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 상용화를 위해서도 역시 필수적인 기술

- ID[1]는 사이버스페이스 상에서 개인식별을 가능하게 함으로써 개인의 안녕과 이해관계에 영향을 미치는 모든 정보로서 식별자(Identifier)와 속성들(Attributes)로 구성되며, '공공기관의 개인정보보호에 관한 법률' 제2조 2항에 정의된 개인정보[2]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 정의
- ID관리 기반 기술은 ID 관리의 기반이 되는 기술로, Identity를 식별할 수 있는 식별자, ID 생성과 유통, 저장, 관리를 위한 공통 프레임워크, 인증, 권한, 속성 정보를 표현하는 보안 토큰(Security Token), ID 서비스를 발

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 포함함)를 말함.

견하는데 사용되는 서비스 디스커버리, ID의 개념과 관계를 정의하는 Identity 온톨로지(Ontology), ID 공유(Identity Sharing)를 위한 ID 공유 기술, 통신 당사자들 간의 신뢰를 관리하는 신뢰 관리 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 관리 모델, 네트워크 ID 인증 및 접근제어, 사용자가 본임임을 확인하는 본인확인 기술 등으로 구성됨

○ 표준화 대상항목의 정의

구분	정의	표준화 대상항목	표준화 내용
ID관리 기반	ID 정보의 식별, 디스커버리, 의미, 형식, 공유 프로토콜 및 공통 프레임워크 기술과 같이 ID 관리의 기반이 되는 표준	Identity 식별자 체계	멀티도메인에서 식별 가능한 식별자의 정의 및 생성 · 관리 규격
		Identity 시스템 공통 프레임워크	ID 생성, 저장, 유통, 관리 서비스를 위한 공통 프레임워크 규격
		보안 토큰 관리	인증, 권한 및 속성, 익명 정보를 포함한 보안토큰의 생성 및 검증 규격
		Identity 서비스 디스커버리	ID 정보의 요청 · 제공, 이를 위한 ID 서비스 발견 메커니즘과 메타데이터의 질의 및 응답 프로토콜 규격
		Identity 온톨로지	시스템 간 자동화된 정보의 교환과 이용이 가능하도록 ID의 개념과 관계를 정의
		Identity 공유	ID 정보 공유를 위한 메시지 형식과 프로토콜 규격
		신뢰 관리	통신 당사자 간의 협상을 통한 신뢰구축 메커니즘과 보안토큰 요청 · 응답 메시지 및 전송에 대한 규격
개인정보보호	개인정보보호 정책, 본인확인, 상호작용 서비스, 개인정보 DB 보안, 사용자단말 개인정보 관리와 같이 사용자 개인정보보호를 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
ID관리응용 및 기타	네트워크상에서의 ID 관리, 인증, 접속제어를 위한 ID 운용 및 상호운용성 확보, 본인확인 기술과 같이 ID관리 응용과 관련된 표준	네트워크 중심의 ID 관리 모델	안전한 네트워크 서비스를 위해 네트워크상에서 접속자와 서비스의 Identity 운용 전주기를 통합적, 체계적으로 관리하는 구조 모델
		네트워크 ID 인증 및 접근제어	안전한 네트워크 서비스를 위해 네트워크 접속자의 Identity를 바탕으로 인증하고 접근 제어하는 기술
		본인확인 기술	온라인상에서 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 시스템들을 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 관련 업체의 ID 응용기술 개발과 이용을 촉진함. 개발되는 표준은 ID 관련 용어 통일, 다양한 연관 표준 수용과 상호운영을 위한 아키텍처 그리고 공통 API를 포함하며, 높은 보안과 프라이버시를 위한 운영 시나리오, 프로파일 등을 마련함
  - 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 새로운 ID 기술은 SAML 보안토큰을 기반으로 사용자의 속성정보를 전달함. 보안토큰 표준화는 Liberty Alliance의 ID-FF(IDentity Federation Framework), W3C의 WS-Security(Web Service Security), OASIS의 WS-Trust 등 기존 표준과의 상호운영을 고려하여 보안토큰의 생성, 전달, 검증, 이용에 관한 표준을 준비하고 ID 공유기술 등과 같은 새로운 기술들에 대응할 수 있는 다양한 프로파일들을 준비함
  - 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 기술. ID 열람 서비스를 제공하는 ID관리 주체는 외부에서 접근할 수 있는 서비스 인터페이스와 정책을 메타데이터 형태로 노출하고, 필요한 경우 서비스 요청 주체와의 협상을 통한 서비스가 가능하도록 함. 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 상호운영을 위한 프로파일을 준비함
  - Identity 온톨로지는 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 판단

의 정확성을 높이기 위해 상황인식 정보(Context-Awareness) 등과의 연계를 위한 관련 표준화가 필요

- 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 필요. 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
- 신뢰관리는 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. 이와 관련된 기술은 WS-Trust 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 마련함. 개인정보보호정책은 개인정보보호 관련 법률과 권고안에서 정한 범위를 준용하면서도 개인정보 취득자의 다양한 비즈니스 상황을 고려해 준비되어야 함. 개인정보보호정책 공개는 P3P와 같은 표준화된 기술을 사용하여 개인정보제공자가 자기정보 제공 시에 취득자의 의무와 이용범위 등을 폭넓게 인식하고 제공여부를 결정할 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 서비스. 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 작성함
- 개인정보를 기반으로 사용자에게 허용되거나 커스터마이즈된 서비스를 제공하는 대부분의 공공기관 또는 기업들은 대용량 개인정보를 효과적으로 검색, 저장, 관리하기 위해 데이터베이스를 활용하고 있음. 따라서 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 개발이 필요
- 사용자단말 개인정보 관리는 다양한 ID 환경에서 ID인증을 위한 입력정보를 비롯하여 ID인증자체를 보호하

기 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 정의

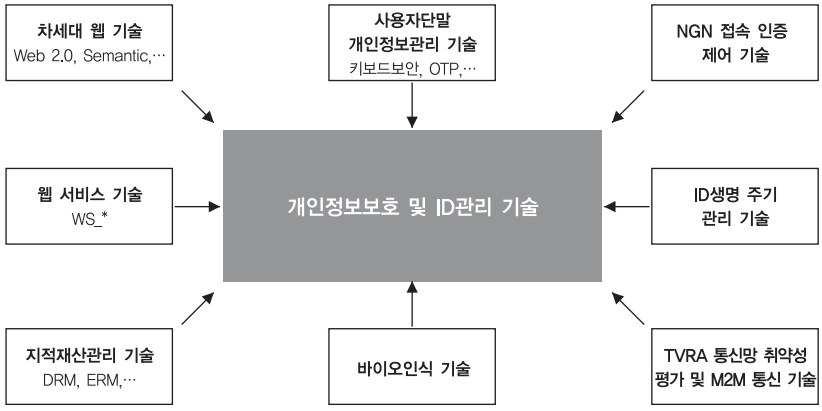
- 네트워크 중심 ID 관리는 통신망에서 운용되는 ID 들을 통신망 사업자 혹은 설계자의 입장에서 관리하는 기술을 정의하며, 현재 ITU-T 에서 개발 중인 차세대 통신망구조 표준에 ID 관리 기술을 접합시키기 위한 제반 작업들로 구성됨. 이는 현재 ITU-T의 ID management GSI(Global Standard Initiative)가 정의하고 있는 내용 중 네트워크중심 ID 관리 프레임워크를 기반으로 하며, 여기에서 거론하고 있는 네트워크 ID 들의 생명주기 관리 모델을 구체화하여, 각 단계별로 기능을 정의하고 NGN 설계에 적용하는 과정으로 대변됨. 그러나, 이러한 과정에서 각 기능 및 절차의 보안성 및 취약성을 정량화 시키는 작업이 아직 진행되지 않은 관계로, 이 부분에 통신망의 취약성 분석 기술인 TVRA(Threat, Vulnerability, and Risk Assessment) 기술을 적용, 표준화된 취약성 설계 기법을 적용하는 작업이 필요
- NGN 구조에 실제 적용된 ID 관리 기능의 설계를 위해서는 ID 관리 데이터 구조를 설계해야 하며, 이 과정에서 Federated ID 관리 혹은 번들 인증 등 NGN/BcN 에 적용될 통신망 기능관련 식별, 인증, 접속 및 상호운용의 기능요구 조건을 반영. 이를 통해 통신망의 NACF, TUP(트랜스포트 사용자 프로파일), SUP(서비스 사용자 프로파일) 의 기능 표준을 개발하며, 접속 및 인증기능을 구현한다. 구체적으로는, 이종 액세스들을 통한 망 접속 시 통합 ID 인증을 위한 프로토콜 및 프로파일 운영 방식, Id의 등록, 바인딩, 신뢰 관계, 위치 정보 관리 등을 위한 추가적인 기능들의 설계 구현방법을 정의하게 됨. Authentication, Authorization, and Access control 기능을 NGN에서 구현
- 응용 및 서비스 중심 ID 관리 기술은 통신망의 응용 및 서비스계층에서 ID 관리를 위한 주소, 번호 관련 정보의 운용관리를 위한 프로파일과 policy의 적용방식 등 서비스 접속제어 기능을 설계 구현하는 표준 기술로 개발됨. 아울러, 차세대 통신망의 응용 서비스 계층에는 인증 ID 관리 기능과 안전하고 편리한 ID 관리 메커니즘을 통합 구성해야 하는데, 이는 3GPP에서 만들어진 GAA(Generic Authentication Architecture)와 GBA(Generic Bootstrapping Architecture) 표준이 정의하는 모바일환경에서의 클라이언트와 서버 간의 상호인증 방식을 주로 참조함. 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 규정. 이러한 안전한 상호인증 메커니즘을 통신망에도 적용하여 IP 망을 기반으로 도입되는 다양한 응용이 안전한 인증프레임워크 상에서 동작하도록 하면서, 동시에 동일하고 일관된 ID 관리 메커니즘을 사용할 수 있도록, Liberty Alliance 의 ID-FF 등 single-sign-on 기술 구조를 도입하여 인증과 ID 관리가 통합되는 구조와 시나리오를 작성하는 작업이 필요
- 상호 접속 및 상호운용성 확보의 측면에서 가장 최신의 기술로 도입되고 있는 것은 도메인 간, 망노드 간, 서비스 간 동적연합을 위한 상호신뢰성 확보 및 접속인증 제어 기술임. 이를 이동통신망에서 응용하는 표준기술로써, 원격지에서 기기 간 통신(M2M) 을 위한 식별기술에 대한 연구가 진행 중이며, 다양한 응용이 예상되고 있음

- 본인확인기술은 웹사이트에 주민등록번호 대신 이용할 수 있는 개인식별번호로써 인터넷상에서 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. i-PIN(Internet Personal Identification Number) 표준화 내용은 i-PIN 서비스 프레임워크, i-PIN 서비스 전달메시지 형식 및 본인확인서비스 중복가입확인정보가 있음

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



〈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	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	W3C, OASIS	표준안 개발/검토	표준화 완료	시제품/ 프로토타입	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 ID관리기술을 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 개인 정보 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	ISO/IEC ITU-T OASIS	표준안 개발/검토	표준안 개발/검토	상용화	상용화
NGN 접속 인증 제어 기술	NGN의 엑세스단에 접속 시도하는 단말을 식별, 인증하고 권한을 확인하여 망 서비스에 접속하도록 configuration 하며, 접속을 위한 사용자 ID를 관리하는 기능을 포함 함	TTA	ITU-T SG11, SG13	표준안 개발다수/ 계속 진행 중	표준안 개발다수/ 계속 진행 중	개발단계	시제품/ 프로토타입
ID 생명주기 관리 기술	통신망 내에서 사용되는 모든 식별자의 생성, 사용, 유지관리, 폐기의 전 과정에 대해 적절한 관리 및 데이터 모델을 제시하는데 적용	FoN	ITU-T SG11, IdM GSI	기초연구	표준안 개발/검토	기초연구	응용연구
TVRA 통신망 취약성 평가 기술	정보시스템의 비밀성, 무결성 및 가용성에 영향을 미칠 수 있는 취약성을 식별하고 정량화 하여 이로 인해 발생하는 위험에 따른 예상 손실을 평가하는 활동으로, ETSI의 표준방법론으로 개발되어 있는데, 이를 ID 관리 시스템 설계에 적용하려는 시도 추진 중	TTA, FoN	ETSI	기초연구	표준안 개발 완료/ 적용 중	응용연구	시제품/ 프로토타입
M2M 통신 기술	사용자가 개입하지 않은 상태에서의 기기 간 통신 기술로, 특히 원격지에서 이루어지는 M2M의 경우 방대한 접속 ID의 관리 및 신뢰성확보를 위한 식별, 인증 이슈가 중요하게 부각 중	TTA	3GPP	기초연구	표준안 개발 진행 중	응용연구	시제품/ 프로토타입

1.2. 추진경과 및 중점 추진방향

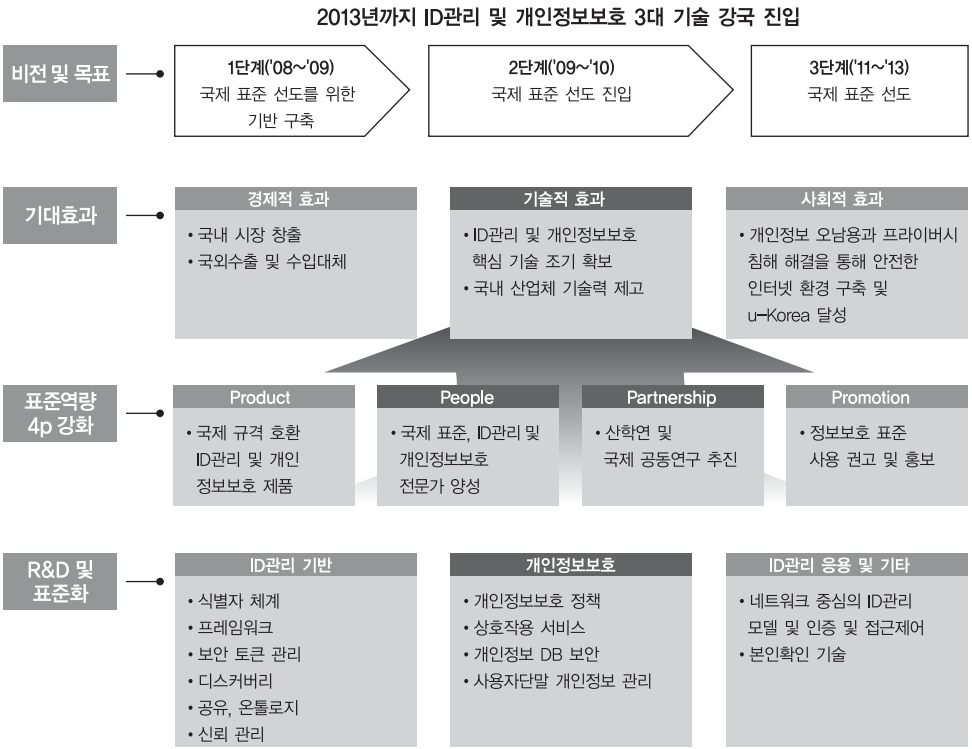
○ 추진경과

- 표준화로드맵 Ver.2009 추진계획은 TTA 표준화본부를 중심으로 관련부처와 전문가Pool을 통해 추진되었으며, 2008년 1월부터 3월까지 기본계획 수립 및 사전 조사 분석이 진행되었으며, 5월에서 6월까지 관련부처 보고 및 중점기술 조정/방향설정이 되었으며 36대 중점기술 선정 및 중점 추진방향이 수립됨. ID관리 및 개인정보보호 기술은 지식 · 정보보안 분야의 중점 기술 중 하나로 선정되었음
- ID관리 및 개인정보보호 기술 분야는 2007년까지의 표준화로드맵에서는 정보보호(일반)의 일부분으로 기술되었으며, 별도의 핵심기술 표준화항목으로 구성되지는 않았음. 그러나 국 · 내외적으로 ID 도용에 따른 피해가 급증하고, 국내의 경우 ID 도용이 사회적인 문제가 되고 시장에서 산업적인 요구사항이 증가함에 따라, ID관리 기술 및 개인정보보호가 정보화/지식 사회의 필수 요소로 인식되고 국 · 내외적으로 ID관리 및 개인정보보호 핵심 기술의 개발이 활발히 진행되고 있으며, 이들 핵심 기술에 대한 표준화 작업이 ITU-T, ISO 등과 같은 국제 표준화 단체에서 활발히 진행됨에 따라, 2008년부터 ID관리 및 개인정보보호 분야가 새롭게 포함되어 중장기 표준화로드맵을 수립하게 되었음. ID관리 및 개인정보보호 중장기 표준화 로드맵 Ver.2009에는 정보통신 중점기술 표준화로드맵 Ver.2008의 개인정보보호 및 ID관리 부분의 내용을 바탕으로 현재 이 분야의 기술 발전, 국내외 환경 변화 및 국제 표준화 추세를 반영하여 주요 이슈를 현행화하고 추진전략을 조정하고 보완함

○ 중점 추진방향

- ID관리 및 개인정보보호 분야의 기술과 표준화 필요성에 대한 이해 제고를 위해 기술 개요, 국 · 내외 기술개발 동향, 국 · 내외 정책 동향, 국 · 내외 시장 동향 및 표준화 동향을 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 표준화별 세부전략을 수립하고 중장기 표준화 로드맵을 작성함

1.3. 표준화의 Vision 및 기대효과



○ ID관리 및 개인정보보호 기술의 경제적 효과

- 국내의 경우, ID관리 및 접근제어 시장이 2007년 308억 원 규모에서 연평균 11.5%의 성장을 보이며 2012년 531억 원 규모의 시장으로 성장할 것으로 전망하고 있음
  - 한국 IDC, "Korea Security Software 2008-2012 Forecast and Analysis", 2008.7.10
- 전 세계적으로 ID관리 및 접근제어 시장 규모를 2005년 2,766백만 달러에서 연평균 10.7%의 성장을 보이며 2011년에 4,975백만 달러에 이를 것으로 전망하고 있음
  - IDC, "Worldwide Identity and Access Management 2007-2011 Forecast and 2006 Vendor Shares", 2007.07
- 2007년도 한국정보보호진흥원 조사에 의하면, 국내의 경우 인터넷 이용자들이 느끼는 연간 개인정보보호에 대한 총 가치는 약 1조 2,982억 원에 달하고 있음
  - 한국정보보호진흥원, "개인정보의 경제적 가치 연간 약 1조 3천억 원에 달해", 2007.1
- 2006년 8월까지 12개월 간 온라인 신원도용 피해를 입은 미국인이 약 1천 5백만 명에 이르며, 그 피해규모는 2005년 7억 1천 4백만 달러 규모에서 2010년에는 16억 달러에 이를 것으로 예상하고 있음

- vnunet.com, ID theft levels on the rise, http://www.vnunet.com/computing/news/2185090/id-theft-rise
- IDC, "Worldwide Identity Theft Black Market 2006-2010 Forecast", 2006.12

1.3.1. 표준화의 필요성

○ 인터넷의 활용이 커져가면서 사용자는 수많은 사이트에 ID를 등록하게 되고 자신의 개인정보를 여러 곳에 방치하게 됨으로써 ID관리의 불편함뿐만 아니라 개인정보 오·남용으로 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 나타남
  - 한국정보보호진흥원, "舊 정보통신부 보도자료", 2007.1
- 사용자의 ID 수가 증가하고 개인정보 공유에 대한 요구가 증가함에 따라, ID관리의 불편함뿐만 아니라 개인정보 오·남용으로 인한 피해가 증가하고 있음
  - MIC & KISA, "u-정보보호 마스터플랜", 2006.10
  - OECD WPISP, "Background paper on digital identity management", 2006.10

○ NGN/BcN은 통신망에 인터넷 기술의 특성을 추가하고 있어 사용자가 임의의 접속점을 통해 망에 접속하는 것이 가능함. 이에 따라 사용자 로그인 및 인증절차가 필수적으로 요구되며, 관련 ID들을 적절하고 안전하게 관리하는 표준화된 방법을 정의하는 것이 NGN/BcN의 상용화 도입을 위해 필수적임

- 인증을 위한 개인의 ID는 NGN/BcN 망 내에서는 다양한 망 요소들 간의 ID 및 프로파일의 형태로 전환되어 존재하게 되는데, 이들 ID의 생성과 소멸 등 생명주기가 적절히 관리되지 않고 망 내에 방치될 경우, 혹은 이들 ID들이 적절히 보호되지 않고 제 3자에 의해 탈취 가능한 상태에 놓일 경우, 해당 사용자 및 통신망은 도용 등 금전적인 문제를 포함한 각종 위협에 놓이게 되며, 이러한 위협은 궁극적으로 NGN/BcN의 상용화 서비스 자체를 불가능하게 할 수 있음
- NGN/BcN의 도입이 가시화되어 감에 따라, 네트워크 기반의 ID 관리를 위해 생명주기 전반의 취약성 분석 설계 능력 확보가 요구되고 있음. 또한 통신망에서 ID는 상호식별, 인증 및 상호운용성을 위해 사용되므로, 접속단에서 인증 및 policy 제어를 적용하는 표준의 개발이 필요하며, 이질적인 도메인 간/서비스 간/망노드 간 동적 연합이 빈번하게 발생하는 IP 기반 통합망에서는 trusted computing 기반의 ID 상호운용성 확보가 필요하게 됨

○ 이와 같은 문제를 해결하기 위해, 국내에서도 ID관리 및 개인정보보호 핵심 기술에 대한 연구 및 개발이 진행되고 있으며 이들 기능이 탑재된 제품이 출시되고 있는 상황임. 이들 제품의 기술 경쟁력을 확보하고 국제 경쟁

력을 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

○ 또한 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 시스템 간 상호운용성 부재로 중복, 저장되어 있고 개인정보 활용 시 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 문제는 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

○ 최근 국내 최대 인터넷 쇼핑몰의 1,000만여 명 회원 정보가 해커에 의해 유출되어 회원의 개인정보와 금융정보가 노출된 후 스팸 및 보이스 피싱 등 2차 공격에 악용된 사고나 유명 통신업체에 의한 조직적, 고의적 제3자 개인정보 제공 사건 등은 개인정보를 수집하고 이용, 관리하는 사업자의 개인정보 관리의무가 기술적으로 강화되어야 할 시급성을 보이는 계기가 됨. 이에 따라 방송통신위원회는 패스워드와 생체정보만 암호화하도록 되어있는 개인정보 범위를 확대하여 주민번호와 금융정보 등이 포함되도록 관련 규정개정을 추진할 계획임

  • 행정안전부, “2010년까지 정보보호 사회안전망 구축”, 2008.07.22.

○ 현재 개발되어 사용 중인 ID관리 시스템들은 각 ID관리 시스템들이 사용되는 응용분야 특성에 따라 제공되는 서비스, 서비스 구현을 위해 사용되는 프로토콜이나 메커니즘 등이 다르므로 이종 ID관리 시스템 간 서비스 발견, 안전한 개인정보 공유, 상호운용이 불가능하여 결과적으로 효율적인 ID 서비스 제공과 개인정보 안전한 공유, 관리가 불가능한 문제점이 있음

○ 따라서 ID관리 및 개인정보보호 제품의 기술 경쟁력과 시장 지배력을 향상시키며, 인터넷 사용자들의 개인정보 오남용과 프라이버시 보호 및 시스템 간의 상호운용성을 확보하기 위해서는 ID관리 및 개인정보보호 분야의 표준화가 필요함

1.3.2. 표준화의 목표

○ 2009년까지 1단계로 ID 공유, 본인확인기술 표준 등 국내표준을 개발하여 국제 표준화 기반 구축
○ 2010년까지 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(3rd Generation Partnership Project) 등 ID관리 및 개인정보보호 관련 국제 표준화 단체에 적극적으로 참여함으로써 국제 표준화 기반을 구축

○ 2010년까지 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 시스템 간 서비스 발견, ID 체계 및 ID 공유 프로토콜을 위한 표준 부재로 인해 상호운용이 불가능한 문제점을 안고 있음. 따라서 이러한 단점들을 극복하기 위해 특정 응용분야에 국한되지 않는 포괄적인 ID관리 시스템 요구사항을 정리하고 현재 사용 중인 유 · 무선 통신망뿐만 아니라 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, 온라인상에서 사용자 본인 확인 기술 등을 개발하고 이를 표준화함

○ 계층구조의 통신망인 NGN/BcN 망에서 ID 관리 구조 프레임워크를 개발하고 있는 ITU-T 의 IdM GSI 에 참

여하고, 생명주기 관리 모델을 확장하여 NGN ID 관리 구조 모델을 개발하는데 참여함. 관련하여 ETSI TISPAN 등 참여를 통해 통신망의 보안취약성 분석 도구인 TVRA 기술 표준을 도입, 국내 현실에 맞도록 조정하여 상기 모델에 적용하고, 이를 통해 NGN/BcN 망구조에 실질적으로 적용 가능한 ID 데이터 구조를 도출하여 SG2, SG13 등에서 권고안으로 개발

○ 이를 기반으로 ITU-T SG13 및 SG11 에서 NACF(network attachment control function: 망접속제어기능) 표준을 개발하되, 상기의 취약성 분석 및 Identity Data 구조 모델을 적용하고, 관련 NGN TUP(트랜스포트 사용자 프로파일) 및 SUP(서비스 사용자 프로파일)를 확장하는 권고안을 개정함. NGN에서 policy 제어 기술을 적용하여 접속제어 기술표준 권고안을 개발하고, 이동성을 고려한 통합 인증 및 사용자 데이터 관리 모델을 개발함. 국내적으로 NGN ID 상호운용성 모델 표준개발에 참여하고, 3GPP SA3 을 참여하여 원격지에서 망 노드 및 도메인 간 동적 연합 및 상호신뢰성 접속모델을 개발하는데 참여함

○ 국내에서는 Digital ID 관리 포럼, 통합번호체계 포럼, TTA PG 204(NGN), 206(신호방식) 및 PG 502(개인정보보호 및 ID관리) 등에 참여하며, SG2, SG11, SG13 분과위원회의 협력과 지원을 받아 국제 표준화에 참여

1.3.3. 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 시스템 간 상호운용을 통해 개인정보 중복성 최소화 및 자기정보 통제권 실행을 통해 다양한 통신환경에서 개인화된 서비스 활용이 가능할 것임

○ 다양한 가상 통신망 사업자가 혼재하고, 통합망에서 여러 가지 서비스를 제공받게 되는 미래의 통신 환경에서, 사용자들은 다양한 통신망 서비스에 접속하면서 여러 가지 종류의 ID 사용으로 인한 불편과 정보 노출 위험성에서 노출되는데, 일단 TVRA 검증된 망을 통해 이러한 위협에서 보호되며, ID 관리상의 여러 가지 위협에서 용이하게 보호되는 방법을 제공받게 될 것임

○ 특히 NGN의 이종 액세스를 통합하는 접속 보안 인증 및 액세스 인증 ID관리 등 기술을 표준화된 방법으로 구현하게 되면, 안전한 통신 접속 환경이 보장되어 새로운 서비스를 위한 보안 조치 및 추가 비용 부담이 대폭 절감되며, 통신 서비스를 제공하는 사업자의 입장에서는 통신 시스템의 도용 위협으로부터 자유로워지고, 새로운 서비스 시스템의 도입을 위한 보안 조치 비용 부담이 절감되므로, 이로 인한 비용 절감을 사용자와 공유할 수 있게 될 것임

○ 통합망의 도입과, 국내의 우수한 초고속통신망 및 3G 이동통신망 인프라가 결합되면서, 각종의 이질적 도메인들이 동적 연합하고 다양한 이질적인 기기 간 상호운용성이 필요해지면, trust computing 기반 접속 제어와 ID 기반 상호운용성 모델이 다양하게 응용될 것임

2. 국내 · 외 현황분석

2.1. 시장 현황 및 전망

2.1.1. 국내 시장 현황 및 전망

○ 한국IDC의 2008년 조사에 따르면, 국내 ID관리 및 접근제어 시장이 2007년 308억 원 규모에서 연평균 11.5%의 성장을 보이며 2012년 531억 원 규모의 시장으로 성장할 것으로 전망

〈ID관리 및 접근제어 국내 시장 규모〉

(단위: 백만 원)

구 분	2007년	2008년	2009년	2010년	2011년	2012년	08-12 성장률
ID관리 및 접근제어	30,804	34,229	38,267	42,587	47,485	53,088	11.5%

(한국IDC, 2008)

○ 한국정보보호진흥원의 '2007 국내 정보보호 시장 및 동향보고서'에 의하면 DB암호화 및 접근제어 솔루션을 합친 DB보안시장은 약 190억 원에 달하는 것으로 조사되었음. 또한 2008년의 국내 DB보안 시장은 접근제어에서 약 198억 원, 암호화 부분에서 약 42억 원 등 총 약 240억 원에 이를 것으로 전망하고 있음. 국내 DB 보안 분야는 향후 IT 컴플라이언스 발효에 따른 시장 규모 확대가 예상되며, 시장에서 요구되는 기능 추가 및 안정적인 운영의 정착단계가 2008년부터 시작됨으로써 지속적인 매출 증가가 있을 것으로 예상됨

○ ID관리 시장이 확대되고 있는 추세여서 관련업체들도 경쟁이 치열한 상황이다. 최근 들어 웹 접근통제, 계정관리, 프로비저닝, 디렉토리 관리 등을 포함하는 포괄적인 '통합 계정관리' 솔루션 형태를 갖추고 있음

○ 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 '티볼리' 제품군으로 정책기반 계정관리 정책과 프로비저닝, 워크플로우를 지원함으로써 변화하는 비즈니스 프로세스의 유연성을 확보하며, 감사와 컴플라이언스관리를 위한 정책과 보고 기능을 제공함

○ 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. 한편, 2008년 7월 서울대학교에 공급하며 국내 시장 확보한 RSA 인비전(enVision)은 RSA 인비전 플랫폼은 모든 로그의 자동화된 수집, 분석, 경보, 감사, 보고 및 저장을 통해 컴플라이언스 준수, 보안 강화 및 위험 절감, 그리고 IT 및 네트워크 운영 최적화를 지원하는 종합 로그 관리 솔루션임

○ 한국오라클도 최근 본사에서 인수한 계정관리 업체 오블릭스의 관련 솔루션을 국내에 출시하고 활동을 진행 중임

○ 소프트포럼은 ID관리 솔루션으로 SafeIdentity를 개발하였음. 멀티도메인 간, 다양한 애플리케이션 간의 통합 인증(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 기능이 가능함

○ 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 칼럼별 선택적 암호 및 다이제이트 계산, RSA(1024비트)/3DES(128비트)/SEED(128비트) 등 암호 알고리즘 및 SHA 해쉬 알고리즘을 지원함

○ 이니텍은 INISAFE Nexess를 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 SafeDB는 데이터베이스에 저장된 데이터를 암호화하고 데이터베이스에 대한 접근을 제어함으로써 중요한 데이터를 보호할 수 있는 데이터베이스 보안 솔루션으로서, 기존 애플리케이션의 수정이나 별도의 개발 과정 없이 데이터베이스에 추가 설치하는 과정만으로 중요 데이터를 암호화하고 간편하게 보안정책을 적용할 수 있음. 또한 칼럼 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 다양한 인증방식(id/pw, 인증서, 생체인식, cd-key)을 지원하며 인증 단계에 따른 권한을 선택적으로 부여하는 SSO 솔루션인 Majgic SSO & EAM v3.0 제품을 개발하였음. 사용자인증 및 ACL 발급을 담당하는 인증서버(Policy Server)와 사용자 PC에 설치되고 사용자인증 후 세션을 관리하는 클라이언트 에이전트(Client Agent), 사용자 및 권한관리가 필요한 애플리케이션을 등록하고 권한을 관리하는 인터페이스인 관리자 어드민(Policy Server Admin)으로 구성되어 있음

○ 티맥스소프트의 SysKeeper EAM은 역할기반 접근제어를 수행하는 Policy 서버를 중심으로 Proxy 서버에서 인증 및 접근제어를 처리하는 모델과, WAS/WEB Agent에서 인증 및 접근제어를 처리하는 모델로 구성되어 있음. 또한 디렉토리 정보가 통합되지 않는 ERP, 그룹웨어, 메인프레임 등의 시스템은 커스텀 인터페이스를 통하여 기존 시스템과 통합 관리될 수 있으며, 자사의 WAS 솔루션과 결합하여 EAM 기능을 처리함

○ 펜타시큐리티시스템의 ISign은 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 접근 제어를 다양한 환경에서 보장하여 사용자의 이동성을 증가시켜줌

○ 펜터시큐리티의 D' Amo 통합 DB보안 솔루션은 데이터 암호화, 접근제어 및 감사를 통해 기업 내 중요 데이터 보호서비스를 제공함. 이 제품의 특징은 기존 응용 프로그램의 수정 없이 칼럼 단위로 암호화를 수행하며 칼럼 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 알패스는 회원제로 운영되는 많은 웹사이트의 아이디와 비밀번호를 관리할 수 있는 프로그램으로, 2008년 5월 20일 버전 3.05가 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 방지 기능이 가능함

○ SecuTronix의 이지패스는 웹에서의 로그인뿐만 아니라 각종 메신저 및 응용 프로그램의 로그인까지 지원하는 제품으로, 2008년 8월 현재 2.0.5 베타 버전이 출시되었음. MSN, 네이트온과 같은 메신저 로그인과, Melon, JukeOn 등의 응용프로그램 또한 현재 지원 중임. 추가적으로 USB에 탑재하여 사용할 수 있으며, 한 사이트에 여러 계정을 보유한 경우 또한 지원함. 이지패스 솔루션은 id/pw 방식의 로그인을 기반으로 하며, 지문인식기

가 제공된 경우 지문인증으로 로그인이 가능함

○ 이글로벌시스템의 CubeOne 제품은 ARIA, AES, SEED, DES, 3DES 암호화 알고리즘을 이용하여 데이터베이스 칼럼을 암호화하며 암호화된 컬럼에 대한 인덱스 검색을 지원하는 DB 암호화 솔루션임. 이 제품은 기존 응용 프로그램의 수정 없이 적용될 수 있으며 칼럼별로 접근통제 및 고유 암 · 복호 키를 생성하고, 사용자/IP/응용별 접근통제, DB관리자와 보안관리자의 권한 분리, 보안정책 설정에 대한 보안감사, 암호화된 칼럼에 대한 보안감사 기능 등을 지원함. 현재 이 제품은 Oracle 8.1.6부터 10gR2 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

〈국내 ID관리 및 접근제어 솔루션 개발 현황〉

구분	기관	내용
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 도메인 간, 다양한 애플리케이션 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 2007년 7월 조사에 따르면, 전 세계적으로 ID관리 및 접근제어 시장 규모를 2005년 2,766백만 달러에서 연평균 10.7%의 성장을 보이며 2011년에 4,975백만 달러에 이를 것으로 전망하고 있음

〈ID관리 및 접근제어 세계 시장 규모〉

(단위: 백만 달러)

구분	2005년	2006년	2007년	2008년	2009년	2010년	2011년	06-11 성장률
ID관리 및 접근제어	2,766	2,989	3,370	3,770	4,152	4,548	4,975	10.7%

(IDC, 2007)

○ 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, Netegrity(CA에 합병), Oblix, RSA Security(EMC의 합병)가 있음

○ 연계형 ID관리는 조직 간에 연계된 서비스를 제공하기 위해 ID를 서로 연계하고, 이를 통해 인증, 접근제어 관리 등을 수행하는 솔루션. 관련 벤더로는 HP, Ping Identity, M-Tech, Trustgenix(HP의 합병) 등이 있음

○ Sun은 ID 관리, 보호, 저장, 검증을 위해 Identity manager, Access manager, Directory server, Identity auditor를 포함한 Identity Management Suite를 출시하였음. 이는 중앙집중 Identity 관리, 중앙집중 접근제어, 단일 인증(SSO), 기업용 감사 및 보고, 자동화, self-service, 관리자의 역할 위임, 연방(Federation) 기능을 제공함

○ IBM은 2006년, 기존의 Tivoli Federated Identity Manager, Tivoli Directory Integrator, Tivoli Access Manager를 갱신하고 소규모 조직을 위한 ID관리 full suite인 Tivoli Identity Manager Express와 역시 소규모 조직의 federation을 위한 Tivoli Federated Identity Manager Business Gateway를 출시하였음

○ CA는 웹에서부터 mainframe에 이르기까지 완벽한 IAM(Identity and Access Management) 솔루션을 제공하기 위해 다양한 IAM 제품군을 제공함. CA Identity Manager를 비롯하여 CA SiteMinder 그리고 CA Single Sign-On 등과 같이 다양한 IAM 솔루션을 제공

○ 스토리지 부분의 업계선두인 EMC는 RSA Security를 합병하였음. IDC는 EMC의 스토리지 솔루션에 보안기능을 추가하는 방식이, ID도 결국 스토리지에 저장되는 데이터라는 측면에서 커다란 시너지를 가져올 것이라고 보고 있음

○ Verisign은 서비스제공에 집중하고 있음. 'Verisign Identity Protection fraud detection and authentication' 서비스는 클라이언트 로그인과 트랜잭션 정보 보안을 제공함

○ Oracle은 Oracle Access Manager, Oracle Identity Manager, Oracle Internet Directory, Oracle Virtual Directory, Oracle Identity and Access Management Suite등 full suite를 제공. Oracle은 독립적인 IAM 벤더로 관련시장에 진입했으며 업계 5위의 수준에 이름

○ Microsoft는 독점적인 중앙 관리에서 벗어나 여러 ID 제공자의 다양한 ID 기술들을 상호운용하는 ID 메타시스템 개념을 제안하고, 이 개념을 구현하여 윈도우 Vista에 CardSpace로 구현하였음

○ Neustar는 인터넷 상에서 유일한 식별자를 제공하고 데이터를 공유할 수 있는 OASIS의 XRI/XDI 표준을 주도하며 이 표준의 개념을 구현하는 i-names 서비스를 전 세계로 발표하였으며, SXIP사 등이 참여한 OpenID 표준은 2008년 1억 6천만 명의 사용자를 가질 정도로 급속히 확장하고 있음

○ 금융권 인증수단 강화정책은 미국의 금융권 규제를 대표하는 US FFIEC(Federal Financial Institutions Examination Council)에서 인터넷 뱅킹에 패스워드를 유효하지 않은 인증수단으로 규정하면서 이를 대체하기 위한 시장이 확대될 전망

○ 미국 출입 시 전자여권을 사용하지 않는 경우, 비자를 발급받아야 함에 따라, 현재 비자 면제국인 선진국들이 서둘러 전자여권 발행을 추진하고 있음. 수년 내에 10억 장 이상의 전자여권과 전자 운전면허증이 국제적으로

발행될 것으로 예상되어, IC카드용 칩 제조사 및 솔루션 개발사, 단말기 제조사들의 경쟁이 치열해지고 있음. 전자여권의 경우, ICAO에서 상호운용성 시험을 추진하고 있으나 선진국의 일부 기관들의 기능 검증을 끝낸 2006년 이후 추가적인 상호운용성 시험을 추진하지 않아 후발 국가의 기관들은 시험에 어려움을 겪고 있음

○ i-name은 NETSTAR, Cordance, xdi.org가 인프라를 담당하고 있는 사이트로 OASIS의 XRI 표준을 적용한 서비스를 제공하고 있음. 전 세계적으로 XRI 주소를 해석해주는 역할을 수행하고 있으며, 현재 7개의 서비스 제공자가 가입되어 있음. ooTao의 EZ iBroker, 2idi, LinkSafe, 1id.com, 영국의 =you, @fullXRI 그리고 Vibrant Communication이 있음. 이들 서비스 제공자는 GSS(Global Services Specifications)에 따라 서비스를 구축하며, GSS는 법적, 관리상의 정책, GRS의 운영 · 등록 · 주소해석 정책 등을 명시함

○ AOL은 외부의 애플리케이션이 AOL의 온라인 서비스에 쉽게 접근하여 상호운용 될 수 있도록 하기 위해 Liberty의 ID-WSF 기술을 적용하였음. 이로 인해 2005년 10월, D-LINK는 AOL의 인터넷 브로드캐스팅 서비스인 Radio@AOL를 접근할 수 있게 되었으며, 2,400만 명의 사용자들에 해당 서비스를 제공하였음. 또한 SAML 2.0을 도입하여 파트너 사이트와 SSO를 제공함으로써, 사용자가 우선 AOL에 로그인 한 뒤에, AOL에서 링크로 연결된 파트너 사이트에는 추가적인 로그인 과정을 거치지 않아도 되도록 하였음

○ AOL은 OpenID 제공자가 되어 자사의 고객이 별도의 작업 없이도 OpenID를 사용할 수 있도록 하였음. Yahoo는 자사의 인증 API인 BBAuth를 이용하여 가입자에게 OpenID를 제공함. 대표적인 블로그 업체인 Six Apart는 자사의 LiveJournal과 Vox 사이트에 OpenID를 적용하였음. 또한 SUN은 자사 직원에게 OpenID를 제공하기로 하고, 자사의 SSO 솔루션인 OpenSSO와 OpenID 라이브러리를 통합하여 서비스를 구축하였음

○ 일본 NTT Communication은 Liberty Alliance의 Federation 기술을 적용하여 400만 가입자들에게 MasterID라는 SSO서비스를 제공했음. 또한 2007년 7월 3일, NTT Communication은 NTT 레조난트 주식회사의 gooID와의 제휴를 통해 통합 서비스를 제공하기 시작했음. 본 제휴는 NTT 소프트웨어 주식회사의 TrustBind/Federation Manager 기반 제품으로 가능하며, 이 제품은 Liberty의 상호운용성 시험을 통과한 것임

○ 프랑스 텔레콤은 Orange 프로젝트를 통해 Liberty ID-FF 기술로 자사의 1억 7천만 사용자에게 SSO 서비스를 제공하였으며, 2006년 2월에는 1,000만 사용자에게 소액 지불 서비스인 Wanadoo를 제공하였음

○ Google은 자사의 솔루션인 Google App에 SSO 및 인가 기능을 제공하기 위해 SAML 2.0 표준을 지원하였음. Google은 Google Apps를 기업용 버전과 교육용 버전을 배포하였으며, 2006년 10월 미국의 애리조나 주립 대학은 이 제품을 도입하기로 결정하였으며 2007년 말까지 6만 5천 명의 학생들에게 서비스를 제공할 예정임.

또한 2007년 4월 일본 대학교에서 10만 명의 학생에서 서비스를 제공하기로 했음. 일본 대학교는 향후 졸업생과 교직원을 포함하여 50만 명에게 서비스를 확대할 예정임

○ Ping Identity는 2007년 2월 CardSpace 지원 모듈을 제공하여 Apache 서버에서 인증 메커니즘의 하나로 InfoCard를 사용할 수 있도록 하였음. 또한 2007년 6월 SignOn.com 이라는 사이트를 오픈하였음. 이 사이트는 OpenID 제공자이며, 인증 수단의 하나로 Microsoft CardSpace를 통한 InfoCard를 지원함

○ Ping Identity는 SAML 1.x와 2.0, WS-Federation을 적용하여 사이트 간의 Federated SSO를 제공하는 PingFederate 5을 개발하였음. 또한 WS-Trust 표준을 준용하여 SAML, Kerberos, X.509, id/pw 등의 토큰을 처리하는 보안 토큰 서비스인 PingFederate Web Services를 제공하고 있음

○ Sxipper는 Firefox 브라우저의 확장 기능을 이용한 패스워드 관리 애플리케이션으로, WebWare에서 선정한 2007년 100대 웹 소프트웨어임. 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

○ Password Manager XP(eXtra Protection)는 보안상 중요한 정보를 저장 관리하는 애플리케이션임. 모든 로그인 id, 패스워드, PIN 코드, 신용카드 번호, 접근 코드, 파일, 기타 중요 정보들을 한 곳에 안전하게 저장할 수 있음. 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 데이타베이스를 USB 플래시 드라이브와 같은 착탈식 장치에 저장할 수 있는 기능, 패스워드 데이타베이스의 백업 및 복원기능 등이 제공됨. 현재 Password Manager XP는 버전 2.3이 공개되어 있음

○ P3P는 해당 웹사이트를 방문하지 않고 검색 프로그램을 이용하여, 해당 웹사이트와 자신의 프라이버시 선호수준을 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. P3P 관련 S/W는 크게 에이전트와 정책생성기, 사업자용과 이용자용으로 나누어 개발되며, 대부분의 S/W는 무료로 보급되고 있으나 정책 생성기는 일부 유료로 제공되고 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, 칼럼별 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 칼럼에 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

〈국외 ID관리 및 접근제어 솔루션 개발 현황〉

구분	기관	내용
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 메시징 과 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 전 세계에 서비스를 런칭 하였음
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

구분	기관	내용
I&AM	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 애플리케이션 및 기업 시스템에 대한 ID 기반 관리
	Oblix	– NetPoint with COREid, IDLink – SSO를 통한 편리한 웹 접근 관리 방법 제공 – End-to-End 프로비저닝 – 도메인 간의 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 종류는 5가지로 가상주민번호(한국신용평가정보), OnePASS(한국정보인증), 나이스아이핀(한국신용정보), 그린버튼 서비스(한국전자인증, 이니텍), Siren24아이핀(서울신용평가정보)이 서비스 중이며, 신원을 확인하는 방법으로 대면 확인, 공인인증서, 신용카드정보, 휴대폰 SMS 등이 가능함
  - i-PIN 제도는 2005년 10월부터 시범적으로 도입된 이후로 2008년 6월말 현재 135개 웹사이트가 도입하여 운영 중이며, 2008년 5월 정보통신망법 개정에 따라 i-PIN을 도입해야 하는 웹사이트는 증가하게 될 것임. 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
  - 방송통신위원회측은 주요 포털업체와 공동으로 주민번호 노출 위험성과 i-PIN 이용에 대한 캠페인을 실시할 예정으로, 인터넷 사업자를 대상으로 설명회를 지속적으로 개최하고 있으며, 2007년 9월 i-PIN 적용 사례집과 2007년 12월 i-PIN 도입 매뉴얼 등을 배포하여 i-PIN 도입을 고려하는 웹사이트의 도입 절차 및 활용의 이해를 돕도록 하였음. 또한, 방송통신위원회는 i-PIN 도입 업체에게는 'ePrivacy 마크' 인증 심사 시, 가산점을 부여하는 방식의 회유책을 병행함으로써, i-PIN 보급 확산을 위한 노력을 지속적으로 추진하고 있음
- 행정안전부는 공공기관에서의 개인정보보호를 위한 ID 관리 체계 구축을 핵심으로 한 통합ID관리 서비스를 추진하고 있음. 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 추진계획을 마련했음
  - 통합ID관리 서비스는 g-PIN으로 명칭을 변경하였으며, 2008년 7월 현재 행정안전부는 g-PIN 센터(http://g-pin.go.kr)를 구축하여 시범적용 테스트를 진행 중임. 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

– 방송통신위원회와 행정안전부는 기존에 각각 진행 중이던 i-PIN와 g-PIN을 상호 연계하기로 함에 따라, 방송통신위원회에서 진행하던 기존 5개의 i-PIN은 민간 i-PIN으로 명명하고, 행정안전부에서 진행하던 g-PIN은 공공 i-PIN으로 명명하며, 하나의 i-PIN 체계로 통합하였음. 이를 통해 사용자는 i-PIN 중 자신이 발급 받은 하나의 PIN을 이용하여 민간 i-PIN 또는 공공 i-PIN이 도입된 민간 및 공공의 웹사이트 서비스를 이용할 수 있게 되어 이용 편리성을 확보하고자 함

• 행정안전부의 g-PIN 센터는 i-PIN 서비스를 제공하는 제6의 본인확인기관으로 민간 i-PIN을 상호 연계하여 서비스를 제공하기로 함

• 2008년 7월 현재 민간 i-PIN과 공공 i-PIN과 상호연계 시범서비스를 제공하고 있으며, 시범서비스가 종료되는 시점에 본격적인 i-PIN 서비스가 대국민 및 웹사이트를 대상으로 제공될 예정임

– 방송통신위원회는 2008년 6월 '정보통신망 이용촉진 및 정보보호 등에 관한 법률(정보통신망법)' 의 제23조의 2를 다음과 같이 신설하여 주민등록번호만 웹사이트 회원가입에 사용하는 경우 개인정보의 침해가능성을 해소하고자 함

• ① 정보통신서비스 제공자로서 제공하는 정보통신서비스의 유형별 일일 평균 이용자 수가 대통령령으로 정하는 기준에 해당하는 자는 이용자가 정보통신망을 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

– 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 암호화하도록 함으로서 무분별한 개인정보 이용에 대한 사회적 관행과 개인정보 오남용을 개선할 예정

• 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 계획

– 방송통신위원회는 인터넷 이용환경의 안전성 제고 및 인터넷 경제의 신뢰기반 조성을 목표로 하는 인터넷 정보보호 종합대책을 발표하였다. 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 예정

- 또한 개인정보 유출 시 추가적인 활용이 불가능하도록 계좌번호 등 중요 개인정보는 암호화하여 저장하도록 의무화할 계획
- 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 변형한 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 진행하고 있음
- g-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 g-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 사이트

에 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 사이트를 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

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 ID를 공유시킴으로 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 ID 카드 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 65,000명의 비즈니스 가입자를 신규로 받고 있음
- 일본은 신뢰기관을 통한 사용자 인증기반을 마련하여 사용자의 개인정보를 보호하기 위해 차세대 전자인증 프로젝트를 진행 중임. 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 위해 전자인증 업무 모델 체계를 수립함. 또한 인증프레임워크, 보증레벨을 결정하는 절차, 운영 및 기술기준으로 구성된 인증가이드라인을 개발하고, 사용자와 인증서비스 제공자 간 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 도입
  - 호주의 경우 프라이버시법에서 간략한 프라이버시 고지를 활용할 것을 장려하고 정부 분야에서는 세계에서 처음으로 2005년 7월부터 다단계 고지를 웹사이트에 게시

• 미국의 경우 US Postal service가 웹사이트에 다단계 고지를 도입

○ 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 지원했음. 2008년 상반기에 Bandit은 DigitalME의 핵심 기능을 개선하고 OpenID를 지원하는 등의 작업을 수행하는 버전 2.0 개발을 진행 중임. 2008년 3월부터 Bandit 2.0과 Higgins 1.0을 개발하기 시작하였으며, 6월에는 DigitalME를 개발하기 시작하였음. Bandit의 마일스톤에 따르면 2008년 10월에 Bandit 2.0이 완성될 전망
- Higgins 프로젝트는 2004년 Eclipse 재단에서 'Eclipse Trust Framework' 라는 이름으로 시작되었으며, 2006년부터 IBM, Novell, Google, Microsoft 등이 지원하는 프로젝트. Higgins는 다양한 사이트, 애플리케이션, 디바이스에 흩어져 있는 ID/프로파일/소셜 관계 정보를 통합 제공하는 인터넷 ID 프레임워크를 지향. 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
- 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 확장됨
- OSIS(Open Source Information System)는 2006년에 만들어진 단체로 사용자 중심의 ID 관리 기술들의 상호운용성을 목표로 함. 이 목표에 따라 OSIS는 Microsoft의 CardSpace 표준인 ISIP(Identity Selector Interoperability Profile)를 기준으로 타 Information Card 프로젝트들의 호환성을 주도했음. 지금까지 3차례의 상호운용성 시험을 수행하였으며, RSA 2008에서 열린 최근의 상호운용성 시험에는 17개의 IDP와 39개의 RP가 참여함
- Liberty Alliance는 2005년에 Liberty ID-FF, ID-WSF, ID-SIS 표준을 만들었으며, 해당 내용을 SAML 표준에 반영시켰음. 이후에는 여러 도메인 간의 정책이나 프라이버시 보호 정책을 반영한 표준화된 프레임워크를 개발하고 있으며, 구체적인 결과물로 IAF와 IGF라는 프레임워크를 개발 중임. 이들 프레임워크를 통해 상호운용성, 보안 정책 기반의 ID 솔루션 시장 확대, 사용자를 ID 도용이나 침해로부터 보호하며 기업들

의 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
- IGF(Identity Governance Framework)는 기업 내 시스템 간의 ID 정보 교환 체계를 두어, ID 정보를 효과적으로 처리하기 위한 목적으로 2006년 11월에 발족한 프로젝트. 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
- Concordia 프로젝트는 기존의 ID 관리 프로토콜이 해결하지 못하는 문제나 시나리오에 대처하기 위한 방안을 고안하는 프로젝트로, 2007년 4월부터 Liberty Alliance의 주관으로 운영 중임. Concordia는 상호 연동성과 프라이버시 보호 기능을 제공하는 ID 계층을 개발함으로써 개발 및 구축 과정에서 더 높은 성공률과 생산성을 보장하려는 목적을 가짐

– 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

– Shibboleth 프로젝트는 American Chemical Society를 비롯한 20개 기관이 Information Provider로 동작하며, GridShip과 Napster를 비롯한 25개 시스템과 연동. 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 교육기관을 대상으로 국가적인 federation을 구축하는 목적으로 2006년 10월에 제품화를 시작한 CRU 프로젝트, 핀란드 대학 간의 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

- 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 7월 말 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 ID 관리 기술과, CardSpace, OpenID 등의 사용자 중심의 ID 관리 기술로 양분되어 진행되고 있음. 기업 위주의 ID 관리 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 ID 관리 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

2.2.3. 국내외 IPR 보유현황 및 확보 가능분야

○ 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 네트워크 Networked 프레임워크에 대한 특허 등 3건이 조사됨
  - 국내와 유럽의 경우에는 관련 특허가 조사되지 않음
- 보안 토큰 관리
  - 보안 토큰 관리와 관련된 특허는 다른 기술에 비해 상대적으로 많은 특허가 조사됨
  - 국내의 경우 보안 토큰을 이용한 전자거래 방법에 관련된 특허가 출원되었음
  - 미국의 경우 출력가능한 클레임을 포함하는 보안 토큰에 대한 특허 등 10건이 조사됨
  - 유럽의 경우 사용자 인증을 위한 보안 토큰과 방식 등 2건이 조사됨
  - 일본의 경우 인증기관 간 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 공유
  - 최근에 연구가 많이 진행되고 있는 Identity 공유에 대한 특허는 많지 않은 상태임
  - 국내의 경우 2건이 조사됨
  - 미국의 경우 contacting identity 공유 등 2건이 조사됨
  - 유럽의 경우 2건이 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 2건이 조사됨
- 미국의 경우 기업, 개인 등에 대한 프라이버시 보호 관련 특허가 17건 조사됨
- 유럽의 경우 프라이버시 보호 시스템 등 5건의 특허가 조사됨

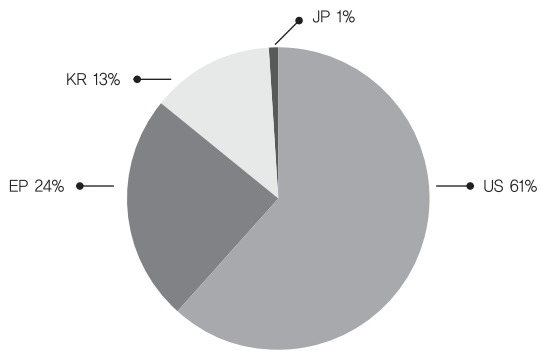
– 네트워크 중심의 ID 관리
- 네트워크 중심의 ID 관리 모델과 ID 인증 및 접근제어에 대한 특허는 아직 많지 않은 상태임
- 국내의 경우 1건이 조사됨
- 미국의 경우 분산 컴퓨터 시스템에서 시스템 자원에 대한 접근 제어를 촉진시키는 방법과 시스템에 대한 특허 등 6건이 조사됨
- 유럽의 경우 3건이 조사됨

– 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 2건이 조사됨
- 미국의 경우 데이터베이스 보안 제공 방법에 대한 특허 등 8건이 조사됨
- 유럽의 경우 6건이 조사됨

○ IPR 현황 분석 및 전망

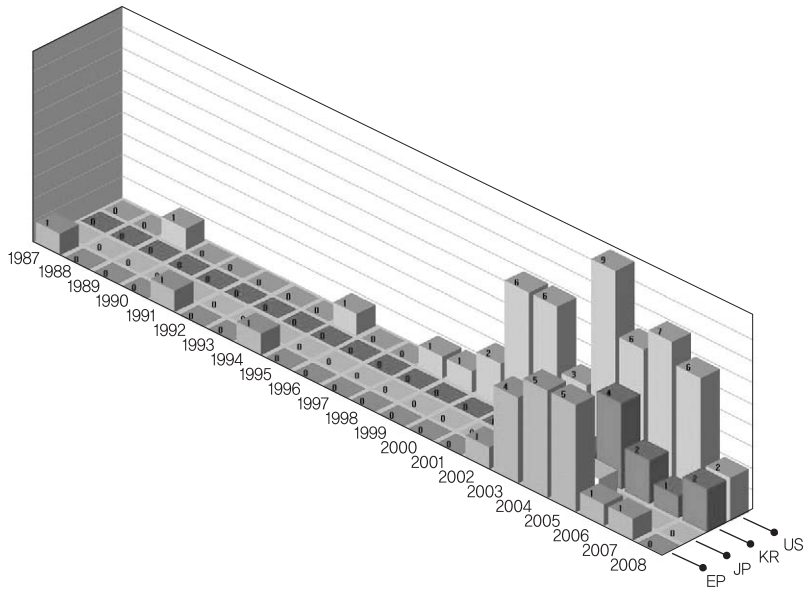
– ID관리 및 개인정보보호 분야와 관련되어 조사된 특허는 총 83건으로, 1987년부터 2008년에 걸쳐 출원이 됨

– 아래 그림은 조사된 특허의 국가별 특허 출원 점유율로 미국이 51건으로 61%의 점유율을 보이며, 유럽이 24%, 한국이 13% 그리고 일본이 1%의 점유율을 가지고 있음을 보임



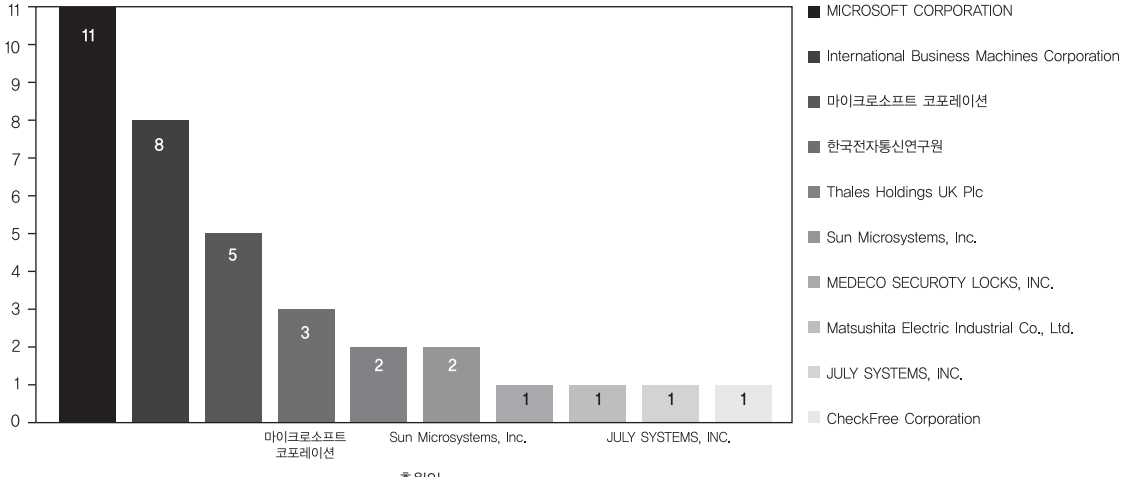
〈국가별 점유율 분석〉

– 아래 그림은 조사된 특허의 국가별 시계열 분석으로, 1987년부터 특허가 출원되기 시작하여, 2005년에 가장 많은 특허가 출원되었음을 보임



〈국가별 시계열 분석〉

– 아래 그림은 조사된 특허의 출원인을 분석한 것으로, 마이크로소프트가 가장 많은 특허를 보유하고 있으며, 국내의 경우 한국전자통신연구원이 가장 많은 특허를 보유하고 있음을 보임



〈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 및 ID 온톨로지 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

○ 개요

- 인터넷 환경에서 제공되는 정보보호는 시스템 간의 연동과 확장성을 위해 반드시 표준을 준용하여야 함. ID 관리 기술에 대한 표준화는 국제적으로 활발히 진행되고 있으나 개인정보 공유 및 보호 기술에 대한 표준화는 아직 초기 단계임
- 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, 한국정보보호진흥원, 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 방법으로 추진되고 있는데, 한 가지 방법은 사실표준화단체가 표준초안을 개발하고, TTA에서 정보통신 단체표준으로 개발하는 방법이고, 다른 방법은 TTA에서 표준 초안이 개발되고 관련 PG를 통하여 최종 표준을 확정하는 방법으로 표준안을 개발하는 방법임
- 한국인터넷진흥원(http://www.nida.or.kr)은 국가인터넷주소자원 관리기관으로 전 분야에 걸친 이슈를 담당하고 있음. 최근 한국인터넷진흥원은 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
- 국내 개인정보보호 관련 표준화는 개인정보보호 정책, 개인정보 프라이버시 관리 모델 등에 대해서 표준이 제정된 상태임

– TTA 개인정보보호 및 ID관리 프로젝트 그룹(PG 502)

- TTA에서 개인정보보호 관련 표준화는 TC1 PG101 정보보호기반 프로젝트 그룹에서 주로 관리하였으나, 더 구체적이고 다양한 ID 관리 분야의 국내 표준개발을 위해 2008년 현재는 TC5(정보보호 기술위원회) PG 502 개인정보보호 및 ID관리 프로젝트 그룹으로 새로 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 제정됨
- 2008년 현재 확장형 자원 식별자(XRI) 문법 V2.0, 공통 아이덴터티 데이터 모델과 상호운용성 및 신뢰를 위한 글로벌 ID 관리 시스템 요구사항, 자기통제 강화형 디지털 아이덴터티 공유 프레임워크, 본인확인기술인 i-PIN 서비스 전달 메시지 형식과 서비스 중복가입 확인정보, 확장성 접근제어 생성언어 3.0, 프라이버시 강화형 역할기반 접근통제 정책언어 및 개인정보 DB 관리 기술의 보안요구사항 등에 대한 표준화가 진행되고 있음

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

관련분야	표준번호	표준내용	제정년도	제정현황
ID관리 및 개인정보 보호	TTAS.IT-X1141_1	SAML 2.0 주장과 프로토콜	2006	제정완료
	TTAS.IT-X1141_2	SAML 2.0 바인딩	2006	제정완료
	TTAS.IT-X1141_3	SAML 2.0 프로파일	2006	제정완료
	TTAS.KO-06.0111	RFID 프라이버시 보호 가이드라인	2006	제정완료
	TTAS.IT-X1141_4	SAML 2.0 메타데이터	2007	제정완료
	TTAS.IT-X1141_5	SAML 2.0 인증문맥	2007	제정완료
	TTAS.IT-X1141_6	SAML v2.0 – 호환성 요구사항과 보안 및 프라이버시 고려사항	2007	제정완료
	TTAS.KO-06.0146	모바일RFID 프라이버시 보호 프레임워크	2007	제정완료
	TTAS.KO-12.0051	개인정보보호정책 설정 및 협상 규격	2007	제정완료
	TTAS.KO-12.0053	개인정보 생명주기별 프라이버시 관리 모델	2007	제정완료
	TTAS.KO-12.0054	i-PIN 서비스 프레임워크	2007	제정완료
	TTAS.KO-12.0055	i-PIN 서비스 전달 메시지 형식	2007	제정완료
	2008-667	확장형 자원 식별자(XRI) 문법 V2.0	2008	진행 중
	2008-668	공통 아이덴터티 데이터 모델	2008	진행 중
	2008-669	상호호환성 및 신뢰를 위한 글로벌 ID 관리 시스템 요구사항	2008	진행 중
	2008-670	개인정보 DB 관리 기술의 보안요구사항	2008	진행 중
	2008-671	프라이버시 강화형 역할기반 접근통제 정책언어	2008	진행 중
	2008-737	자기통제 강화형 디지털 아이덴터티 공유 프레임워크	2008	진행 중
	2008-738	확장성 접근제어 생성언어 3.0	2008	진행 중
	2008-739	i-PIN 서비스 중복가입 확인정보	2008	진행 중
	2008-740	i-PIN 서비스 전달 메시지 형식	2008	개정진행 중

2.3.2. 국외 표준화 현황 및 전망

- 2006년 12월에 결성된 ITU-T SG17 Focus Group on Identity Management(FG IdM)에서는 포괄적인 IdM 프레임워크 개발을 촉진하고 분산환경에서 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 Next Generation Network(NGN) 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 제출했음. 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 ID 관리 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
- ITU-T SG17 내에서 ID 관리의 표준 개발을 직접적으로 담당하고 있는 곳은 Q6/17임. FG IdM의 결과물 중 IdM 상호운용성 요구사항은 'X.1250: Requirements for global identity management trust and interoperability' 라는 제목으로 표준화를 진행하여 2008년 4월 SG17회의에서 표준으로 결정되어 현재 승인 절차를 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 진행 중에 있음
- ITU-T SG17은 4년 회기를 마감하는 회의를 2008년 9월 개최하였으며, 이 회의에서 X.1250은 표준승인을 받지 못하고 다시 6개월 동안 검토를 받는 단계에 머물기로 결정(Re-determination)이 되었고 X.idif(X.1251)는

표준승인 절차에 들어가는 것으로 결정(Determination)이 되었음. 이번 회의에서 승인된 IdM 관련 신규 표준 과제는 X.idmsg(Security Guidelines for Identity Management Systems), X.priva(Criteria for Assessing the Level of Protection for Personally Identifiable Information in the IdM), 그리고 X.idm-ifa(Framework architecture for interoperable identity management systems)이 있음

- X.idmsg: ID 관리 시스템에서의 보안 가이드라인으로, ID 관리 시스템의 보안 위협 및 위험을 분석하고 ID관리 시스템 설치 및 운영에 필요한 보안 지침을 제공하기 위한 표준
- X.priva: IdM 서비스 제공자의 PII(Personally Identifiable Information) 보호정책 및 기술적 조치 현황 등을 평가함으로써 해당 IdM 서비스의 PII 보호수준에 적절한 PII 만을 제공할 수 있도록 PII 보호 수준에 대한 평가기준 개발하기 위한 표준
- X.idm-ifa: ID 관리 시스템의 모듈라 프레임워크 구조를 제안함. 제안하는 구조는 사용자 중심, 네트워크 중심, 그리고 서비스 중심의 ID 관리 시스템의 다양한 요구사항을 만족하는 일반화된 참조 구조(Reference Architecture)

- ISO/IEC JTC1 SC27 WG5에서는 ID 관리 프레임워크 국제표준 개발을 진행 중에 있으며, 현재 ID 관리 프레임워크, 프라이버시 프레임워크, 프라이버시 참조 구조, 엔티티 인증 보증 등과 같은 Working Document를 작성한 상태. 또한 ID 관리 프레임워크 개발을 위한 선행되어야 할 작업으로 ID 온톨로지 정의의 필요성을 제시하고 있음. ID 온톨로지는 실제적인 ID 관리에 필요한 용어와 개념 공유를 위해 필수적이며, ID 관리 프레임워크 이용자에게 ID 관리와 관련된 일관성 시각을 제공하는 한편 서로 상이하거나 연관된 목적을 가진 다른 사용자와의 협력을 가능하게 하는 중요한 역할을 담당하고 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-T 외에 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
- Liberty Alliance 프로젝트의 ID-SIS PP(Person Profile), EP(Employee Profile)에서는 사용자 및 고용자에 대한 개인정보 구성요소를 규정하고 있으며 필요에 따라 개인정보 스키마를 확장할 수 있는 기능을 제공하고 있음
- ETRI는 ID 관리기술인 '자기 통제 강화형 디지털 아이덴티티 공유 프레임워크'에 관한 기고문을 발표하여 X.idif라는 표준과제로 채택되었고 1명의 에디터가 선정되어 2008년 9월에 표준승인을 목표로 표준화 작업을 진행하고 있음
- 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 ID 관리 분야 표준에 중추적이고 핵심적인

표준으로 자리를 잡을 것으로 예상되며 SG17에서 IdM의 표준화 중요성이 부각되어 2009년 새로운 회기부터는 ID 관리 분야의 표준과제를 전담하는 새로운 Question이 만들어 질것으로 예상됨

- SG17 외에도 ITU-T에는 ID 관리와 관련된 SG들이 있는데 FG IdM에서 미완성으로 중단된 IdM 프레임워크는 Q.15/13(NGN Security)에서는 다음과 같이 진행되고 있음
  - 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 있다. 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, Globally Unique Identifier), RFC4474(Enhancements and 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 호환성 있는 추상적 식별자와 결정(resolution) 프로토콜에 대한 표준을 정의하고 있음. WS-Security 표준에서는 웹 서비스 메시징에 적용되는 무결성 및 비밀성 지원을 위한 프로토콜을 정의하고 있음
- OMA(Open Mobile Alliance)는 멀티벤더 환경에서 응용과 서비스를 효과적이고 안정적으로 구축, 설치, 관

리하도록 하는 공개형 표준기반 프레임워크를 개발하여 가입자에게 시장, 사업자, 그리고 모바일 단말기 등에 결처 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 결성되었고, 웹 서비스의 소비자들이 ID 정보에 대한 프라이버시와 보안을 유지하면서 온라인 업무를 어디에서든지 더 쉽게 할 수 있게 하는 것을 목표로 하고 있음. ID들이 연계되어 연결되고, 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, 위치추적, 사용자 상태나 경고등을 위한 ID 기반의 서비스를 다루는 ID-SIS로 구성되어 있음
- Liberty Alliance project는 기본적인 프레임워크인 FF나 WSF 외에도 Identity 서비스를 평가하고 검증할 수 있는 Identity Assurance Framework를 개발하였고 엔티티들 간의 Identity 정보의 원활한 교환과 프라이버시 제한을 정책으로 설정할 수 있는 Identity Governance Framework 표준안도 현재 개발되어 발표되었음
- 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. 이 중 XRI는 인터넷 규모의 URI 기반 추상화된 ID를 정의하는 명세와 XRI 데이터 공유를 위한 조율 프로토콜, 도메인 상호 간에 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 상호 간에 서로 공유하고 링킹, 동기화하는 표준화를 제안하고 있음
- ID관리 및 개인정보보호 관련 국제 표준은 다음과 같음

표준화기관	표준식별자	제목
Liberty Alliance	liberty-idff-bindings-profiles	Liberty ID-FF Bindings and Profiles Specification V1.2
	liberty-idff-protocols-schema	Liberty ID-FF Protocols and Schema Specification V1.2
	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 V2.1
	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 Makrup 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-xacml-2.0	Hierarchical resource profile of XACML V2.0
	oasis-xacml-2.0	Multiple resource profile of XACML V2.0
	oasis-xacml-2.0	Privacy policy profile of XACML V2.0
	oasis-xacml-2.0	SAML 2.0 profile of XACML V2.0
	oasis-xacml-2.0	XML Digital Signature profile of XACML V2.0
	os-pstc-spml2-dsml-profile-os	Service Provisioning Markup Language(SPML) V2.0 – DSML V2 Profile
	os-pstc-spml2-xsd-profile-os	Service Provisioning Markup Language(SPML) V.02 – XSD Profile
	os-pstc-spml-cd-2.0	Service Provisioning Markup Language(SPML) V2.0
	xri-syntax-v2.0-cd-01	XRI Syntax V2.0 Committee Draft 01
	xri-resolution-v2.0-cd-01	XRI Resolution V2.0 Committee Draft 01
	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)
ISO/ IEC JTC1	WD 24760	A Framework for Identity Management
	WD 29100	A Privacy Framework
	WD 29101	A Privacy reference architecture
	WD 29115	Entity authentication assurance

2.4. 표준화 대상항목별 현황 분석

구분		ID관리 기반	개인정보보호	ID관리 응용 및 기타
표준화 대상항목		Identity 식별체계, Identity 시스템 공통 프레임워크, 보안 토큰 관리, Identity 서비스 디스커버리, Identity 온톨로지, Identity 공유, 신뢰관리	개인정보보호 정책 Interaction Service 개인정보 DB보안 사용자단말 개인정보 관리	네트워크 중심의 ID관리 모델 네트워크 ID인증 및 접근제어 본인확인기술
시장 현황 및 전망	국내	– 한국IDC의 2008년 조사에 따르면, 국내 ID관리 및 접근제어 시장이 2007년 308억 원 규모에서 연평균 11.5%의 성장을 보이며 2012년 531억 원 규모의 시장으로 성장할 것으로 전망하고 있음		– 한국IDC의 2008년 조사에 따르면, 국내 ID관리 및 접근제어 시장이 2007년 308억 원 규모에서 연평균 11.5%의 성장을 보이며 2012년 531억 원 규모의 시장으로 성장할 것으로 전망하고 있음
	국외	– IDC의 2007년 7월 조사에 따르면, 전 세계적으로 ID관리 및 접근제어 시장 규모를 2005년 2,766백만 달러에서 연평균 10.7%의 성장을 보이며 2011년에 4,975백만 달러에 이를 것으로 전망하고 있음		– IDC의 2007년 7월 조사에 따르면, 전 세계적으로 ID관리 및 접근제어 시장 규모를 2005년 2,766백만 달러에서 연평균 10.7%의 성장을 보이며 2011년에 4,975백만 달러에 이를 것으로 전망하고 있음
기술 개발 현황 및 전망	국내	– ETRI에서 보안토큰 생성 · 분배, 디스커버리, ID 연계 기술 개발 – SSO, EAM 시스템 제품군 출시 – OpenID, XRI 식별체계를 지원하는 제품군 출시 – ID 공유 기술 개발 중 – PKI, 메타데이타를 통한 시스템 간의 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	– 네트워크 중심 ID관리 기술 연구 중 – BcN 의 통합 인증기술 개발 중(KT등) – BcN 통합 접속제어 기술 개발 중(ETRI) – KISA에서 주민번호대체 기술인 i-PIN을 이용한 본인확인 기술을 개발
	국외	– 식별체계, 보안토큰 생성 · 분배, 디스커버리, ID 연계 등 핵심 기술이 다수 개발된 상태임 – SSO, EAM 등 개별 기능 제품군에서 ID를 종합적으로 관리하는 I&AM 제품군이 다수 출시됨 – 최근 사용자 중심 ID 제품군이 출시되고 있음 – PKI, 메타데이타를 통한 시스템 간의 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	– 유럽에서는 ETSI 회원국들을 중심으로 NASS 표준기술을 적용, 유선 통신사업자의 IP 망 구축을 지원 – 관련 식별, 접속, 인증에 대한 다양한 solution이 제안되고 있음 – 특히 M2M 접속, trusted computing 기술들이 다양하게 개발 중 – i-PIN과 같은 본인확인 기술은 미개발된 상태임
기술개발 수준	국내	기술기획–상용화	기술기획–시제품	상용화
	국외	시제품–상용화	시제품–상용화	상용화/응용단계
	기술격차	1년	1~2년	1~2 년, 부분적으로 선도
	관련제품	PKI, EAM, I&AM	PKI, EAM, I&AM, 정보보호 제품 전반, Portal	BcN/NGN 인증 및 접속제어 제품 전반, 포털
IPR 보유현황	국내	보안 토큰, 디스커버리, ID 공유 등에서 IPR 확보	개인정보보호정책, 개인정보 DB 보안 분야에서 IPR 확보	미흡
	국외	프레임워크, 보안 토큰, 디스커버리, ID 공유 등에서 IPR 다수 확보	개인정보보호정책, Interaction Service, 개인정보 DB 보안 분야에서 IPR 확보	네트워크 ID 관리 관련 IPR 확보
IPR확보 가능분야		프레임워크, ID 공유, ID 온톨로지	Interaction Service	번들 인증 등 NGN 에 대한 신규 기능 설계 분야 본인확인기술
IPR확보 가능성		높음	보통	높음

표준화 현황 및 전망		– 국내의 경우, 보안 토큰에 대한 국내 표준화가 제정되었으며, 식별자, 프레임워크 및 ID 공유에 대한 표준화가 진행되고 있음 – 국외의 경우, 보안 토큰, 식별자, 디스커버리에 대한 표준을 제정하였으며, ID 핵심 기술 전전에 대한 표준화가 진행되고 있음	– 국외의 경우, Liberty Alliance에서 Interaction Service에 대한 표준이 개발되었으며, OASIS에서 개인정보보호정책에 대한 표준이 제정되었음 – 개인정보 DB 보안과, 사용자단말 개인정보 관리의 경우, 국내외적으로 표준이 아직 미비한 상황임	– NGN 표준개발의 진행이 가속화되고, 이동성과 인증 식별의 문제가 ID 관리의 문제로 확대 중 – ITU-T 를 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
표준화 기구/단체	국내	TTA, 디지털 ID관리 포럼	TTA / ECIF	TTA, FoN
	국외	ITU-T SG17, OASIS, Liberty Alliance	ISO, OASIS, Liberty Alliance	ITU-T, OASIS, Liberty Alliance, GSI/SG3/SG11, 3GPP, ETSI
	국내참여 업체	TTA, ETRI, KISA 등	TTA, ETRI, KISA 등	TTA, ETRI, KISA, KT, Xener 등
	국내기여도	높음	높음	높음
표준화 수준	국내	표준기획 – 표준개발/검토	표준기획	표준제정
	국외	표준안 개발/검토 – 표준안 최종검토	표준안 개발/검토 – 표준 개발	표준제정
국내표준화의 인프라수준		높음	높음	높음

3. 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, 인터넷에 기반을 둔 전자상거래와 전자정부가 활성화되고 있는 최근에야 문제의 심각성이 일반인에게 인지되고 사회적인 문제로 인지되고 있는 상황임

○ 현재 ID관리 및 개인정보보호 기술에 대한 표준화를 진행하고 있는 국제단체는 ITU-T SG17과 ISO/IEC JCT1/SC27이 있으며, 이들 단체에서는 최근에서야 ID관리 및 개인정보보호 기술에 대한 표준화를 진행하고 있음. 따라서 ID관리 및 개인정보보호 기술에 대한 핵심 기술을 개발하고 우수 핵심 기술을 국제 표준화 단체의 표준으로 채택하도록 하여 많은 IPR을 확보하기에는 현재가 적기임

○ 국내에서는 현재 TTA의 개인정보보호 및 ID관리 프로젝트 그룹인 PG 502에서 표준화가 진행되고 있음. 그러나 TTA의 표준화가 주로 ETRI, KISA 등과 같은 연구기관과 학계를 통해 이루어지고 있으며 상대적으로 산업체의 참여가 저조한 문제가 있었음. 2008년에는 이러한 문제를 해결하기 위해, 통신사 및 중요 포털을 포함하는 산업계의 요구가 수렴될 수 있는 디지털 ID관리 포럼이 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 가능해야 하며 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. 향후 사용자 중심의 환경을 고려한 개인정보보호 기술 개발이 필요

○ “네트워크 및 응용 중심 ID 관리”는 ID 관리 모델이나 인증, 식별등 요소 기술 자체는 정보보호 분야에서 연구되어 온 유관 분야이나, NGN 및 차세대 유무선 통신망이라는 새로운 통신망 환경에 적용하는 과정에서 광범위한 엔지니어링 노력이 필요하여 간단히 표준제정의 수준에 도달하기 어려우며, 기초연구가 소요되어 표준개발의 진도가 느리다는 난점이 있음

○ 특히 북미 등 서구의 ID 관리 기술은 상당한 시장을 가진 산업 기반을 가지고 있어서, 풍부한 인적 자원을 동원 가능하나, 국내의 경우 KISA , NIDA 등 특정 영역을 담당하는 정책기관에서 업무를 수행해 온 관계로 기술진

들이 분화되어 있고 기술의 시너지를 내기 어려움

○ 해당 분야가 통신망 기술 중 새로운 시너지를 만들어 내는 첨단 분야여서, 각국의 기술 표준 경쟁이 치열하고 국제 협력관계 구축을 통한 연구 진행이 어려움

3.1.2. SWOT 분석 및 표준화 추진방향

<table>
<tr><th colspan="3" rowspan="2">국내역량요인 / 국외환경요인</th><th colspan="2">강 점 요 인 (S)</th><th colspan="2">약 점 요 인 (W)</th></tr>
<tr><td>시장</td><td>– 정보통신 인프라구축이 잘 되어 있고, 새로운 기술 수용이 매우 빠름
– 방송통신위원회 민간 i-PIN, 행정안전부 공공 i-PIN 등 ID관리에 대한 국가 인프라 구축의지</td><td>시장</td><td>– 정보보호 시장 규모의 상대적 협소
– 정보보호 산업체의 영세성, 브랜드 인지도 부족으로 경제성 형성의 한계
– 정보보호 구축에 많은 비용이 소요되나 투자 대비 회수 비용의 산정이 매우 어려움</td></tr>
<tr><td>기술</td><td>– 정부의 확고한 지원 정책(14대 IT 핵심기술) 추진으로 인한 새로운 정보보호 서비스와 새로운 정보보호 장치 개발의 필요성 대두
– ETRI를 통한 선도 기술개발을 통한 핵심 기술 확보 가능</td><td>기술</td><td>– 기술개발 고급 인력 부족
– 정보보호 기능이 구현되는 플랫폼 기술이 전무하여, 응용 위주의 제품 생산</td></tr>
<tr><td colspan="3">표준</td><td>– 국제표준화 활동에 조기참여 및 대응
– 정부의 강력한 IT 분야의 국제표준전문가 양성 프로그램 시행</td><td>표준</td><td>– 정보보호 표준 전문가의 부족
– 업체의 표준 추진 의지 미흡
– 행정편의성 증진 등의 사유로 개인정보 보호에 다소 소극적임</td></tr>
<tr><td rowspan="3">기회요인 (O)</td><td>시장</td><td>– ID 도용과 개인정보 유출 피해 증가에 따른 ID관리 및 개인정보보호 기술에 대한 관심 고조
– ID관리 분야의 시장 규모가 급속히 증가될 예정임</td><td colspan="2" rowspan="3">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 SG11의 기득권(의장직)을 활용한 공세적인 NGN 접속 제어 표준개발 및 IPR 포함 표준 확보</td><td colspan="2" rowspan="3">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
– 디지털 ID관리 포럼 등을 통해 국내 산업계의 요구사항을 수렴하고 TTA PG 502를 통해 국내 표준화를 수행
– ITU-T SG13을 통한 'Network Aspect of Id management' 부문 표준화 신규생성에 적극 참여 (새로운 기회 확보를 추구)</td></tr>
<tr><td>기술</td><td>– 웹2.0의 등장 등의 외부 환경변화에 따라 ID관리 및 개인정보보호 관련 핵심 기술 개발 필요성 증가</td></tr>
<tr><td>표준</td><td>– ID관리 관련 국제표준화가 ITU-T와 ISO에서 초기 단계이기 때문에, 국제 표준화 참여 및 선도 가능</td></tr>
<tr><td colspan="3">SO전략: 공격적 전략(강점사용-기회활용)</td><td>SO</td><td>WO</td><td colspan="2">WO전략: 만회 전략(약점극복-기회활용)</td></tr>
<tr><td colspan="3">ST전략: 다각화 전략(강점사용-위협회피)</td><td>ST</td><td>WT</td><td colspan="2">WT전략: 방어적 전략(약점최소화-위협회피)</td></tr>
<tr><td rowspan="3">위협요인 (T)</td><td>시장</td><td>– 미국, 유럽 등 ID관리 제품을 제공하는 기업들의 독점 우려
– 개인정보보호의 경우 국가별 정책, 규제 등과 일치시켜야 하는 문제 발생</td><td colspan="2" rowspan="3">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 PG 502와 디지털 ID관리 포럼을 통해 국내 표준화를 수행하고 국책연구기관의 표준전문가를 적극 활용하여 국제표준화 추진
– 인터넷 중심의 식별자 기술로 무장된 북미의 ID 관리 기술에 대항하여, 한국이 적극적인 ITU-T NGN 의 scope를 기반으로 기존 활동의 확대를 추구</td><td colspan="2" rowspan="3">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 탈피한 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 ID 관리 기술보유 기관들과 연합 및 협력체계 구축 모색</td></tr>
<tr><td>기술</td><td>– 국외 일부 국가와 회사에서 핵심 원천기술에 대한 기술적 우위 선점</td></tr>
<tr><td>표준</td><td>– 국가 간, 업체 간 경쟁이 치열
– 선진국의 경우 국제표준 경험 및 전문 인력 풍부
– 국가주의에 의한 개인정보 보호에 대한 우려</td></tr>
</table>

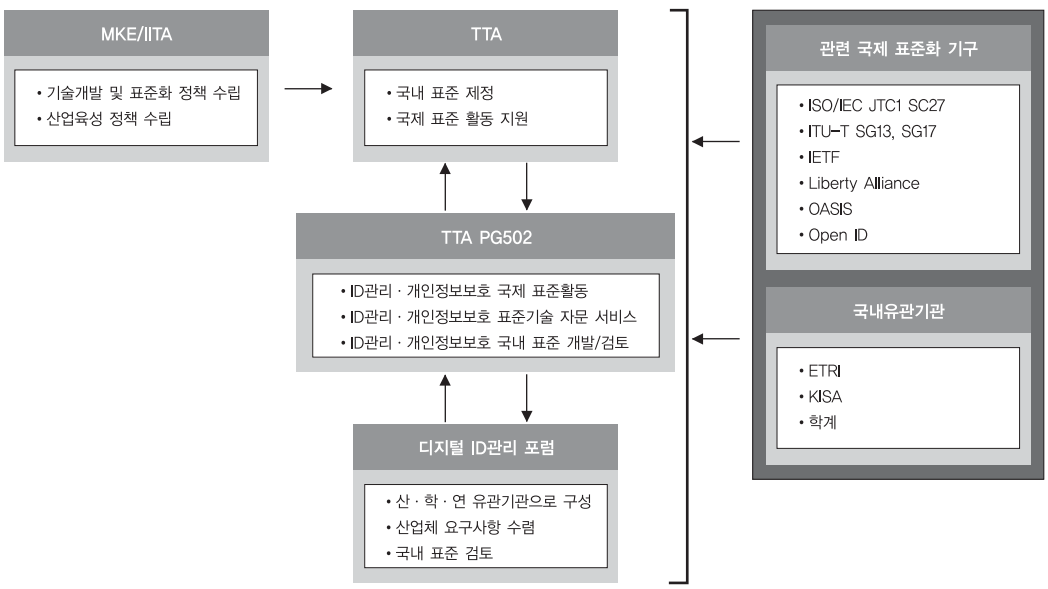
○ 현황분석을 통한 우선순위: WO→SO→ST→WT

- ETRI, KISA 등 국책 연구기관에서 산 · 학과 연계하여 ID관리 및 개인정보보호 기술 분야의 핵심 기술을 개발하여, 국내 독자 IPR을 확보하고, 이를 TTA PG 502를 통해 국내 표준화를 진행하고, ITU-T/SG17, ISO/IEC JTC1/SC17, SC27 등을 통해 국제 표준화를 수행함
- 네트워크 중심 ID 관리는 현재 국제 표준화가 진행 중인 SG11 의 접속 및 인증 제어 기술표준개발을 강화하고, 이를 ID 관리로 확대하는 전략을 추구하며, SG13 등을 통한 새로운 활동 형성에 주력함

○ 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 PG 502에서 추진하며, 관련 산업계와 학계의 구심적 역할을 수행하는 디지털 ID관리 포럼을 통해 산업체의 요구사항을 수렴함
- 국제 표준화는 ITU-T/SG17, ISO/IEC JTC1/SC17, SC27에 참여하여 수행함
- 네트워크 및 응용 중심 ID 관리에 대한 표준화는 국내의 경우 PG206에서 추진하며, 디지털 ID관리 포럼, 인터넷 식별자 포럼, 통합번호체계 포럼 등을 통해 산업체의 요구사항을 수렴함. 국제 표준화는 ITU-T SG13, SG11, SG2 를 통해 추진함

3.1.3. 표준화 추진체계



○ 국내 표준은 ETRI, KISA 그리고 정보보호 산업체에서 국내 표준 초안을 개발하고 TTA를 통하여 정보통신 단체표준으로 개발함. 정보통신 단체 표준은 TTA TC5 PG 502를 통하여 추진

○ ID관리 및 개인정보보호 기술을 집중적으로 다루는 디지털 ID관리 포럼을 통해 학계의 기반 기술과 산업계의 요구사항을 수렴하여 표준을 개발

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

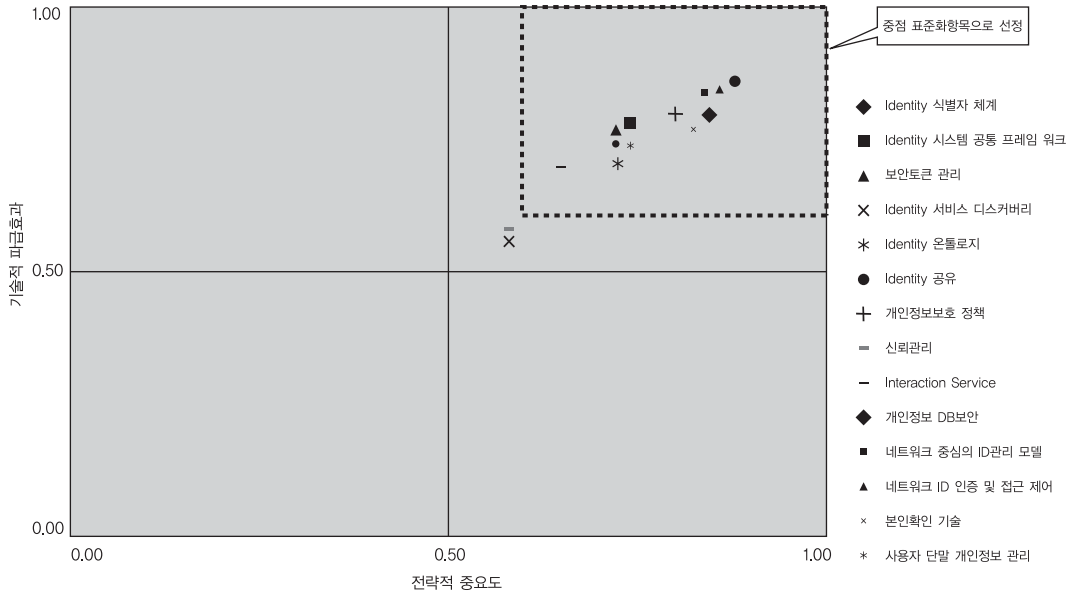
○ 네트워크 및 응용 중심 ID 관리에 대한 표준화는 국내의 경우 TTA PG206에서 추진하고 있으며, 점차 PG 502와 연계하여 표준을 개발하는 방안을 연구함. 디지털 ID관리 포럼, 인터넷 식별자 포럼, 통합번호체계 포럼 등을 통해 산업체의 요구사항을 수렴하고, 국제 표준화는 ITU-T SG13, SG11, SG2 를 통해 추진

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 산업 전략과의 연관성, 국내기업의 표준화 참여 및 관심도 등)	P2 공공성(사용자 편리성, 중복투자 방지 등)	P3 적시성	P4 기술적 선도 가능성 (국제표준 경쟁력, IPR확보 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)
평가지표의 중요도 / 표준화 대상항목	9.00	9.00	8.00	8.00	8.00	–	7.00	8.00	9.00	9.00	8.00	–
Identity 식별자 체계	7.00	8.00	7.00	7.00	7.00	**0.72**	7.00	7.00	8.00	8.00	7.00	**0.74**
Identity 시스템 공통 프레임워크	7.00	8.00	8.00	7.00	7.00	**0.74**	8.00	8.00	8.00	8.00	7.00	**0.78**
보안토큰 관리	7.00	8.00	7.00	7.00	7.00	**0.72**	7.00	8.00	8.00	8.00	7.00	**0.76**
Identity 서비스 디스커버리	6.00	6.00	6.00	5.00	6.00	**0.58**	6.00	6.00	5.00	5.00	6.00	**0.56**
Identity 온톨로지	8.00	8.00	7.00	6.00	7.00	0.72	6.00	7.00	7.00	8.00	7.00	**0.70**
Identity 공유	9.00	8.00	9.00	9.00	9.00	**0.88**	9.00	8.00	9.00	9.00	8.00	**0.86**
개인정보보호 정책	8.00	8.00	8.00	8.00	8.00	**0.80**	8.00	8.00	8.00	8.00	8.00	**0.80**
신뢰관리	5.00	6.00	6.00	6.00	6.00	**0.58**	6.00	6.00	5.00	6.00	6.00	**0.58**
Interaction Service	8.00	8.00	6.00	5.00	5.00	**0.65**	4.00	4.00	8.00	10.00	8.00	**0.70**
개인정보 DB보안	9.00	9.50	8.50	7.50	7.50	**0.84**	7.50	7.00	8.50	9.00	7.50	**0.80**
네트워크 중심의 ID관리 모델	8.00	8.00	9.00	8.00	9.00	**0.84**	8.00	9.00	8.00	8.00	9.00	**0.84**
네트워크 ID 인증 및 접근 제어	8.00	8.00	9.00	9.00	9.00	**0.86**	8.00	8.00	9.00	9.00	8.00	**0.84**
본인확인 기술	8.50	9.50	8.00	7.50	7.50	**0.82**	7.50	7.00	8.00	8.00	8.00	**0.77**
사용자 단말 개인정보 관리	7.00	8.00	8.00	7.00	7.00	**0.74**	7.00	8.00	8.00	7.00	7.00	**0.74**



3.2.2. 중점 표준화항목 선정사유

○ ID관리와 개인정보보호 분야의 표준화 항목 중에서 전략적 중요도와 기술적 파급효과가 모두 0.5보다 큰 분야를 2009년도 ID관리 및 개인정보보호 분야의 12개 중점 표준화 항목을 선정함

○ 프레임워크, ID 공유, 네트워크 중심 ID관리 모델과 네트워크 ID 인증 및 접근제어는 전략적 중요도가 매우 큰 분야이며, 특히 네트워크 중심 ID관리 모델과 네트워크 ID 인증 및 접근제어는 국제적으로 통신망의 진화와 관련한 핵심 표준화 분야로 부각되고 있는 분야여서, 조기 선점을 위한 표준화 연구개발의 필요성이 큼

○ 식별자와 ID 온톨로지, 프레임워크는 개인정보보호와 ID관리의 기반이 되는 기술로 ID 분야의 기반 요소로 기술적 파급효과가 매우 큰 분야임

○ 보안 토큰 관리는 ID관리 시스템 운용의 핵심 요소 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

○ 개인정보 DB 보안은 개인정보가 최종저장, 관리되는 DB를 대상으로 사전 접근통제, 데이터 암호화 및 변조 방지, 개인정보 사용기록 관리 등 안전한 개인정보 저장 및 관리와 자기정보통제권 보장기능을 제공하면서, 최근 개인정보보호 관련 법안 개정추진과 연관되어 산업적 파급효과가 큰 분야임

○ 사용자단말 개인정보 관리 기술은 향후 이용자 중심 환경 구축을 위하여 필수적인 분야이며, 기술규격 완성 시 국제 표준으로 추진도 가능한 분야임

○ 네트워크 중심 ID 관리 모델은, 날로 복잡해져 가는 통합망의 식별자 통합 운용 상황을 해결해줄 핵심 기능을 설계하기 위한 기반 작업으로, 최근 ITU-T NGN 표준 개발의 중요이슈로 부각된 상태이며, ITU-T 의 차기회기 중 NGN 설계의 핵심 표준화 이슈가 될 분야임

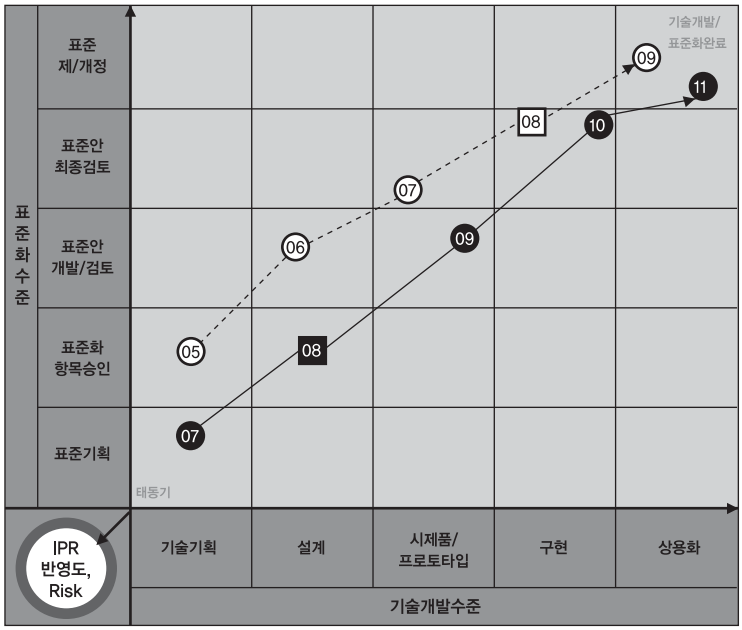
○ 네트워크 ID 인증 및 접근제어 기술은, NGN 접속제어 기능에 ID 관리 기능을 부가하는 것으로, 지난 3년간 ITU-T에서 한국이 주도 해 온 NGN 접속 제어 기능을 확장하는 작업에 해당함. 해당 부분은 한국의 표준화 역량을 최대한 발휘할 수 있는 부분이며, 특히 M2M 접속 인증 제어 등 최근의 신기술 표준이 도전하고 있는 분야이기도 함

○ 본인확인기술은 정부 정책 의지가 매우 큰 분야이며, 특히 i-PIN의 경우 온라인상에서의 본인확인 용도를 위해 필수적인 분야임

3.3. 중점 표준화항목별 세부전략(안)

3.3.1. Identity 식별자 체계

○ 표준상태전이도(표준화 & 기술개발 연계분석)

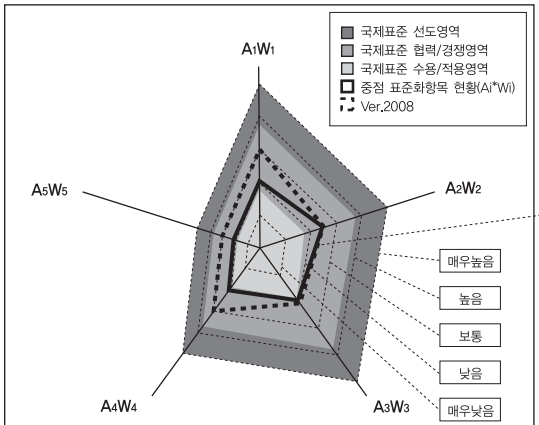


표준화 중요도	국내개발주체		관련 국제 표준화 기구
고(★★★) 중(★★) 저(★)	표준개발	기술개발	
★★	TTA ID관리포럼	ETRI KISA	IETF OASIS

범례

- 08 중점 표준화항목의 국내상태
- 08 중점 표준화항목의 국제상태
- → 중점 표준화항목의 국내 표준상태전이
- -▸ 중점 표준화항목의 국제 표준상태전이
- ↑ 선행표준(선 표준화 후 기술개발)
- ↗ 동시표준(표준화 & 기술개발 동시추진)
- → 후행표준(선 기술개발 후 표준화)

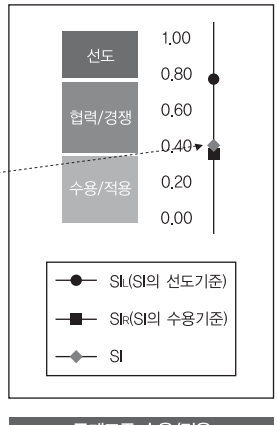
○ 국제표준화 전략목표 도출



A1 : 국외대비 국내표준화수준
A2 : 국외대비 국내기술개발수준
A3 : IPR확보가능성
점선 : Ver.2008현황
A4 : 국내표준화 인프라수준
A5 : 국제표준화 기여도
Wi : Ai의 가중치

SI(표준화 전략지수)	
SI_L (SI의 선도기준)	0.75
SI_R (SI의 수용기준)	0.35
SI	0.42

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



국제표준 수용/적용 (일부 협력/경쟁)(Ver.2008)
⬇
국제표준 협력/경쟁 (수용/적용)(Ver.2009)

○ 세부전략(안)

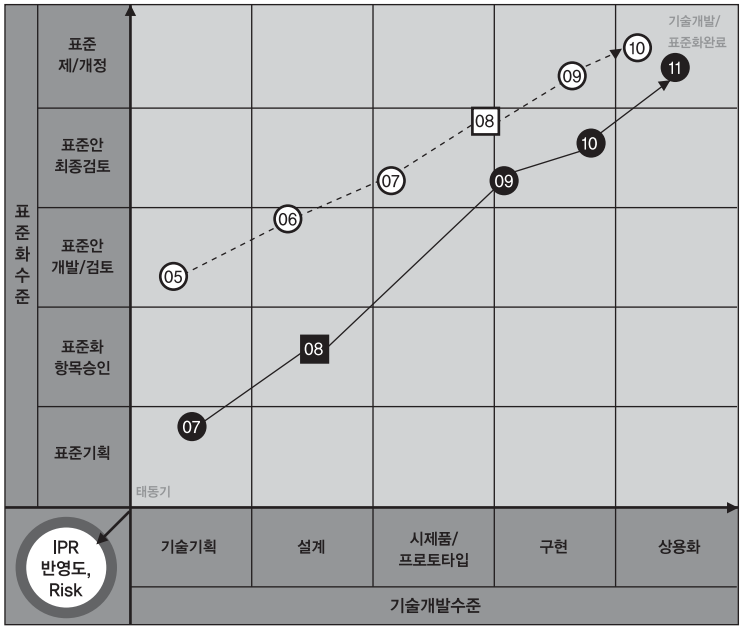
- URL, IRI 등 IETF의 국제 표준이 널리 활용되고 있으며, OASIS의 XRI 2.0 표준에 대한 국내 표준화 작업이 진행되고 있어, 개발된 국제 표준의 국내 수용이 필요함

○ 항목별 전략

- 국내외 표준화 현황분석에 따른 세부 전략
  - 현재 IETF 1738 URL(Uniform Resource Locators)과 IETF 3987 IRI(Internationalized Resource Identifiers) 표준은 TTA 국내 표준으로 수용되어 있는 상태임
  - ID 자원에 대한 식별자로 현재 개발이 완료된 OASIS의 XRI 2.0을 수용한 국내 표준화 작업이 TTA에서 진행 중인 상태임
  - 국제적으로 표준 작업화 작업이 완료되었으며 국내 산업계에서도 활용하고 있는 식별자 관련 표준을 적극적으로 국내에 수용하는 전략이 필요함
- 국내외 기술개발 현황분석에 따른 세부 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 필요
- 국내 IPR 보유 현황분석 및 확보가능성 분석에 따른 세부 전략
  - 식별자 기술에 대한 국내외 IPR은 확보되어 있지 않은 상태로, 국제적으로 통용될 수 있는 식별자 기술에 대한 국내 표준을 개발하고 국제표준으로 상정함으로써 IPR 확보도 가능할 것임
- 국내 표준화 인프라 수준 분석에 따른 세부 전략
  - 2008년 8월 디지털 ID 관리 포럼이 발족하여 산업체의 다양한 의견이 반영될 수 있는 토대가 마련되었으므로, 디지털ID 관리 포럼을 통해 산업계의 요구를 바탕으로 TTA 개인정보보호 및 ID 관리 프로젝트 그룹(PG502)를 통하여 국내 산업에 필요한 식별자 기술에 대한 국제 표준을 신속히 수용하는 노력이 필요함
- 국제표준화 기여도 분석에 따른 세부 전략
  - 식별자 기술에 대한 국제 표준화 기여도는 현재 매우 미흡한 실정으로, 국제 표준을 국내 표준으로 수용하면서 발생하는 기술적인 사항들을 국제 표준화 단체에 기고함으로써 국제 표준화에 기여도를 높이는 것이 필요함

3.3.2. Identity 시스템 공통 프레임워크

○ 표준상태전이도(표준화 & 기술개발 연계분석)

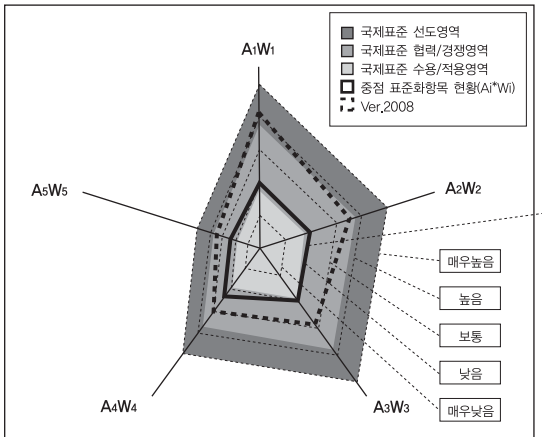


표준화 중요도	국내개발주체		관련 국제 표준화 기구
고(★★★) 중(★★) 저(★)	표준개발	기술개발	
★★	TTA ID관리포럼	ETRI KISA	ISO Liberty

범례

- 08 중점 표준화항목의 국내상태
- 08 중점 표준화항목의 국제상태
- → 중점 표준화항목의 국내 표준상태전이
- -▸ 중점 표준화항목의 국제 표준상태전이
- ↑ 선행표준(선 표준화 후 기술개발)
- ↗ 동시표준(표준화 & 기술개발 동시추진)
- → 후행표준(선 기술개발 후 표준화)

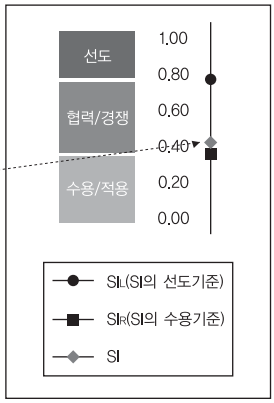
○ 국제표준화 전략목표 도출



A1 : 국외대비 국내표준화수준
A2 : 국외대비 국내기술개발수준
A3 : IPR확보가능성
점선 : Ver.2008현황

A4 : 국내표준화 인프라수준
A5 : 국제표준화 기여도
Wi : Ai의 가중치

SI(표준화 전략지수)	
SI_L (SI의 선도기준)	0.75
SI_R (SI의 수용기준)	0.35
SI	0.43



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

$$(0 \le W \le 1, 0 < SI \le 1)$$

국제표준 선도(Ver.2008)
⬇
국제표준 협력/경쟁 (수용/적용)(Ver.2009)

○ 세부전략(안)

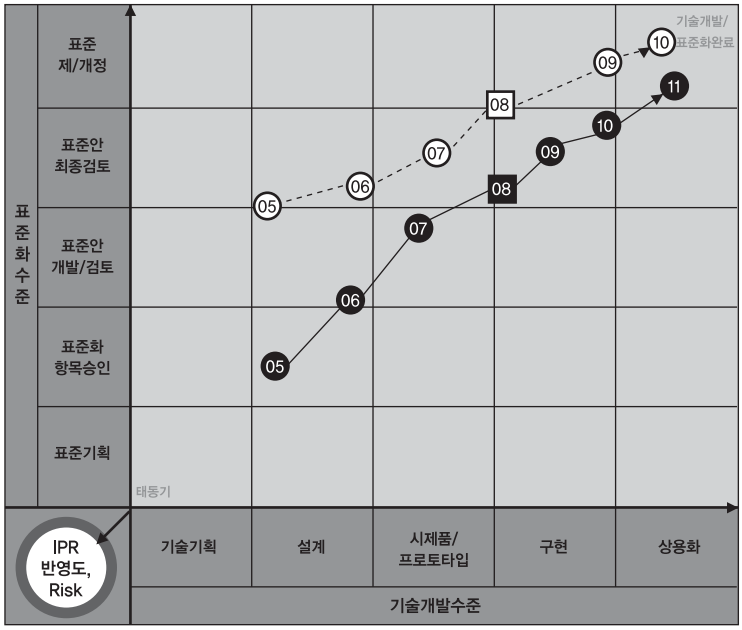
- Liberty Alliance, ISO/IEC SC27, ITU-T SG17 등에서 표준이 제정되었거나 진행 중인 상태로, 이들 표준을 국내 환경에 맞게 수용하는 것이 필요하며, 국내에서 개발되고 있는 ID 프레임워크 기술이 국제 표준으로 반영되도록 노력하는 것이 필요함

○ 항목별 전략

- 국내외 표준화 현황분석에 따른 세부 전략
  - Liberty Alliance에서 ID 프레임워크로 개발한 ID-WSF 2.0을 산업계 표준으로 제정한 상태이며 ISO의 SC27에서는 ID관리 기술에 대한 프레임워크 표준화를 제정 중에 있음
  - ITU-T SG17에서 2007년 ID관리 기술 Focus 그룹을 운용하여 ID관리 프레임워크 표준화에 대한 선행 작업을 수행하였음
  - 국내에서는 Liberty Alliance의 ID-WSF와 ISO, ITU-T 표준화 진행을 참고하고, ID-WSF 개발 경험을 토대로 국내 환경에 적합한 ID관리 프레임워크 표준을 제정하는 것이 필요함
- 국내외 기술개발 현황분석에 따른 세부 전략
  - ID 관리 프레임워크를 구성하는 세부 기술에 대한 국내외 기술 격차는 거의 없는 상황이나, 세부 기술을 통합하여 제공하는 ID 프레임워크 기술에서는 국내외 기술력의 차이가 존재하는 상태임
  - 따라서, 국내 산업계에서 기술 개발에 적극 활용할 수 있도록 국제 표준을 국내 환경에 맞게 수용하려는 노력이 필요함
- 국내 IPR 보유 현황분석 및 확보가능성 분석에 따른 세부 전략
  - ID 관리 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
- 국내 표준화 인프라 수준 분석에 따른 세부 전략
  - 2008년 8월 결성된 디지털ID 관리 포럼을 통한 산업계의 요구를 바탕으로 TTA 개인정보보호 및 ID 관리 프로젝트 그룹(PG 502) 등 국내 표준화 인프라는 잘 갖추어져 있기 때문에 이를 활용하여 산업계의 요구사항을 수렴하고, 학계와 연구소의 연구를 국내 표준화하는 것이 필요함
- 국제표준화 기여도 분석에 따른 세부 전략
  - ITU-T SG17에서 지속적인 국제 표준화 활동을 통해 국내에서 개발되는 ID 프레임워크 기술이 국제 표준으로 반영되도록 하는 노력이 필요함

3.3.3. 보안 토큰 관리

○ 표준상태전이도(표준화 & 기술개발 연계분석)

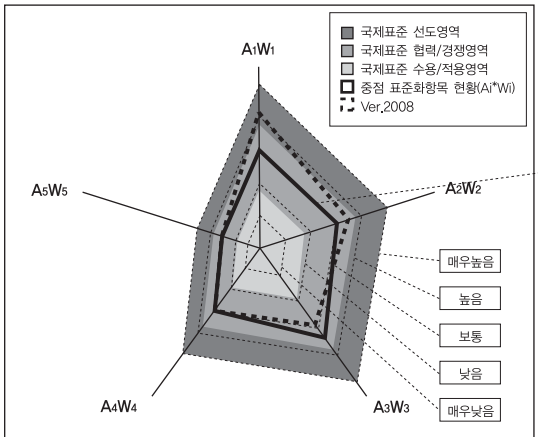


표준화 중요도	국내개발주체		관련 국제 표준화 기구
고(★★★) 중(★★) 저(★)	표준개발	기술개발	
★★	TTA ID관리포럼	ETRI	ITU-T OASIS

범례

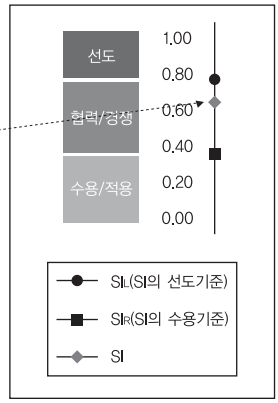
- 08 중점 표준화항목의 국내상태
- 08 중점 표준화항목의 국제상태
- → 중점 표준화항목의 국내 표준상태전이
- -▸ 중점 표준화항목의 국제 표준상태전이
- ↑ 선행표준(선 표준화 후 기술개발)
- ↗ 동시표준(표준화 & 기술개발 동시추진)
- → 후행표준(선 기술개발 후 표준화)

○ 국제표준화 전략목표 도출



A1 : 국외대비 국내표준화수준
A2 : 국외대비 국내기술개발수준
A3 : IPR확보가능성
점선 : Ver.2008현황
A4 : 국내표준화 인프라수준
A5 : 국제표준화 기여도
Wi : Ai의 가중치

SI(표준화 전략지수)	
SI_L (SI의 선도기준)	0.75
SI_R (SI의 수용기준)	0.35
SI	0.63



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

$$(0 \le W \le 1, 0 < SI \le 1)$$

국제표준 선도(Ver.2008)
⬇
국제표준 협력/경쟁(Ver.2009)

○ 세부전략(안)

– 현재 ITU-T에서 국제 표준화가 진행되고 있고 TTA에서 기반 표준 기술을 수용한 상태이며, 다양한 ID 관리 프레임워크에서 공통적으로 사용될 수 있는 표준을 개발하여 국제 표준과 협력/경쟁하는 것이 필요함

○ 항목별 전략

– 국내외 표준화 현황분석에 따른 세부 전략

• ITU-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

• ID관리에서 필요한 보안 토큰 구조에 대한 연구를 통해 국내 표준을 생성하고 이를 국제 표준화 단체에 기고하여 국제 표준화하는 노력이 필요함

– 국내외 기술개발 현황분석에 따른 세부 전략

• 국외에서 SSO, EAM 등 다양한 제품군이 출시되고 있으며, 국내에서도 SSO, EAM 시스템 제품군이 출시되고 있으며, ETRI에서 보안 토큰 생성 분배 관련 기술을 개발하여 보유한 상태로, 국내외 기술 격차가 크지 않은 상황임

• 다양한 ID관리 프레임워크에 공통적으로 사용될 수 있는 Uniform Identify Transfer Token과 서로 다른 보안 토큰을 해석하여 교환할 수 있는 Token Transformation 기술을 개발하여 국제 표준을 협력/경쟁하는 것이 필요

– 국내 IPR 보유 현황분석 및 확보가능성 분석에 따른 세부 전략

• 보안 토큰 분야에서의 IPR은 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 Identify Transfer Token과 서로 다른 보안 토큰을 해석하여 교환할 수 있는 Token Transformation 기술을 개발하여 국제 표준화함으로써 IPR을 확보하는 것이 필요함

– 국내 표준화 인프라 수준 분석에 따른 세부 전략

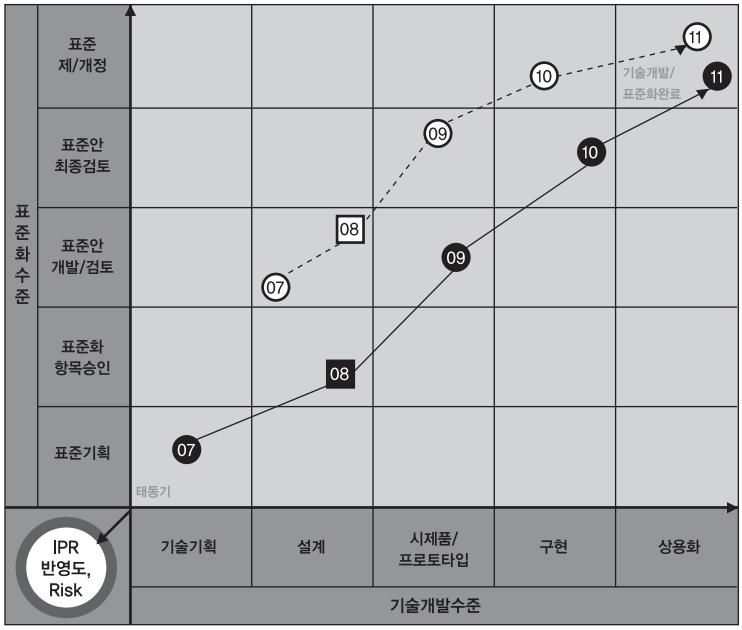
• 기존 국내 표준 제정 인프라는 충분히 확충되어 있으며, 기반 기술인 암호관련 대칭키와 공개키 표준이 이미 제정되어 있으므로, 국내 표준화에 이들 기반 인력과 기술을 활용할 수 있을 것임

– 국제표준화 기여도 분석에 따른 세부 전략

• 국내 기술과 국제 기술의 차이가 그리 크지 않기에, 보안 토큰의 국제 표준화 작업에 적극적으로 참여하여 국내기술을 표준에 반영하도록 하는 전략이 필요. 또한, 기 개발된 국제 표준의 국내 수용 또는 협력/경쟁이 필요

3.3.4. Identity 온톨로지

○ 표준상태전이도(표준화 & 기술개발 연계분석)

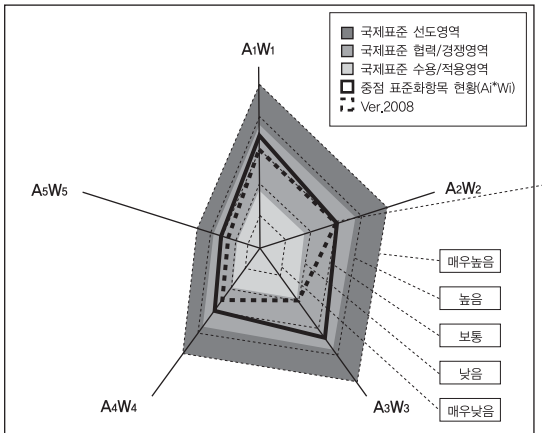


표준화 중요도	국내개발주체		관련 국제 표준화 기구
고(★★★) 중(★★) 저(★)	표준개발	기술개발	
★★	TTA ID관리포럼	ETRI	ISO/IEC W3G Liberty

범례

- 08 중점 표준화항목의 국내상태
- 08 중점 표준화항목의 국제상태
- → 중점 표준화항목의 국내 표준상태전이
- -▸ 중점 표준화항목의 국제 표준상태전이
- ↑ 선행표준(선 표준화 후 기술개발)
- ↗ 동시표준(표준화 & 기술개발 동시추진)
- → 후행표준(선 기술개발 후 표준화)

○ 국제표준화 전략목표 도출



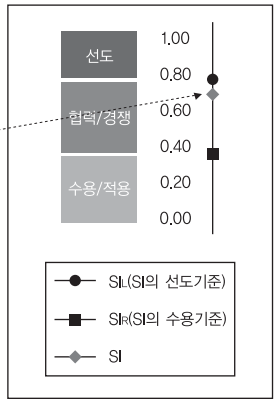
A1 : 국외대비 국내표준화수준
A2 : 국외대비 국내기술개발수준
A3 : IPR확보가능성
점선 : Ver.2008현황

A4 : 국내표준화 인프라수준
A5 : 국제표준화 기여도
Wi : Ai의 가중치

SI(표준화 전략지수)	
SI_L (SI의 선도기준)	0.75
SI_R (SI의 수용기준)	0.35
SI	0.65

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

$$(0 \le W \le 1, 0 < SI \le 1)$$



국제표준 수용/적용
(일부 협력/경쟁)(Ver.2008)
⬇
국제표준 협력/경쟁
(일부 선도)(Ver.2009)

○ 세부전략(안)

– Identity 온톨로지는 ISO/IEC SC27, ITU-T 등에서 표준화 제정을 위한 연구가 진행 중이며 현재 추진 중인 공통 아이덴터티 데이터 모델 표준화 작업이 완료될 경우 국제표준과의 협력/경쟁뿐만 아니라 일부 선도가 가능

○ 항목별 전략

– 국내외 표준화 현황분석에 따른 세부 전략

• 국외에서 Identity 온톨로지 표준화 작업은 ISO/IEC SC27 WG5, ITU-T SC17 등의 국제 표준기구, 그리고 Liberty Alliance, OpenID Foundation, EU의 PRIME 프로젝트 등에서 진행되고 있음. Identity 온톨로지는 국가별, 적용 영역별로 구성요소가 다른 특성으로 인해 단기간 내에 국제표준이 제정되기 어려운 점이 있음. 따라서 이러한 특징을 감안하여 국내 현실에 맞는 공통 아이덴터티 데이터 모델 표준화를 진행하면서 W3C에서 제정한 시맨틱 웹 기술을 활용한 Identity 온톨로지 표준을 국제표준으로 상정하고 국내에서 시맨틱 웹 기술 기반 Identity 온톨로지 구축 및 활용 소프트웨어를 선도 개발할 필요가 있음

– 국내외 기술개발 현황분석에 따른 세부 전략

• ISO, ITU-T 등 국제 표준화 단체에서 진행 중인 Identity 온톨로지 표준은 각 국의 법률 및 사회 여건에 따라 확장 또는 수정이 필요할 것으로 판단됨

• 한편, Identity 온톨로지 구축 및 활용에 이용될 수 있는 대표적 기술은 W3C에서 표준화한 XML, RDF, RDFS, OWL 등이며 EU에서 진행 중인 PRIME 프로젝트에서 이들 기술을 이용하여 Identity 온톨로지 설계가 시도되고 있음

• 따라서 국내 현실을 반영한 아이덴터티 구성요소를 대상으로 하는 공통 아이덴터티 모델 국내 표준을 제정하고 시맨틱 웹 기술을 활용한 공통 아이덴터티 표준모델 개발을 통해 아이덴터티 관리시스템에서 Identity 온톨로지를 활용할 수 있는 기술을 확보하여 국제 표준을 선도하는 것이 필요

– 국내 IPR 보유 현황분석 및 확보가능성 분석에 따른 세부 전략

• Identity 온톨로지에 대한 구현 및 처리기술로 활용 가능한 시맨틱 웹 관련 표준은 W3C 표준으로 제정된 상태로 국내에서는 이와 관련된 IPR이 확보되어 있지 않지만, 이들 기술을 활용한 Identity 온톨로지 국내 표준을 개발하고 국제표준으로 상정함으로써 IPR 확보도 가능

– 국내 표준화 인프라 수준 분석에 따른 세부 전략

• 2008년 8월 디지털 ID 관리 포럼이 발족하여 국내 주요 표준화기구, 연구기관 및 산업체들이 디지털 ID 보호관련 표준화 제정 및 제품, 기술 개발이 촉진될 것으로 예상되고 있으며, TTA 내 개인정보보호 및 ID 관리 프로젝트 그룹(PG502)에서 공통 아이덴터티 데이터 모델 표준 제정을 추진 중 있어 Identity 온톨로지 표준화를 위한 국내 인프라는 확보된 것으로 판단

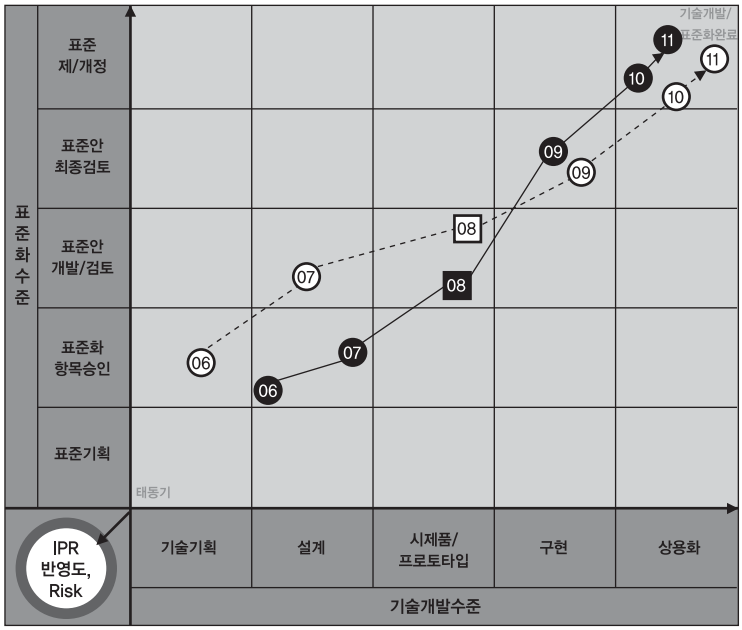
– 국제표준화 기여도 분석에 따른 세부 전략

• 시맨틱 웹 관련 국제표준은 W3C에 의해 표준제정이 이루어진 상태이지만, 아이덴터티 관리시스템에서 실질적으로 활용할 수 있는 시맨틱 웹 관련 기술을 이용한 국내 아이덴터티 모델을 개발한 후 국제 표준으

로 상정을 추진하는 전략이 필요

3.3.5. Identity 공유

○ 표준상태전이도(표준화 & 기술개발 연계분석)

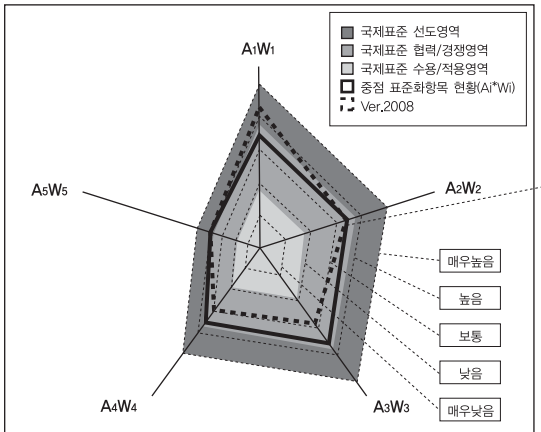


표준화 중요도	국내개발주체		관련 국제 표준화 기구
고(★★★) 중(★★) 저(★)	표준개발	기술개발	
★★★	TTA ID관리포럼	ETRI	ITU-T OASIS Liberty

범례

- 08 중점 표준화항목의 국내상태
- 08 중점 표준화항목의 국제상태
- → 중점 표준화항목의 국내 표준상태전이
- -▸ 중점 표준화항목의 국제 표준상태전이
- ↑ 선행표준(선 표준화 후 기술개발)
- ↗ 동시표준(표준화 & 기술개발 동시추진)
- → 후행표준(선 기술개발 후 표준화)

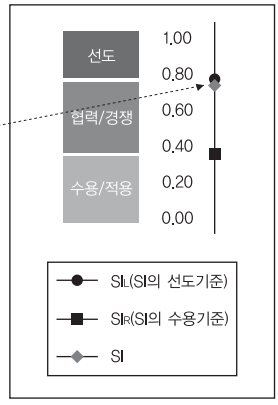
○ 국제표준화 전략목표 도출



A1 : 국외대비 국내표준화수준
A2 : 국외대비 국내기술개발수준
A3 : IPR확보가능성
점선 : Ver.2008현황
A4 : 국내표준화 인프라수준
A5 : 국제표준화 기여도
Wi : Ai의 가중치

SI(표준화 전략지수)	
SI_L (SI의 선도기준)	0.75
SI_R (SI의 수용기준)	0.35
SI	0.71

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



국제표준 선도
(일부 수용/적용)(Ver.2008)
⬇
국제표준 협력/경쟁
(선도)(Ver.2009)

○ 세부전략(안)

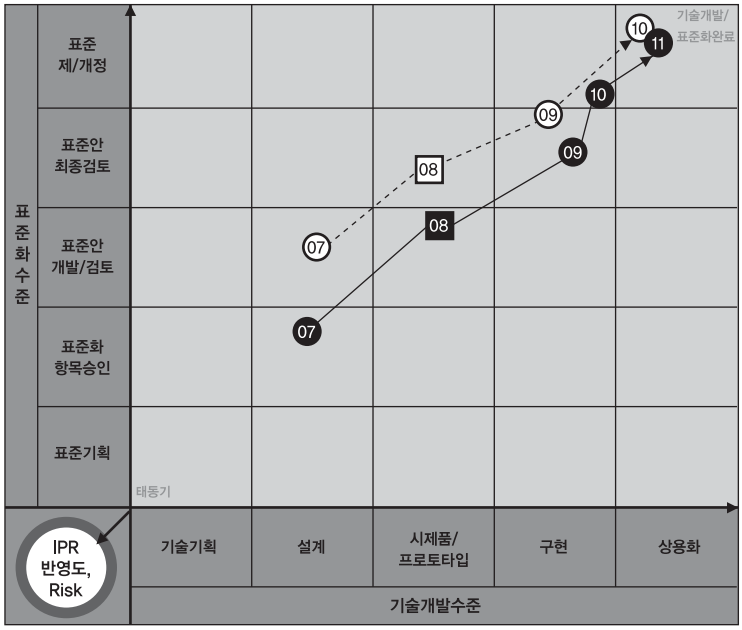
- Liberty Alliance의 ID-WSF, OASIS의 XDI 표준을 참조하고, ID-WSF 기반 인터넷 환경의 ID 공유 및 교환 서비스 개발경험을 토대로 Identity 공유기술의 국제 표준 제/개정 작업을 선도

○ 항목별 전략

- 국내외 표준화 현황분석에 따른 세부 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 ID 관리기술인 '자기 통제 강화형 디지털 아이덴티티 공유 프레임워크'에 관한 기고문을 ITU-T에 제출하여 X.idif라는 표준과제로 채택되어 표준화 작업이 진행되고 있으며, 2008년 9월 현재 표준으로 Determination되어 X.1251 표준번호를 부여받은 상태이며, 국내에서는 TTA에서 표준화가 진행 중임
  - 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 선도
- 국내외 기술개발 현황분석에 따른 세부 전략
  - 국내에서는 ETRI에서 ID-WSF 기반 Identity 공유 기술을 개발하여 산업체에 기술 이전함으로써 다수 산업체에서 Identity 공유 기술을 보유하게 되었으며, 2008년 현재 수행 중인 '자기통제 강화형 전자ID지갑 시스템 기술개발' 과제를 통해 사용자 중심 Identity 공유 기술을 개발하고 있음
  - 국외에서는 다수의 ID관리 관련 업체에서 ID-WSF 기반 Identity 공유 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 필요
- 국내 IPR 보유 현황분석 및 확보가능성 분석에 따른 세부 전략
  - Identity 공유 분야에 대한 IPR은 아직 많이 축적되지 않은 상태이므로 IPR 확보 가능성은 상대적으로 높은 편임
  - 따라서 Identity 공유 기술에 대한 국내 표준을 개발하고 국제표준으로 상정함으로써 IPR을 확보하는 것이 필요
- 국내 표준화 인프라 수준 분석에 따른 세부 전략
  - 2008년 8월 디지털 ID 관리 포럼이 발족하여 Identity 공유 기술에 대한 국내 주요 표준화기구, 연구기관 및 산업체들의 공동 연구가 가능해지고, TTA PG502을 통해 국내 표준화를 수행할 수 있어 국내 인프라 수준은 높은 편임
  - 따라서, 산학연 전문가들과 표준 전문 인력을 활용하여 국내 및 국제 표준화에 적극적으로 진행하는 것이 필요함
- 국제표준화 기여도 분석에 따른 세부 전략
  - ITU-T SG17에 지속적으로 참여하며 기고문을 제출하는 등 국제 표준화에 기여도가 높아 국제 표준화 환경이 좋은 분야이기 때문에, 국내에서 개발되는 Identity 공유 기술의 국제 표준화에 집중할 필요가 있음

3.3.6. 개인정보보호정책

○ 표준상태전이도(표준화 & 기술개발 연계분석)

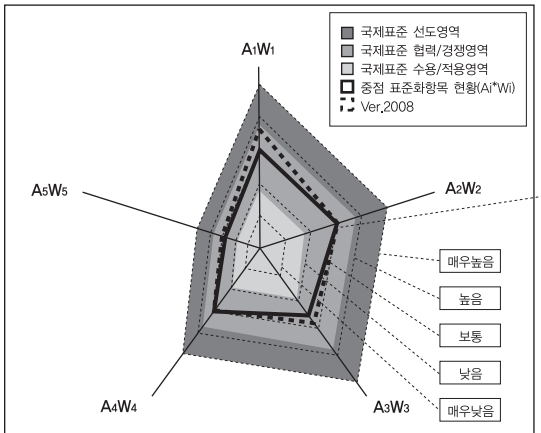


표준화 중요도	국내개발주체		관련 국제 표준화 기구
고(★★★) 중(★★) 저(★)	표준개발	기술개발	
★★★	TTA ID관리포럼	KISA ETRI	ITU-T W3C OASIS

범례

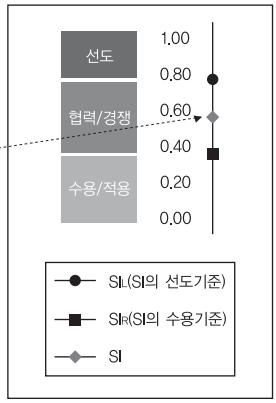
- 08 중점 표준화항목의 국내상태
- 08 중점 표준화항목의 국제상태
- → 중점 표준화항목의 국내 표준상태전이
- -▸ 중점 표준화항목의 국제 표준상태전이
- ↑ 선행표준(선 표준화 후 기술개발)
- ↗ 동시표준(표준화 & 기술개발 동시추진)
- → 후행표준(선 기술개발 후 표준화)

○ 국제표준화 전략목표 도출



A1 : 국외대비 국내표준화수준
A2 : 국외대비 국내기술개발수준
A3 : IPR확보가능성
점선 : Ver.2008현황
A4 : 국내표준화 인프라수준
A5 : 국제표준화 기여도
Wi : Ai의 가중치

SI(표준화 전략지수)	
SI_L (SI의 선도기준)	0.75
SI_R (SI의 수용기준)	0.35
SI	0.57



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

$$(0 \le W \le 1, 0 < SI \le 1)$$

국제표준 선도
(일부 수용/적용)(Ver.2008)
⬇
국제표준 협력/경쟁(Ver.2009)

○ 세부전략(안)

– W3C, OASIS에서 P3P, XACML 표준을 제정하고 있으며, 국내에서도 이를 수용하여 표준화를 진행하였으며, 향후 ID관리 분야에서의 개인정보보호 수준에 대한 평가기준 등에 대한 지속적인 ITU-T 표준화 활동을 통해 개인정보보호 분야에서의 국제 표준과 협력/경쟁하는 것이 필요

○ 항목별 전략

– 국내외 표준화 현황분석에 따른 세부 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
- RFID에서의 개인정보보호를 위한 가이드라인의 ITU-T 표준화 추진과 함께 ID관리 분야에서의 개인정보보호 수준에 대한 평가기준 등에 대한 지속적인 ITU-T 표준화 활동을 통해 개인정보보호 분야에서의 국제 표준과 협력/경쟁하는 것이 필요함

– 국내외 기술개발 현황분석에 따른 세부 전략

- 웹 브라우저에 내재되어 많이 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

– 국내 IPR 보유 현황분석 및 확보가능성 분석에 따른 세부 전략

- 개인정보보호정책에 대한 IPR은 외국에 비해 국내 보유양이 적은 편으로 통상적인 개인정보보호정책 기술로는 IPR을 확보하기가 쉽지 않음
- 따라서 국제적으로 통용되는 일반적인 기술 보다는 새로운 방향의 개인정보보호정책 기술을 개발하고 이를 표준화함으로써 IPR을 확보하는 것이 필요

– 국내 표준화 인프라 수준 분석에 따른 세부 전략

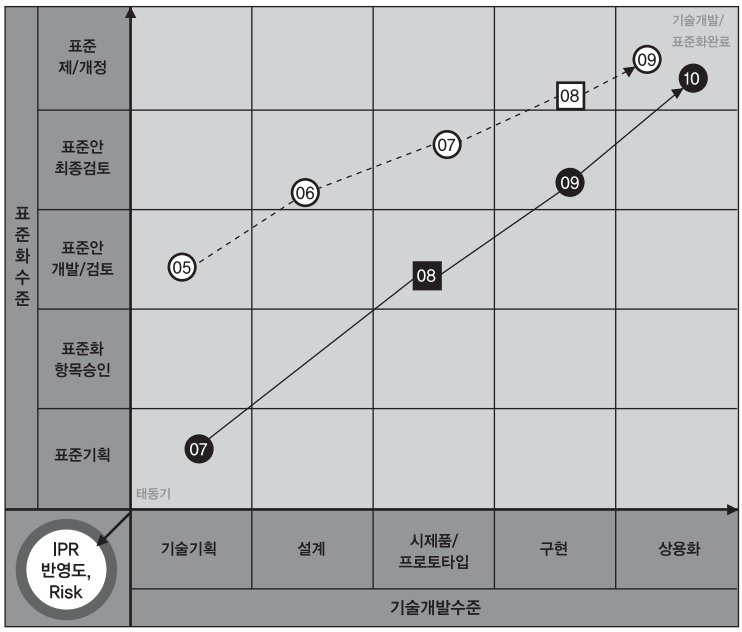
- 산학연 공동 연구가 가능한 디지털 ID 관리 포럼과 국내 표준화 단체인 TTA 등 국내 표준화 인프라 수준은 높은 편임
- 따라서, 디지털 ID 관리 포럼에서 산업체의 요구사항을 수렴하여 산업에서 필요한 표준 드래프트를 개발하고 이를 TTA의 표준 전문 인력이 감수하여 국내 및 국제 표준화를 진행하는 것이 필요함

– 국제표준화 기여도 분석에 따른 세부 전략

- TTA, KISA, ETRI 등 ITU-T SG17에 지속적으로 참여하며 기고문을 제출하는 등 국제 표준화에 기여도가 높아 국제 표준화 환경이 좋은 분야이기 때문에, 국내에서 개발되는 개인정보보호정책 표준을 ITU-T에 지속적으로 기고하여 국제 표준화를 수행하는 것이 필요함

3.3.7. Interaction Service

○ 표준상태전이도(표준화 & 기술개발 연계분석)

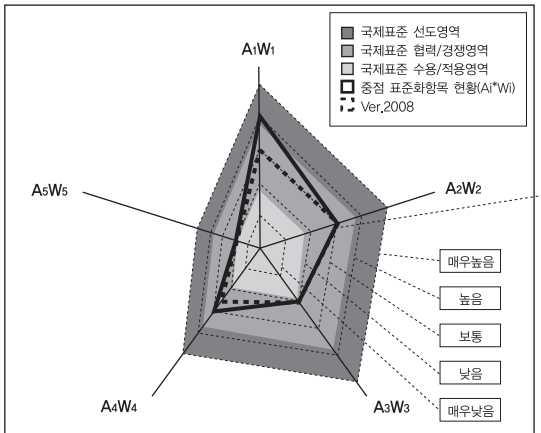


표준화 중요도	국내개발주체		관련 국제 표준화 기구
고(★★★) 중(★★) 저(★)	표준개발	기술개발	
★★★	TTA ID관리포럼	ETRI KISA	Liberty

범례

- 08 중점 표준화항목의 국내상태
- 08 중점 표준화항목의 국제상태
- → 중점 표준화항목의 국내 표준상태전이
- -▸ 중점 표준화항목의 국제 표준상태전이
- ↑ 선행표준(선 표준화 후 기술개발)
- ↗ 동시표준(표준화 & 기술개발 동시추진)
- → 후행표준(선 기술개발 후 표준화)

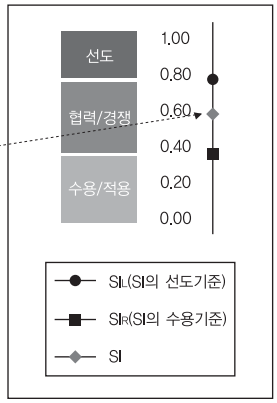
○ 국제표준화 전략목표 도출



A_1 : 국외대비 국내표준화수준
A_2 : 국외대비 국내기술개발수준
A_3 : IPR확보가능성
점선 : Ver.2008현황

A_4 : 국내표준화 인프라수준
A_5 : 국제표준화 기여도
W_i : A_i의 가중치

SI(표준화 전략지수)	
SI_L (SI의 선도기준)	0.75
SI_R (SI의 수용기준)	0.35
SI	0.58



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

$$(0 \le W \le 1, 0 < SI \le 1)$$

국제표준 선도
(일부 수용/적용)(Ver.2008)
⬇
국제표준 협력/경쟁(Ver.2009)

○ 세부전략(안)

– Liberty Alliance에서 2007년에 ID-WSF 2.0 Interaction Service를 제정한 상태로 국내 수용이 필요하며, 사용자에게 편리하고 일관성 있는 동의 획득 방법에 대한 기술을 개발하여 국내 표준화를 수행하고, 국제 표준과 협력/경쟁하는 것이 필요함

○ 항목별 전략

– 국내외 표준화 현황분석에 따른 세부 전략

• Liberty Alliance에서 제정된 ID-WSF 2.0 스펙의 일부분으로서 Interaction Service가 제정되어 있음. 이에 비하여 국내의 표준화 현황은 매우 미비함. 그러나, 국내의 환경은 이 표준을 구현하기에 충분한 서비스 인프라를 보유하고 있음. 따라서, 국제표준을 수용/적용하되 국내의 다양한 현실을 적용한 제품의 상용화를 추진, 시장 선점을 도모할 필요가 있음

– 국내외 기술개발 현황분석에 따른 세부 전략

• 사용자 중심 ID 관리와 개인정보의 자기통제권 확보 등을 위한 새로운 지침 및 표준 개발이 요구됨에 따라 기존에 표준화되어 있지 않은 Interaction Service의 표준 제정이 필요한 시기임

• 사용자 중심 ID 관리와 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

• 계속되는 개인정보 유출 사고에 의한 개인정보보호 법률제정이 진행되고 있으므로 평가 기술 표준의 제정과 밀접한 연관을 갖고 진행하는 것이 필요함. 표준제정 과 법률제정 직후 상용화 시기의 선점을 위한 집중적인 기술개발이 함께 진행되어야 함

– 국내 IPR 보유 현황분석 및 확보가능성 분석에 따른 세부 전략

• 표준 기술의 실용적 적용을 위한 관련 기술 분야의 IPR을 확보하기 위한 좋은 시기로, 다양한 Interaction 단말 환경과의 Interaction Service 모델 개발 과 비즈니스 모델 개발 등 분야에서 IPR 확보가 가능할 것임

– 국내 표준화 인프라 수준 분석에 따른 세부 전략

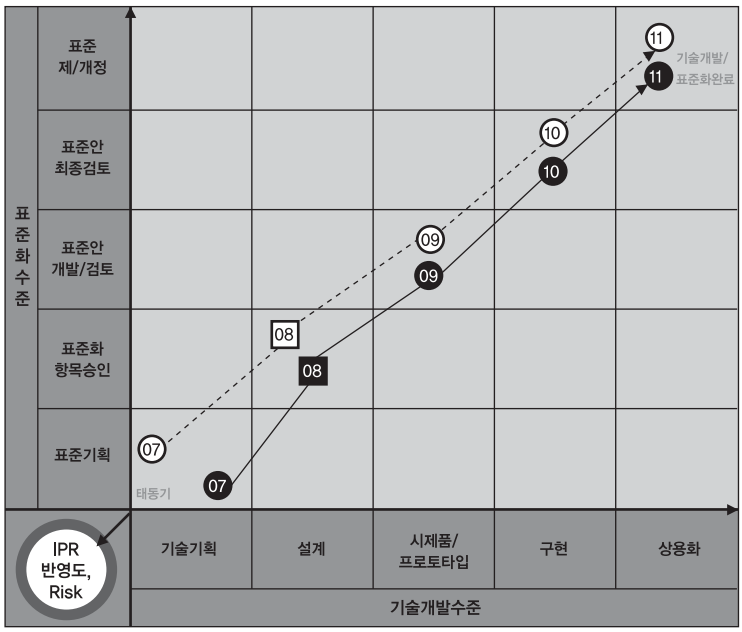
• 기존 국내외 표준 제정 인프라는 충분히 확충되어 있으므로 Interaction Service 분야에 적용될 수 있는 기술 표준과 제도 정비에 전문 인력을 충분히 활용할 수 있을 것임. 그러나, 시의적절한 표준의 제정과 이에 대한 상용화가 뒤따르지 않는다면 해외 선도 업체의 기술을 그대로 도입할 가능성이 높음

– 국제표준화 기여도 분석에 따른 세부 전략

• 다양한 커뮤니케이션 단말 환경의 지속적인 혁신이 진행되고 있으므로, 적극적으로 표준화에 참여하여 국내기술을 표준에 반영하도록 하는 전략이 필요함

3.3.8. 개인정보 DB 보안

○ 표준상태전이도(표준화 & 기술개발 연계분석)

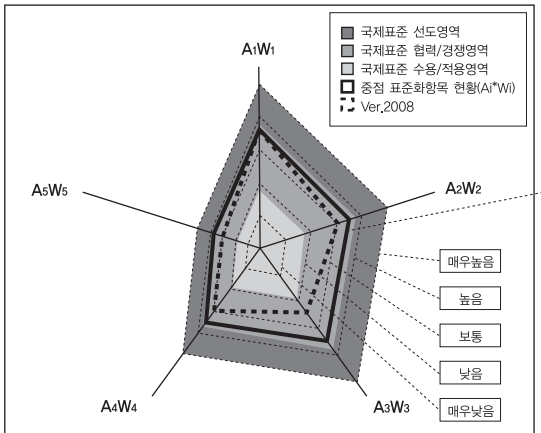


표준화 중요도	국내개발주체		관련 국제 표준화 기구
고(★★★) 중(★★) 저(★)	표준개발	기술개발	
★★★	TTA ID관리포럼	ETRI KISA	ISO/IEC IETF

범례

- 08 중점 표준화항목의 국내상태
- 08 중점 표준화항목의 국제상태
- → 중점 표준화항목의 국내 표준상태전이
- -▸ 중점 표준화항목의 국제 표준상태전이
- ↑ 선행표준(선 표준화 후 기술개발)
- ↗ 동시표준(표준화 & 기술개발 동시추진)
- → 후행표준(선 기술개발 후 표준화)

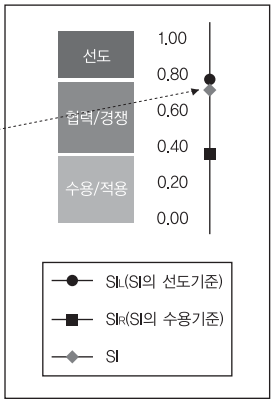
○ 국제표준화 전략목표 도출



A_1 : 국외대비 국내표준화수준
A_2 : 국외대비 국내기술개발수준
A_3 : IPR확보가능성
점선 : Ver.2008현황

A_4 : 국내표준화 인프라수준
A_5 : 국제표준화 기여도
W_i : A_i의 가중치

SI(표준화 전략지수)	
SI_L (SI의 선도기준)	0.75
SI_R (SI의 수용기준)	0.35
SI	0.70



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

국제표준 수용/적용 (일부 협력/경쟁)(Ver.2008)
⬇
국제표준 협력/경쟁 (선도)(Ver.2009)

○ 세부전략(안)

– 일반적인 DB 보안에 사용되는 인증 및 암호기술은 ISO/IEC, ITU-T 등 국제 표준기구에 의해 표준이 제정된 상태이지만 DB에 저장된 개인정보에 대한 프라이버시 보호를 위해 추가로 요구되는 표준에 대한 국내 표준 제정을 먼저 추진하고 이후 국제 표준으로 상정할 필요가 있음

○ 항목별 전략

– 국내외 표준화 현황분석에 따른 세부 전략

• DB 보안을 위해 사용되는 대표적 정보보호 기술들은 접근통제, 암호기술 등으로 관련 기술들에 대한 국내외 표준은 이미 제정되어 있는 상태임

• 그러나 개인정보를 저장, 관리하는 개인정보 DB는 일반 데이터를 저장하는 경우와는 달리 프라이버시 보호를 위한 추가적인 보안요구사항이 필요하며, 국내의 경우 TTA PG502에서는 개인정보 DB 관리 보안요구사항 등 관련 표준 제정이 진행 중에 있음

– 국내외 기술개발 현황분석에 따른 세부 전략

• DB 보안을 위해 접근통제 또는 암호기술을 적용한 DB 보안제품이 S/W, H/W 형태로 이미 개발되어 상용환경에서 사용 중에 있으며 주요 상용 DBMS에서도 테이블 및 특정 필드에 대한 암호 또는 사용 내역에 대한 보안감사기능을 기본적으로 지원하고 있음

• 국내 정보보호 전문 업체에서도 접근통제 및 표준 암호기술을 활용한 DB 보안제품을 개발한 상태로 일본 등 해외에 제품을 공급하고 있어 국외 기술과 격차는 크지 않은 것으로 평가됨

• 그러나 개인정보를 저장하고 있는 개인정보 DB에서 추가로 요구되는 보안 및 프라이버시 보호 요구사항에 대한 표준이 아직 제정되어 있지 않은 이유로 개인정보 DB를 위한 기술개발은 추가로 요구되고 있는 상태임

– 국내 IPR 보유 현황분석 및 확보가능성 분석에 따른 세부 전략

• 국내외 표준기구에서 표준으로 제정한 인증, 접근통제, 암호화 기술 등에 대한 IPR을 추가로 확보하기 보다는 개인정보 DB에서 요구되는 프라이버시 보호 요구사항을 표준화하고 이를 지원하는 기술에 대한 IPR을 새롭게 확보하는 것이 필요함

– 국내 표준화 인프라 수준 분석에 따른 세부 전략

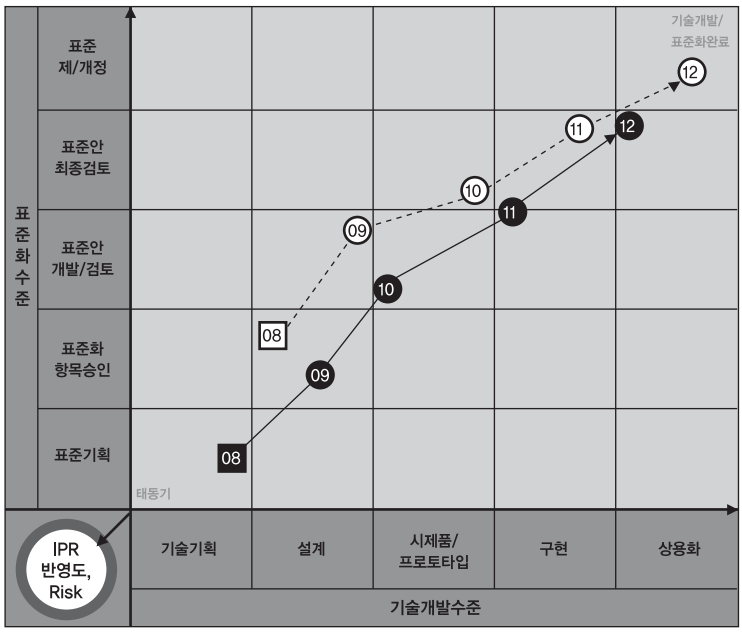
• 개인정보보호에 대한 사회적 인식 증가와 법 · 제도 강화로 개인정보 DB 보호 표준제정에 대한 여건은 성숙되고 있으며, 2007년부터 개인정보보호에 관한 국내표준 제정을 활발히 진행 중인 TTA PG502에서 개인정보 DB 보안 및 프라이버시 보호를 위한 추가 표준 제정을 추진할 필요가 있음

– 국제표준화 기여도 분석에 따른 세부 전략

• 현재까지 DB 보안을 위해 적용된 표준기술은 사전 차단 기능과 연관되어 있었으나 개인정보 DB 보안에서는 프라이버시 보호에 대한 국제규범을 준용한 사후 점검기능 지원을 위한 DB 보안감사로그 표준 등 국내표준을 먼저 추진하고 이후 국제표준으로 상정하는 방안을 고려해야 함

3.3.9. 네트워크 중심 ID 관리 모델

○ 표준상태전이도(표준화 & 기술개발 연계분석)

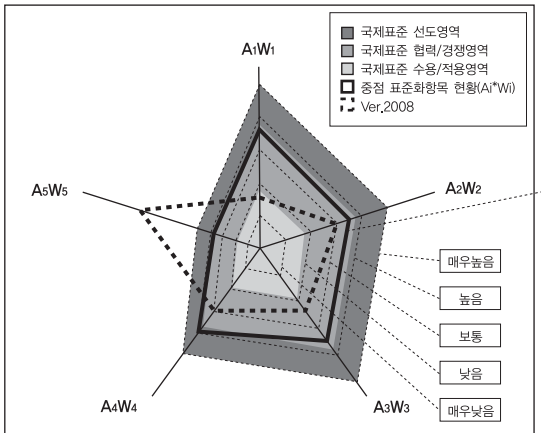


표준화 중요도	국내개발주체		관련 국제 표준화 기구
고(★★★) 중(★★) 저(★)	표준개발	기술개발	
★★★	TTA ID관리포럼	ETRI	ITU-T 3GPP

범례

- 08 중점 표준화항목의 국내상태
- 08 중점 표준화항목의 국제상태
- → 중점 표준화항목의 국내 표준상태전이
- -▸ 중점 표준화항목의 국제 표준상태전이
- ↑ 선행표준(선 표준화 후 기술개발)
- ↗ 동시표준(표준화 & 기술개발 동시추진)
- → 후행표준(선 기술개발 후 표준화)

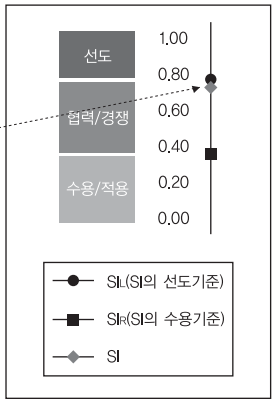
○ 국제표준화 전략목표 도출



A_1 : 국외대비 국내표준화수준
A_2 : 국외대비 국내기술개발수준
A_3 : IPR확보가능성
점선 : Ver.2008현황
A_4 : 국내표준화 인프라수준
A_5 : 국제표준화 기여도
W_i : A_i의 가중치

SI(표준화 전략지수)	
SI_L (SI의 선도기준)	0.75
SI_R (SI의 수용기준)	0.35
SI	0.72

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



국제표준 부분 선도/협력 경쟁 (Ver.2008)
⬇
국제표준 협력/경쟁 (선도)(Ver.2009)

○ 세부전략(안)

– 현재 ITU-T에서 국제 표준화가 진행되고 있으며, 본격적인 국제 표준 개발이 시작되는 단계이므로, 해당 국제표준의 선도를 위한 협력과 경쟁이 필요

○ 항목별 전략

– 국내외 표준화 현황분석에 따른 세부 전략

- ITU-T IDM FG(현재는 IdM GSI)에서 작성하여 SG17에 제출한 결과문서에 기반하여, 향후 ITU-T에서 ID 관리에 관한 표준화 작업이 활성화될 것이며, 이 중 보안 측면(security aspect)은 SG17로, 네트워크 측면(network aspect)은 SG13으로 나뉘어 수행될 예정
- 해당 보고서(gap analysis report)는 NGN의 구조 내에서 사용되는 ID들이 생명 주기(life cycle) 관리를 받아야 함을 설명하고 있으며, 이를 통해 NGN에서 ID 관리 구조를 개발할 것임을 설명하고 있음
- 해당 보고서의 개념 정리와 ITU-T 구조조정에 따라 진행되는 관련 표준화 진행을 주시하고, SG13과 SG17에서 정의되는 후속 표준화 작업에 참여하면서, 네트워크 중심의 ID 관리 기술표준분야를 국내의 기술개발 방향을 바탕으로 제안 및 선도해 나갈 필요가 있음

– 국내외 기술개발 현황분석에 따른 세부 전략

- 네트워크 기술은 성숙 단계인 기술이지만 네트워크 ID 관리 모델에 대한 기술은 국내외적으로 아직 개발 시작 단계인 기술임
- 따라서, 네트워크 ID 관리 데이터 모델의 표준화를 선도하여 국내외 기술 개발을 선도하는 것이 필요

– 국내 IPR 보유 현황분석 및 확보가능성 분석에 따른 세부 전략

- 표준 기술의 제/개정에 따른 차별성을 부여할 수 있는 관련 기술 분야의 IPR을 확보하기 위한 좋은 시기로, NGN 의 ID 관리 및 정보보호 기술 개발, 기타 평가 도구의 적용 등 분야에서 IPR 확보가 가능할 것임

– 국내 표준화 인프라 수준 분석에 따른 세부 전략

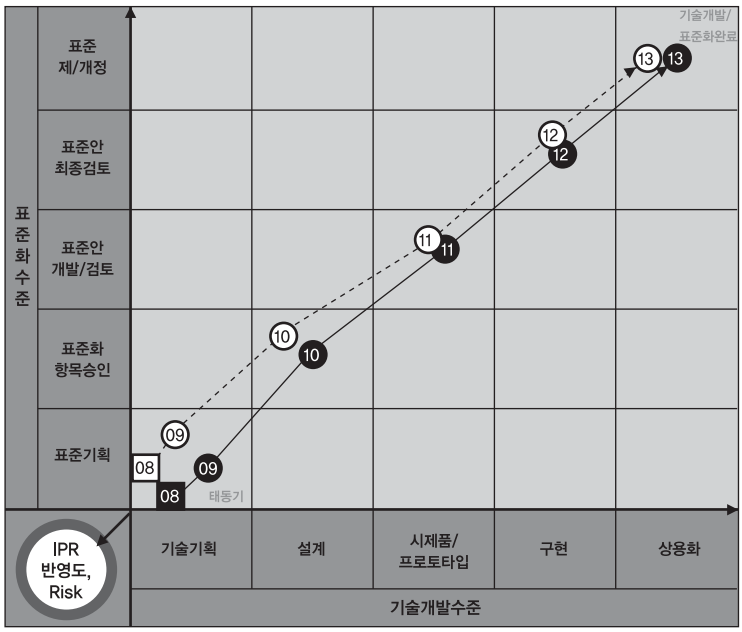
- 기존 국내의 ID 관리 기술개발 및 표준 제정 인프라는 충분히 확충되어 있는 편이며, 신설 디지털ID 관리 포럼 등을 통해 관련 전문 인력을 충분히 활용할 수 있을 것임. 그러나 TVRA 등 새로운 기술의 도입과 평가 서비스 운용을 위해 관련 기술 표준에 대한 요구가 매우 높으며, 시기적절한 표준기술 연구가 지원되지 않으면 해외 선도 업체의 기술을 그대로 도입할 가능성이 높음

– 국제표준화 기여도 분석에 따른 세부 전략

- ITU-T SG13에 지속적으로 참여하며 기고문을 제출하는 등 국제 표준화에 기여도가 높은 편이기 때문에, 국내에서 개발되는 네트워크 ID 관리 모델 기술을 바탕으로 ITU-T GSI, SG13 및 SG17에 적극적인 기고를 통해 국제 표준화를 수행하는 것이 필요함

3.3.10. 네트워크 ID 인증 및 접근제어

○ 표준상태전이도(표준화 & 기술개발 연계분석)

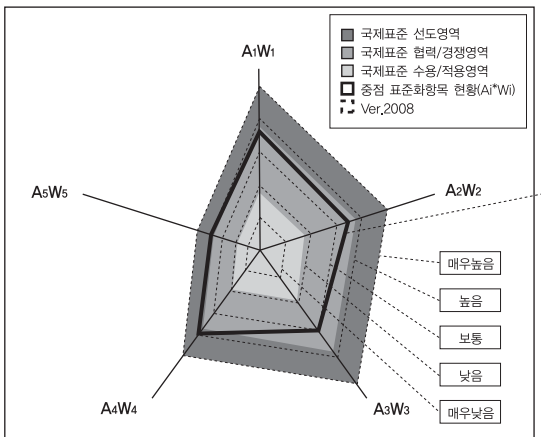


표준화 중요도	국내개발주체		관련 국제 표준화 기구
고(★★★) 중(★★) 저(★)	표준개발	기술개발	
★★★	TTA ID관리포럼	ETRI KISA	ITU-T

범례

- 08 중점 표준화항목의 국내상태
- 08 중점 표준화항목의 국제상태
- → 중점 표준화항목의 국내 표준상태전이
- -▸ 중점 표준화항목의 국제 표준상태전이
- ↑ 선행표준(선 표준화 후 기술개발)
- ↗ 동시표준(표준화 & 기술개발 동시추진)
- → 후행표준(선 기술개발 후 표준화)

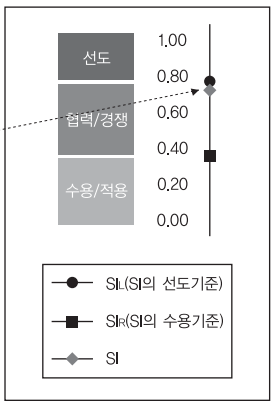
○ 국제표준화 전략목표 도출



A_1 : 국외대비 국내표준화수준
A_2 : 국외대비 국내기술개발수준
A_3 : IPR확보가능성
점선 : Ver.2008현황

A_4 : 국내표준화 인프라수준
A_5 : 국제표준화 기여도
W_i : A_i의 가중치

SI(표준화 전략지수)	
SI_L (SI의 선도기준)	0.75
SI_R (SI의 수용기준)	0.35
SI	0.71



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

국제표준 협력/경쟁 (선도)(Ver.2009)

○ 세부전략(안)

– 현재 ITU-T에서 진행 중인 NGN 표준화에 있어, 부분적으로 실효적인 국제 표준 개발을 선도하고 있으므로, 본격적인 경쟁과 주도의 노력이 필요

○ 항목별 전략

– 국내외 표준화 현황분석에 따른 세부 전략

• ITU-T IDM FG(현재는 IdM GSI)에서 작성하여 SG17에 제출한 결과 보고서들은 NGN에서 ID 관리 기능을 개발할 주된 작업영역으로 NACF(Network Attachment Control Function)를 지적하였음. 국내에서 ETRI가 주도하고 있는 ITU-T SG11의 Q.7은 Network Attachment 기능 블록을 담당하고 있는 Question으로, 한국이 주도하고 있으므로, 이를 기반으로 한 표준화 작업의 진행이 용이한 상태임

• 관련하여 서비스 NGN 접속인증 프로토콜, NGN 액세스 – 서비스 번들인증, NGN 접속제어 등의 기능들을 표준화하고 있으며, 향후 사업자 ID의 도입, M2M 기능의 도입을 위한 접속 및 인증, resolution 및 discovery 등 기능을 구현하게 될 예정임. 국제 표준을 선도하기 위해, 한국이 주도하고 있는 Q.7/11의 역량을 최대한 확대하는 노력이 필요

– 국내외 기술개발 현황분석에 따른 세부 전략

• 최근 북미 중심 세력인 Telcordia 및 Verisign은 ITU-T를 중심으로 NGN 서비스 ID 기술을 국제적으로 도입하기 위한 표준를 추진 중임. 한국의 경우 이러한 서비스 ID 표준화보다는 3GPP 등을 참조하는 서비스 구조(SOA) 등 NGN 서비스 개발에 더 주력하고 있는 상황임. 그러나 서비스의 인증, 접근제어, 신뢰성 확보 등을 위해 표준화된 ID 체계가 필요하므로, 국제 기술개발 동향을 분석하고 한국의 대응 입장을 개발하는 작업이 시급함

• 3GPP에서는 GAA(Generic Authentication Architecture)와 GBA(Generic Bootstrapping Architecture) 표준을 제정한 상태임. 국내에서는 3GPP의 표준안들을 기반으로 모바일 환경에서의 클라이언트와 서버 간의 상호인증 문제들을 해결하는 표준안을 개발하는 것이 필요하며, 이를 바탕으로 국제표준을 선도하는 것이 필요함

– 국내 IPR 보유 현황분석 및 확보가능성 분석에 따른 세부 전략

• 네트워크 ID 인증 및 접근제어 기술에 대한 IPR은 매우 미흡한 실정이나, 통합망을 추구하는 NGN에서 통합액세스간의 통합 인증, 접근제어 등을 표준화하는 기술로 IPR의 확보를 추진 중이며, 향후 M2M 기술의 도입, OID resolution 기능의 도입 등의 과정을 통해 추가적인 IPR 확보에 노력하는 전략이 필요함

– 국내 표준화 인프라 수준 분석에 따른 세부 전략

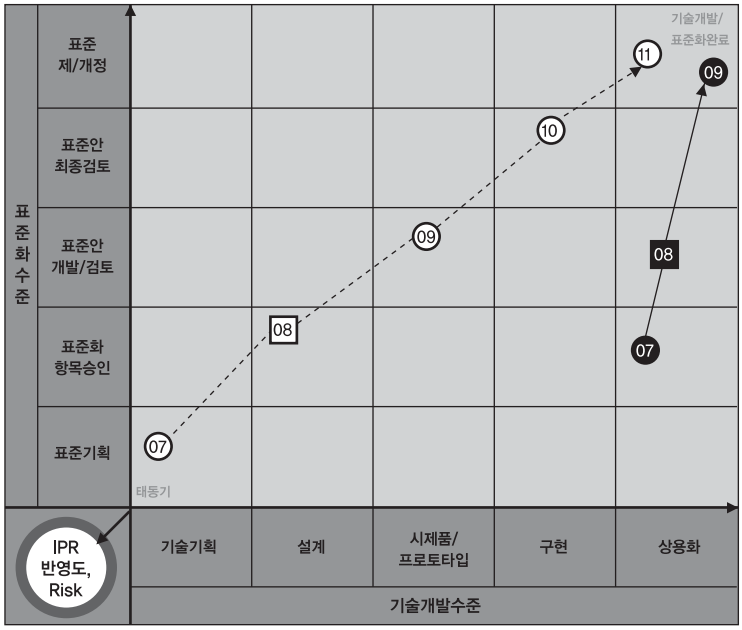
• 기존 국내의 NGN 인증 및 접근제어, 관련 ID 관리 기술개발 및 표준 제정 인프라는 충분히 확충되어 있는 편이며, 신설 디지털ID 관리 포럼 등을 통해 관련 전문 인력을 충분히 활용할 수 있을 것임. 그러나 ID, M2M 식별자 및 인증 등 새로운 기술에 대한 해외 선도 업체와의 기술 경쟁력을 유지하기 위해서는 시기

적절한 표준기술 연구가 지원되는 것이 필요함

- 국제표준화 기여도 분석에 따른 세부 전략
  - 국내에서 진행한 표준화 협력에 기인하여, ITU-T GSI의 주력 멤버들이 NACF 및 Q.7/11에 대해 우호적이며, 국내 ETRI에서 Q.7/11을 담당하고 있는 라포터는 SG2의 번호체계에 대한 연구도 병행 하고 있어, IdM FG의 주력 멤버들에게 관심을 끌고 있는 등, 향후 무난한 표준화 주도가 가능한 상황임. 지속적으로 표준화 협력관계를 유지 확대하는 노력이 필요함

3.3.11. 본인확인기술

○ 표준상태전이도(표준화 & 기술개발 연계분석)

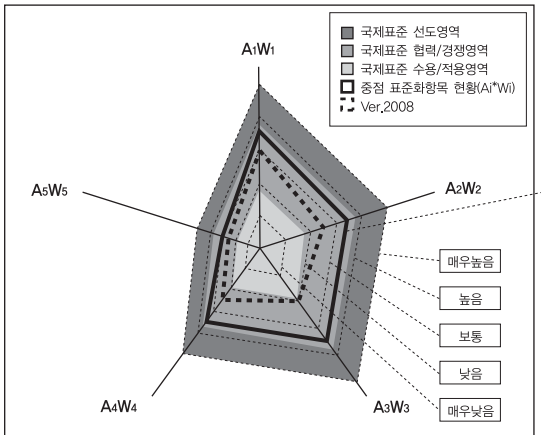


표준화 중요도	국내개발주체		관련 국제 표준화 기구
고(★★★) 중(★★) 저(★)	표준개발	기술개발	
★★★	TTA ID관리포럼	KISA ETRI	ITU-T

범례

- 08 중점 표준화항목의 국내상태
- 08 중점 표준화항목의 국제상태
- → 중점 표준화항목의 국내 표준상태전이
- -▸ 중점 표준화항목의 국제 표준상태전이
- ↑ 선행표준(선 표준화 후 기술개발)
- ↗ 동시표준(표준화 & 기술개발 동시추진)
- → 후행표준(선 기술개발 후 표준화)

○ 국제표준화 전략목표 도출



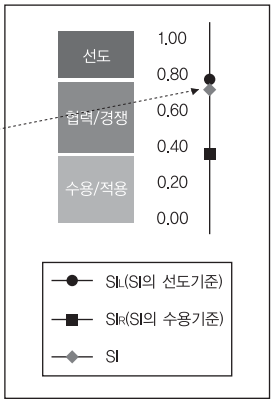
A1 : 국외대비 국내표준화수준
A2 : 국외대비 국내기술개발수준
A3 : IPR확보가능성
점선 : Ver.2008현황

A4 : 국내표준화 인프라수준
A5 : 국제표준화 기여도
Wi : Ai의 가중치

SI(표준화 전략지수)	
SI_L (SI의 선도기준)	0.75
SI_R (SI의 수용기준)	0.35
SI	0.69

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

$$(0 \le W \le 1, 0 < SI \le 1)$$



국제표준 부분 선도/협력 경쟁 (Ver.2008)
⬇
국제표준 협력/경쟁 (선도)(Ver.2009)

○ 세부전략(안)

– i-PIN과 g-PIN의 상호연계에 따른 TTA 표준의 개정을 2008년 내로 완료하며 국제 환경에 맞는 i-PIN 규격을 개발하여 ITU-T에 기고하여 국제 표준화를 선도하는 것이 필요함

○ 항목별 전략

– 국내외 표준화 현황분석에 따른 세부 전략

- 인터넷 상에서 본인확인을 위한 기술인 i-PIN의 서비스 프레임워크, 서비스 전달 메시지 형식에 대한 표준이 2007년 국내 표준으로 제정되었음
- 공공 i-PIN과 상호연계에 따라 i-PIN 서비스 전달 메시지 형식과 서비스 중복가입 확인 정보에 대한 표준이 TTA에서 2008년 내로 완료될 예정임
- i-PIN 서비스의 중복가입확인정보와 같이 단일 체계 내에서 유일한 식별자를 생성하는 방법을 활용하여 전 세계적으로 단일 식별자를 생성할 수 있는 방안을 개발하여 개발하여야 함
- i-PIN은 주민등록번호와 같은 실세계의 단일 식별자 체계를 대체하는 기술로 국제 환경에 맞는 i-PIN 규격을 개발하여 ITU-T에 기고하여 국제 표준화를 선도하는 것이 필요함

– 국내외 기술개발 현황분석에 따른 세부 전략

- i-PIN은 인터넷 포털 등에서 주민등록번호 대신 사용자 본인확인 시 활용될 수 있도록 기술 개발이 완료된 상태이며, 일부 인터넷 서비스 사이트에 적용되어 있는 상황임
- ETRI, KISA, MS는 전자ID지갑 과제를 통해 현재의 i-PIN을 고도화하는 기술을 개발하고 있음
- 주민등록번호를 인터넷 상에서 대체하는 본인확인기술은 국내만 보유한 기술로, 국제적으로 아직 필요성이 공감되고 있지 못하고 있는 상황임. 따라서 국제 환경에 맞는 i-PIN 규격을 개발하여 ITU-T에 기고하여 국제 표준화를 선도하는 것뿐만 아니라 i-PIN이 활용될 수 있는 환경을 가진 국가와의 협력 또한 매우 필요함

– 국내 IPR 보유 현황분석 및 확보가능성 분석에 따른 세부 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 필요

– 국내 표준화 인프라 수준 분석에 따른 세부 전략

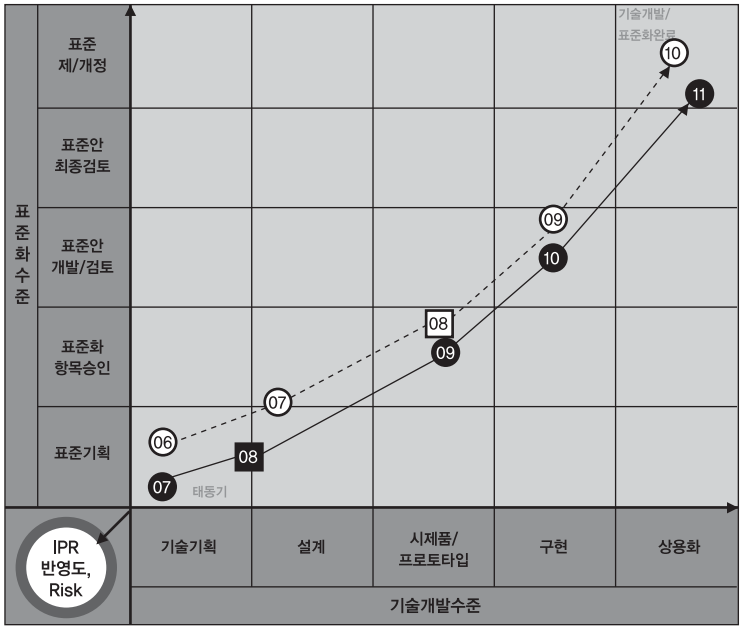
- 2008년 8월 결성된 디지털ID 관리 포럼, TTA 개인정보보호 및 ID 관리 프로젝트 그룹(PG 502) 등 국내 표준화 인프라 수준은 높은 편이며, 이들 기반과 인력을 활용하여 국제 환경에 맞는 본인확인 기술을 개발하여 국내 및 국제 표준화를 진행하는 것이 필요함

– 국제표준화 기여도 분석에 따른 세부 전략

- 본인확인기술은 국제적으로 아직 표준 수요가 거의 발생하고 있지 않은 분야이기 때문에, 본인확인기술이 적용 가능한 환경을 가진 국가를 발굴하여 국제적으로도 필요한 기술이라는 공감대를 형성하는 노력이 우선적으로 필요하며 이후 국제 환경에 맞는 i-PIN 기술을 개발하여 국제 표준을 선도하는 것이 필요

3.3.12. 사용자단말 개인정보 관리

○ 표준상태전이도(표준화 & 기술개발 연계분석)

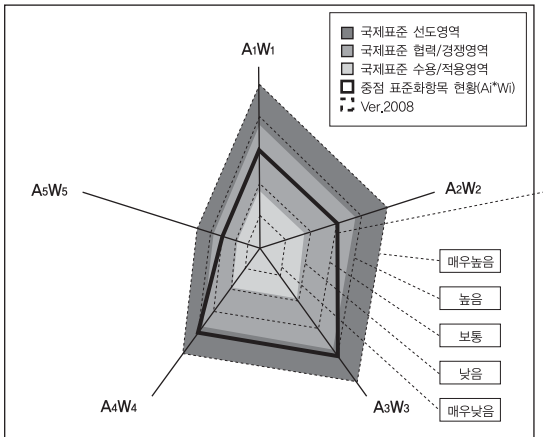


표준화 중요도	국내개발주체		관련 국제 표준화 기구
고(★★★) 중(★★) 저(★)	표준개발	기술개발	
★★	TTA ID관리포럼	ETRI KISA	ITU-T IETF

범례

- 08 중점 표준화항목의 국내상태
- 08 중점 표준화항목의 국제상태
- → 중점 표준화항목의 국내 표준상태전이
- -▸ 중점 표준화항목의 국제 표준상태전이
- ↑ 선행표준(선 표준화 후 기술개발)
- ↗ 동시표준(표준화 & 기술개발 동시추진)
- → 후행표준(선 기술개발 후 표준화)

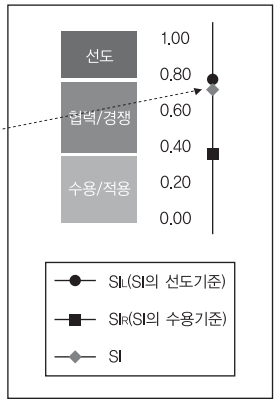
○ 국제표준화 전략목표 도출



A1 : 국외대비 국내표준화수준
A2 : 국외대비 국내기술개발수준
A3 : IPR확보가능성
점선 : Ver.2008현황

A4 : 국내표준화 인프라수준
A5 : 국제표준화 기여도
Wi : Ai의 가중치

SI(표준화 전략지수)	
SI_L (SI의 선도기준)	0.75
SI_R (SI의 수용기준)	0.35
SI	0.69



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

$$(0 \le W \le 1, 0 < SI \le 1)$$

국제표준 협력/경쟁 (선도)(Ver.2009)

○ 세부전략(안)

– 국내에서는 보안토큰 관련 표준으로 PKCS#11 프로파일 표준이 제정되어 있으나, 다양한 기술이 연계되어야 하는 특징으로 인해 사용자단말 개인정보 관리 기술에 대한 표준화는 더딘 상황. 따라서, 국내에서 기술의 바람직한 방향 제시를 위한 표준화 기술 항목을 도출하고 이를 통해 국제 표준을 선도하는 것이 필요

○ 항목별 전략

– 국내외 표준화 현황분석에 따른 세부 전략

• 국내에서는 인증서를 안전하게 보관하기 위한 보안토큰 관련 표준으로 PKCS#11 프로파일 표준이 제정되어 있으며, 국제적으로는 RSA의 de-factor 표준인 PKCS 시리즈 표준이 제정된 상태임

• ETRI는 2009년 9월 ITU-T SG17 Q.9에 'Security requirements and reconfiguration for mobile multi-homed wireless communication' 라는 제목으로 모바일 멀티홈드(multi-homed) 장치에서 발생하는 보안 위협과 보안 요구사항을 정의하고, 이를 위한 보안 서비스 시나리오를 개발하기 위한 표준화 과제를 제안하여 X.msec-5라는 신규 표준과제로 승인을 받음

• 사용자단말 개인정보 관리 기술은 단일 기술만으로 이루어지지 않고 다양한 기술이 서로 연계하여야만 구현될 수 있는 기능이어서 표준화에 있어서는 그 진척이 더딘 상황임. 따라서, 국내에서 기술의 바람직한 방향 제시를 위한 표준화 기술 항목을 도출하고 이를 통해 국제 표준을 선도하는 것이 필요

– 국내외 기술개발 현황분석에 따른 세부 전략

• 키보드보안이 널리 사용되고 있으나 궁극적으로 키보드 입력에 대한 방어가 되지 않고 있으며 사용자 환경의 다양함으로 방어기술 적용에도 어려움을 겪고 있음

• 금융권에서 일회용패스워드(OTP)를 도입하여 배포되고 있으나 일회용패스워드 자체가 지니는 오류 허용으로 인해 그 취약점이 노출되어 있고 한 개로 여러 기관이 사용을 하고 있는 상황이어서 그 공격은 더욱 쉬워지고 방어가 어려운 상황임. 최근 등장한 콤후킹(COM Hooking)과 메모리 해킹은 조작된 정보가 사용자의 눈에는 정당한 것으로 보여 사용자가 공격 사실을 인지하지 못하게 하는 공격 방법으로 보안을 네트워크 영역에서 프리젠테이션 영역까지 확대 적용할 필요가 있음

• 기술에 있어서 국내가 많이 뒤쳐져 있었으나 최근 금융권과 공공분야에서의 필요성에 의하여 빠른 속도로 추격을 하고 있으며 국내 서비스 환경이 국제 수준보다 더 높은 수준을 요구하고 있어 빠른 시간 안에 기술 격차를 줄일 수 있는 기회가 형성되고 있음

– 국내 IPR 보유 현황분석 및 확보가능성 분석에 따른 세부 전략

• 사용자단말 개인정보 보호에 대한 IPR은 미흡한 상태지만, 기술적인 격차가 줄어든 지금이 IPR 확보에 적기이며 이를 위해 IPR이 가능한 기술 분야를 도출하고 도출된 분야에 표준화 역량을 집중하는 것이 필요함

– 국내 표준화 인프라 수준 분석에 따른 세부 전략

• 2008년 8월 결성된 디지털ID 관리 포럼, TTA 개인정보보호 및 ID 관리 프로젝트 그룹(PG 502) 등 국내 표준

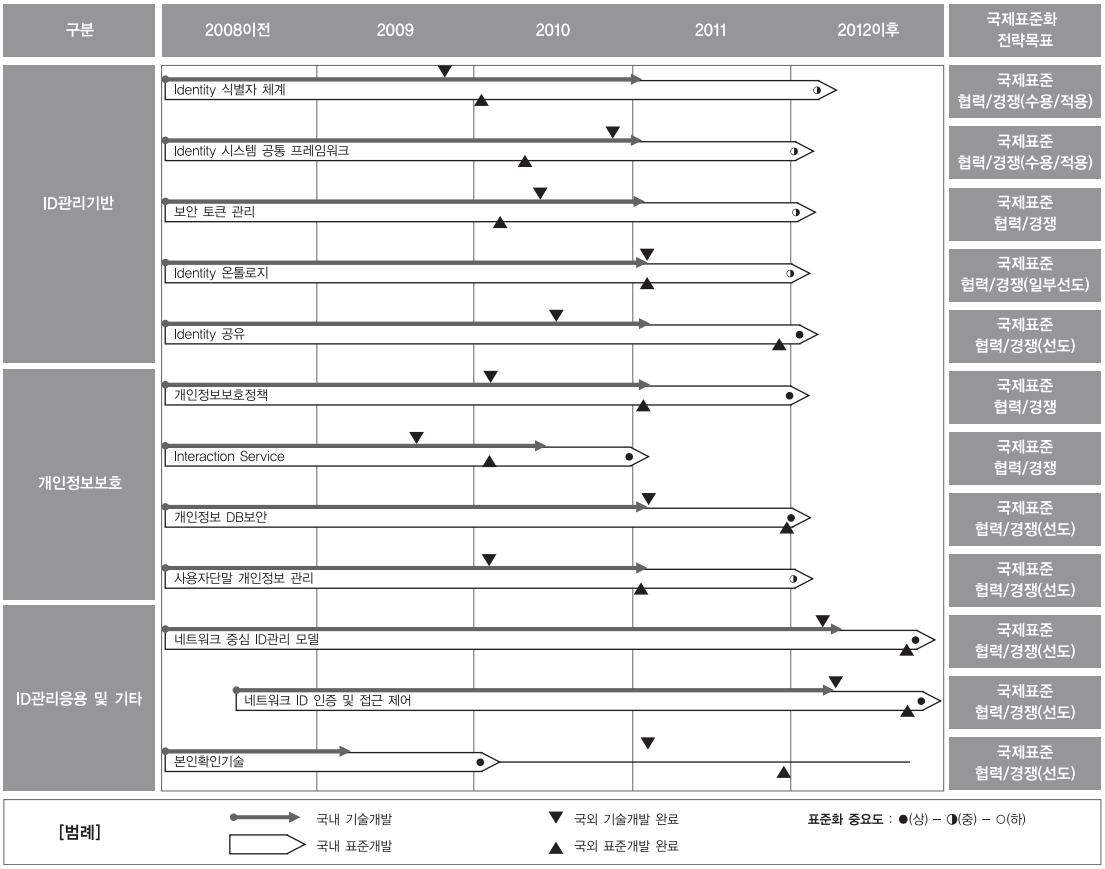
화 인프라 수준은 높은 편이며, 이들 기반과 인력을 활용하여 국내 및 국제 표준화를 진행하는 것이 필요함

– 국제표준화 기여도 분석에 따른 세부 전략

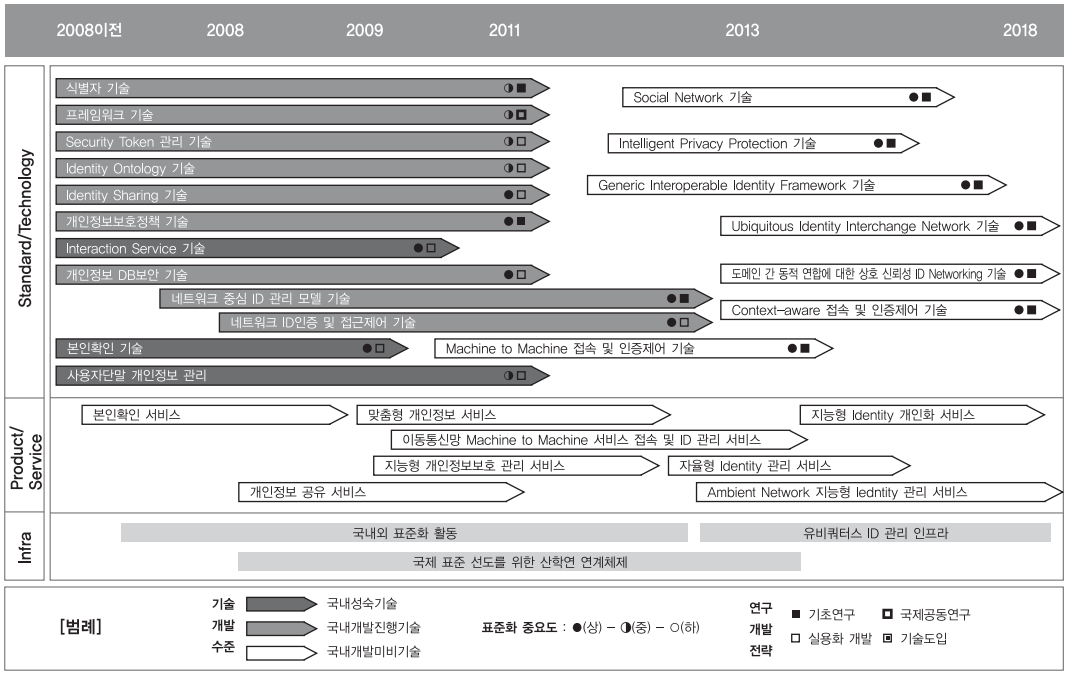
- 사용자단말 개인정보 보호에 대한 국제 표준화 단체의 활동은 매우 미흡한 실정이기 때문에, 국제 표준화의 필요성을 이해시키고 국내에서 개발된 기술이 국제 표준화 단체의 표준으로 채택되도록 하는 노력이 필요함

3.4. 중장기 표준화로드맵

3.4.1. 중기('09~'11) 표준화로드맵



3.4.2. 장기 표준화로드맵(10년 기술예측)



[국 · 내외 관련표준 대응리스트]

구분	표준명	기구(업체)	제정연도	재개정현황	국내관련표준	국내 추진기구
ID관리 및 개인정보 보호	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	제정 중	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	2005	제정	-	TTA
	ID-WSF Discovery Service	Liberty Alliance	2005	제정	-	TTA
	ID-WSF Interaction Service 2.0	Liberty Alliance	2005	제정	-	TTA
	P3P(Platform for Privacy Preferences) 1.1	W3C	2006	제정	-	TTA
	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	제정	TTAS.OT-10.0040/R1	TTA
	i-PIN 서비스 프레임워크	TTA	2007	제정	TTAS.KO-12.0055	TTA
	i-PIN 서비스 전달 메시지 형식	TTA	2007	제정	TTAS.KO-12.0055	TTA
	Q.3201 Signalling Requirements and Protocols – EAP-based security signalling protocol architecture	ITU-T SG11	2007	제정		TTA
	Q.3202.1 Authentication protocols for interworking among 3GPP, WiMax and WLAN in NGN	ITU-T SG11	2008	제정		TTA
	Q.sup.58 Organization of transport user data	ITU-T SG11	2008	제정		TTA
	TS 43.020 "Security-related network functions"	3GPP	2001	제정		TTA
	TS 33.102 "3G security; Security architecture"	3GPP	2001	제정		TTA
	TS 33.203 "IMS security"	3GPP	2003	제정		TTA
	TS 33.210 "Network domain security: IP layer"	3GPP	2004	제정		TTA
	TS33.108 "Handover interface for Lawful Interception" (created by SA3 LI subgroup)	3GPP	2004	제정		TTA
	TS 33.220-222 "Generic Authentication Architecture"	3GPP	2004	제정		TTA
	TS 33.234 "WLAN interworking security"	3GPP	2005	제정		TTA
	TS 33.246 "Security of MBMS"	3GPP	2005	제정		TTA
	TS 33.310 "Network domain security: Authentication Framework"	3GPP	2006	제정		TTA
	TR 33.978 "Early IMS security"	3GPP	2006	제정		TTA
	TS 55.205 "GSM-MILENAGE algorithms: An example algorithm set for A3 and A8"(originated by SAGE)	3GPP	2006	제정		TTA
	TS 55.216-218 "A5/3 and GEA3 specifications" (originated by SAGE)	3GPP	2006	제정		TTA
	TS 43.020 "Security-related network functions"	3GPP	2006	제정		TTA

구분	표준명	기구(업체)	제정연도	재개정현황	국내관련표준	국내 추진기구
	TS 33.110 Key establishment between a UICC and a terminal	3GPP	2006	제정		TTA
	TS 33.204 Network Domain Security; Transaction Capabilities Application Part(TCAP) user security	3GPP	2007	제정		TTA
	확장형 자원 식별자(XRI) 문법 V2.0	TTA	2008	제정 중	–	TTA
	공통 아이덴터티 데이터 모델	TTA	2008	제정 중	–	TTA
	상호호환성 및 신뢰를 위한 글로벌 ID 관리 시스템 요구사항	TTA	2008	제정 중	–	TTA
	개인정보 DB 관리 기술의 보안요구사항	TTA	2008	제정 중	–	TTA
	프라이버시 강화형 역할기반 접근통제 정책언어	TTA	2008	제정 중	–	TTA
	자기통제 강화형 디지털 아이덴터티 공유 프레임워크	TTA	2008	제정 중	–	TTA
	확장성 접근제어 생성언어 3.0	TTA	2008	제정 중	–	TTA
	i-PIN 서비스 중복가입 확인정보	TTA	2008	제정 중	–	TTA
	i-PIN 서비스 전달 메시지 형식	TTA	2008	제정 중	–	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] GUIDE, http://istrg.som.surrey.ac.uk/projects/guide/

[09] Higgins Project, http://www.eclipse.org/higgins/

[10] ID 관리 기술 및 표준화 동향, 한국정보과학회 정보과학회지, 2007.5

[11] IDC, "Worldwide Identity and Access Management 2007-2011 Forecast and 2006 Vendor Shares", 2007.7

[12] IDC, "Worldwide Identity Theft Black Market 2006-2010 Forecast", 2006.12

[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 17, http://www.itu.int/ITU-T/studygroups/com17/index.asp

[19] ITU-T Living List of Identity Management Forums, http://www.ituwiki.com/index.php?title=Living_List_of_Identity_Management_Forums

[20] ITU-T SG13 국제표준회의 참가보고, TTA 저널, No. 111, TTA, 2007.5

[21] Joaquin Miller, SXIP Specification, Version 1.0, http://yadis.org/papers/yadis-v1.0.pdf

[22] Liberty Alliance http://projectliberty.org/

[23] MIC & KISA, "u-정보보호 마스터플랜," 2006.10

[24] NIST, An Ontology of Identity Credentials Part 1: Background and Formulation, NIST SP 800-102 Draft, 2006. 10.

[25] OASIS SAML(Security Assertion Markup Language) v2.0 고찰 및 응용, 한국멀티미디어학회 학회지, 2006.3

[26] OASIS, Extensible Resource Identifier(XRI) TC , http://www.oasis-open.org/committees/xri/

[27] OASIS, OASIS News, http://www.oasis-open.org/news/

[28] OASIS, Security Services(SAML) TC, http://www.oasis-open.org/committees/security/

[29] OASIS, XRI Data Interchange(XDI) TC, http://www.oasis-open.org/committees/xdi/

[30] OECD WPISP, "Background paper on digital identity management," 2006.10

[31] OpenID Community, http://openid.net/

[32] OpenID 국내 커뮤니티, http://openid.or.kr/

[33] Password Manager XP, http://cp-lab.com/

[34] PRIME, https://www.prime-project.eu/

[35] Scott Kveton, The State of OpenID, http://openid.net/pres/openid-solt-final.pdf

[36] Security-Enhanced Callback URL Service in Mobile Device, ICACT 2007, 2007.2

[37] Shibboleth Project, http://shibboleth.internet2.edu/

[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, SAM08 - The 2008 Internation Conference on Security and Management, 2008.7.15

[44] Windows CardSpace, http://cardspace.netfx3.com/

[45] Windows Communication Foundation(WCF), http://wcf.netfx3.com/

[46] 국내외 ID관리 기술 표준화 동향, 주간기술동향, 2008-07-16

[47] 방송통신위원회, 인터넷 정보보호 종합대책, 2008.7.22

[48] 사용자 중심 ID 관리 기능을 제공하는 전자ID지갑 시스템, 전자통신동향분석, 2008.8.15

[49] 사용자 중심의 ID관리 프로젝트 동향, 주간기술동향, 2008.7.9

[50] 신원도용 대응기술 동향, 주간기술동향, 2006.9

[51] 오픈소스 ID관리 프로젝트 동향, 주간기술동향, 2007.6

[52] 웹환경에서 정책기반 개인정보호 기술, 전자통신동향분석, 2007.8

[53] 유럽의 eID 기술동향, 주간기술동향, 2006.6

[54] 인터넷 ID 관리 서비스, 전자통신동향분석, 2005.2

[55] 인터넷 환경에서의 Identity 공유 기술 동향, 주간기술동향, 2007.6

[56] 인터넷ID관리시스템 개요 및 비교, 전자통신동향분석, 2007.6
[57] 인터넷식별자포럼, http://www.uriforumor.kr/
[58] 한국IDC, "Korea Security Software 2008-2012 Forecast and Analysis", 2008.7.10
[59] 한국전자통신연구원, "Digital Identity Management - 2007년 기술 백서", 2007.11
[60] 한국정보보호진흥원, "2007 국내 정보보호산업 시장 및 동향 조사", 2007.11
[61] 한국정보보호진흥원, "개인정보의 경제적 가치 연간 약 1조 3천억 원에 달해", 2007.1
[62] 한국정보보호진흥원, 디지털 ID현황 및 정책적 시사점, 2007.6

[약어]

3GPP	3rd Generation Partnership Project
adapID	advanced applications for electronic Identity cards in Flanders
FFIEC	Federal Financial Institutions Examination Council
FIDIS	Future of Identi쇼 in the Information Society
GAA	Generic Authentication Architecture
GBA	Generic Bootstrapping Architecture
GRS	Global Registry Service
GSS	Global Services Specifications
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
IMRA	Identity Management Readiness Assessment
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
TVRA	Threat, Vulnerability, and Risk Assessment
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
URN	Uniform Resource Name
W3C	World Wide Web Consortium
WCF	Windows Communication Foundation
WSDM	Web Services Distributed Management
WSIT	Web Services Interoperability Technologies
WS-Security	Web Service Security
XACML	eXtensible Access Control Markup Language
XDI	XRI Data Interchange
XRI	eXtensible Resource Identifier