



스마트폰 기반의 물리시설 접근제어 기술

AutoPassword IoT Controller 제품소개서

01

제품 개요

02

주요 특징

03

레퍼런스

04

회사소개

스마트폰 기반 물리시설 접근제어 기술



**AutoPassword
IoT Controller**



**AutoPassword
ID Card**

AutoPassword IoT Controller는 스마트폰 기반 물리시설 접근제어 솔루션으로, 물리시설이 기존의 지문인식기나 얼굴인식기와 같이 사용자의 생체정보를 직접 수집·저장하는 방식의 한계를 해결하기 위해 설계된 기술입니다.

본 솔루션은 사용자의 생체정보를 물리시설이나 서버에 저장하지 않고, 사용자 스마트폰에 내장된 생체인증 기능을 통해서만 접근 요청을 수행하며, 검증된 인증값만을 서버 기반 상호인증 구조로 전달하여 물리시설 접근을 제어합니다. 본 기술은 국제표준 ITU-T X.1268에 기반합니다.



Demo

AutoPassword ID Card ITU-T X.1268

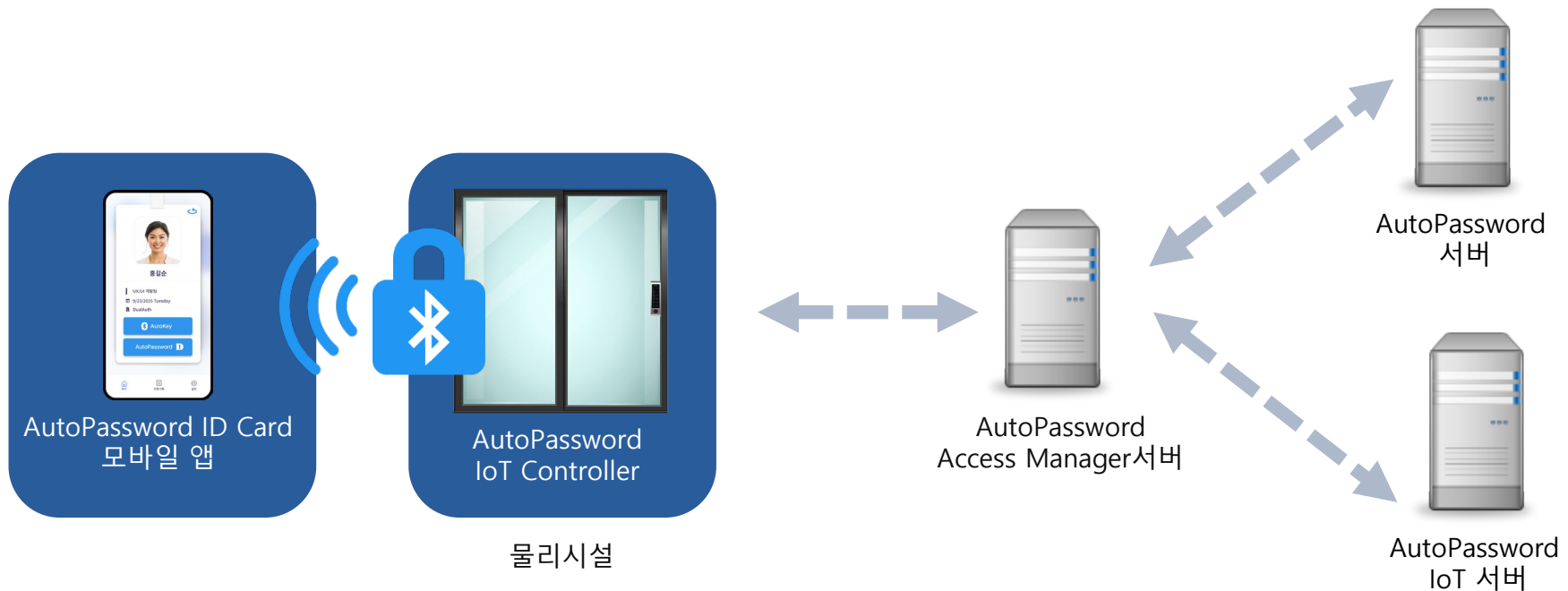
Door Access Control

<https://youtu.be/S3favCBySLY>

AutoPassword IoT Controller 아키텍처

스마트폰 생체인증을 물리시설 접근제어에 적용하기 위해서는 기존 물리시설에 AutoPassword IoT Controller를 부착하고, AutoPassword Server 및 AutoPassword Access Manager Server를 구성한 뒤 사용자에게 AutoPassword ID Card 모바일 앱을 배포하면 됩니다.

AutoPassword IoT Controller는 블루투스(BLE) 인증 비컨을 주기적으로 송출합니다. 인증비컨은 시설 식별값에 60초마다 변경되는 동적 인증값이 포함되어 있어 고정 신호 복제에 의한 리플레이 공격을 원천적으로 차단합니다. 사용자는 BLE 유효 범위(약 10m) 이내에서만 시설을 확인할 수 있으며, 확인된 시설을 스마트폰 화면에서 직접 선택한 후 스마트폰 생체인증을 통해 명확한 시설 사용 의도를 전달합니다. 요청된 시설 사용 요청은 AutoPassword 서버에서 사용자 인증·권한·시설 정보 등을 검증한 후 물리시설을 작동시킵니다.



01

제품 개요

02

주요 특징

03

레퍼런스

04

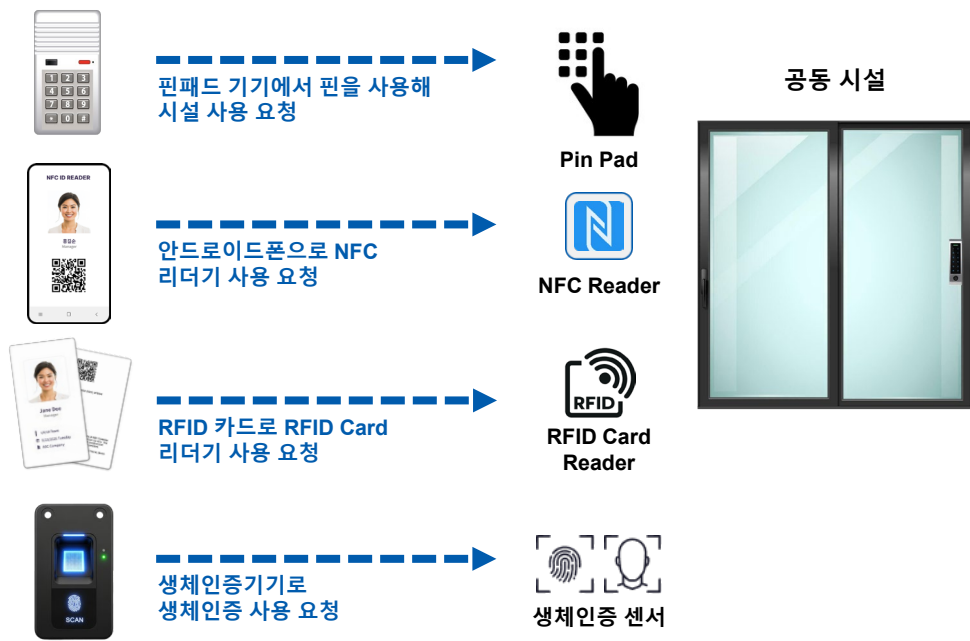
회사소개

특징 1 – 공동시설에 최적화된 스마트폰 기반 접근제어 기술

여러 사용자가 함께 이용하는 공동시설의 경우, 개인용 IoT 기기와 달리 높은 범용성과 표준화된 사용자 경험이 요구됩니다. 공동 비밀번호나 출입카드 방식은 분실·도용 위험이 높고 사용자 변경 및 관리가 어렵다는 한계가 있으며, 기존 NFC 카드 에뮬레이션 방식은 안드로이드 폰만 지원하여 아이폰 사용자에게 대한 공동시설 적용에 제약이 있었습니다.

AutoPassword ID Card는 아이폰과 안드로이드폰을 구분하지 않고 동일하게 동작하여 표준화된 사용자 경험을 제공하며, 스마트폰 생체인증을 기반으로 작동하기 때문에 타인 도용이 불가능합니다. 또한 별도의 리더기를 외벽에 노출할 필요 없이 천정 매립형 설치가 되어 외관 훼손없이 공동주택·사무빌딩·공공시설에서 사용 할 수 있습니다.

입력기반의 시설 접근제어 기술



시설 출력 기반의 시설 접근제어 기술

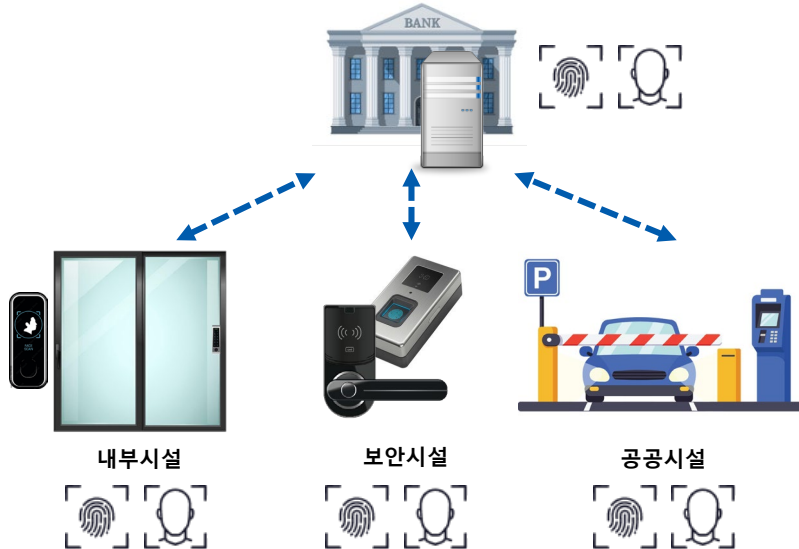


특징 2 – 개인의 생체정보를 수집하지 않는 안전한 생체인증 기술

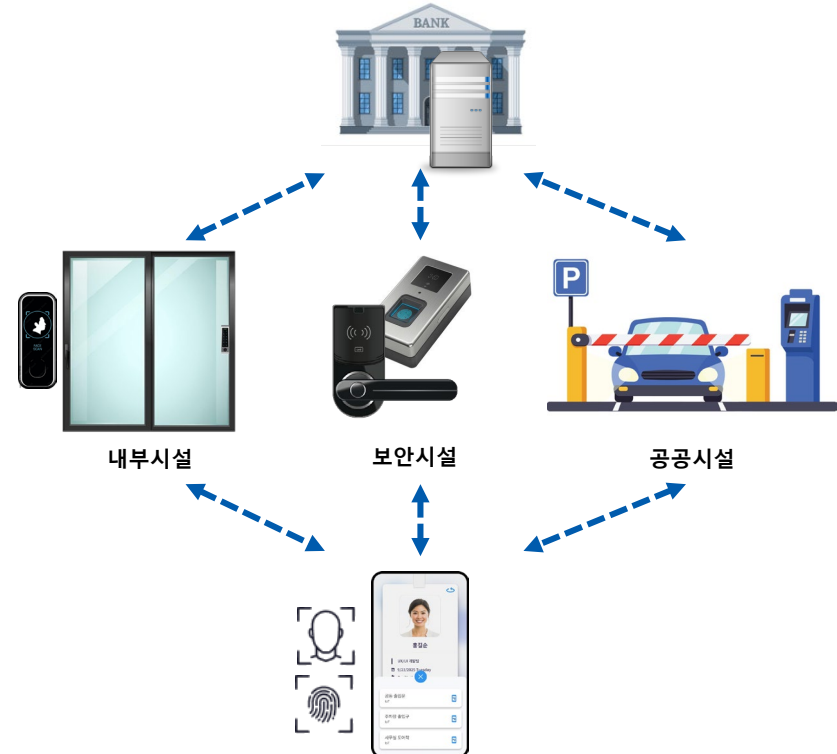
AutoPassword ID Card는 사용자가 물리시설에 생체정보를 직접 입력하거나 등록하는 방식이 아닙니다. 물리시설이 BLE 인증 비컨을 송출하고, 사용자는 스마트폰에서 시설의 인증 비컨을 검증한 뒤 스마트폰 생체인증을 통해 시설 제어 명령을 네트워크로 전달합니다.

이러한 대역외(Out-of-Band) 상호인증 구조로 인해 물리시설마다 별도의 생체정보 DB를 구축할 필요가 없으며, 사용자의 생체정보는 오직 개인 스마트폰 내부에서만 보관·사용됩니다. 이를 통해 프라이버시 침해 위험을 원천적으로 제거합니다.

시설마다 생체 정보관리가 필요한 **대역내 생체인증**



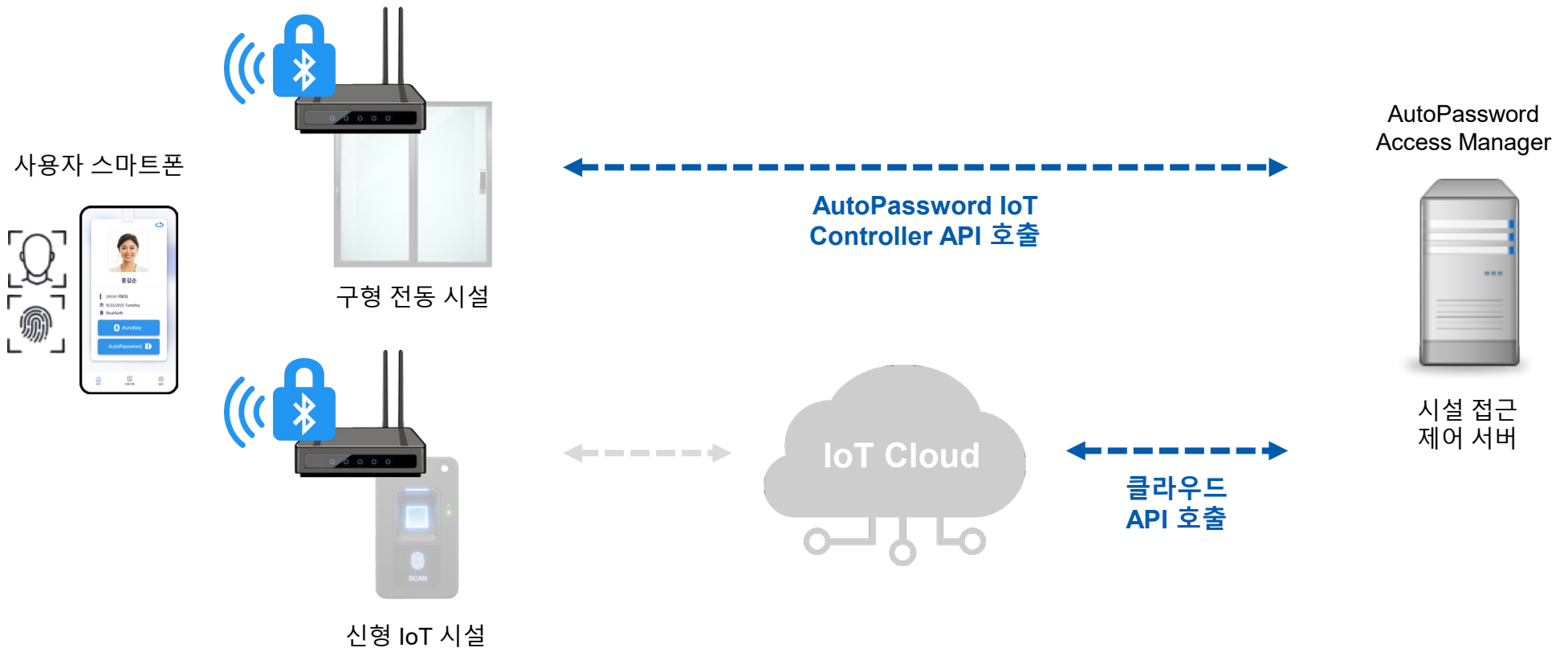
시설마다 생체 정보관리가 필요없는 **대역외 생체인증**



특징 3 – 구형 전동시설부터 개인용 IoT 기기까지 공용 IoT기기로 전환

AutoPassword IoT Controller는 공용시설에서 사용 중인 전동출입문, 전등 스위치, 주차 차단기와 같은 구형 전동시설을 스마트폰으로 제어 가능한 공용 IoT 기기로 전환해주는 컨트롤러입니다.

또한 개인 사용을 전제로 설계된 최신 IoT 기기의 경우에도, AutoPassword IoT Controller를 추가 설치하고 해당 IoT 기기의 클라우드 서버와 API 연동을 통해 공용 환경에서 안전하게 사용할 수 있도록 확장할 수 있습니다



특징 4 – AutoPassword IoT Controller 상세 제원

AutoPassword IoT Controller는 인증 비컨을 송출하고 AutoPassword Access Manager 서버와 통신하기 위한 네트워크 API를 지원하는 IoT 제어 장치입니다.본 장치는 구형 전동시설의 동작 상태를 감지하기 위한 6개의 입력 포트와 제어 신호를 전달하기 위한 6개의 출력 포트(I/O Port)를 제공하며, 자동 도어, 주차 차단기 등 공용 전동시설의 상태 파악 및 원격 제어에 활용할 수 있습니다.



AutoPassword IoT Controller	
Model No	ES-MT1266
Manufacturer	eSTORM
Communication	Supports Wi-Fi 2.4 GHz and wired LAN communication
Power Supply	DC 5 V / 2 A
Control Voltage	≤ DC 12 V
Control Current	≤ 1 A
Switch Status Output	2-wire status detection
Detection Voltage	DC 3 V when switch is connected (ON)

01

제품 개요

02

주요 특징











03

레퍼런스

04

회사소개

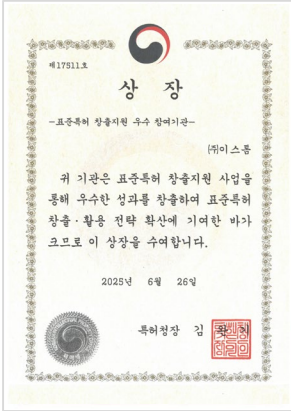
03 레퍼런스

 KB국민은행	KB국민은행 – 제로트러스트 도입 시범사업을 통한 상호인증 기반의 강화된 사용자 인증 체계 구축 및 적용
 우리은행	우리은행 – 우리은행 임직원 대상 패스워드리스 기반 PC 접근관리 및 애플리케이션 접근관리
 유안타증권	유안타증권 – 유안타증권 임직원 대상 패스워드리스 기반 PC 접근관리 및 애플리케이션 접근관리
 통계청	국회도서관 – 통계청에서 도입하여 도서관내에 설치된 통계정보 열람 PC에 대한 로그인 권한 제어
 KORAIL	한국철도공사 – 차세대 나라장터 시스템 사용자 단말 인증 보안 강화를 위한 패스워드리스 인증 구축
 KOMSA 한국해양교통안전공단	한국해양교통안전공단 – 외부 웹메일 로그인 시 패스워드리스를 이용한 사용자 로그인 보안강화
 한국관광공사	한국관광공사 – 대한민국구석구석 시스템 개발 운영을 위한 관리자 및 협력사 인증 보안 강화
 KIAT	한국산업기술진흥원 – 임직원용 내부 업무시스템에 도입하여 내부망과 외부망 에서의 개별적인 접근제어 운영
 구리시	구리시청 – 중요 서버 접근 시 로그인 보안 및 패스워드 자동변경을 통한 보안 컴플라이언스 대응
 CW 건설근로자공제회 Construction Workers Mutual Aid Association	건설근로자공제회 – 내부 시스템 운영 개선을 위한 서버 시스템의 로그인 보안 강화

주요 시상

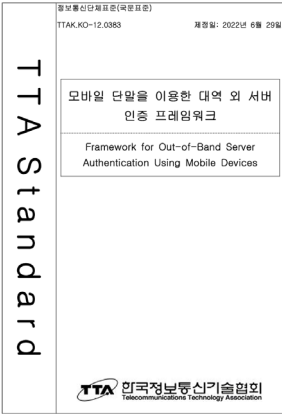


대한민국 인터넷대상

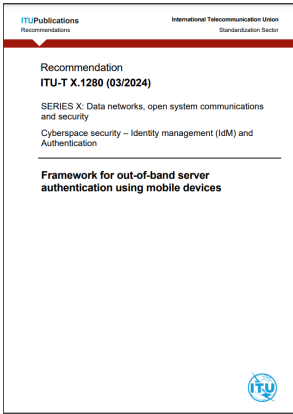


특허청장상

표준 기술



[TTAK.KO-12.0383](https://www.tta.or.kr/standard/ITAK-KO-12.0383)



[ITU X.1280](https://www.itu.int/ITU-T/recommendations/TXT/X.1280-03-2024)

주요 발표



NEW YORK
FinovateFall 2016
Presenter

<https://youtu.be/w2NtbPVaHSk>



<https://youtu.be/rBUK45fdBtY?t=838>



NEW YORK
FinovateFall 2018
Presenter

<https://youtu.be/-DG-LYmRVfk>



<https://youtu.be/nF72E24BCec>

주요 인증



ISO/IEC 25023, 25051, 25041



01

제품 개요

02

주요 특징

03

레퍼런스

04

회사소개

패스워드리스 기반 신원인증 및 접근관리 전문회사

듀얼오스는 패스워드리스 기반 신원인증 및 접근관리 솔루션을 제공하는 기술회사입니다. 듀얼오스의 주요 솔루션으로는 패스워드리스 솔루션, 통합ID 및 접근관리 솔루션, 모바일 신분증 솔루션, 물리시설 접근관리 솔루션 등이 있습니다. 이 기술들은 UN산하 국제표준화기구인 ITU에서 X.1280와 X.1268로 제정될 만큼 뛰어난 사용성과 보안성을 갖추고 있으며, 제로트러스트 시대에 핵심 기술로 주목받고 있습니다. 듀얼오스는 ESG 실현을 위하여 전세계 B2C 온라인 서비스의 패스워드 문제를 해결할 수 있는 무료 Passwordless X1280 솔루션을 스위스 제네바에 위치한 패스워드리스 얼라이언스를 통하여 보급하고 있습니다.

제로트러스트 구축을 위한 패스워드리스 기반 신원인증 및 접근관리

패스워드리스 인증기술

AutoOTP 

AutoPassword 

통합ID 및 접근관리 기술

AutoPassword 

 AutoPassword
Access Manager

모바일 신분증 기술

 AutoPassword
ID Card

 AutoPassword
ID Card Reader

물리시설 접근관리 기술

 AutoPassword
ID Card

 AutoPassword
IoT Controller



- 회 사 명 : (주)듀얼오스
- 홈페이지 : www.dualauth.com
- 문의메일 : support@dualauth.com

도입 문의

- 주소 : (08589) 서울특별시 금천구 디지털로 130 남성프라자 13층
- 전화번호 : +82-2-6925-1305
- 사업문의 : sales@dualauth.com



감사합니다.