시각장애인을 위한 FIDO 인증 시스템 설계

김성수○ 조진성
경희대학교 컴퓨터공학과
korkeep@khu.ac.kr, chojs@khu.ac.kr

Design of FIDO Authentication System for Visually Impaired

Sungsu Kim○ Jinsung Cho
Department of Computer Science and Engineering, KyungHee University

요 약

현대인들은 사물인터넷(IoT; Internet of Things)의 확산에 따라 다양한 ICT 서비스를 누리고 있다. 반면 장애인에게 ICT 서비스의 진입 장벽은 오늘날에도 높게 느껴진다. 특히 시각장애인의 경우 ICT 서비스를 이용하기 위한 첫 번째 관문인 로그인 단계부터 어려움을 겪는다. 본 논문은 공개키 기반 생체인증 프로토콜인 FIDO(Fast Identity Online)와 개인키 관리 모듈인 SE(Secure Element)를 이용해 시각장애인도 쉽게 사용할 수 있는 인증 시스템을 제안한다. 본 연구는 로그인 단계의 진입 장벽을 허무는 것을 시작으로 '배리어-프리(Barrier-Free)' 환경을 구축하기 위한 ICT 기술의 활용 방향성 제시를 목표로 한다.

1. 서 론

현대인들은 사물인터넷(IoT; Internet of Things)의 확산에 따라 다양한 ICT 서비스를 사용하고 있다. 하지만 기술이 발전하면서 생기는 편리함은 ICT 서비스를 적극적으로 활용하는 계층과 그것으로부터 소외된 계층 간의 불균형을 심화시키는 기제로 작용하기도 한다. 특히 장애인과 비장애인 사이의 정보격차는 점점 커지고 있다. 이러한 현상은 단순히 ICT 서비스의 활용 격차에 그치지 않고 커뮤니케이션의 단절, 새로운 정보 획득 및 가공의 어려움, 정보 불평등으로 인한 기회 불균등, 사회 네트워크 형성의 어려움 등의 사회적 문제로 이어질 수 있다 [1].

장애인의 스마트 기기 접근성을 보장하기 위한 제도는 지난 2018년 2월 <국가정보화기본법> 개정을 통해 법제화됐다. <국가정보화기본법> 제 32조 '장애인·고령자 등의 정보 접근 및 이용 보장'에서 ICT 관련 제조업자는 제품을 설계, 제작, 가공할 때 장애인이 쉽게 접근하고 이용할 수 있도록 노력해야 한다. 하지만 이와 같은 제도가 마련됐다 하더라도 장애인에게 ICT 서비스의 진입 장벽은 오늘날에도 높게 느껴진다. 특히 시각장애인의 경우 ICT 서비스를 이용하기 위한 첫 번째 관문인 로그인 단계부터 어려움을 겪는다.

본 논문은 시각장애인이 ICT 서비스를 이용하기 위한 첫 번째 관문인 로그인 단계의 진입 장벽을 허무는 것을 시작으로 '배리어-프리(Barrier-Free)' 환경을 구축하기 위한 ICT 기술의 활용 방향성을 제시하는 것을 목표로 한다. 본 논문에서는 시각장애인도 쉽게 사용할 수 있는 FIDO(Fast Identity Online) 인증을 응용한 시스템을 제안한다. 본 인증 시스템은 공개키 기반 생체인증 프로토콜인 FIDO와 개인키 관리 모듈인 SE(Secure Element)를 이용해 RoT(Root of Trust) 환경에서 생체인증 방식으로 로그인할 수 있는 기능을 제공한다.

이 논문은 교육부 및 한국연구재단의 기초연구사업(NRF-2017R1D1A1B04035914)과 과학기술정보통신부 및 정보통신기획평가원의 SW중심대학 사업(2017-0-00093)의 지원으로 수행된 연구결과임.

논문의 구성은 다음과 같다. 2장에서 FIDO 프로토콜과 SE의 역할을 간략하게 설명하고 이를 이용한 FIDO Authenticator의 개념을 소개한다. 3장에서는 FIDO 인증 시스템의 핵심기능을 Sequence Diagram으로 도식화하고 KHU-FIDO Architecture 및 주요 구성요소에 관해 설명한다. 마지막으로 4장에서 기대 효과와 활용 예시를 들면서 논문은 마무리된다.

2. 관련 연구

2.1 시각장애인의 ICT 보조기기 수요 및 설계 방향

고용노동부의 시각장애인 ICT 보조기기 지원사업은 한국장애인고용공단에서 주관하고 있다. 현재 국가에서 지원하는 주요 보조기기는 [표 1]에서 정리한 바와 같다 [2].

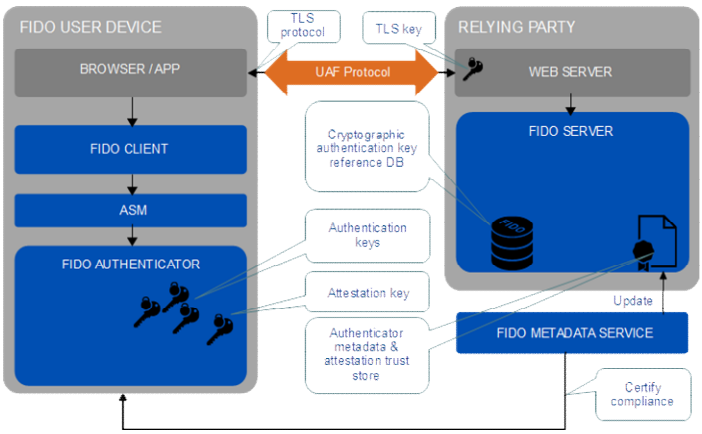
[표 1] ICT 보조기기

품목	설명
점자정보단말기	• 점자와 음성을 통해 문서 입·출력을 수행할 수 있는 휴대용 점자 단말기
점자 프린터	• 점자로 변환된 문자 정보 또는 점자 정보를 출력해주는 프린터
화면 확대기	• 컴퓨터 화면의 고배율 확대가 가능한 하드웨어 및 소프트웨어
음성 출력기	• 텍스트 또는 웹페이지 등을 음성으로 변환해 읽어주는 하드웨어 및 소프트웨어
문서 인식기	• 문자 또는 이미지를 텍스트로 변환하는 하드웨어 및 소프트웨어
입력보조장치	• 입력장치의 활용이 어려운 장애인을 위해 스틱, 키가드 등의 보조 기능을 추가한 장치
선택장치	• 기존 ICT 보조기기에 접근이 어려운 장애인을 위해 특별히 고안된 입·출력 장치

2010년부터 2014년까지 국가에서 보급된 시각장애인의 ICT 보조기기는 '음성 출력기' 수요가 1,041개로 가장 많았다. 뒤이어 '화면 확대기'의 수요는 832개, '문서 인식기'는 817개, '점자정보단말기'는 687개로 확인됐다 [3]. 이렇듯 시각장애인 전용 ICT 보조기기의 종류는 다양해지고 있으나, 이들의 요구를 만족하기에는 한계가 있다.

첨단 기술을 통해 장애를 극복할 수 있을 것이라는 예측에도 불구하고 장애인은 ICT 서비스를 사용할 때 여전히 어려움을 겪고 있다. 특히 시각장애인에게는 음성 변환 기능과 촉각적 요소가 적용된 인터페이스가 필수적이다. 이러한 기능이 제공되지 않는 한 이들은 또다시 제약을 경험할 수밖에 없다 [4]. 모바일 뱅킹 및 모바일 페이와 같은 경우 시각장애인 사용자를 위한 접근성은 아직도 열악한 상황이다 [5]. 그러므로 시각장애인을 위한 ICT 보조기기는 이들 관점에서의 UX/UI를 신중히 반영해서 설계, 제작, 가공되어야 한다.

2.2 FIDO UAF



[그림 1] FIDO UAF

FIDO 프로토콜은 FIDO Alliance에서 표준화한 공개키 기반의 생체인증 기술이다. FIDO는 지난 2015년부터 간편결제, 스마트 뱅킹 등 핀테크(Fin-Tech) 서비스에 적용됐으며 현재는 기업보안, 물리보안 등 응용 분야를 넓혀가고 있다 [6]. 본 시스템에는 FIDO 유니버셜 인증 프레임워크(UAF; Universal Authentication Framework)가 사용됐다. FIDO UAF는 사용자의 생체 정보가 패스워드처럼 활용되면서 인증하는 방식이다. [그림 1]은 FIDO UAF의 동작 구조이다 [7]. FIDO UAF의 주요 구성요소에 관한 설명은 [표 2]로 정리했다.

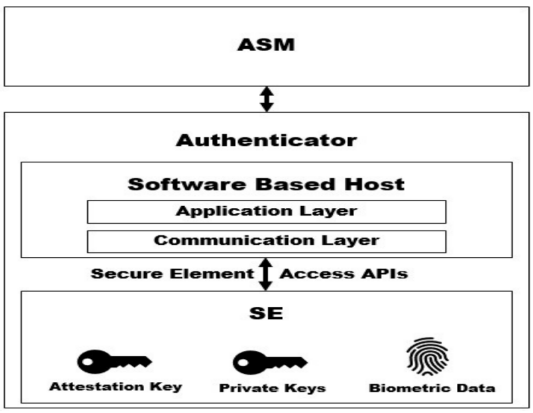
[표 2] FIDO UAF 구성요소

구성요소	설명
Client	• ASM ↔ Browser/App의 Data 전달 매개
ASM	• Client ↔ Authenticator 통신을 위한 플러그인
Authenticator	• 전자서명 생성, 개인키 및 생체 정보 저장
Server	• 전자서명 검증, 공개키 및 증명 정보 저장
Metadata	• Authenticator의 신뢰성 검증을 위한 데이터

2.3 SE

SE는 IoT(Internet of Things) 기기의 보안 강화를 위해 국제 표준 기구인 Global Platform에서 제안한 하드웨어 보안 모듈이다 [8]. SE에는 외부의 공격으로부터 데이터를 안전하게 보관할 수 있는 저장소가 있다. SE는 하드웨어 기반의 암호화 가속기를 이용해 자체적으로 키를 생성할 수 있고, 내부에서 생성된 키를 전자서명 및 데이터 암·복호화에 활용할 수 있다.

2.4 SE를 이용한 FIDO Authenticator

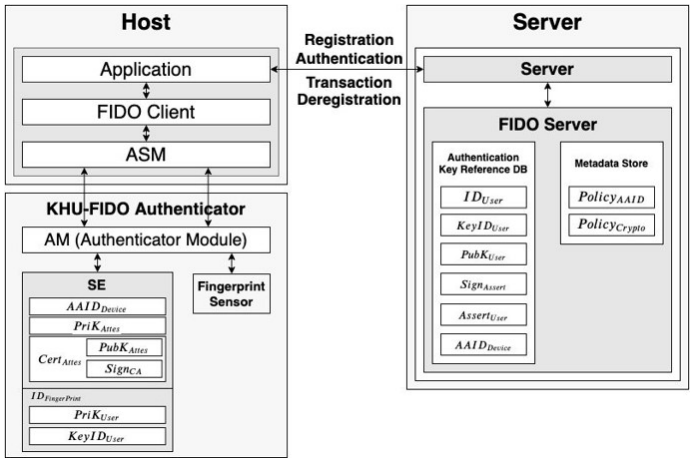


[그림 2] SE를 이용한 FIDO Authenticator

[그림 2]의 구조에서는 FIDO Authenticator에 SE를 추가함으로써 RoT 환경에서 안전하게 인증할 수 있는 기능을 제공하고 있다 [9].

3. FIDO 인증 시스템 설계

3.1 KHU-FIDO Architecture



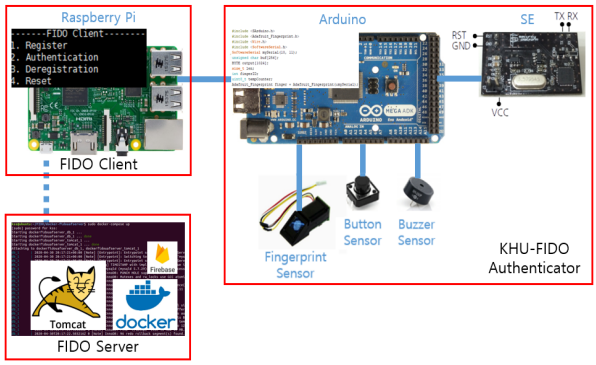
[그림 3] KHU-FIDO Architecture

[그림 3]의 KHU-FIDO Architecture는 [그림 2]에서의 SE를 이용한 FIDO Authenticator를 FIDO UAF에 적용함으로써 RoT 환경에서 지문인증 방식으로 로그인할 수 있는 기능을 제공한다. FIDO 인증 시스템에서 사용되는 SE의 데이터는 [표 3]에서 정리한 바와 같다.

[표 3] SE의 데이터

데이터	설명
AAID	• FIDO Authenticator 고유의 기기 ID
PriK(Attes)	• 전자서명 과정에 사용되는 개인키
Cert(Attes)	• 전자서명 정보, FIDO Server로 전송됨
Pub(Attes)	• 전자서명 과정에 사용되는 공개키
Sign(CA)	• FIDO Authenticator 고유의 기기 인증 정보
PriK(User)	• 지문 등록 단계에서 생성된 개인키
KeyID(User)	• 개인키를 참조할 수 있는 고유 식별자

3.2 주요 하드웨어 및 소프트웨어



[그림 4] FIDO 인증 시스템

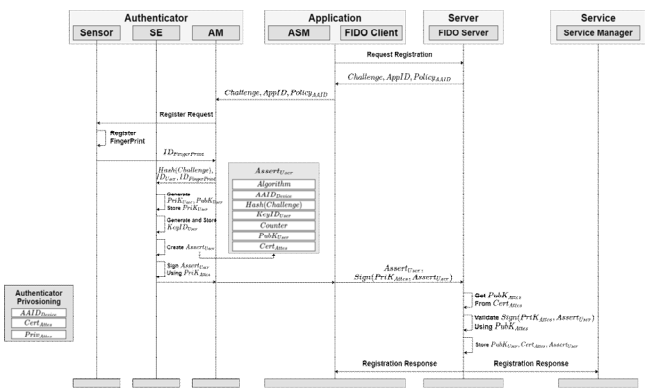
[그림 4]는 실제 FIDO 인증 시스템의 하드웨어 및 소프트웨어 구조이다. 특히 시각장애인도 쉽게 사용할 수 있도록 외부 구조를 단순화했고, 소리를 통해 진행 상황을 알려주는 Buzzer 기능을 추가했다. 주요 구성요소의 역할은 [표 4]로 정리했다. 개발 환경에 대한 설명과 통신 과정에서의 데이터 Log는 참고문헌 [10]의 영상 링크에서 자세히 확인할 수 있다.

[표 4] FIDO 인증 시스템 구성요소

구성요소	설명
Raspberry Pi	• FIDO Client 역할, Raspberry Pi 부팅과 동시에 에이전트 파일이 자동 실행되도록 설정
Tomcat	• FIDO Server와 연동, Apache에서 개발한 웹 애플리케이션 Server
Docker	• FIDO Server는 Docker 환경에서 실행됨, 가상화 환경의 컨테이너 기반 Server 관리 툴
Firebase	• 인증 성공 시 Service Manager에게 푸시 알림 전송됨, FCM(Firebase Cloud Messaging) 이용
Arduino	• AM(Authenticator Module) 역할, SE와 각종 센서를 제어하는 마이크로컨트롤러
SE	• RoT 환경 제공, 개인키 및 생체 정보 저장
Fingerprint	• 지문 센서, 지문 정보를 디지털 데이터로 변환
Button	• 버튼 센서, 인터럽트로 Arduino에 신호 전달
Buzzer	• 알림 센서, 시각장애인을 위한 음성 안내 기능

3.3 Sequence Diagram

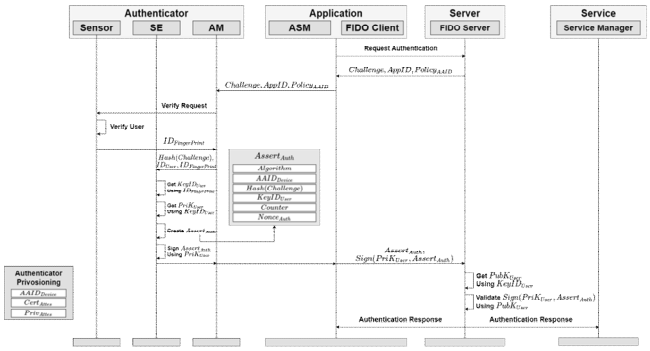
3.3.1 등록



[그림 5] 등록 단계

등록 단계는 KHU-FIDO Authenticator에서 생성된 사용자 정보를 FIDO Server에 등록하는 과정이다. FIDO 인증 시스템의 RoT 환경인 SE에서 사용자의 공개키-개인키 쌍이 생성된다. 개인키와 사용자의 지문 정보는 SE 내부의 안전한 저장소에 보관되고, 공개키와 증명 정보는 FIDO Server에 전달된다. FIDO Server는 Metadata를 이용해 공개키와 증명 정보의 신뢰성을 검증하고, 데이터베이스에 공개키와 증명 정보를 저장한다.

3.3.2 인증



[그림 6] 인증 단계

인증 단계는 등록된 사용자 정보를 이용해 전자서명을 수행하는 과정이다. KHU-FIDO Authenticator는 입력받은 지문과 SE에 저장된 사용자 지문 정보의 일치 여부를 판단하고, 개인키를 이용해 전자서명을 생성한다. SE는 APDU(Application Protocol Data Unit) 프로토콜을 이용해 FIDO Client와 통신하면서 인증을 수행한다. 전자서명은 증명 정보와 함께 FIDO Server에 전달된다. FIDO Server는 공개키와 증명 정보를 이용해 전자서명을 검증하고, 결과를 Service Manager에게 반환한다.

4. 결 론

본 논문은 시각장애인도 쉽게 사용할 수 있는 FIDO 인증 시스템을 제안하고 있다. 특히 핀테크와 같이 본인인증이 필요한 첨단 ICT 서비스의 경우 FIDO 인증 시스템이 도입된다면 시각장애인의 접근성은 크게 향상될 것으로 예상한다. 본 논문을 시작으로 ICT 분야에서 배리어-프리 환경을 구축하기 위한 담론이 형성되기를 기대해본다.

참고문헌

[1] 김정언·노용환·최두진·정부연·김재경, 「고령화와 정보격차; 정보격차 결정요인 분석」 정보통신정책연구원, 16-17. (2007)
[2] 한국장애인고용공단, 「2020년 보조공학기기 지원안내서」 4-6. (2020)
[3] 국가인권위원회, 「장애인 건강권 증진방안에 관한 연구」 58-65. (2014)
[4] 손지영·김동일. 「장애학생을 위한 스마트러닝 환경 구축의 정책적 방향 탐색」 특수교육저널, 453-480. (2011)
[5] 김경식, 「스마트폰 이용이 시각장애인 삶에 미치는 영향」 에이블뉴스, (2016)
[6] 한국정보통신기술협회, 「표준안내서 사용자 인증 - 파이도(FIDO)를 중심으로」 11-18. (2017)
[7] FIDO Alliance, 「FIDO UAF Protocol Specification」 FIDO Alliance Review Draft, (2017)
[8] Global Platform, 「Secure Element Configuration v2.0」 (2018)
[9] 박우진, 「SE를 이용한 FIDO Authenticator 설계」 한국소프트웨어종합학술대회 논문집, 1654-1656. (2019)
[10] 시연 영상, https://youtu.be/5gr_ALTcr3s