정 보 보 호 학 회 지
제26권 제2호, 2016. 4

독일의 eID 동향 및 기술 분석

이 동 혁*, 박 남 제*, 강 유 성**, 최 두 호**

요 약

eID는 여러 편의성을 제공하지만, 개인정보보호의 불확실성에 대한 우려로 활성화가 쉽지 않다는 단점이 있다. 이미 선진국에서는 eID의 도입을 추진해 왔으며 특히 EU에서 적극적으로 시도한 바 있다. 안전한 eID 시스템을 위해서는 개인정보보호 뿐 아니라 시스템 자체의 보안에 대한 고려도 동시에 이루어져야 한다. 보안성이 신뢰되지 않는다면, 개인정보보호에 대한 신뢰도 존재할 수 없을 것이다. 본 고에서는 EU에서도 특히 활발한 움직임을 보이고 있는 독일의 eID 현황 및 보안 메커니즘을 살펴본다. 그리고 안전한 eID 시스템 구성을 위한 보안 요구사항을 분석한다.

Ⅰ. 서 론

현재 사용되고 있는 주민등록증은 주민등록번호, 주소 등 민감정보가 육안으로 쉽게 확인됨으로써 개인정보의 침해 가능성이 매우 높다. 이러한 관점에서는 eID 카드는 물리적인 노출에서는 안전할 수 있다.

eID 기술은 여러 편리성을 가져다 줄 수 있다. 예를 들어, 온라인 인증 시 현재는 각각의 사이트에서 사용자 이름 및 암호를 관리해야 하는 번거로운 측면이 있으나, eID 시스템에서는 비교적 간편히 PIN을 입력하는 것으로 로그인이 가능하다. 또한 온라인 거래, 공공기관의 서비스 등 여러 방면에서 편리하게 온라인 서비스를 제공받을 수 있을 것이다.

그러나, eID 카드는 전력 분석 공격과 같은 여러 공격 방법이 존재할 수 있다. 이러한 정보 노출 우려는 개인정보보호에 대한 침해로 고스란히 이어질 수 있다. 과거 행자부에서는 전자주민증에 대한 단계적인 도입을 시도하였으나, 시민단체의 반발로 무산된 바 있다. 정보보호에 대한 안심이 없다면 eID 카드는 활성화될 수 없을 것이다.

여러 선진국에서는 eID의 도입을 시도하였고, 특히 EU에서는 정책적으로 많은 노력을 기울이고 있다.

본 고에서는 독일의 eID 현황을 중심으로 살펴본다. 또한, 독일 eID에 적용된 보안 메커니즘을 살펴보고, eID 시스템의 요구사항을 분석한다.

Ⅱ. 유럽의 eID 동향

본 장에서는 eID 정책 및 프로젝트 동향을 위주로, EU와 독일의 추진현황에 대해 살펴본다.

2.1. EU

과거 EU는 여러 프로젝트를 통하여 선도적으로 eID를 도입한 사례가 있다. 그러나, 국가간 기술의 상호 운용성 부족과, 일반적인 법적 이해의 부족에 따라 기존의 체계로는 범유럽 서비스를 진행하기에 한계점이 있어, 2014년 7월을 기점으로 EU의 새로운 규정인 “Electronic identification and trust services (eIDAS)”를 시행하였으며, 이를 모든 회원국에 적용하였다. 이 규정은 각 회원국의 식별시스템간 상호 인증 시스템을 구축하여 국가간 온라인 서비스 및 전자상거래에 대해 신뢰와 효율성을 향상하는 것을 목표로 한다.

eIDAS는 크게 전자식별, 신뢰서비스, 전자문서의 3가지의 장으로 나뉘어 있고, 이 항목에 따라 세부 규정을 정하고 있다. 최근 이러한 eIDAS와 관련된 표준 개

이 연구는 2013년도 정부(교육부)의 재원으로 한국연구재단의 기초연구사업 지원을 받아 수행되었으며(과제번호:2013R1A1A4A01013587), 또한 ETRI의 연구개발과제인 K-SCARF 프로젝트(과제명:암호키 누출 검증 및 방지 원천 기술 연구)로 수행된 것임.
** 제주대학교 일반대학원 컴퓨터교육전공 ({bonfard,namjepark}@jejunu.ac.kr, 교신저자[namjepark])
** 한국전자통신연구원 사이버보안연구본부 암호기술연구실 ({youskang,dhchoi}@etri.re.kr)

발이 진행되고 있다. 이 지침에 따라 규격의 통폐합이 진행되고 있으며, 이 지침은 유럽 각국에 강제력을 가지는 표준이 되므로, 각국의 제품과 서비스는 이 규격을 따라야 한다.

또한, 2011년에 종료된 STORK의 후속 프로젝트로 STORK 2.0이 진행된 바 있으며, 이는 STORK의 결과를 바탕으로, 유럽 내의 eID에 대한 수용을 더욱 높이고자 하는 목적으로 2012년부터 2015년까지 진행되었다. STORK 2.0에서는 각 유럽 국경간의 전자식별 및 인증이 주요 관심사로, 유럽 전역에서 전자식별 및 인증이 원활히 작동하는데 초점을 두고 있다.

한편, EU의 지원으로 11개국 연합으로 2012년 11월부터 FutureID가 3년간 진행된 바 있으며, 이는 신규 eID 기술 및 신뢰 인프라를 유연하게 통합하고자 하는 것을 목적으로 한다. 이는 응용프로그램 및 서비스 제공업체가 FutureID 인프라에 통합 시 큰 비용 없이 eID에서 제공하는 강력한 보안 혜택을 제공받을 수 있다는 점을 특징으로 한다.

2.2. 독일

독일은 정부 주도하에 eID에 대한 과감한 추진을 진행한 편이다. 2010년 11월부터 eID 카드를 도입하였으며, 2013년 기준으로 2,100만의 eID카드를 발행한 바 있다.

또한, 행정/사회/경제 분야에 대해 예측하기 어려운 우려에 대응하기 위해 법적 및 보안 문제를 적극적으로 고려하고 있다. 과거 eID 클라이언트 어플리케이션인 AusweisApp이 일부 알려진 보안 문제가 발생한 사례가 있으며, 이러한 문제에 대하여 비교적 적극적으로 대처한 사례가 있다.

또한, 독일 연방정부 내각은 “디지털 정부 2020”을 채택한 바 있으며, 이는 효율적인 연방정부의 전자관리 작업을 목적으로 한다. 이를 위해 연방정부의 프레임워크를 eID 기능과 통합하는 것을 추진하고 있다.

한편, 독일 연방경제 및 에너지부 (Federal Ministry for Economic Affairs and Energy)의 “Trusted Cloud” 프로그램의 일환으로 2011년부터 SkIDentity가 진행중에 있으며, 이는 클라우드 ID를 기반으로 클라우드 등 외부 시스템과 연동할 수 있게 한다. 이를 위해, eID내에 저장된 데이터를 추출하고, 필요한 경우 이를 기반으로 별도의 클라우드 ID를 만들 수 있게 하며, 이러한 클라우드 ID는 암호화로 보호한다. 해당 클라우드 ID를 통하여 익명 로그인 및 자기 증명이 가능하다.

Ⅲ. eID 카드 보안 메커니즘

3.1. 개요

eID 카드에 대한 IT 인프라는 개인정보보호, 신원 문서의 진정성 및 위조가 되지 않게 하는 부분을 충분히 고려하고 설계되어야 한다. 따라서, eID카드와 단말기간 비접촉 인터페이스를 보장하는 솔루션에 특별한 주의가 필요하다. 이러한 보안목적을 달성하기 위해 표 1과 같은 프로토콜이 BSI(독일 연방정보보안청)의 참여하에 개발되어 있다.

〔표 1〕 eID카드 보안 메커니즘

용 어	역 할
PACE (Password Authentication Connection Establishment)	- 접근제어의 목적 - RF칩을 보호
EAC (Extended Access Control)	- 보안링크 확립 - RF칩 복제 여부 감지 - 터미널장치 인증
PA (Passive Authentication)	- RF칩 데이터의 무결성을 확인
RI (Restricted Identification)	- 칩과 공급자간 가명을 생성
CSCA (Country Signing Certificate Authority)	- eID내 서명 데이터에 대한 디지털 인증서 계층구조
CVCA (Country Verifying Certificate Authority)	- eID의 권한을 읽는 부분에 대한 디지털 인증서 계층구조

3.2. PACE

PACE는 ID카드의 RF칩이 명시적 접근을 하지 않고서는 판독될 수 없다는 것을 보장하며, 데이터가 암호화된 형태에서 단말장치와 교환된다. PACE에 사용할 수 있는 비밀번호는 단말 측 장치의 권한 증명서에 의존한다. 일반적으로, 이것은 신분증 소지자가 알고 있는 6자리의 비밀번호 (PIN)이다.

PACE의 장점은 패스워드의 길이가 암호의 보안 수

준에 영향을 미치지 않는다는 점이다. CAN(Card Access Number) 또는 PIN이 비교적 짧게 설정되어 있는 경우라고 하더라도, ID카드의 RF칩 상의 데이터가 전송 중에 안전하게 보호되는 것을 보장할 수 있다.

3.3. EAC Box

EAC 프로토콜은 CA(Chip Authentication)과 TA(Terminal Authentication)으로 구성된다. 이 두 프로토콜은 PACE및 PA와 함께 실행된다.

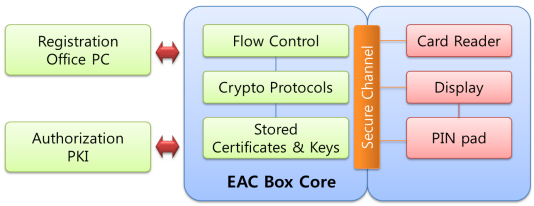
CA의 목적은 인증고자 하는 칩이 실제 칩인 것을 확인하는 것, 즉, 위조나 복제되지 않았음을 판단하고 칩과 카드 리더기 및 칩과 서비스 공급자 간의 안전한 연결을 보장하기 위함이다.

칩 인증은 Diffie-Hellman 키 교환 방식을 근간으로 한다. 칩의 공개키는 그것을 생성한 과정에서 서명되며, 서명된 키의 사용은 칩의 신뢰성을 검증한다. 또한, 온라인 인증을 받을 경우, 강한 암호화와 채널간 인증이 칩과 서비스 제공자 간에 확립된다.

ID 카드의 모든 데이터는 기밀로 취급되어야 하며, 권한이 없는 사람으로부터 읽혀지는 것을 방지해야 한다. 단말 인증(TA) 프로토콜은 이러한 목적을 위해 개발되었다. ID 카드 소지자의 민감 정보는 이 프로토콜이 정상적으로 수행되었을 때만 읽혀질 수 있다. CVCA 인증서는 이 권한을 확인하기 위해 RF칩에 저장되어 있다. 단말 인증에서, 리더는 단말 인증서 형식으로 RF칩에 대한 읽기 권한을 보낸다. 또한, CVCA 인증서와 두 인증서 사이의 계층에 있는 모든 인증서를 보낸다. 이것은 단말의 인증서에 대한 신뢰성과 무결성을 확인할 수 있게 한다. RF칩은 이 인증서가 신뢰할 수 있는지를 알고 있다.

리더에 의해 송신 단말 증명서의 신뢰성 및 무결성이 확립되면, RF칩은 이 인증서가 실제로 이 장치에 발행된 것을 확인한다. 이를 위해, RF칩은 단말 증명서에 속하는 개인 키를 사용하여 카드 리더기에 난수를 송신하면 카드 리더기는 다시 RF칩에 서명된 난수를 송신한다. 단말기 인증서에 포함되어 있는 단말 장치의 공개키를 사용하여 RF칩은 난수의 서명을 확인하고 소유자의 인증서와 일치하는 개인키를 가지고 있는지 여부를 판정할 수 있다.

ID카드의 데이터에 엑세스하려는 각 카드 리더기는



〔그림 1〕 EAC Box

그에 대응하는 권한 인증서가 필요하며, 소유한 비밀키와 공개키는 PKI를 통해 정기적으로 갱신해야 한다. EAC Box는 인증된 환경에서 캡슐화된 형태로 이런 기능을 제공하며, 표준화된 인터페이스를 통해 외부 구성요소 및 서비스와 통신한다.

그림 1은 EAC Box를 나타내며 이를 통해 칩과 서비스 제공자간 안전성을 확립한다.

3.4. PA

PA의 목적은 신분증의 RF칩 데이터의 신뢰성과 무결성을 확인하는 것이다. 전자 신분증의 제조 과정상 RF칩에 저장된 데이터는 전자서명이 되어 있다. 신원 문서를 읽을 때 수동 인증 RF칩에 저장된 데이터의 서명을 확인하고 CSCA 인증서로 그것을 추적하여 이 신분 증명서의 데이터가 공식적으로 승인된 ID 제조업체 RF칩 상에 기록되었는지 여부 및 무결성이 손상되지 않았는지 여부를 판단할 수 있다.

3.5. CSCA

eID 카드는 두개의 PKI(공개키 기반 구조)가 필요하다. 하나는 전자신분증명서(PA)의 진정성을 확인하기 위함이며(CSCA), 다른 하나는 신분 증명서상의 지문을 보호하기 위한 것이다(CVCA). BSI의 기술 가이드라인에서는 이러한 인프라의 기본적인 기능과 요구사항에 대한 내용이 구체적으로 설명되어 있다.

CSCA는 eID내 서명 데이터에 대한 디지털 인증서 계층구조로써, BSI에 의해 운영되고 있다. 이것의 권한으로 여권이나 ID카드 제조업체의 문서 서명 인증서상 개인키의 근간인 루트 인증서(CSCA 인증서)를 생성한다. 여권이나 ID카드 제조업체는 전자 신분증 파일에 서명하는 문서에 서명 인증서의 개인키를 사용하고 있다. 문서의 서명 인증서는 전자 신분증에 저장되어 있

다. 루트 인증서를 사용하여 전자 신분증이 실제 발행 국가를 대행하여 생성되었는지에 대한 확인이 가능하며, 생성 이후에 변경사항이 있는지 여부도 확인할 수 있다.

3.6. CVCA

BSI는 국가 확인 인증 기관(CVCA)를 운영하고 있다. 이 기관은 독일어 루트 인증서를 생성하고, 이러한 인증서의 개인 키는 문서 검증 인스턴스 (DV 인스턴스)의 문서 검증 인증서에 서명하는데 사용된다.

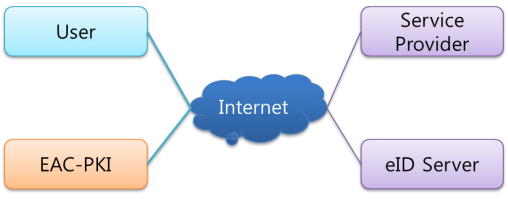
DV 인스턴스는 전자 신분 증명서의 읽기 권한을 부여하는 인증서를 발급할 책임이 있다. 또한, 신분 증명서에서 읽을 수 있는 정보, 즉 개인의 읽기 권한을 정의한다. 이 권한은 단말 인증 상 전자 ID의 RF 칩에 의하여 검증된다.

Ⅳ. eID 요구사항

본 장에서는 eID 시스템의 구성요소를 간략히 살펴본 후 eID 시스템의 요구사항을 분석한다.

4.1. eID 시스템 구성요소

그림 2는 eID 시스템의 구성요소를 나타내고 있다. 사용자는 eID 클라이언트를 통해 서비스 제공자에 접근하며, eID 인증 시 eID 서버가 서비스 제공자와 eID 클라이언트의 중재 역할을 하며 사용자 인증에 관여한다. 즉, 서비스 제공자의 eID 식별 기능의 사용을 용이하게 하기 위해 eID 서버가 필요하다. eID 서버는 식별 기능의 복잡성을 캡슐화하여, 서비스 제공자를 위한 간단한 인터페이스를 제공한다. BSI TR-03130[1]은 웹 응용 프로그램과 정보를 교환하기 위한 데이터 포맷 인터페이스를 지정하고 있다.



〔그림 2〕 eID 시스템 구성요소

하드웨어 및 소프트웨어 구성요소로 eID 서버는 eID 클라이언트인 AusweisApp과 통신을 설정하고, 단말기의 권한 증명서(DVCA 인증서) 및 CSCA인증서 요청에 대한 통신을 핸들링한다.

여러 서비스 제공자가 사용할 수 있도록, eID서버는 논리적으로 독립된 서버로 제공되며, 이것은 제삼자에 의해 원격으로 작동될 수도 있다. 공용 네트워크를 통해 전송될 때 처리된 데이터의 기밀성과 무결성을 유지하기 위해 eID 서버와 어플리케이션 서버 사이의 안전한 전송을 위해 데이터는 암호화되어 서명되어야 한다. eID 서버가 EAC 프토토콜을 수행을 마치면 서비스 제공자는 사용자를 인증할 수 있게 된다.

4.2. eID 시스템 요구사항

4.2.1. 기밀성 유지

eID 데이터는 기밀사항이므로, 등록 또는 허가 없이 전달 될 수 없다. 이러한 관점은 특히, 인가된 개인 데이터를 가져오는 부분과 eID 카드의 RF칩과 데이터의 수신측 사이의 통신에 적용된다. eID서버에 의해 수행되는 동작은 권한 인증서를 소유한 서비스 제공자를 대신하여 처리되기 때문에 적용하고 식별된 데이터는 인증 과정에서 필요한 기간보다 오래 eID 서버에 보관되지 않아야 하며, 문제 발생시 사용자에게 통보될 수 있어야 한다. 또한 인증 과정에서 필요하지 않은 데이터가 eID 서버로 전달될 경우는 지체없이 삭제해야 한다.

4.2.2. 무결성 및 신뢰성 보장

eID 인증 과정에서 읽혀진 데이터, 프로세스, 애플리케이션의 정확성은 서버에서 항상 보장해야 한다. 만약 정확성이 유지되지 않는다면 인증 과정이 정상적으로 수행되지 않게 될 것이다.

또한, eID 데이터의 신뢰성은 반드시 검증 가능해야 한다. 동시에, eID 데이터를 액세스하고자 하는 측의 신뢰성도 반드시 보장되어야한다.

4.2.3. 서버 가용성

eID 서버는 공인된 서비스 제공자의 요청에 따라 온

라인 인증을 수행 할 수 있어야 한다. 가용성의 레벨은 서비스의 요구사항에 따라 달라질 수 있다.

그것은 일반적으로 “높음”으로 간주되어야하며, 서비스 제공업체의 특정 요구사항에 따라 “정상”으로 낮출 수는 있다. 만약 eID 서비스를 이용하는 하나 이상의 서비스 개체가 있다면, 가용성은 최대가 되어야 한다.

4.2.4. 해지 관리

도난/분실시 ID 카드의 부정 사용을 방지하기 위해 카드 소지자는 폐기 관리를 통해 eID 카드를 차단하거나 취소할 수 있어야 한다.

즉, 서비스와 카드 해지 속성의 사용을 통하여, 서비스 제공자가 신원 문서를 악용 할 수 없어야 한다. 이것은 연중무휴, 1일 24시간 장소에 관계없이 잃어버린 ID 카드에 대한 취소가 언제든지 가능해야 한다.

Ⅴ. 결 론

eID에 대한 보안은 아무리 강조해도 지나치지 않다고 할 수 있다. 과거 전자주민증의 도입도 보안상의 우려로 인하여 진행되지 못했다고 해도 과언이 아닐 것이다. 그러나 eID는 지금까지 전자여권, 전자공무원 증 등으로 다양한 방면에서 시도되어 왔으며, 향후에도 다른 형태로 등장할 수 있다.

eID 시스템의 보안이 이루어지려면, 칩과 각 구성요소간 안전한 상호인증이 이루어져야 한다. eID의 특성상 중요하고 민감한 사안인 만큼, 보안상 얼마나 안전한지에 대해서 면밀히 검토되어야 할 것이다.

본 고에서는 EU 가운데서도 독일의 eID 현황에 대하여 살펴보았다. 또한, eID에 사용되고 있는 보안 메커니즘을 살펴 보았으며, eID 시스템의 구성요소와 이에 따른 요구사항을 분석하였다.

안전이 보장되는 전제하에서, eID는 생활에 편리하게 사용할 수 있는 기술로서 여러 불편을 감소시킬 수 있다. 안전성의 불안을 해소하기 위해 다양한 방면에서의 검토가 필요하며, 특히 개인정보보호 측면에서 어떠한 추가적인 고려사항에 있는지에 대한 연구가 필요할 것으로 보인다.

참 고 문 헌

[1] BSI TR-03130, https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03130/tr-03130.html

[2] BSI, "Innovations for an eID Ar- chitecture in Germany", http://www. bsi.bund.de, 2011.

[3] A. Poller, U. Waldmann, S. Vowé, S. Türpe, "Electronic Identity Cards for User Authentication - Promise and Practice", IEEE Security & Privacy, 10(1), pp.46-54, Feb 2012.

[4] H. Zwingelberg, M. Hansen. "Privacy Protection Goals and their implications for eID systems", Privacy and Identity Management for Life, Springer Berlin Heidelberg, 375, pp. 245-260, Sep. 2011.

[5] J. Essbach, "An approach to a decentral mobile payment system using nfc and the german eid-card", Wireless Systems (IDAACS-SWS), IEEE 1st International Symposium on, pp. 67-71, Sep 2012.

[6] M. Margraf, "The new german id card." ISSE 2010 Securing Electronic Business Processes. pp. 367-373, Nov. 2010.

[7] T. Messerges, E. Dabbish, R. Sloan, "Examining smart-card security under the threat of power analysis attacks", IEEE Transactions on Computers, 51(5), pp. 541-552, May 2002.

[8] B. Zwattendorfer, D. S., "Privacy -preserving realization of the stork framework in the public cloud", Security and Cryptography, 2013 International Conference on. IEEE, pp. 1-8, Jul 2013.

[9] C. Cuijpers, J. Schroers. "eIDAS as guideline for the development of a pan European eID framework in FutureID", Open Identity Summit, 237, pp.23-28, Jan 2014.

[10] H. Leitold, "Challenges of eID interoperability: The STORK project", Privacy and Identity Management for Life. Springer Berlin Heidelberg, 352, pp.144-150, Aug. 2010.

[11] S. Arora, "National e-ID card schemes: A

European overview", Information Security Technical Report, 13(2) pp.46-53, 2008.

[12] Volker Reible, Andre Braunmandl. "The eID Function of the nPA within the European STORK Infrastructure.", ISSE 2010 Securing Electronic Business Processes. pp.392-398, 2010.

[13] Sebastian Feld, Norbert Pohlmann. "Security analysis of OpenID, followed by a reference implementation of an nPA-based OpenID provider.", ISSE 2010 Securing Electronic Business Processes, pp. 13-25, 2010.

〈저 자 소 개〉

이 동 혁 (Donghyeok Lee)
정회원

2007년 2월 : 동국대학교 전자상거래기술전공 공학석사
2007년 6월~2008년 5월 : 한국전자통신연구원 정보보호연구단 연구원
2008년 11월~2015년 6월 : KT 플랫폼개발단 과장
2015년 9월~현재 : 제주대학교 컴퓨터교육전공 박사과정
<관심분야> 클라우드 보안, 스마트그리드 보안, 데이터베이스 보안

박 남 제 (Namje Park)
종신회원

2008년 2월 : 성균관대학교 컴퓨터공학과 박사
2003년 4월~2008년 12월 : 한국전자통신연구원 정보보호연구단 선임연구원
2009년 1월~2009년 12월 : 미국 UCLA대학교 공과대학 Post-Doc,WINMEC 연구센터 Staff Researcher
2010년 1월~2010년 8월 : 미국 아리조나 주립대학교 컴퓨터공학과 연구원
2010년 9월~현재 : 제주대학교 교육대학 초등컴퓨터교육전공 교수
<관심분야> 융합기술보안, 컴퓨터교육, 스마트그리드, IoT, 해사클라우드 등

강 유 성 (Yousung Kang)
정회원

1997년 2월: 전남대학교 전자공학과 졸업
1999년 8월: 전남대학교 전자공학과 석사
2015년 8월: KAIST 전기 및 전자공학과 박사
1999년 11월~현재: 한국전자통신연구원 책임연구원
<관심분야> 부채널분석, IoT보안, 보안 프로토콜 등

최 두 호 (Dooho Choi)
정회원

1994년 2월 : 성균관대학교 수학과 졸업
1996년 2월 : KAIST 수학과 석사
2002년 2월 : KAIST 수학과 박사
2002년 1월~현재 : 한국전자통신연구원 책임연구원, 암호기술연구실장
<관심분야> 암호 엔지니어링, 부채널분석, IoT보안 등