

## 유럽의 eID 기술 동향

김승현\* 조진만\*\* 진승현\*\*\* 정교일\*\*\*\*

정보 기술이 발전함에 따라 디지털 정보로 개인의 특성을 표현할 수 있는 방법들이 늘어나고 있다. 하지만 기존의 방법으로는 개인들을 제대로 식별하기 어려워지고 있다. 유럽 연합은 매우 활발한 eID 관련 프로젝트를 운영하고 있으며, 개인의 프라이버시를 보장하면서 신뢰와 보안을 제공해주는 기술을 개발하고 있다. eID는 전자 신원을 의미하는 용어로서, 사용자의 식별, 인증, 그리고 전자 서명 기능을 통해 온·오프라인 환경에서 사용자의 신원을 안전하고 신뢰성있게 관리하는데 사용된다. eID 관련 기술을 연구하는 대표적인 프로젝트로는 GUIDE, FIDIS, PRIME 등이 있으며, 관련 정책을 연구하는 프로젝트로는 Modinis 등이 존재한다. 본 기고서에서는 이들 프로젝트를 살펴봄으로써 eID 관련 기술의 현황과 향후 방향에 대해 알아보았다



### 목 차

- I. 서 론
- II. 유럽의 eID 연구 프로젝트
- III. eID의 상호호환성
- IV. 결 론

### I. 서 론

eID란 '전자 신원(electronic Identity)'을 의미하는 용어로서 정부와 같은 신뢰 기관이 공인한 전자 신분증들이 eID에 해당한다. eID는 기업의 사원증, 회원 카드를 비롯하여 전자 여권, 시민카드, 전자 건강 카드와 같은 물리적인 형태에 국한되는 것이 아니라, 공인인증서나 특수한 방식의 보안 인증 체계와 같이 다양한 미디어나 토큰에 구축될 수 있는 컨셉 및 절차까지도 포함된다.

eID는 사용자의 식별, 인증, 그리고 전자 서명에 주로 사용되며 관리 절차를 간소화하고 서비스를 효율적으로 제공하는 것이 주요 목적이다. eID는 대상 응용 분야나 사용 환경에 따라 구분되는 특징을 가지고 있으며, 전자 건강 카드나 사회 보장 카드와 같은 eID는 특정한 분야에만 사용되기도 한다. eID는

\* ETRI 디지털 ID 보안연구팀/연구원  
 \*\* ETRI 디지털 ID 보안연구팀/선임연구원  
 \*\*\* ETRI 디지털 ID 보안연구팀/팀장  
 \*\*\*\* ETRI 정보보호기반연구그룹/그룹장

여러가지 정보를 저장하여 다양한 용도로 사용될 수 있으며, 그림 1 은 eID 가 활용될 수 있는 여러 분야들을 보여주고 있다.

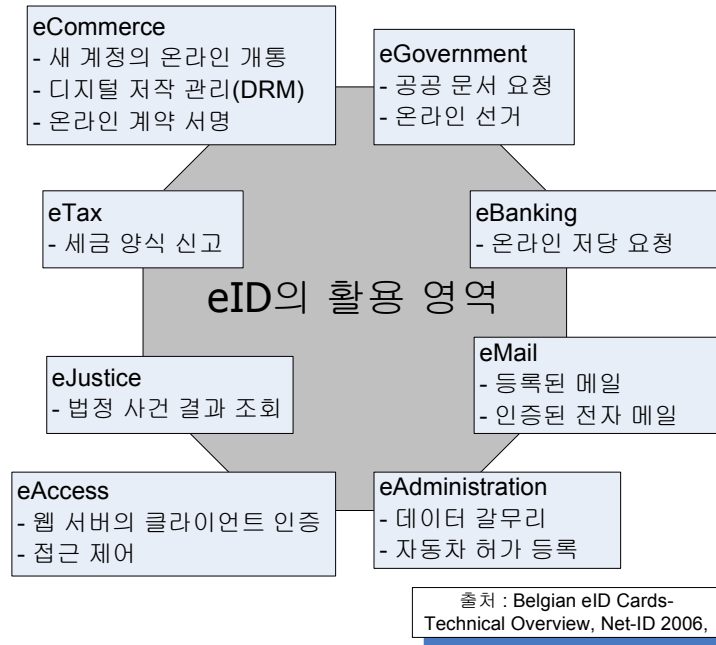


그림 1 eID 의 활용 영역

eID 는 기존의 오프라인에서 사용되는 신원 확인 정보를 대체하여 더욱 안전하고 신뢰성 있는 개인의 식별을 가능하게 하며, 온라인 환경에서도 일관성있게 사용할 수 있다는 이점이 있다. eID 가 주로 제공하는 기능들은 다음과 같다.

- 식별(Identification) – eID 소유자의 신원을 확인할 수 있는 정보 제공(이름, 생년 일자 및 장소, 주민등록번호 등)
- 인증(Authentication) – 유효한 토큰을 발급하여, eID 소유자가 정당하게 식별된 사용자임을 증명함
- 디지털서명(Digital Signature) – 특정 거래가 eID 소유자에 의해 분명히 허가받았음을 증명함

eID 는 단순히 기술적 측면에서 접근해야 하는 차원의 문제가 아니다. 사회, 경제, 법률과 같이 여러 분야에 영향을 미칠 수 있는 기술이기 때문에 eID 를 사용하기 위해서는 다양한 관점이 요구된다. 그러나 본 기고문에서는 우선 프라이버시, 보안, ID 관리와 같이 기술적인 관점에 국한하여 eID 를 바라봄으로써 eID 의 특성을 쉽게 이해할 수 있도록 한다.

프라이버시 관점에서는 eID 를 사용하는 과정에서 개인의 프라이버시가 보장되는지 여부를 살펴본다. eID 와 관련된 정부의 법적 규제 항목은, 매우 엄격하고 세밀한 평가를 통해 프라이버시를 보호하고 있다. 예를 들어 유럽의 공정 정보 활용법 또는 데이터 보호 법안을 살펴보면, 데이터의 저장과 사용 목적은 미리 고지되어야 하고 데이터는 해당 목적에만 사용될 수 있으며 데이터 처리에 대한 정보가 궁금한 개인은 누구나 이를 열람할 수 있음을 명시하고 있다. 프라이버시를 보호하기 위해서는 개인이 자신의 정보를 직접 제어할 수 있어야 하고, 누가 무엇을 알고 있는지, 데이터가 어떻게 처리되는지를 인식해야 한다. 또한 사용자의 명백한 동의 없이 자동적으로 절차가 진행되는 것은 매우 심각한 문제이며 지양해야 한다. eID 가 고려해야 하는 프라이버시 항목을 정리하면 다음과 같다. [1]

- 데이터 최소화 - 해당 목적에 필요한 데이터만 저장하고 사용해야 됨. 데이터 간의 연관 관계를 추적하지 않으며, 개인 데이터는 사용 즉시 폐기함.
- 데이터의 분리 - 사용자를 식별하기 위하여 다른 사용자와 구분되는 데이터를 의도적으로 저장하지 않으며, 포괄적인 데이터를 보유하거나 중앙화된 DB 를 구축하는 것은 회피해야 됨.
- 자신의 프라이버시를 보호하기 위한 권한 부여 - 본인의 개인 정보에 접근하여 데이터를 삭제할 수 있는 권리를 제공하고, 법적으로 무력화 할 수 없는 경우에는 동의 내용을 취소할 수 있음

보안 관점에서는 신원과 관련된 모든 정보들을 eID 가 적절히 보호하는지를 고려한다. 가장 분명한 목표는 eID 가 데이터의 무결성을 보호하고, 관리자가 내리는 결정을 신뢰하는 것이다. 왜냐하면 이 절차들은 eID 데이터에 영향을 미칠 뿐만 아니라 심지어 전체 과정을 제어할 수 있기 때문이며, 모든 관리(governmental) 활동의 핵심이므로 개인 뿐만 아니라 특정 그룹이나 사회 전체까지 영향을 미칠 수 있다. 따라서 중요한 보안 요구사항인 신뢰성, 무결성, 가용성은 다양한 솔루션을 통해 반드시 지원되어야 하며, 이들 요구사항은 eID 매체에 저장된 모든 데이터

와 저장소가 관리하는 데이터, 그리고 통신 네트워크를 통해 이동되는 데이터에도 반영되어야 한다. 예를 들어 모든 통신은 종단간(end-to-end) 암호화와 같이 안전한 채널을 통해 이루어져야 하며, 추가로 네트워크 통신 레벨에서 데이터를 보호해야 하거나 사용자의 특정 행동을 보호해야 할 지점에서는 익명화된 상태로 개인이 행동할 수 있어야 한다. 익명화된 상태지만 증명서 변환을 통해 계정을 추적할 수 있는 방법을 통해 통신상의 프라이버시와 보안이 동시에 지원될 수 있다. 또한 ID 도용을 막기 하여 eID 를 사용하기 전에 인증을 요구하고, 타인의 신원을 도용하기 어렵도록 처리 단계를 복잡화하는 방안들이 고려되고 있다.

eID 에서 사용되는 ID 관리는 안전하고 신뢰성 있는 통신을 제공하는 것과 개인의 프라이버시 공간을 제어하는 것을 주요 목표로 한다. eID 는 상황에 따라 개인의 신원 정보 중의 일부를 선택적으로 사용할 수 있기 때문에, 신원 정보를 분리시켜 개인이 원하지 않는 프라이버시 침해 를 예방한다. 또한 eID 는 본인의 신원을 스스로 관리할 수 있는 기술들을 제공한다. 사용자는 본인의 신원 정보를 누가 알려고 하는지를 알게 되고, 사용자가 원하는 만큼의 정보를 제공할 수 있다.

## II. 유럽의 eID 연구 프로젝트

유럽 연합(EU: European Union)은 개인의 프라이버시를 보장하는 동시에 신뢰와 보안을 제 공해주는 기술을 연구하고 있다. 정보 기술이 발전함에 따라 디지털 정보로 개인의 특성을 표현 할 수 있는 방법들이 늘어나고 있으며, 기존에 제안된 방법으로는 개인들을 제대로 식별하기 어 려운 상태이다. 새로운 방법들은 별명(pseudonym)과 익명성(anonymity)과 같이 프라이버시를 보호해주는 특징을 보유하고 있으며, 보안 및 편리성을 제공한다. 이들 새 신원(Identity)들을 통 해, 사회와 비즈니스 세계가 변화하고 있으며 신원의 전통적인 의미마저 바뀌어지고 있다.

이러한 정보 기술의 발전에 따라 유럽은 매우 활발하게 eID 관련 프로젝트를 운영하고 있다. eID 관련 기술을 연구하는 대표적인 프로젝트로는 GUIDE, FIDIS, PRIME 등이 있으며, 관련 정 책을 연구하는 프로젝트로는 Modinis 등이 존재한다. 본 기고서에서는 이들 프로젝트를 살펴봄 으로써 eID 관련 기술의 현황과 향후 방향에 대해 알아보겠다.

### 1. FIDIS (Future of Identity in the Information Society)



IT 기술의 발달로 인해 현재의 eID 에 적용된 기술은 빠르게 대체될 전망

이다. ID 카드에 생체정보, PKI(공개키 기반 구조)와 같은 최첨단 기능이 도입되고 모바일 통신(GSM)과 같은 새로운 플랫폼에서도 전세계적으로 통용될 수 있는 ID 토큰 개념이 소개되고 있다. 또한 eID에 대한 인식도 변하고 있다. 주민등록번호처럼 단순히 숫자로 개인을 구분하는 것이 아니라, 개인의 신원을 나타내는 데이터들의 집합으로 신원을 구분하는 진화된 형식의 프로파일의 등장하고 있다. 게다가 유럽 연합은 eID 관리 시스템을 유럽 레벨에서 통합하여 제공할 의도를 가지고 있다. 기존에 유럽 국가들은 서로 다른 eID를 사용했지만, 유럽 연합은 이들 시스템들을 통합함으로써 중복되는 노력과 불편함을 극복한다. 하지만 ID 시스템들의 호환을 위해서는 여러가지 문제를 해결해야 한다.

FIDIS 프로젝트[2][18]는 유럽의 정보 사회에서 개인의 신원을 적절히 식별하기 위한 여러 계층의 이해를 구하고, 공정한 방법으로 ID 관리를 수행한다는 비전을 가지고 있다. 이를 위해 FIDIS는 유럽의 정보 사회에서 사용할 신원을 관리하기 위한 요구사항을 정립하고, 필요한 기술과 기반구조를 개발하고 있다. 또한 ID 도용과 프라이버시 문제를 해결하고 전 유럽에서 통용될 수 있는 신원 표현 방식과 식별 방식을 제공하려는 목표를 가지고 있다.

FIDIS 프로젝트는 2004년 4월 1일부터 2009년 3월 31일까지 5년의 과제 기한을 가지고 진행되며 24개의 산학연 컨소시엄이 10개의 워킹 그룹을 구성하여 프로젝트를 수행한다. FIDIS는 ID 관리 시스템, ID 법안, 유즈케이스와 같은 유럽 국가들의 연구 결과를 여러 관점에서 수집한 뒤에, 전문가들의 분석을 통해 이 정보를 활용한다. FIDIS는 아래의 7가지 분야로 연구 분야를 구성하고 있으며, 각 분야의 결과물들은 유럽의 연구 단체, 과학 커뮤니티, 표준화 단체, 정책 결정권자와 같은 다양한 계층에게 영향력을 미칠 것으로 전망하고 있다.

- ID(Identity)의 용어정리 및 파악
- 프로파일링
- 발행된 eID, ID 관리 시스템 간의 상호운용성
- 포렌식(forensic)
- 식별 제거(de-identification)
- 최신의 식별 기술
- 이동성을 고려한 신원

FIDIS 프로젝트는 기존의 연구 결과를 통합하고, 법적, 사회-경제학적, 사용성, 응용 등의 관

점에서 도출한 요구사항들, 공개 아키텍처와 스펙을 프로젝트의 결과물로 예상하고 있다. 현재 FIDIS 는 2 차년 과제를 수행중이며 표 1 의 결과물을 이미 도출한 상태이다..

**표 1 FIDIS 프로젝트의 결과물**

항목	내용
1 차 결과물(2004/2005)	Fidis Communication Infrastructure
	Inventory of Topics and Clusters
	Set of use cases and scenarios
	Models
	Overview on IMS
	Study on Mobile Identity Management
2 차 결과물(2005/2006)	Manual of the Extended Wiki System
	A study on PKI and biometrics
	Workshop on ID-Documents
	Structured account of approaches on interoperability
	Set of requirements for interoperability of Identity Management Systems
	A survey on legislation on ID theft in the EU and a number of other countries
	Forensic Implications of Identity Management Systems
	Descriptive analysis and inventory of profiling practices
	Report on Actual and Possible Profiling Techniques in the Field of Ambient Intelligence
	Implications of profiling practices on democracy
	A Specification for FIDIS Journal

## 2. GUIDE



GUIDE[3]는 유럽 연합의 재정지원을 받는 기술 연구 프로젝트로서, 22개 기관의 컨소시엄으로 구성되어 있다. GUIDE 프로젝트는 유럽의 안전하고 상호운용성있는 전자정부를 위해 eID 서비스와 트랜잭션을 제공하는 기술적, 조직적, 정책적, 사회 경제학적인 아키텍처의 연구 및 기술 개발을 담당한다.

GUIDE의 비전은 EU의 전자정부 서비스를 제공하기 위한 아키텍처를 개발하고 유럽을 전자 정부 솔루션의 선두 주자로 자리매김하는 것이다. 이를 위해 GUIDE 프로젝트는 신원 인증 및 관리를 제공하는 공개 아키텍처를 개발하고 전 유럽의 상호 합의에 기반하여 eID 관리를 수행할 계획이다.

eID를 안전하게 관리하기 위해서는, 프라이버시에 대한 시민들의 우려 같은 사회/정책적 문제를 비롯하여 데이터 보호법 준수와 같은 복잡한 법적/정책적인 문제들이 고려되어야 한다. GUIDE의 목적은 eID를 위한 안전한 '공개 아키텍처' 솔루션을 만들어서 모든 요구 사항을 만족시키는 동시에, 기존의 유럽 국가들이 제공하는 서비스들간의 상호호환성을 보장하는 것이다. 이를 위해 프로젝트는 EU의 모든 국가들 간에 존재하는 제도상의 차이점을 극복하는 기술적, 정책, 단계적인 해결 방안을 연구하고 있다.

유럽 연합의 시민들은 타국의 직장, 여행 정보, 건강 관리에 관련된 사회 보장 접근 서비스를 사용하고 싶어 하지만, 현재는 모든 국가들이 독자적인 eID 솔루션을 가지고 있기 때문에 타국의 솔루션과는 호환되지 않는 실정이다. 유럽 레벨에서 효율적인 신원 검증과 인가 작업을 제공하기 위해서, GUIDE 프로젝트는 국가간의 호환 문제를 해결해주는 아키텍처를 만드는 것뿐만 아니라, 25개의 유럽 연합 가입국에게 경계없는 eID를 개발해야 하는 필요성을 인식시키고 있다. 또한 전자정부 솔루션을 위한 공개 신원 관리 아키텍처를 설립함으로써, GUIDE는 정부의 고수준 서비스를 비즈니스와 시민들에게 효과적으로 제공할 계획을 가지고 있다.

GUIDE 프로젝트는 절반 이상이 진행된 상황이며, 기반 기술, 법적, 정치적, 사회적 연구 분야의 작업이 이미 완료되었다. 최근에는 아키텍처 디자인이 완성되었고, 유효성을 검증하는 단계를 지나 2005년 겨울부터는 복잡성 증가 시험을 착수하였다. 아키텍처는 우선 E101 시스템에 구축되어 시험 과정을 거치게 되는데, 이 E101 시스템은 사회 보안을 관리하고 EU 내의 국가간 임시 근로자를 위한 보안 관리와 연금 분야를 담당하는 시스템이다. 2차 시험은 2006년 초에 수행되며 eProcurement 분야를 대상으로 한다.

GUIDE 프로젝트는 유럽 레벨에서의 ID 검증 절차를 수립함으로써, 더욱 안전하고 쉬운 방식으로 유럽 연합 국가 간의 어플리케이션이 호환될 수 있는 기반을 제공할 것이다. 시민과 업

계에서는 GUIDE 프로젝트를 통해 관료를 줄이고, 사기와 같은 범죄를 줄이며, 사용하기 쉽고 향상된 보안을 제공받을 것으로 기대하고 있다. GUIDE는 법이나 정책에 기대지 않고 유럽 레벨에서의 상호호환되는 eID 관리 절차를 체계화시켜, eID를 사용하는 전자정부의 모범을 보일 것이다.

### 3. MordinisIDM

MordinisIDM 프로젝트[4][16]는 벨기에의 K.U.Leuven, 오스트리아의 A-SIT, 벨기에의 Lawfort - ICT Law Department의 컨소시엄으로 구성되어 있다. 데이터 보호 기능을 제공하는 유럽 연합의 프레임워크 위에서 eID의 상호호환성 문제를 해결하는 것이 MordinisIDM 프로젝트의 목표이며, 각국의 법률과 문화적 차이를 고려하여 해결 방안을 도출하려고 한다. 이 프로젝트는 2005년 1월 1일부터 2007년 2월 28일까지 26개월 동안 수행된다.

MordinisIDM은 유럽 연합의 국가들을 대상으로 전자정부 서비스에서 사용하는 eID 관리 기술을 전파하려 한다. 이를 위해 한 국가의 전자정부 서비스 경계를 넘어서는 정책의 평가, 유럽 레벨에서 가능한 정책과 솔루션에 대한 향후 분석, ID 관리 시장 개발과 기술적 요구사항에 대한 정보 제공, 프레임워크 개발 방법론 제공, ID 관리 분야에서의 실제 활용 방안과 그에 대한 분석 등을 수행하고 있다. 또한 MordinisIDM 프로젝트는 국가 ID 관리 기반 구조와 정책에 대한 정보를 수집하고, 기존 모델의 어려움과 잠재적인 해결책에 대한 평가를 내린다. 그리고 분석을 통해 적절한 정책을 도출하고 형식화 하는 단계로 작업을 처리한다. MordinisIDM의 최종 목표는 전 유럽의 ID 관리 기술이 상호호환 되는 것이다.

MordinisIDM 프로젝트의 예상 결과물은 EU 멤버 국가와 유럽 위원회에 공개될 것이며, 브뤼셀에서의 5번의 워크샵과 ID 관리 리포트, 정기적인 뉴스레터, 전자정부를 위한 ID 관리 워킹 그룹의 운영을 수행할 계획이다. 이러한 예정에 따라 MordinisIDM 프로젝트는 2005년 5월, 2005년 11월, 2006년 2월까지 3번의 워크샵을 이미 개최하였다.

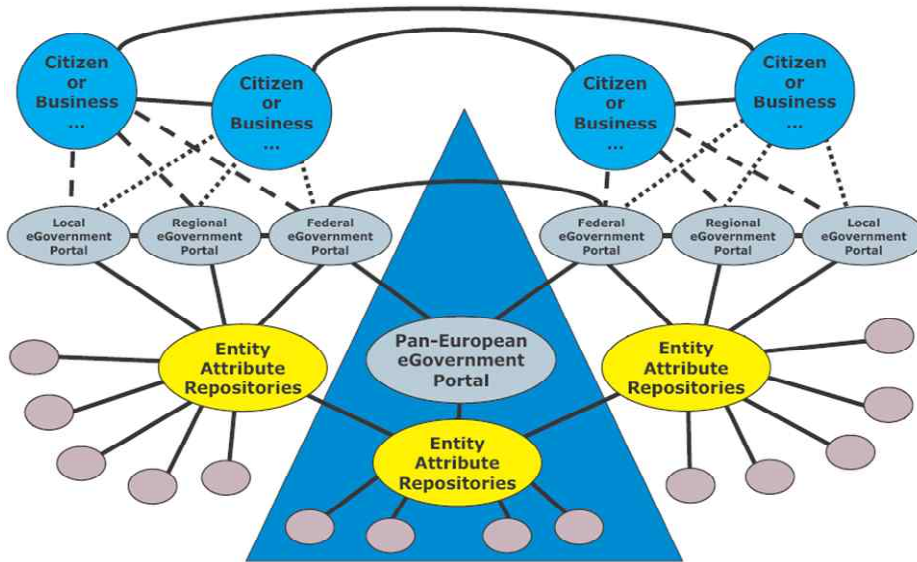


그림 2 MordinisIDM 프로젝트의 개념 프레임워크

#### 4. PRIME (Privacy and Identity Management for Europe)

디지털 사회는 모든 분야에서 이익을 가져오며, 개인화와 유비쿼터스 기술은 더욱 편리하고 효과적인 서비스를 제공하고 있다. 그러나 이 기술들은 개인의 프라이버시와 밀접한 관련이 있기 때문에 프라이버시 법과 같은 문제들이 우선 고려되어야 한다. 이를 위해 PRIME 프로젝트 [5][19][21]는 전송 레벨의 익명성을 비롯하여 최대한으로 사용자의 프라이버시를 제공하여, 디지털 사회에서 사용자들이 안전하게 자신의 개인 정보를 제어할 수 있는 방법을 제공하려고 한다. PRIME 프로젝트는 유럽 연합의 FP(Framework Programme) 6 와 스위스 연방 교육과 학청의 지원을 받고 IST[22]가 프로젝트를 통합 관리하고 있으며, 프로젝트 수행 기간은 4 년 (2004.3-2008.2)이고 예산은 1600 만 유로, 참가인원은 20 명이다.

PRIME 프로젝트는 사용자가 직접 eID 를 제어할 수 있는 시스템을 구축하려고 한다. 이론적 기술을 바탕으로 현재 유럽 연합의 IT 환경과 미래의 활용 방안을 고려하여, 프라이버시가 강화된 최신의 ID 관리 기술을 개발하는 것이 목적이다. 이를 위해 프라이버시와 보안을 만족시키는 수준의 통신과 검증 방법을 개발하고, 프라이버시 문제를 현실적으로 해결할 수 있는 대안을 고려한다. 또한 유럽의 프라이버시 법안과 규제를 기술적으로 지원하는 방법과, 개인에게 권한을 부여하여 프라이버시를 제어할 수 있는 정보의 자기 결정권(self-determination)을 제공하는

다. 이 기술들을 통해 PRIME 은 실세계에 활용될 ID 관리 솔루션을 개발한다. PRIME 프로젝트는 다음의 운영 원칙을 가지고 프로젝트를 진행하고 있다.

- 최대한의 프라이버시를 제공하는 설계
- 명시적인 프라이버시 규칙에 의거한 시스템 활용
- 프라이버시 규칙은 단순히 지적하는 것이 아니라, 실제로 적용되어야 함
- 신뢰할 수 있는 프라이버시 정책 적용
- 사용자에게 쉽고 직관적인 추상화 레벨의 프라이버시 제공
- 프라이버시에 대한 통합된 접근
- 응용 프로그램에 통합된 프라이버시

PRIME 프로젝트는 다섯 가지의 개발 계획을 가진다. 첫째로 요구 사항을 수집하고 이에 대한 평가를 수행한다. 수집되는 요구 사항은 법적, 사회-경제학적, 일반 어플리케이션까지 다양한 범위를 포괄한다. 두번째는 어플리케이션의 프로토타입을 개발하는 것으로, 실제 환경에서 PRIME 프로젝트가 지향하는 목표와 아키텍처 기술이 제대로 동작하는지를 검증한다. 현재 진행 중인 프로토타입으로는 온라인 헬스케어 시스템, 위치 기반 서비스, 프라이버시를 보호하는 고객 데이터베이스, 모바일 노동자를 위한 인프라의 익명 접근, E-Learning, 프라이버시가 강화된 유비쿼터스 기술 등이 있다. 세번째는 eID 관련 기술의 연구 개발이다. PRIME 프로젝트의 목표를 완수하기 위해서 고객의 프라이버시 요구사항에 맞는 서비스를 보장하는 기술, HCI(Human-Computer Interaction), 프라이버시 도메인에서 여러 프레임워크 간의 통신 고도화를 위한 온톨로지와 프라이버시 요소, 인가 모델, 암호화 기술, 통신 기반 구조, 사용자/서버 측 eID 관리가 v 필요하다. 네번째는 프레임워크와 아키텍처 구축이며, 그림 3 은 PRIME 에서 제안하는 아키텍처를 보여준다[20]. 그리고 다섯번째는 PRIME 아키텍처의 관리 및 확장이다.

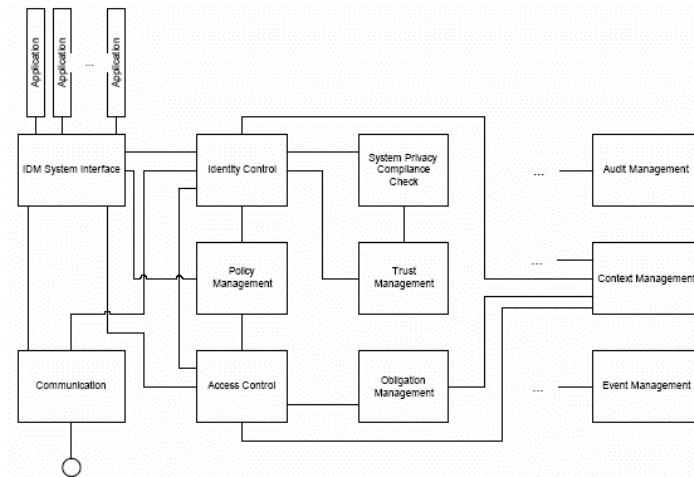


그림 3 PRIME 프로젝트가 제안하는 아키텍처

### 5. InspireD (Intergrated Secure Platform for Interactive Trusted Personal Devices)



스마트 카드는 전세계적으로 가장 널리 활용되는 모바일 컴퓨터 장비임에도 불구하고, 개인용 컴퓨터나 다른 네트워크 장비와 잘 호환되지 못한다는 문제가 있다. 새로운 응용 프로그램에 스마트 카드를 사용하기 위해서는 별도의 터미널이 필요하고, 느린 통신 프로토콜을 감수해야 하며, 부가적인 소프트웨어를 설치해야 된다. 이러한 문제는 스마트 카드 시장이 제대로 성장하지 못하게 만드는 요인이다.

유럽의 연구 프로젝트인 InspireD[6][7][17]의 주 목적은 이러한 격차를 줄이는 것이다. InspireD는 유럽의 스마트 카드 업체들에 의해 주도되며, 대형 스마트 카드 제조사와 반도체 공급자, 대학과 연구 기관을 비롯한 다양한 응용 분야를 포함하여 5개국의 18개 기관이 컨소시엄을 이루고 있다. InspireD 프로젝트는 2004년에 시작했으며 1700만 유로의 예산으로 3년 동안 프로젝트를 수행할 계획이다.

스마트 카드 산업이 성공하기 위해서는 안전한 접속 및 이동성과 보안을 중요하게 고려해야 하는데, 그러기 위해서는 스마트 카드의 근본 기술을 변화시켜야 할 뿐만 아니라 새로운 방식의 공개 기술 플랫폼을 만들어야만 한다. 스마트 카드는 안전하고, 개인적이며 휴대할 수 있는 1세대 장치로서 수백만의 사용자에게 은행과 통신사와 같은 오프라인 서비스를 사용할 때 주로 활

용되었다. InspireD 프로젝트는 제 2 세대 장치로 새롭게 개발된 스마트 카드를 제안하고, 여러 IT 응용 분야의 신뢰 개인 장치(TPD; Trusted Personal Device)에 스마트 카드를 통합하려 한다. 신뢰 개인 장치는 미래의 유비쿼터스 컴퓨팅 환경에서의 온라인 서비스를 제공하기 위해 필요하며, InspireD 는 차세대 통신 장비로 개인의 신뢰를 확장시킬 수 있게 된다.

InspireD 는 스마트 카드 분야에 특화된 유럽의 eID 프로젝트로, 하드웨어/소프트웨어 아키텍처와 개발 툴 개발을 담당한다. 스마트 카드의 모든 기술들을 새로 개발하며, 스마트 카드와 보안 산업을 위한 공개 플랫폼의 새로운 표준을 작성한다. 공개 플랫폼에는 실리콘 컴포넌트 플랫폼, 데이터 보호를 위한 암호와 보안 인증 프로토콜, 운영 시스템, 그리고 소프트웨어 응용 계층이 포함된다. InspireD 프로젝트는 다음을 목적으로 한다.

- 소프트웨어와 하드웨어를 위한 공개 아키텍처
- 네트워킹이 가능한 객체들
- 모든 설계 레벨에서의 보안 제공
- 생체정보 기술의 적용
- 프라이버시, 편리성, 신뢰 기능과 같은 최종 사용자들의 요구사항 반영

InspireD 프로젝트는 여러 워킹 그룹으로 구성되어 있으며, 각각의 워킹 그룹은 하드웨어와 소프트웨어의 분석, 디자인, 개념 구현뿐만 아니라 보안과 개발 툴의 구축을 담당한다. 그림 4 는 InspireD 프로젝트의 조직 구성을 보여준다. 향후에는 기술 활동뿐만 아니라 개념 전파, 표준화, 개발, 사용자 패널 조직과 같은 기술 외적인 활동이 이루어질 계획이다.

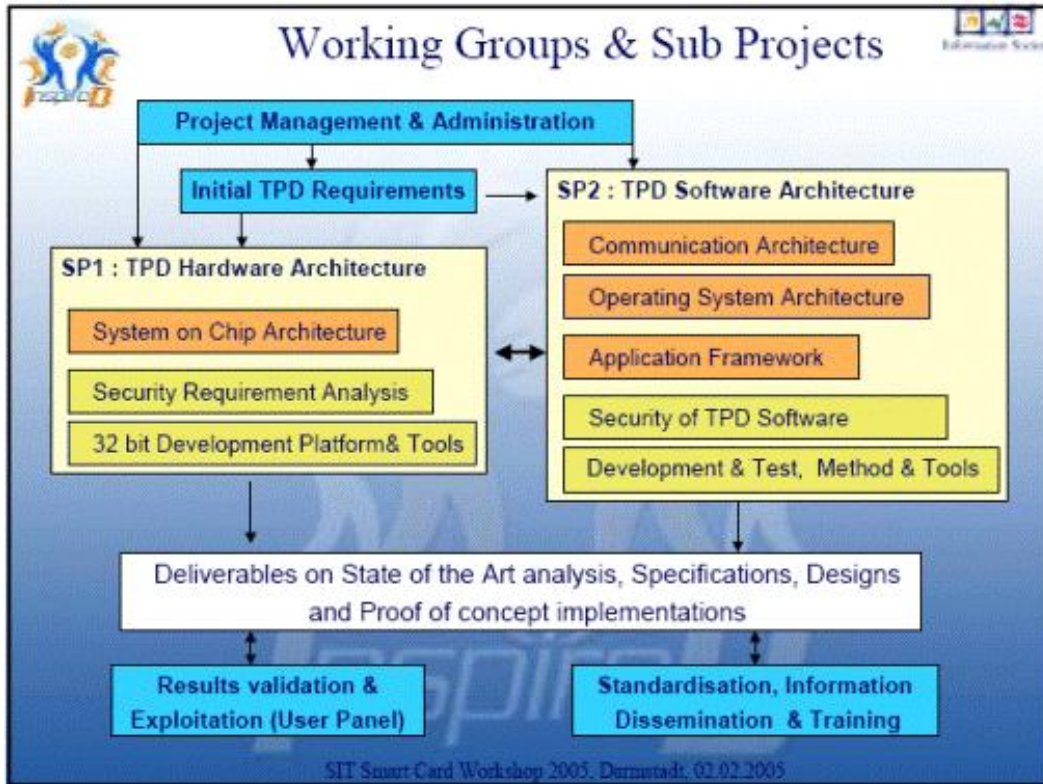


그림 4 InspireD 프로젝트의 구성도

InspireD 는 하드웨어에 대한 프로파일과 소프트웨어 아키텍처를 이미 작성한 상태이며, 그림 5 와 그림 6 은 해당 결과물을 보여주고 있다.

Profile ID	Name	Minimum RAM	Minimum Non Volatile Memory	ISO 7816 Data Transfer Rate	USB Data Transfer Rate	MMC Data Transfer Rate	Contactless NFC Data Transfer Rate	Contactless ISO Data Transfer Rate
S3	System on SIM	64 Kbyte	8 Mbyte 4 Gbyte (1)	128 Kbit/s 5 Mbit/s	1.5 Mbit/s 480 Mbit/s	-	106 Kbit/s 6670 Kbit/s	106 Kbit/s 847 Kbit/s (2)
S4	ContactMSC	64 Kbyte	8 Mbyte 4 Gbyte (1)	-	1.5 Mbit/s 480 Mbit/s	3 Mbit/s 20 Mbit/s	-	-
M3	System on Token	512 Kbyte	8 Mbyte 4 Gbyte (1)	-	1.5 Mbit/s 480 Mbit/s	-	-	-
M4	Combi SoT	512 Kbyte	8 Mbyte 4 Gbyte (1)	-	1.5 Mbit/s 480 Mbit/s	-	106 Kbit/s 6670 Kbit/s	106 Kbit/s 847 Kbit/s
M8	System on Card	512 Kbyte	8 Mbyte 4 Gbyte (1)	128 Kbit/s 5 Mbit/s	1.5 Mbit/s 480 Mbit/s	-	-	-

그림 5 InspireD 프로젝트에서 제안한 TPD 하드웨어 프로파일

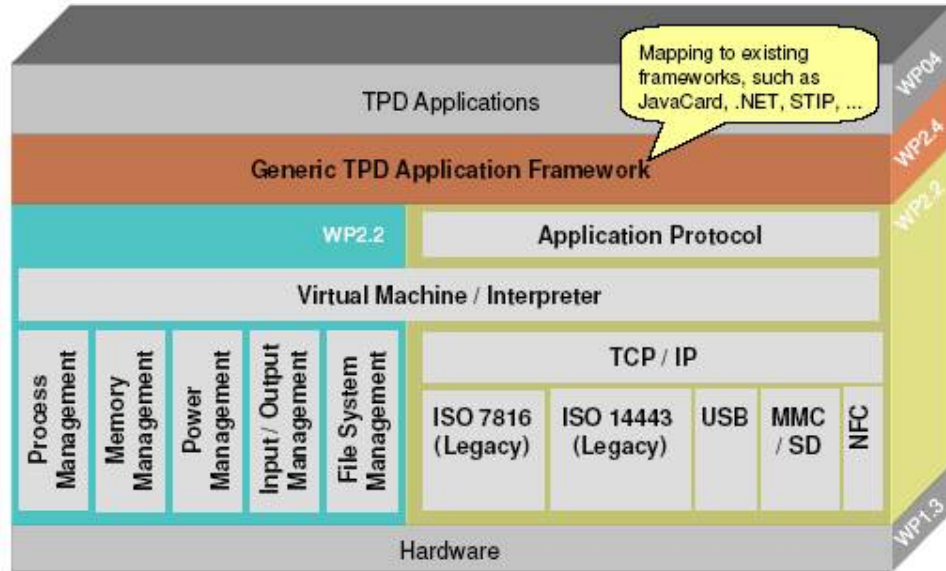


그림 6 InspireD 프로젝트에서 제안한 TPD의 소프트웨어 아키텍처

InspireD 프로젝트의 결과물은 특정 기술에 종속적이지 않으며, 향후 스마트 카드를 개발하는 과정에서 기능, 보안, 성능에 제한이 없다는 이점이 있다.

InspireD 프로젝트는 2004년에 요구 사항 분석과 아키텍처에 대한 초기 설계를 마쳤으며, 여러 종류의 TPD 프로파일에 대한 주요 컴포넌트와 인터페이스를 정의하였다. 기술 명세서와 보안 분석은 2005년에 완료되었으며, 현재는 개념을 증명하는 차원에서 스펙을 구현하는 단계이다.

## 6. DAIDALOS (Designing Advanced network Interfaces for the Delivery and Administration of Location independent, Optimised personal Service)



네트워크가 발전함에 따라 유럽 시민들은 직장, 교육, 레저 생활을 선택할 때, 언제 어디서나 온라인 서비스를 받는 것을 우선적으로 고려하게 되었다. 이렇게 빠른 사회 변화와 새롭게 등장하는 여러 서비스들은 네트워크 시스템을 복잡하게 만들었다.

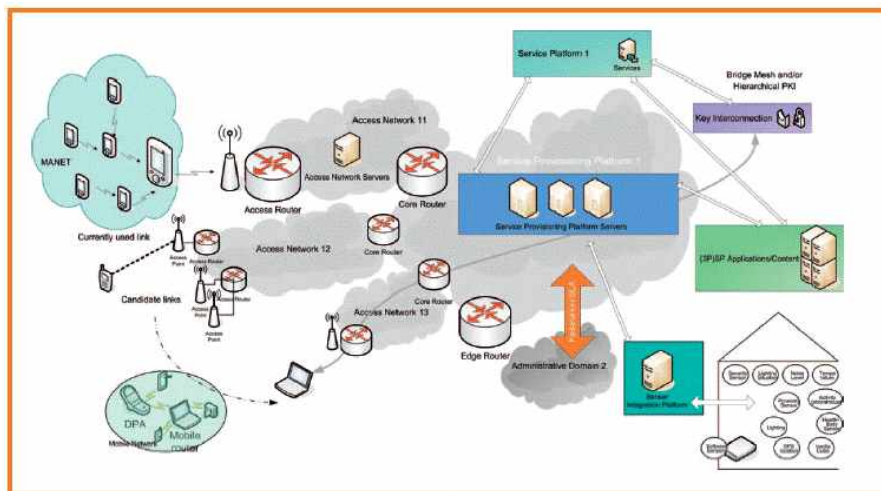
DAIDALOS[8]는 유럽 연합의 FP(Framework Programm) 6인 IST[22]가 관리하는 통합 프로젝트로서, 서로 다른 종류의 네트워크 기술을 통합하여 네트워크 관리자와 서비스 제공자에

게 이익이 되는 서비스를 창출하고, 사용자에게는 개인화된 음성, 데이터 멀티미디어 서비스 같은 부가 서비스를 제공한다는 비전을 가지고 있다. DAIDALOS 프로젝트의 예산은 1 단계에 2억 5700 만 유로였으며, 2 단계는 2억 2100 만 유로이다. 이 프로젝트의 1 단계에서는 46 개의 기업과 학계가 참여하였고, 2 단계에는 38 개의 기관이 컨소시엄을 구성하고 있다. 현재 DAIDALOS 프로젝트는 2 단계 과정을 수행중이며, 2008 년 말까지 진행될 예정이다.

DAIDALOS 프로젝트의 목적은 공통 네트워크 프로토콜(IPv6)에 기반한 공개 아키텍처를 개발하고 시연하는 것이며, 전체 목적은 다음과 같다.

- 설계, 프로토타입, 필요한 인프라와 컴포넌트의 검증을 통해 3 세대 통신 이후의 다양한 네트워크 기술을 커버할 수 있는 서비스를 효과적으로 분산함
- 상호보완적인 네트워크 기술을 통합하여 사용자를 중심으로 하는 유비쿼터스 서비스를 제공함
- 최적화된 신호 시스템을 개발하여 네트워크 통신과 관리 지원에 사용함
- 사용자를 중심으로 한 기술 개발을 통해 결과물을 시연함

DAIDALOS 프로젝트는 네트워크 아키텍처에 대한 근본적인 재고를 이끌어 내며, 이를 통해 사용자가 중심인 통신 인프라 세대를 만들 것으로 전망된다.



The Daidalos architecture introduces pervasive personalized services and mobility enabled broadcast

그림 7 DAIDALOS 아키텍처

DAIDALOS 프로젝트는 여러 워킹 그룹으로 나뉘어 연구 개발을 수행하고 있다. 프로젝트 관리 표준, 시나리오 및 아키텍처를 위한 요구사항 분석, 설계, 명세화, 평가 작업이 거의 완료된 상태이며, 향후에는 아키텍처를 실제로 개발하고 모든 서브 시스템들을 통합 운용할 계획이다.

### 7. adapID (advanced applications for electronic Identity cards in Flanders)

국가는 eID 를 통해 시민에게 편리하고 안전한 서비스를 제공해 줄 수 있게 되었다. 하지만 eID 에 적용된 국가 식별 번호, 공개키, 인증서와 같은 암호화 기능은 모든 응용 프로그램에서 접근할 수 있으며 시민들의 프라이버시를 침해할 수 있다는 우려를 안고 있다. 게다가 최종 시스템과 서비스에 대한 시민들의 신뢰 부족은 eID 도입을 저해시키는 요소이다.

adapID 프로젝트[9]는 플랑드르 지방의 연구원과 기업 대표자들의 컨소시엄으로 구성되었으며 2003년 발의되었다. 2004년 2월, 이 컨소시엄은 플랑드르 정부에게 현재 eID 카드의 프라이버시와 보안 문제를 설명한 리포트를 제출하였으며, 이 문제를 해결하는 방안으로 eID 카드를 새로 설계하기 위한 4년간의 산학 연구 프로젝트를 제안하였다. 2005년 초반에 adapID는 플랑드르의 과학 기술 정책 입법 회의(IWT-Flanders)로부터 재정적인 지원을 받기 시작했으며, 공식적으로는 2005년 7월 1일 프로젝트가 시작되고 2009년 6월 30일까지 진행될 예정이다.

adapID 프로젝트의 목표는 개인의 프라이버시가 고려된 보안 프레임워크를 개발하여 전자정부, e-health, 신뢰 보관 어플리케이션 등에 활용하는 것이다 또한 기술적, 법적 측면에서 프레임워크를 평가하는 동시에 강화된 버전의 eID 카드를 위한 기술을 조사한다.

adapID의 가장 큰 요구 사항은 사용자의 프라이버시를 보호하는 것이다. 사용자 신원 정보의 일부만으로도 대부분의 작업을 처리할 수 있기 때문에, eID 카드 소유자는 최소한의 정보만을 제공할 수 있어야 한다. 그리고 시민들은 각자 다른 별명(pseudonym)으로 각각의 조직에 인식되며, 이들 별명은 서로 연결되지 않아야 한다. 조직은 시민의 더 많은 개인 정보를 이끌어내기 위한 목적으로 DB를 결합시키면 안된다. 또한 eID 카드 소유자는 익명의 상태로 어플리케이션을 사용할 수 있어야 하며, 이 경우에 어플리케이션은 사용자를 식별하지 않아야 한다.

adapID 프로젝트는 플랑드르 지방의 eID 카드를 적용한 프레임워크를 개발하여, eID 카드에 기반한 어플리케이션이 개인의 프라이버시를 저해시키지 않으며 충분히 신뢰있는 서비스를 제공할 수 있도록 한다. 이를 위해 가장 관련있는 어플리케이션의 요구사항을 수집한다. 첫 단계에서 개발한 기반 기술과 어플리케이션은 현재의 eID 카드 아키텍처가 가지는 한계를 극복한 것이다. 두번째 단계에서 개발되는 특징은 차세대 eID 카드에 적용되며 2008년 이후에 구축될 예

정이다. 개발된 프레임워크는 안전한 인터페이스를 통해 상호호환성을 보장하며, 향후의 구축 작업에 활용되거나 관련 기술을 이해하는데 핵심적인 역할을 수행할 것이다.

adapID 프로젝트는 아키텍처뿐만 아니라 하부 기술도 개발할 계획이다. 기술/법률적인 분야와의 제휴 연구를 통해 개인의 신원을 드러낼 필요없이 비밀 증명서를 통해 서비스를 사용할 수 있는 방법, 생체정보를 암호화에 사용, 프라이버시와 신뢰성 있는 협상, 안전한 어플리케이션을 위한 신뢰 모듈, 공개 네트워크에서의 신뢰에 관한 서비스와 법적 측면들을 고려한다. adapID 프로젝트의 주요 연구 분야는 다음과 같다.

- eID 를 위한 프라이버시 강화 기술
- 별명(pseudonym), 유일 식별자의 연결 제거 기술, 익명 통신, 익명 증명서 등
- 생체 정보
- 신뢰 모듈
- 정형화된 방법론

adapID 프로젝트가 개발한 프레임워크와 기본 기술은 전자 정보 보관, e-Health, 전자 정부의 세 가지 주요 어플리케이션에 적용하는 것으로 검증된다. 이들 각각의 분야는 엄격한 제한 사항과 목표가 명시되어 있으며 현재 이를 구현하고 있다. adapID 프로젝트는 eID 카드를 활용할 여러 어플리케이션들을 쉽게 개발할 수 있는 고도화된 플랫폼을 제공한다. 이 플랫폼은 e-learning, DRM(Digital Rights Management), e-payments 와 e-business 서비스를 제공할 수 있으며, 플랑드르 정부와 비영리 기관에게 제공될 것이다. 시민들은 높은 수준의 서비스를 제공 받으며, 또한 IT 와 전자 보안 분야에 관련된 플랑드르 지방의 기업들에게도 새로운 사업 기회를 제공할 것이다.

adapID 프로젝트는 1, 2 세대의 eID 카드의 보안과 프라이버시 문제들을 조사하여 3 세대 eID 에 적합한 디자인을 제안할 계획이다. 2005 년 7 월 발의한 이후 2005 년 12 월까지 6 개월 동안 adapID 프로젝트는 기존의 eID 시스템에 대한 개략적인 분석과 기술을 통해 향후 기술 연구를 위한 요구 사항을 수집하였다. adapID 프로젝트에서 도출한 eID 의 개념, 프로토타입, 구현에서의 많은 부분들은 FIDIS 프로젝트와 같은 다른 프로젝트에서도 유용하게 활용될 것으로 예상된다.

### III. eID의 상호호환성

여러 국가들은 시민들에게 eID 를 발급하기 위한 계획을 세웠거나 이미 발급하고 있다. 이 과정에서 유럽 연합과 같은 지역 단위뿐만 아니라 전세계적인 상호호환성(Interoperability)이 필요하다는 인식이 생기고 있다. 현재 발행된 eID 는 국가마다 상이한 형식을 가지며, 소프트웨어 솔루션도 국내용으로 개발되어 있다. 이런 추세라면 지역적인 표준화로 인해, 전세계에는 수많은 종류의 eID 카드가 존재할 것이다.

InteropEID 워킹 그룹[11]은 전세계에 유통되는 대다수의 eID 와 상호 동작할 수 있는 소프트웨어 솔루션을 목표로 한다. 클라이언트와 서버 컴포넌트 모두를 고려하며 다양한 운영 체제와 휴대용 컴퓨팅 플랫폼까지 모든 잠재적인 플랫폼에 이러한 개념을 적용한다. 이러한 시도는 현재 진행되고 있는 유럽과 전세계의 eID 표준화 작업과 상호보완적인 역할을 하게 된다.

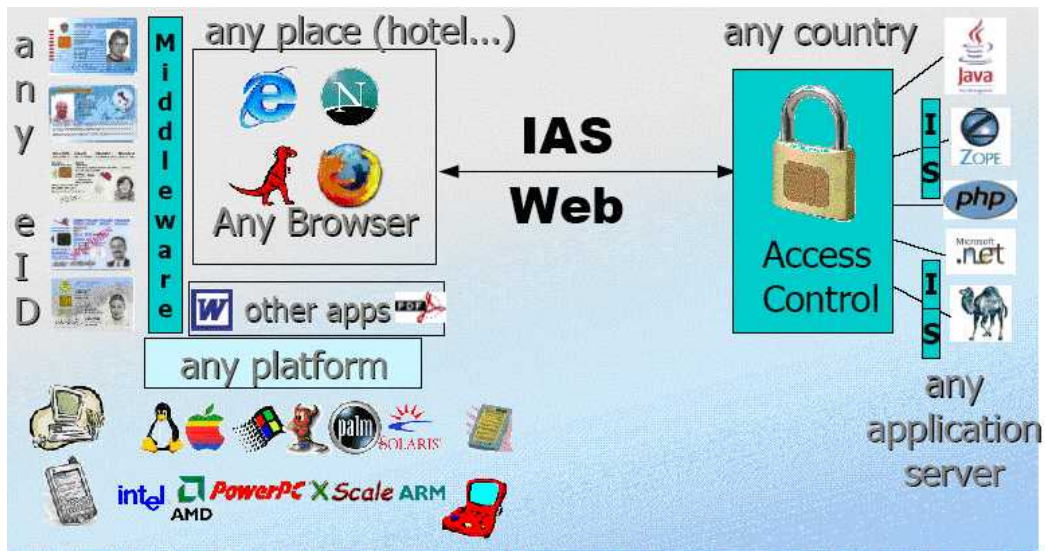


그림 8 InteropEID 의 목적

InteropEID 는 eID 도메인에 활동하는 전문가들의 비공식적인 단체로서, eID 의 상호호환성을 제공하려는 공통의 비전을 공유하고 있다. InteropEID 커뮤니티는 Porvoo 그룹[23], 상호호환되는 eID 를 위한 글로벌 협력 포럼(유럽 연합, 일본, 미국, 글로벌 플랫폼)처럼 eID 도메인을 구성하는 기존 포럼과 긴밀한 관계를 맺고 있다. 또한 정책 결정권자인 IDABC 2005[24]를 비롯한 유럽 위원회, ModinisIDM, FIDIS, GUIDE 와 같은 관련 프로젝트와도 공조하고 있다.

InteropEID 워킹 그룹은 최소한 다음의 결과물을 제공할 계획이다.

- 인가, 인증, 서명 기능을 제공하는 상호호환적인 클라이언트/서버 솔루션의 오픈 소스 참조 구현
- 다양한 eID 카드에 대한 스펙과 자세한 정보, 비교
- 다른 eID 카드와 호환하는 주요 어플리케이션
- 상호동작하는 솔루션을 작성하기 위한 개발자 가이드라인
- 상호동작하는 솔루션을 위한 아키텍처 추천
- 툴킷과 컴포넌트에 사용할 수 있는 형식
- 서버측 프라이버시 강화 컴포넌트

InteropEID 워킹 그룹은 여러 기관이 개발한 소프트웨어 솔루션이 다양하게 구현될 수 있음을 보여준다. 정부, 국제 협회, 운영체제 업체, 그리고 오픈소스 커뮤니티와 같은 기관들이 저마다 개발한 소프트웨어가 서로 공존하며, 개발자는 이를 통해 다른 소스의 컴포넌트들을 서로 조합하여 사용할 수 있게 된다. 예를 들어, 상업적인 웹 브라우저나 이메일 클라이언트는 오픈 소스 미들웨어를 통해 eID 서비스에 접근할 수 있으며, 정부로부터 공인받을 수도 있다.

현재 InteropEID 커뮤니티는 상호동작 솔루션을 개발하기 위하여 오픈소스/무료소스 커뮤니티와 긴밀히 작업하고 있다. 클라이언트 측 소프트웨어는 OpenSC[12]에 주로 기반하고 있으며 OpenSignature[13] 부분은 Apache[14]와 OpenPortalGuard[15]에 기반한다.

구현 방법에 중립적이기 때문에, InteropEID 는 오픈 소스를 사용하여 저-레벨의 미들웨어를 개발한다. 일반적으로 오픈소스는 비용이 저렴하다는 이점이 있지만, InteropEID 프로젝트는 오픈소스와 같은 조직적인 모델이야말로 상호운용 도메인에서 전세계적인 협력을 이끌어내는 유일한 모델이라고 보고 있다. 특히 오픈소스 프로젝트에는 형식적인 동의가 필요없고, 완전히 독자적인 자치권을 유지하며, 중앙의 조직이 이를 조절할 필요가 없이 모든 개인이 직접 제어할 수 있다는 이점이 존재한다. 게다가, 오픈소스는 소프트웨어 개발, 통합 과정에서 발생하는 과도한 복잡성을 피하며, 수많은 플랫폼에서 신뢰를 평가할 수 있다.

그림 9 는 InteropEID 워킹 그룹이 제안한 미들웨어 아키텍처이다. 미들웨어는 OpenSC 와 OpenSignature 프로젝트를 기반으로 하고 있으며, 일반 통신과 보안 통신을 구분하여 다양한 용도에 적합하게 활용하도록 한다. 현재 InteropEID 는 미들웨어를 개발하는 단계에 있는데, 고

수준의 다양성을 고려하여 미들웨어를 관리하고 표준에 기반한 솔루션을 사용한다.

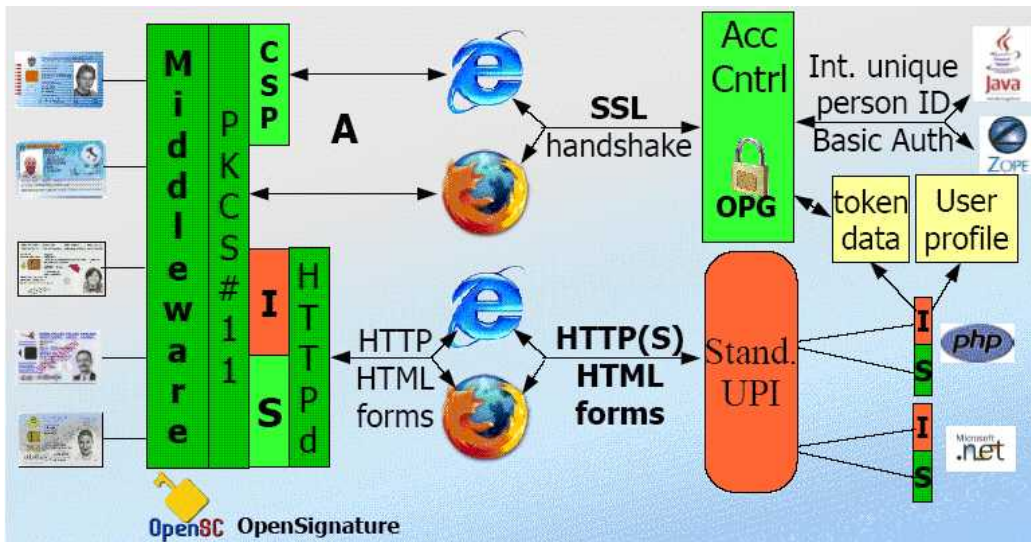


그림 9 InteropEID 미들웨어 아키텍처

2005년 10월 13일, 브뤼셀에서 개최된 세미나[12]에서 InteropEID가 공개한 미들웨어는 인증 부분과 식별/서명 부분의 아키텍처 구현 상황을 보여주고 있다. InteropEID 프로젝트는 표준화를 준비하고 있으며 7-10년의 기간이 소요될 것으로 예상하고 있다. 이 작업은 기존의 eID에 대한 수정, 구현, 완료 작업들과 병행하여 수행될 계획이다.

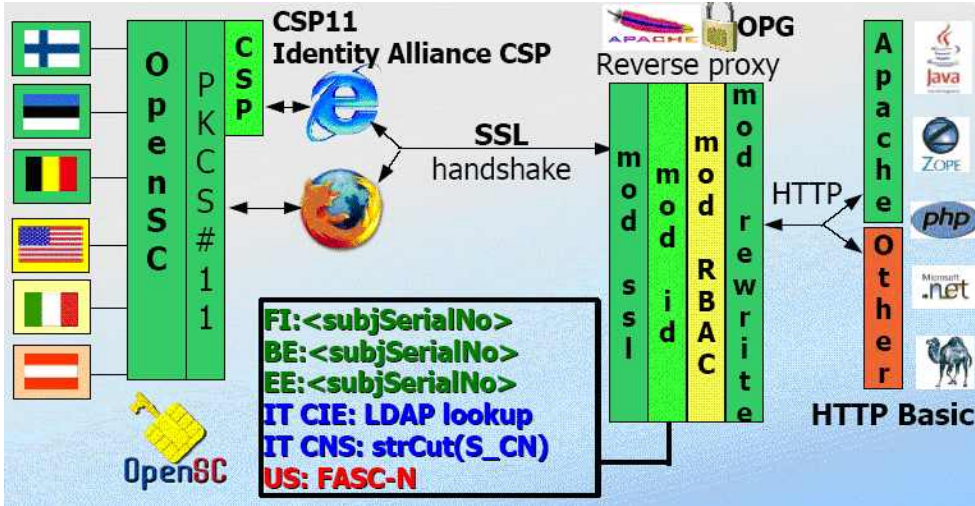


그림 10 InteropEID 미들웨어 개발 현황 - 인증 부분

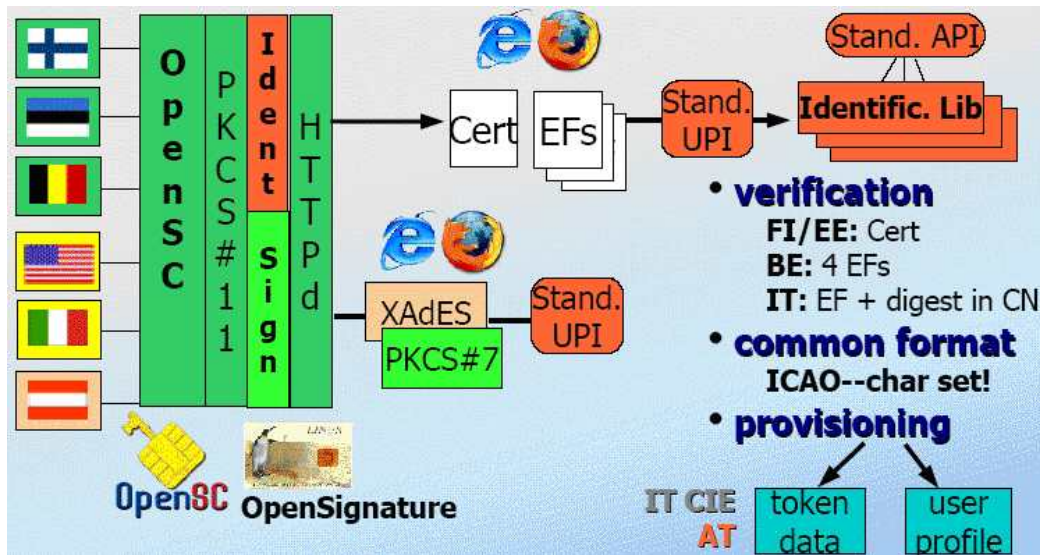


그림 11 InteropEID 미들웨어 개발 현황 - 식별, 서명 부분

#### IV. 결론

전자 신원을 의미하는 eID 는 정보 사회에 있어서 매우 중요한 역할을 수행한다. 대면하지

않은 온라인 상황에서도 eID 를 통하여 안전하게 사용자를 식별하고 인증하며, 개개인의 보유 권한을 제공하고 전자서명도 가능케 할 수 있어, 온·오프라인 환경에서 사용자의 신원을 안전하고 신뢰성있게 관리할 수 있게 되었다. 또한 eID 의 안전한 관리와 운용을 통하여 사용자의 가치있는 정보를 보호할 수 있고, 사용자 스스로도 개인의 정보를 지킬 수 있는 프라이버시 보장 환경을 제공할 수 있는 것이다. 현재 유럽 연합의 여러 멤버 국가에서 eID 를 구축하려는 계획이 빠르게 진행 중이며, 관련 프로젝트들이 활발하게 진행되고 있다. 본 기고문에서는 유럽의 대표적인 eID 연구 프로젝트인 FIDIS, GUIDE, MordinisIDM, PRIME, InspireD, DAIDALOS, adapID, interopEID 에 대한 간략한 소개를 통해 eID 의 현황 및 전망에 대해 알아보았다.

국내에서도 행정자치부의 주도하에 eID 에 대한 연구 및 논의가 적극적으로 추진되고 있다. 다소간의 논란이 제기되기는 하였지만, 주민등록번호 대체 기술에 대한 연구가 지속적으로 진행되고 있다. 현재의 주민등록번호 체계에 많은 개인 정보가 담겨있어 이에 대한 지속적인 개선 요구에 대한 대응이나, 이미 국내 모든 분야에서 개인 신원 확인용 Key 로 사용되고 있는 주민등록번호의 대체시 사회적 비용의 초래 및 신원 확인과 관련한 문제 유발의 가능성이 있으므로, 좀더 심도깊은 연구와 행정자치부 이외에 IT 담당 주무부처인 정보통신부 및 주민등록번호를 활용하고 있는 정부부처 모두가 함께 참여하여 의견수렴 및 방안 마련이 필요한 시기이다. 또한 행정자치부에서는 2005 년부터 현행 주민등록증의 IC 카드화에 대한 타당성 조사 사업을 시행하였다. 주민등록 발전모델의 이름으로 추진되고 있는 이 사업은 현행 주민등록증이 육안식별용으로서 위변조에 다소 취약하고 많은 정보가 주민등록증 표면에 노출되어 있다는 개선의 요청에 따라 추진되고 있다. 다만, 1996 년도에 중단했던 사업의 연장선으로 파악하는 일부의 시각에 대한 대응 및 한번 발행되면 5 년 이상 사용될 증서의 특성에 따라 카드 및 단말기 등에 대한 표준화와 시험 인증을 통한 안전성 보장에 대한 다양한 전문가들의 의견 개진이 요구된다.

국내에서 현재 개인의 신원확인용으로 사용되는 증서로는 주민등록증, 운전면허증, 여권, 공무원증 등이 있다. 현재까지는 이들 증서 모두 주민등록번호 체계로 연동되고 있으며, 근시일내에 각각 순차적으로 IC 카드화가 예상된다. 물론 이들 각각 고유의 번호체계로 유지될 가능성이 매우 크며, 주민등록번호의 연관성이 현재보다 감소될 것으로 예상된다. 따라서, 전자투표를 비롯한 다양한 전자정부 서비스를 제공받기 위하여 주민등록번호 대체수단 또는 기술에 대한 체계적이고 지속적인 연구가 필요하다.

한국전자통신연구원 디지털 ID 보안연구팀에서는 온라인 환경에서의 eID 를 제공하기 위하여 ‘e-Identity 보호용 공통보안서비스플랫폼 기술개발’ 과제를 수행 중에 있다. SAML2.0 표준을

이용하여 한번의 로그인으로 여러 사이트의 서비스를 간편하게 이용할 수 있는 단일 로그인 기능, XACML1.1 표준을 이용하여 사용자가 직접 개인정보의 공유 정책을 제어할 수 있는 서비스, ID-WSF2.0 표준을 통한 여러 사이트에 분산된 ID 관리 등의 기능을 제공한다. 이 과제는 2004년부터 2006년까지 3차년의 수행기관을 가지며, 2차년도에 결과물이 2006년 행정자치부의 시범과제로 선정된 대전광역시 공공기관의 통합 ID 관리 시스템에 구축되며, 차후에는 전국의 지자체에 확대 적용될 계획이다. 이 서비스를 통해 정부 기관은 주민번호를 비롯한 개인정보를 안전하게 관리하면서, 필요한 시점에 최소한의 정보만을 사용할 수 있게 된다. 그리고 다른 기관과 정보를 자유롭게 공유할 수 있으며, 시민들은 전국의 모든 정부 기관의 서비스를 편리하게 제공받을 수 있을 전망이다. 또한 상기 팀에서는 ‘대한민국 국가 IC 카드에 대한 표준 플랫폼 규격과 이를 활용하기 위한 가이드라인 개발 과제’를 수행하고 있다. 즉, 공공 분야의 각종 증서들을 IC 카드화 하는 것을 전제로 하여 부처별로 독자적인 규격의 발주가 아닌, 안전성이 보장되는 공통 플랫폼 하에서 특정 기능들만을 추가한 형태로 사업 추진을 유도하고자 하는 것이다. 이를 통하여 사용자 및 시스템에 대한 최소한의 안전성 보장과 시스템 인프라 구축 비용의 중복 투자 방지를 도모하고자 하는 것이다. 그리고 표준화 관점에서 최근 논의되고 있는 한중일을 중심으로하는 아시아 eID에 대한 논의에도 적극적으로 참여하고 있으며, 이는 InteropEID 프로젝트와 협력하여 진행할 수 있을 것으로 기대된다.

eID가 많은 관심을 받으면서 활발히 개발되고 있지만, 현재 eID와 관련된 기술과 사회적인 요소들은 몇 가지 보완할 사항들이 존재한다[1]. 첫번째로 기술적인 측면에서 eID에 사용중이거나 제안된 기술들은 성숙되거나 충분히 제어할 상태가 아닌 경우가 많으며, 이에 대한 연구가 지속적으로 수행되어야만 한다. 그리고 각국이 개별적으로 개발하고 있는 eID 프로젝트들은 상호호환성을 고려하여, 미래의 활용을 염두에 두어야만 한다. 두번째로 eID를 적절히 사용하기 위해서는 개인을 위한 교육과 훈련이 필요하다. 충분한 교육 없이 사용자가 자신의 eID를 사용하는데 적절히 주의를 기울이지 않는다면, 개인의 신원은 쉽게 노출되어 버릴 것이다. eID 아키텍처가 아무리 신뢰성있고 안전한 프레임워크에 기반하고 있더라도 사용자의 노력이 없이는 무용지물일 따름이다. 세번째로 eID 기술은 여러 계층의 합의에 따라서 설계되고 구현되어야 한다. 마지막 네번째로는 규격에 대한 검증 및 구현된 제품의 시험/인증이 수반되어야 한다. 이는 eID의 특성상 한번 제공되면 함부로 수정되어서는 안되며, 문제가 발생하여 eID 시스템을 교체할 경우 예상되는 사회적 비용과 반발 등의 문제점이 상상 이상으로 커질 수 있기 때문이다. 이들 절차는 많은 시간과 노력이 소요되지만, eID가 사회 구성원들 모두에게 도움이

될 수 있는 첫걸음이 될 것이다.

### <참 고 문 헌>

- [1] Marit Hansen, “eID in Europe – The Privacy and Security Perspective,” NET-ID 2006, Jan 2006
- [2] FIDIS(Future of Identity in the Information Society), <http://www.fidis.net>
- [3] GUIDE, <http://istrg.som.surrey.ac.uk/projects/guide/>
- [4] ModinisIDM, <https://www.cosic.esat.kuleven.be/modinis-idm/>
- [5] PRIME(Privacy and Identity Management for Europe), <http://www.prime-project.eu.org/>
- [6] Inspired(Integrated secure platform for interactive Trusted Personal Device), [https://rami.jrc.it/rami\\_coverages\\_registry/eu/050523143147\\_5](https://rami.jrc.it/rami_coverages_registry/eu/050523143147_5)
- [7] F.Bormann, L.Maneau and A.Linke, “Integrated secure platform for interactive Trusted Personal Device,” SIT Smart Card Workshop 2005, Feb 2005
- [8] DAIDALOS(Designing Advance network Interfaces for the Delivery and Administration of Location independent, Optimized personal Services), <http://www.ist-daidalos.org/daten/>
- [9] adapID(advance applications for electronic Identity cards in Flanders), <https://www.cosic.esat.kuleuven.be/adapid/>
- [10] InteropEID, <http://www.comune.grosseto.it/interopEID>
- [11] Bud P. Bruegger et al, “Open Source for eID Interoperability,” Porvoo Group eID Workshop, Oct 2005
- [12] Aniyam Varghese, “Next steps for Electronic Identification and Authentication in EU for Public Services,” Porvoo Group eID Workshop, Oct 2005
- [13] OpenSignature, <http://opensignature.sourceforge.net/english.php>
- [14] Apache Project, <http://httpd.apache.org>
- [15] OpenPortalGuard, <http://openportalguard.sourceforge.net/>
- [16] The Modinis IDM Study Team, “Identifying obstacles to pan-European IDM,” Second ModinisIDM Workshop, Nov 2005
- [17] Andreas Linke and Laurent Manteau, “Report on the European Research Project Inspired: The future of Smart Cards,” Information Security Solutions Europe, Sep 2005
- [18] Kai Rannenberg, “FIDIS-Future of Identity in the Information Society,” An FP6 Network of Excellence, 2005
- [19] Marit Hansen and Henry Krasemann, “Privacy and Identity Management for Europe – PRIME White Paper,” PRIME consortium, Jul 2005
- [20] Anna Buchta, Michael Vanfleteren and Peter Keller, “Framework V1,” PRIME consortium, Jun 2005

- [21] PRIME consortium, "PRIME Project Overview version 1.2," PRIME consortium, Oct 2004
- [22] IST(Information Society Technologies), <http://www.cordis.lu/ist/>
- [23] Porvoo Group, <http://porvoo7.fjarmalaraduneyti.is/>
- [24] IDABC(Interoperable Delivery of European eGovernment Services to public Administrations, Business and Citizens), <http://europa.eu.int/idabc/en/home/>