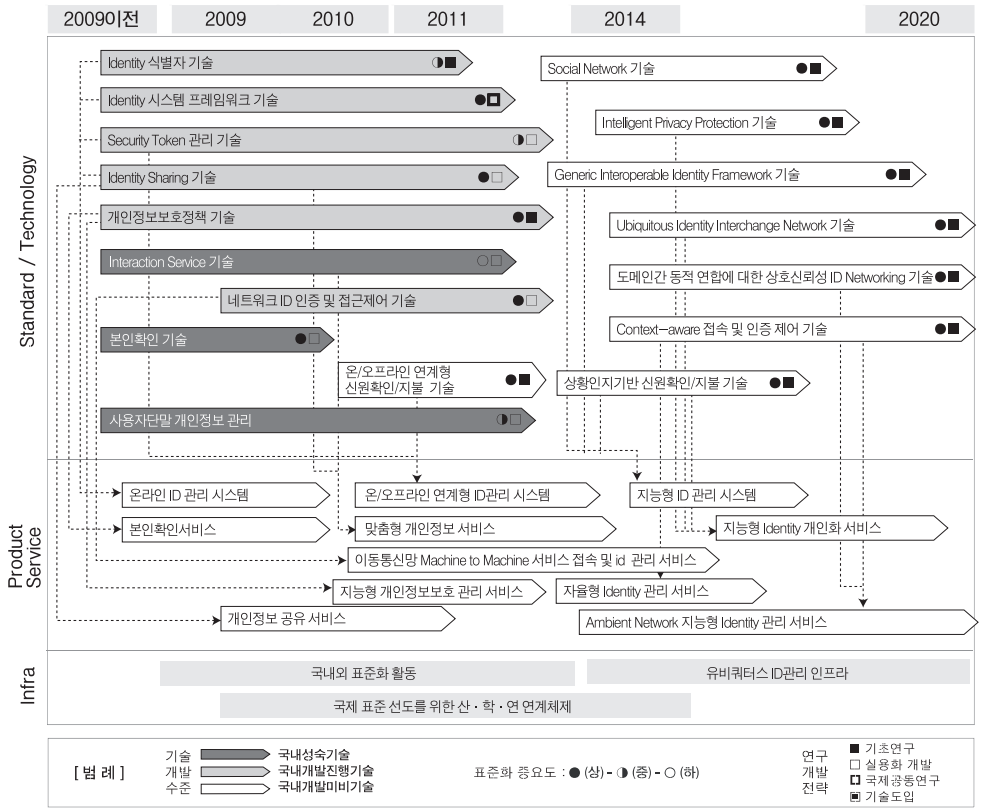
국제표준화 전략목표	국제표준 협력/경쟁(선도)(Ver.2009) ⟼ 국제표준 선도(Ver.2010)
Trace Tracking (Ver.2009 ⟼Ver.2010)	- i-PIN 2.0 적용에 따라 i-PIN 서비스가 본격적으로 적용됨에 따라 Ver.2010에서는 Ver.2009에 비해 국외대비 국내기술개발수준이 상향 평가됨
세부전략(안)	- 국외대비 국내표준화수준 분석에 따른 전략: · 국내 인터넷 상에서 본인확인을 위한 기술인 i-PIN의 서비스 프레임워크, 서비스 전달 메시지 형식에 대한 표준이 2007년 국내 표준으로 제정되었으며, 공공 i-PIN과 민간 i-PIN간의 상호연동 등을 위해 i-PIN 서비스 전달 메시지 형식 및 중복가입 확인정보에 대한 표준이 2008년 개정되었음 · ITU-T, ISO/IEC 등에서 특정 본인확인 기술에 대해서는 따로 표준화가 추진되고 있지는 않음. 다만, ID관리 서비스의 기능 중 하나로 ID Proofing 과정에서 사용자 인증의 하나로 본인확인에 대해 언급하고 있으나, 세부적인 기술은 포함하고 있지 않음 · ITU-T, ISO/IEC 등에서의 ID관리 기술의 표준화가 아직은 초기 단계로 서비스 프레임워크 등에 대한 표준화만 추진되고 세부 기술에 대해서는 추진되고 있지 않으므로 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 - 국외대비 국내기술개발수준 분석에 따른 전략: · 최근 정보통신망법 개정으로 일정 규모 이상의 웹사이트에 대해 주민등록번호 외의 정보로도 회원가입이 가능하도록 규정하고 있는 상황에서 2009년부터 제한적 본인확인제가 강화됨에 따라, i-PIN과 같이 주민등록번호 외에 본인확인을 지원하기 위한 기술의 필요성이 증가하고 있음 · 국내에서는 i-PIN 서비스가 유용할 것으로 판단되나, i-PIN에서 사용하는 중복가입확인정보는 단일 체계 내에서 유일한 식별자를 생성하는 방법을 취하고 있어 국제적으로 활용하기에는 어려움이 따름 · i-PIN 기술개발 및 서비스 구축 경험을 기반으로 i-PIN 기술을 보다 일반화하거나 혹은 국제적으로 활용할 수 있는 추가적인 본인확인 기술을 개발하고 이를 국제 표준화하려는 노력이 필요함 - IPR확보가능성 분석에 따른 전략: · 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 - 국내표준화인프라수준 분석에 따른 전략: · TTA PG502(개인정보보호 및 ID관리 프로젝트 그룹) 및 디지털아이디관리포럼 등을 통해 산업계의 요구사항을 수렴하고 ISO/IEC, ITU-T 등에서의 ID 관리 기술 표준화 추진 흐름을 사전에 파악하여 국제 환경에 적합한 본인확인 기술을 개발, 국제 표준화 추진하는 것이 필요함 - 국제표준화기여도 분석에 따른 전략: · ITU-T, ISO/IEC 등에서의 활발한 표준화 참여를 통해 국내 본인확인 기술이 국제적인 ID-Proofing 기술로 표준화되도록 노력하는 것이 필요함
IPR 확보방안	- 국내 환경에 적합한 i-PIN 등을 국제 환경에 맞는 기술로 수정 · 보완하여 국제 표준화와 동시에 IPR 확보하는 것이 필요함

3.4. 중장기 표준화로드맵

3.4.1. 중기('10~' 12) 표준화로드맵



3.4.2. 장기 표준화로드맵(10년 기술예측)



[국내외 관련 표준 대응리스트]

구 분	표준화 항목	표준명	기구 (업체)	제정 연도	제개정 현황	국내 관련표준	국내 추진기구
ID관리 및 개인 정보보호	ID관리 기반	RFC 1738, Uniform Resource Locators (URL)	IETF	1994	제정	TTAS.IF-RFC1738	TTA
		RFC 3987, Internationalized Resource Identifiers (IRIs)	IETF	2005	제정	TTAE.IF-RFC3987	TTA
		Extensible Resource Identifier(XRI) Syntax V2.0	OASIS XRI TC	2005	제정	TTAE.OT-12.0007	TTA
		X.1141, 'Security Assertion Markup Language (SAML 2.0)	ITU-T	2006	제정	TTAS.IF-X1411_1~6	TTA
		ID-WSF(Web Service Framework) 2.0	Liberty Alliance	2007	개정	-	TTA
		ID-WSF Discovery Service	Liberty Alliance	2007	개정	-	TTA
		확장형 자원 식별자(XRI) 문법 V2.0	TTA	2008	제정	TTAE.OT-12.0007	TTA
		상호호환성 및 신뢰를 위한 글로벌 ID 관리 시스템 요구사항	TTA	2008	제정	TTAI.IT-X1250	TTA
		자기통제 강화형 디지털 아이덴터티 공유 프레임워크	TTA	2008	제정	TTAK.KO-12.0074	TTA
		공통 아이덴터티 데이터 모델	TTA	2009	제정중	-	TTA
		사용자중심 ID관리 서비스의 안전성 검증 기준	TTA	2009	제정중	-	TTA
		자기제어 강화형 디지털 아이덴터티 공유 프로토콜	TTA	2009	제정중	-	TTA
		자기제어 강화형 디지털 아이덴터티 공유 계약 문법	TTA	2009	제정중	-	TTA
		자기제어 강화형 디지털 아이덴터티 인증 프로토콜	TTA	2009	제정중	-	TTA
	개인 정보보호	P3P(Platform for Privacy Preferences) 1.0	W3C	2002	제정	TTAE.OT-10.0015	TTA
		XACML(eXtensible Access Control Markup Language) 2.0	OASIS	2005	개정	TTAS.OT-10.0040/R1	TTA
		P3P(Platform for Privacy Preferences) 1.1	W3C	2006	개정	-	TTA
		RFID 프라이버시 보호 가이드라인	TTA	2006	제정	TTAS.KO-06.0111	TTA
		개인정보 생명주기별 프라이버시 관리 모델	TTA	2007	제정	TTAS.KO-12.0053	TTA
		개인정보보호정책 설정 및 협상 규격	TTA	2007	제정	TTAS.KO-12.0051	TTA
		ID-WSF Interaction Service 2.0	Liberty Alliance	2007	개정	-	TTA
		개인정보 DB 관리 기술의 보안요구사항	TTA	2008	제정	TTAK.KO-12.0072	TTA
		프라이버시 강화형 역할기반 접근통제 정책언어	TTA	2008	제정	TTAK.KO-12.0073	TTA
		확장성 접근제어 생성언어 3.0	TTA	2008	개정	TTAI.OT-10.0040/R2	TTA
		개인정보보호 수준 평가 기준	TTA	2009	제정중	-	TTA
		개인정보보호를 위한 DB 보안감사 로그	TTA	2009	제정중	-	TTA
	ID관리 응용 및 기타	TS 33.220-222 "Generic Authentication Architecture"	3GPP	2004	제정		TTA
		i-PIN 서비스 전달 메시지 형식	TTA	2007	제정	TTAS.KO-12.0055	TTA
		i-PIN 서비스 프레임워크	TTA	2007	제정	TTAS.KO-12.0055	TTA
		i-PIN 서비스 전달 메시지 형식	TTA	2008	개정	TTAK.KO-12.0055/R1	TTA
		i-PIN 서비스 중복가입 확인정보	TTA	2008	개정	TTAK.KO-12.0038/R1	TTA

[참고문헌]

〔01〕 Bandit Project, http://www.bandit-project.org/
〔02〕 Digital Identity 관리 기술 현황 및 전망, 전자통신동향분석지, 2007.2
〔03〕 E-Authentication Solutions, DOE Information Management Conference, 2008.3.19
〔04〕 e-Authentication, http://www.cio.gov/eauthentication
〔05〕 e-Identity 보호용 공통보안서비스 플랫폼 기술 개발, 한국전자통신연구원, 2007.2
〔06〕 ETRI MS 전자ID지갑 엽구협력 체결 및 기대효과, Monthly 사이버시큐리티, 2007.6
〔07〕 FIDIS, http://www.fidis.net/
〔08〕 FTC, "Federal Trade Commission - 2006 Identity Theft Survey Report," 2007.11
〔09〕 GUIDE, http://istrg.som.surrey.ac.uk/projects/guide/
〔10〕 Higgins Project, http://www.eclipse.org/higgins/
〔11〕 ID 관리 기술 및 표준화 동향, 한국정보과학회 정보과학회지, 2007.5
〔12〕 IDC, "Worldwide Identity and Access Management 2009-2012 Forecast: The Initial View," 2009.3
〔13〕 Identity Management Developments at IETF-69, FG IdM DOC 147, 2007.7
〔14〕 Identity Metasystem 기술 및 동향, 전자통신동향분석, 2007.6
〔15〕 I-names, http://inames.net/
〔16〕 ISO/IEC JTC 1/SC 27, Information technology - Security Techniques - A framework for identity management, 3rd Working Draft 24760, 2007. 6. 29
〔17〕 ITU-T IdM Focus Group website, http://www.ituwiki.com/index.php?title=Focus_Group_on_Identity_Management
〔18〕 ITU-T Study Group 13, http://www.itu.int/ITU-T/studygroups/com13/index.asp
〔19〕 ITU-T Study Group 17, http://www.itu.int/ITU-T/studygroups/com17/index.asp
〔20〕 ITU-T Living List of Identity Management Forums, http://www.ituwiki.com/index.php?title=Living_List_of_Identity_Management_Forums
〔21〕 ITU-T SG13 국제표준회의 참가보고, TTA 저널, No. 111, TTA, 2007.5
〔22〕 Joaquin Miller, SXIP Specification, Version 1.0, http://yadis.org/papers/yadis-v1.0.pdf
〔23〕 Liberty Alliance http://projectliberty.org/
〔24〕 MIC & KISA, "u-정보보호 마스터플랜," 2006.10
〔25〕 NIST, An Ontology of Identity Credentials Part 1: Background and Formulation, NIST SP 800-102 Draft, 2006. 10.
〔26〕 OASIS SAML(Security Assertion Markup Language) v2.0 고찰 및 응용, 한국멀티미디어학회 학회지, 2006.3
〔27〕 OASIS, Extensible Resource Identifier (XRI) TC , http://www.oasis-open.org/committees/xri/
〔28〕 OASIS, OASIS News, http://www.oasis-open.org/news/
〔29〕 OASIS, Security Services (SAML) TC, http://www.oasis-open.org/committees/security/
〔30〕 OASIS, Extensible Resource Identifier(XRI) TC, http://www.oasis-open.org/committees/xri/
〔31〕 OASIS, XRI Data Interchange(XDI) TC, http://www.oasis-open.org/committees/xdi/
〔32〕 OECD WPISP, "Background paper on digital identity management," 2006.10
〔33〕 OpenID Community, http://openid.net/
〔34〕 OpenID 국내 커뮤니티, http://openid.or.kr/
〔35〕 PRIME, https://www.prime-project.eu/

〔36〕 Scott Kveton, The State of OpenID, http://openid.net/pres/openid-solt-final.pdf
〔37〕 Security-Enhanced Callback URL Service in Mobile Device, ICACT 2007, 2007.2
〔38〕 Sxipper, http://www.sxipper.com/
〔39〕 U.S E-Authentication Identity Federation Approved Product List(APL), 2008.7.30
〔40〕 url-based Identity Management 기술동향, 주간기술동향, 2007.4
〔41〕 vnunet.com, ID theft levels on the rise, http://www.vnunet.com/computing/news/2185090/id-theft-rise
〔42〕 Web2.0과 URL기반의 ID관리 기술, 주간기술동향, 2006.8
〔43〕 Website Registration using Link for Privacy, SAM 08 - The 2008 International Conference on Security and Management, 2008.7.15
〔44〕 Windows CardSpace, http://cardspace.netfx3.com/
〔45〕 국내외 ID관리 기술 표준화 동향, 주간기술동향, 2008.7.16
〔46〕 방송통신위원회, 인터넷 정보보호 종합대책, 2008.7.22
〔47〕 사용자 중심 ID 관리 기능을 제공하는 전자ID지갑 시스템, 전자통신동향분석, 2008.8.15
〔48〕 사용자 중심의 ID관리 프로젝트 동향, 주간기술동향, 2008.7.9
〔49〕 신원도용 대응기술 동향, 주간기술동향, 2006.9
〔50〕 오픈소스 ID관리 프로젝트 동향, 주간기술동향, 2007.6
〔51〕 웹환경에서 정책기반 개인정보호 기술, 전자통신동향분석, 2007.8
〔52〕 유럽의 eID 기술동향, 주간기술동향, 2006.6
〔53〕 인터넷 ID 관리 서비스, 전자통신동향분석, 2005.2
〔54〕 인터넷 환경에서의 Identity 공유 기술 동향, 주간기술동향, 2007.6
〔55〕 인터넷ID관리시스템 개요 및 비교, 전자통신동향분석, 2007.6
〔56〕 인터넷식별자포럼, http://www.uriforum.or.kr/
〔57〕 한국IDC, "Korea Security Software 2008-2012 Forecast and Analysis: 1H 2008 Update," 2009.1.30
〔58〕 한국전자통신연구원, "Digital Identity Management - 2008년 기술 백서,", 2008.10
〔59〕 한국정보보호진흥원, "개인정보의 경제적 가치 연간 약 1조 3천억원에 달해," 2007.1
〔60〕 한국정보보호진흥원, 디지털 ID현황 및 정책적 시사점, 2007,6

[약어]

3GPP	3rd Generation Partnership Project
adapID	advanced applications for electronic Identity cards in Flanders
FIDIS	Future of Identity in the Information Society
GAA	Generic Authentication Architecture
GBA	Generic Bootstrapping Architecture
GRS	Global Registry Service
GSS	Global Services Specifications
IAF	Identity Assurance Framework
IAM	Identity and Access Management
ID-FF	IDentity Federation Framework
id	Identifier

ID	IDentity
IdM	Identity Management
ID-SIS	IDentity Services Interface Specification
ID-WSF	IDentity Web Services Framework
IEC	International Electrotechnical Commission
IETF	Internet Engineering Task Force
IGF	Identity Governance Framework
i-PIN	Internet Personal Identification Number
IPR	Intellectual Property Rights
IRI	Internationalized Resource Identifier
IS	Interaction Service
ISO	International Organization for Standardization
ITU-T	International Telecommunications Union - Telecommunication Standardization Sector
JCT	Joint Technical Committee
MOTP	Mobile One-Time Password
NGN	Next Generation Network
NIST	National Institute of Standards and Technology
OASIS	Organization for the Advancement of Structured Information Standards
OMA	Open Mobile Alliance
PRIME	Privacy and Identity Management for Europe
RBAC	Role-based Access Control
SAML	Security Assertion Markup Language
SPML	Service Provisioning Markup Language
SSO	Single Sign On
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
URN	Uniform Resource Name
W3C	World Wide Web Consortium
WSDM	Web Services Distributed Management
WS-Security	Web Service Security
XACML	eXtensible Access Control Markup Language
XDI	XRI Data Interchange
XRI	eXtensible Resource Identifier