
SaaS형 MFA(2차 인증) 서비스

signplus

2023. 03

한국정보인증(주)

Contents

I

한국정보인증 소개

- 01. 회사 개요
- 02. 비즈니스 영역

II

SignPLUS 소개

- 1. MFA(2차 인증) 필요성
- 2. SignPLUS 개요
- 3. SignPLUS 시스템 구성
- 4. SignPLUS 장점
- 5. SignPLUS 차별성
- 6. SignPLUS 기술 우수성

별첨

SignPLUS 이용방법
SignPLUS 주요 기능
Reference

한국정보인증 소개

01. 회사 개요

02. 비즈니스 영역

• 차세대 인증 기술을 선도하는 ‘한국정보인증’

한국정보인증은 차세대 인증 기술을 선도하는 IT보안 전문 기업입니다.

20여 년간 전자서명 인증서비스 / 보안인증솔루션 운용 능력을 기반으로 자율주행 보안인증 플랫폼 및 생체인증 서비스 등 보다 안전하고 편리한 세상을 만들기 위해 노력하고 있습니다.

<2022년 12월 말 기준>

회사명	한국정보인증 주식회사
대표이사	김상준
설립일	1999년 7월 2일
자본금	208억원
임직원수	142명
매출액	878억
사업영역	PKI 기반 인증 서비스 및 기업/금융 인증 보안 솔루션
주소	경기도 성남시 분당구 판교로 242 판교디지털센터 C동 5층
홈페이지	www.kica.co.kr
연락처	전화 1577-8787 팩스 02-323-8513



- ✓ 국가 지정 제 1호 공인인증기관
- ✓ 본인확인기관 / 전자서명사업자 허가
- ✓ 국정원 보안성 검토필 제품 인증 획득
- ✓ 국내 최초 FIDO 인증 상용화 (삼성페이)
- ✓ 국내 최초 OTP 개발·공급사

비즈니스 영역

통합인증 보안/ 전자금융 OTP 인증

〈통합 인증 보안 솔루션〉
ID/PW에 2차 인증(생체인증, OTP, QR 등)을 적용한
보안 플랫폼

〈전자금융용 OTP〉
안전한 전자금융거래를 위한 인증보안 서비스

자율주행 보안/ IOT 보안

〈자율주행차량 관련 R&D〉
차량 프라이버시 보호형 Vehicular PKI 인프라 기술 개발

〈IOT 기기인증 서비스〉
IOT 기기를 대상으로한 인증서 발급 서비스

클라우드 인증

〈생체인증 및 페이 서비스〉
지문, 홍채, 안면 등 생체 기반 비밀번호 대체 서비스 및
국내 최초 생체인증서비스 ex)삼성페이, LG페이

〈통합 인증 보안 서비스〉
ID/PW에 2차 인증(생체인증, OTP 등)을 적용한
SaaS형 보안 서비스

전자계약

〈Sign OK〉
회원가입 필요 없는 편리한 전자 계약 서비스
이메일, SNS, MMS 통한 모바일 계약 기능

전자서명인증

〈공동인증서비스〉
전자인찰, 전자세금계산서 등에 쓰이는
공동인증서 발급, 솔루션

〈S-PASS(간편인증)〉
안전하고 간편한 전자서명인증 서비스

SSL(보안서버인증서)

〈SSL/TSL〉
웹서버 간 데이터 암호화 프로토콜 서비스



• 국내 No.1 인증서비스 & 인증 솔루션

국내 1호 공인인증기관으로 시작으로 정보보안 서비스의 대표 기업 한국정보인증은 공공, 금융, 교육, 기업 등 3,000여 개의 사용처를 대상으로 현재 인증 및 보안 서비스, 솔루션 등을 제공하며 법인인증서 및 국내 OTP 시장, 2차 인증 시장(조달기준)의 국내 점유율 1위를 유지하고 있습니다.

SignPLUS 소개

1. MFA(2차 인증) 필요성
2. SignPLUS 개요
3. SignPLUS 시스템 구성
4. SignPLUS 장점
5. SignPLUS 차별성
6. SignPLUS 기술 우수성

MFA(2차 인증) 필요성

해킹은 인증 도용으로 시작



사용자 인증 정보 도용 피해율

20%

2022년 주요 기업 해킹 평균 피해액

43억원



**생체인증, OTP 등 추가 인증 절차
통과 시에만 시스템 접속 허용**

보안정보 내부자 유출이 70%



산업 정보 유출 피해 중소기업 비율

84%

연간 주요 기업 정보 유출 피해액

56조원



**생체인증, mOTP 기반한 인증 정보로
보안 위반 방지, 로그인 로그 관리**

비밀번호 정책의 낮은 실효성



비밀번호 약간 변경 및 재사용 비율

50% ↑

비밀번호 변경 따른 스트레스 체감도

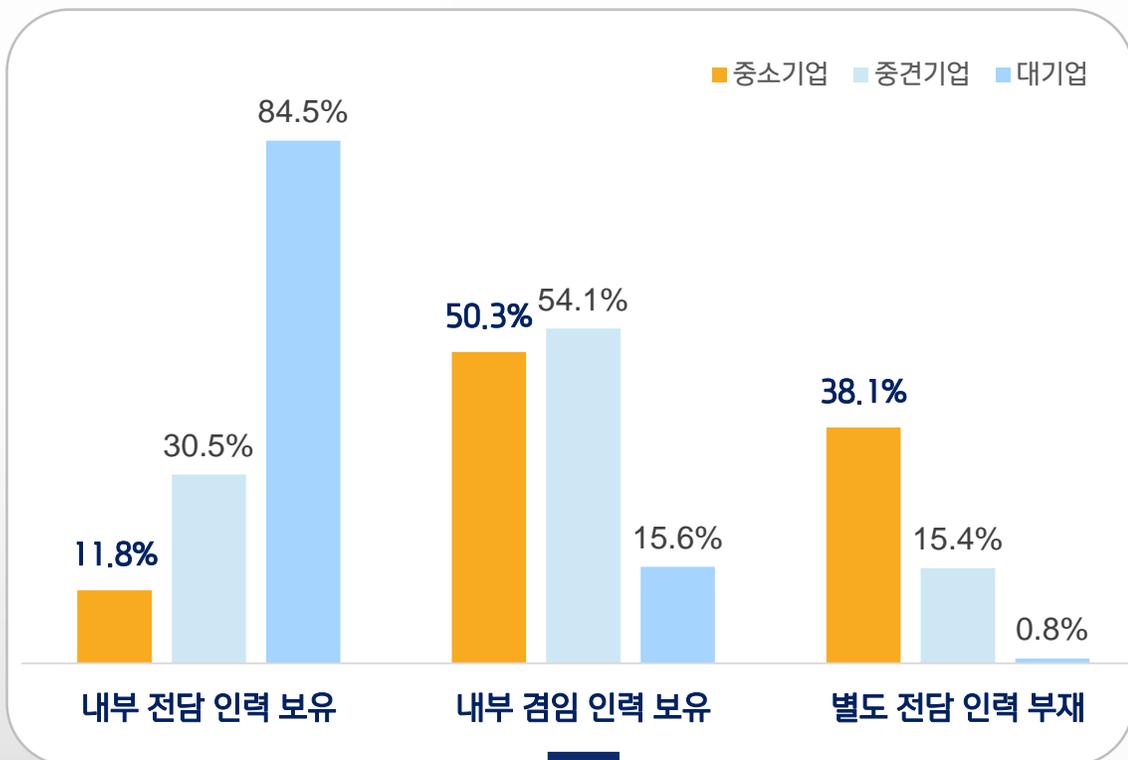
78%



**FIDO(생체인증), OTP 등 사용으로
비밀번호 정책 보완 및 편리성 증대**

MFA(2차 인증) 필요성

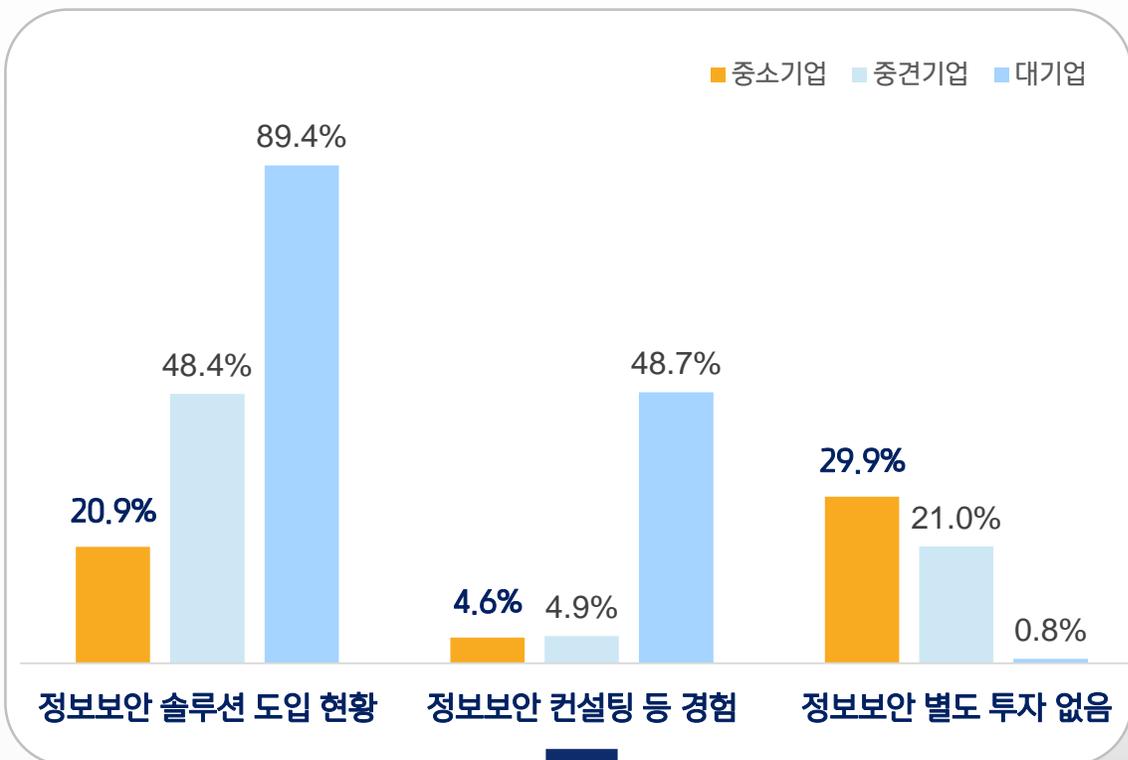
정보보안 전문 인력 부재로 위기 대응력 부족



출처: 2021 중소기업 기술보호 수준 실태조사 보고서

**생체인증(FIDO), OTP 등 추가인증 도입으로
정보보안 대응력 보완 및 내·외부 리스크 사전 예방**

정보보안 관련 소극적인 투자로 낮은 보안 역량



**SaaS형 MFA(2차 인증) 구독 서비스로
중소기업 비용부담 해소, 보안 역량 향상에 기여**

COPYRIGHT 2021 KICA Inc. ALL RIGHTS RESERVED

MFA(2차 인증) 필요성

ISMS 인증 기준 및 추가인증 도입 관련 법규

〈개인정보보호법 제29조(안전조치의무)〉

〈개인정보의 기술적·관리적 보호조치 기준 제4조 4항(접근통제)〉

〈개인정보의 안전성 확보 조치 기준 제5조(접근 권한의 권리)〉
“...비밀번호를 5회 이상 틀린 경우, **추가인증으로 접근권한자임을 확인...**”

〈개인정보의 안전성 확보 조치 기준 제6조(접근통제)〉
“...외부에서 접속한다면, 안전한 접속수단이나 **추가인증 수단을 적용...**”



추가적인 인증 수단(인증서, OTP 등)을 적용



개인정보 보호법에서는 추가인증(인증서, OTP 등) 도입과 관련하여 의무화할 것을 명시함

추가 인증 수단



공동/사설인증서(PKI)



일회성 비밀번호(OTP)



생체인증(FIDO)

누구나 손쉽게 사용 가능한 SaaS형 2차인증 서비스



다양한 인증 방안

- 고객사에 최적화된 인증 방법
- 생체인증, OTP 등 다양한 방법

클라우드 기반 솔루션

- 클라우드 형태 관리 편의성 극대화
- 손쉬운 업데이트, 시스템 연동



신뢰성이 보장된 운영 환경

- 안정적인 운영 시스템
- 안전한 키관리 백엔드 시스템

SignPLUS

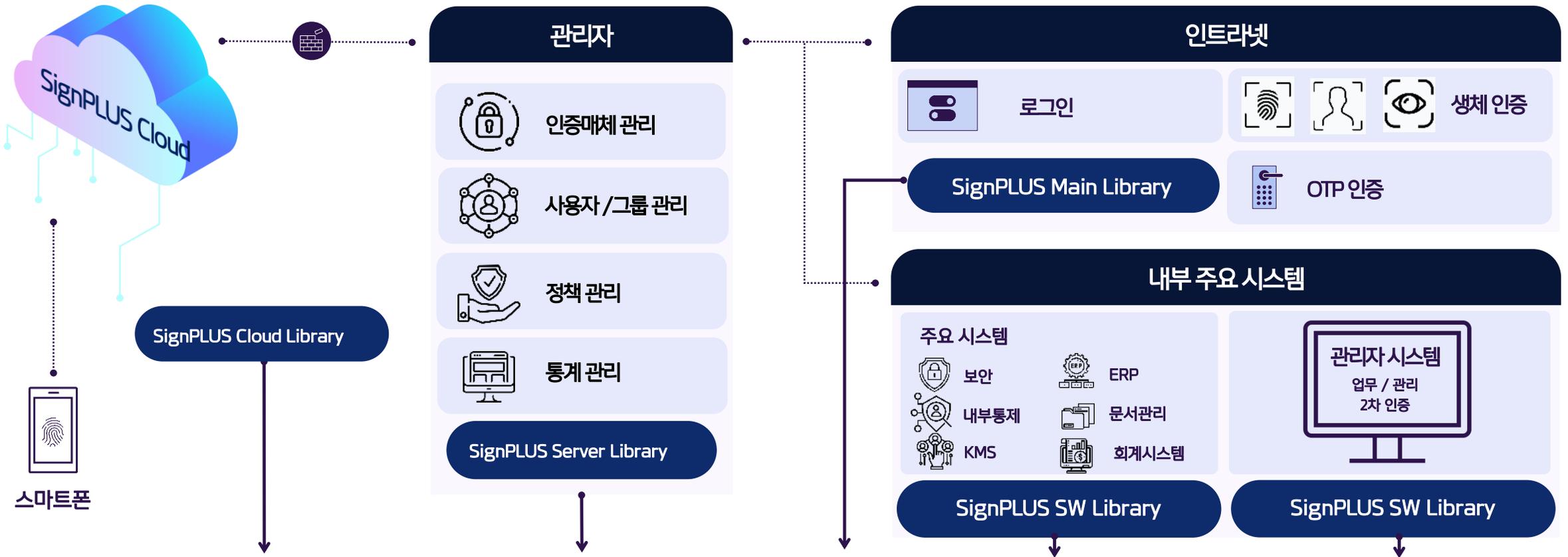


“국내 최초 SaaS형 MFA 솔루션”

- ✓ 별도 서버 구축이 필요 없는 SaaS형
- ✓ User 수 기반 라이선스 구매의 구독 서비스(월간/연간)
- ✓ FIDO(지문, Face ID), OTP, QR 등 다양한 인증 지원
- ✓ 오류에 대한 상시 패치 및 업그레이드 지원
- ✓ 웹 및 오픈 네트워크 업무시스템 연동 지원

SignPLUS 시스템 구성

회사 내부 인트라넷 & 주요 시스템 접근 관리 기능 및 모듈 제공



도입 비용 이점

- 1 저렴한 라이선스 “1 User 3,000원/월”
- 2 필요한 라이선스 수량/기간에 따라 결제
- 3 서버 구축 Zero, 유지보수 비용 Zero

서버 및 솔루션 관리의 편리함

- 1 인프라 관리의 피로도는 LOW
- 2 관리자 대시보드로 유저 관리 편의성 High
- 3 EOS, 업그레이드 관리 필요 없는 SaaS



클라우드 전환 시대, 보안을 서비스로 편리하게

기업과 금융, 공공 모든 분야에서 IT인프라가 클라우드 환경으로 전환되고 있습니다. 클라우드 환경의 SaaS, MFA 'SignPLUS'를 통하여 보안에서도 IT인프라 전환의 이점을 누릴 수 있습니다.

SignPLUS 차별성

프리웨어 대비 더 편리하고, 더 안전한 서비스

차별성

구분	SignPLUS	구글 OTP	비교
구축/연동 방법	API 연동	구글 인증모듈 설치 + 인증 체계 구성 필요	API로 쉽게 연동함으로써 별도 실행 파일 다운로드 불필요 및 사용 편의성 증대
관리자 콘솔	제공	미제공	관리자 페이지에서 MFA 발급에 대한 자체 관리 및 파악에 용이
로그 관리 항목	로그 인증 내역 및 통계 제공	별도 로그 관리 없음	사고 발생 시 데이터 복원, 사고원인 규명 등 가능
인증매체 지원	생체인증(FIDO), 모바일 OTP	모바일 OTP	인증수단 선택 통한 빠르고 간편한 본인인증 진행
재발급 방법	관리자 페이지 내 간편 발급	백업 복구코드 입력(분실시 불가능)	사용자의 문제 발생에 따른 요청 시 대응 가능
재발급 시 로그인 변경	APP 재등록 후 즉시 사용	연동시스템 별 재등록 후 사용	사용자 인증매체 분실에 따른 관리자 공수 최소화

특장점

보안성

표준 해시알고리즘을 통해
일회용 암호키로 데이터 보호

편리성

한 번만 연동 또는 등록하면
별도 추가 작업이 불필요

관리성

제공된 로그 및 발급 관리로
문제 원인 파악 및 대응 가능

SignPLUS 기술 우수성

FIDO와 OTP를 융합한 안전한 인증 제공

최고의 인증 보안을 위한 기술 적용

표준을 준수하여 확장성 보장



FIDO 국제 인증 획득



OTP 기술과 융합 편리성 극대화



검증된 기술력

FIDO 서버



FIDO 클라이언트



FIDO 보이스 인증장치



안전하고 편리한 2차 인증 지원을 통하여 시스템 신뢰성 향상

최신 인증 기술 적용

One Time Password 원천 기술 보유
생체 인증 기술 보유



강화된 보안

지속적으로 변하는
암호화 기술 융합 적용



연계가 가능한

Cloud Service 형태로
다양한 기기 및 서비스에 적용 가능



편리한 플랫폼

표준규격에 맞게 개발, 라이브러리 제공
쉬운 시스템 적용



SignPLUS 이용방법

01. 도입 방법(관리자)
02. 발급 방법(사용자)
03. 사용 방법

SignPLUS 도입 방법(관리자)

SignPLUS 연동 절차

회원가입(관리자)

상품 결제

2차 인증 연동(API)

사용자(일반 사용자) 추가

2차 인증매체 발급(APP)



- 관리자 회원가입 후, 상품 결제(카드, 계좌이체, 무통장) 진행
- 관리자 페이지 내 '개발자시스템' 가이드 따라 연동할 업무시스템 연동 진행
- 사용자 등록 메뉴 통해 일반 사용자 개별 및 일괄 등록
- 일반 사용자들 대상 QR 발송하여 QR코드 발급 or 간편발급 안내 진행

- 앱스토어, 플레이마켓 통해 SignPLUS 다운로드
- 회사ID/개인ID&PW 통한 간편발급 진행
- 관리자로부터 QR코드 수신 시 QR코드 스캔하여 발급 진행

SignPLUS 발급 방법(사용자)

SignPLUS 인증매체 발급 절차

1



관리자가
사용자 등록

signplus
App 다운

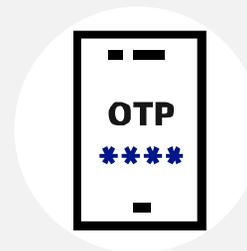
2



원터치로
간편 발급

계정 정보
입력

3



SignPLUS로
사용자 인증

- 관리자 페이지 내 사용자 등록
- 사용 인원의 ID, 이름, 이메일 등 등록

- 사용자는 앱 실행 후 간편 발급 진행
- 별도 추가 작업 없이 바로 발급

- 회사 ID, 사용자 ID, 초기 PW 등 입력
- 개인정보 동의 및 본인확인 후 발급 완료

SignPLUS 사용 방법

SignPLUS 인증(로그인) 절차



- 업무시스템 로그인창 내 ID/PW 입력
- SignPLUS App 자동 실행 또는 Push 터치

- (OTP) SignPLUS에서 OTP 확인 후 입력
- (생체인증) SignPLUS에서 생체인증 진행

- (OTP) 로그인창 내 OTP 입력 후 로그인
- (생체인증) 생체인증 완료 후 자동 로그인

SignPLUS 주요기능

01. 대시보드

02. 사용자/그룹관리

03. OTP관리/이용 설정

04. 정책 설정

05. 결제 관리

06. 설정/관리자

07. 통계

08. 로그 조회

09. 개발자 가이드

홈(대시보드)

관리자 포털의 홈(대시보드)를 통해 전체적인 서비스 사용 현황을 살펴볼 수 있습니다.

The screenshot displays the SignPlus Admin Portal Home Dashboard. It features a left-hand navigation menu with options like '홈', '대시보드', '사용자', '2차인증 연동', 'OTP', 'OTP 이용 정책', '결제 관리', '고객지원', '설정', '통계', '로그 조회', and '개발자 가이드'. The main content area is divided into several sections:

- Alerts:** Four action items with green checkmarks: '사용자를 추가해 주세요.', 'OTP를 발급해 주세요.', '03 2차 인증 연동을 추가해주세요.', and '(권장) OTP 이용 정책을 등록해주세요.'
- Usage Statistics:** A section titled '이용중인 상품 : FREE' showing a 40% usage rate. It lists '제공 사용자 수' (10), '등록된 사용자 수' (4), and '진여 사용자 수' (6). A note indicates '상품 만료일 : 무제한'.
- User Groups:** A section titled '사용자 및 그룹 상태' showing counts for '사용자' (4), '그룹' (2), and '정기 미사용자' (0).
- SignPlus 공지사항:** A section for announcements, currently showing a '테스트' notice dated 2023-01-16 14:59.

사용자/그룹 관리

- 관리자 포털의 사용자/그룹 관리를 통해 사용자를 등록하고 그룹별 구분을 설정할 수 있습니다.

The screenshot displays the SignPLUS user management interface. A modal window titled '그룹 추가하기' (Add Group) is open, allowing for the addition of a new group. The modal includes a search bar for user IDs or names, a table of existing users, and a '저장' (Save) button.

번호	사용자 ID	사용자 이름	
<input type="checkbox"/>	4	mich	김영수
<input type="checkbox"/>	3	bch0	나영희
<input type="checkbox"/>	2	kwj1	이미래
<input type="checkbox"/>	1	jekir	정인한

OTP 관리/이용 설정

- 관리자 포털의 OTP관리/이용 설정을 통해 OTP를 발급 및 폐기하고 유효 정책을 설정할 수 있습니다.

The screenshot displays the SignPLUS administrator portal interface. The left sidebar contains a navigation menu with the following items: 홈, 사용자, 2차인증 연동, OTP (selected), OTP 관리, OTP 이용 설정, OTP 이용 정책, 결제 관리, 고객지원, 설정, 통계, 로그 조회, and 개발자 가이드. The main content area is titled 'OTP' and includes a subtitle 'OTP 발급 현황 및 목록을 확인할 수 있습니다.' The top right corner shows the user's name '이용문익', the role '사용방법', the last login time '마지막 로그인 2023년01월19일 11시13분32초', and a '로그아웃' button.

The main content area is divided into two sections:

- OTP 발급 현황**: A summary dashboard showing three metrics:
 - 전체 OTP**: 10 (Total OTP count)
 - 사용한 OTP**: 2 (Used OTP count)
 - 잔여 OTP**: 8 (Remaining OTP count)
- OTP 발급 목록**: A table listing issued OTPs with a search bar and a dropdown menu for the number of items to display (currently set to 10).

The 'OTP 발급 목록' table contains the following data:

번호	사용자ID	사용자명	OTP 일련번호	발급 상태	발급 일시
2	bdh0	나영희	714bd92d9	발급 완료	2023년01월09일 10시37분48초
1	kwj]	이미재	e9bcbbb58	발급 완료	2022년12월01일 12시58분29초

- 관리자 포털의 OTP관리/이용 설정을 통해 OTP를 발급 및 폐기하고 유효 정책을 설정할 수 있습니다.

The screenshot displays the SignPLUS administrator portal interface for managing OTP policies. The page title is "OTP 이용 정책 등록" (OTP Policy Registration), with a subtitle indicating that policies can be registered through individual settings. The interface includes a navigation menu on the left with options like "홈", "사용자", "2차인증 연동", "OTP", "OTP 이용 정책" (selected), "결제 관리", "고객지원", "설정", "통계", "로그 조회", and "개발자 가이드". The main content area is divided into two sections: "정책 등록" (Policy Registration) and "정책 이름 및 대상 설정" (Policy Name and Target Setting). The "정책 등록" section contains five items: "정책 기본 정보" (Policy Basic Information), "기간 선택" (Period Selection), "정책 설정" (Policy Settings), "정책 만료 시 처리 방식" (Policy Expiry Handling Method), and "정책 설정 확인" (Policy Setting Confirmation). The "정책 이름 및 대상 설정" section includes input fields for "정책 이름" (Policy Name) and "대상" (Target), with a "다음 단계" (Next Step) button.

- 관리자 포털의 결제 관리를 통해 사용 중인 상품을 확인하고 유저 라이선스를 추가 구매할 수 있습니다.

The screenshot shows the SignPLUS administrator portal interface. On the left is a navigation menu with options like '홈', '사용자', '2차인증 연동', 'OTP', '결제 관리' (highlighted), '이용현황', '상품구매', '결제내역', '고객지원', '설정', '통계', '로그 조회', and '개발자 가이드'. The main content area is titled '상품 결제' and '상품을 결제합니다.' It is divided into two columns: '결제 상품 정보' and '주문 정보'.

결제 상품 정보

- BUSINESS**
- 10명 이상의 사용자인 경우 가장 경제적인 가격으로 이용할 수 있는 OTP 서비스 상품입니다.
- 제공 사용자 수 입력: 300 명 (10명 단위로 추가 가능합니다.)
- 기간 선택: 이용개월 선택 (1년, 3년)

주문 정보

- 주문금액: 29,808,000원
- 추가금액: 0원
- 총 결제금액: 29,808,000원
- 결제 수단: 신용카드, 실시간 계좌이체, 무통장
- 결제하기 버튼

Top right navigation includes '이용문의', '사용방법', '마지막 로그인 2023년01월19일 11시13분32초', and '로그아웃'.

설정/관리자

- 관리자 포털의 설정/관리자를 통해 MFA 마스터 권한을 가진 관리자를 추가, 제거할 수 있습니다.

signplus

관리자 목록 관리자 목록을 조회하고 상세정보를 열람할 수 있습니다.

이용문의 사용방법

마지막 로그인 2023년01월19일 11시13분32초

로그아웃

> 홈

> 사용자

> 2차인증 연동

> OTP

> OTP 이용 정책

> 결제 관리

> 고객센터

> **설정**

관리자

회사 정보

> 통계

> 로그 조회

> 개발자 가이드

관리자 목록

검색: 전체 검색어를 입력하세요.

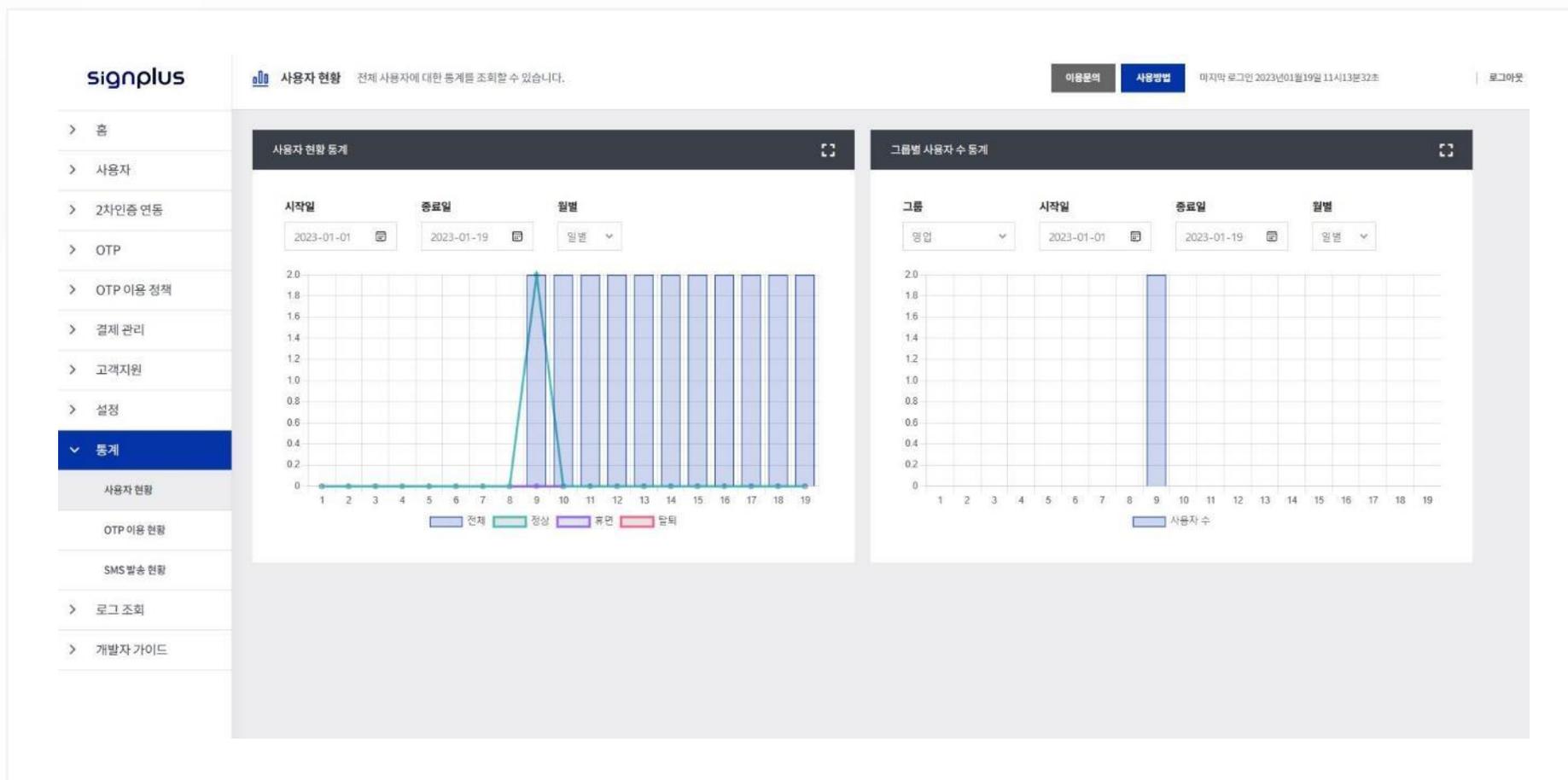
총 1 개 항목 중 10 개 항목을 조회 중입니다.

신규등록

번호	관리자 ID	대상	마지막 로그인 일시	마지막 로그인 IP
1	jek	abc, 영업	2023년01월19일 11시13분32초	922.168.92.11

1

- 관리자 포털의 '통계'를 통해 사용자 및 인증매체 발급현황, 매체별 인증 현황 등을 살펴볼 수 있습니다.



관리자 포털의 '로그 조회'를 통해 인증 로그 및 API 로그를 검색하고 살펴볼 수 있습니다.

API 로그 API 관리 기록을 조회합니다.

이용문의 사용방법 마지막 로그인 2023년01월19일 11시13분32초 로그아웃

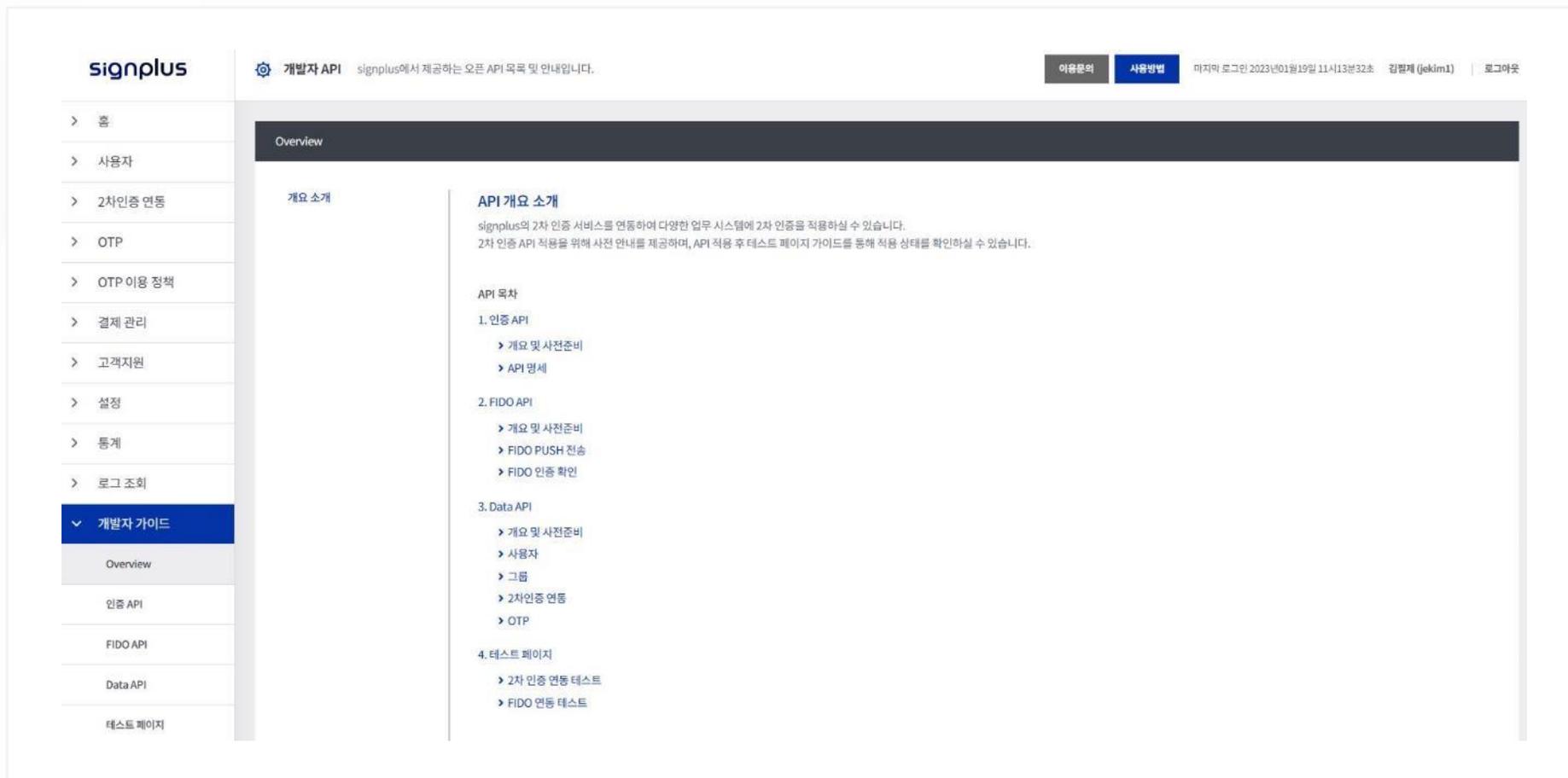
API 로그 목록

API 유형 전체 처리 결과 전체 시작일 년-월-일 종료일 년-월-일 검색 검색어를 입력해주세요

총 407 개 항목 중 10 개 항목을 조회 중입니다.

번호	로그 날짜	API 유형	사용자	처리 결과	리턴 코드	상태 메시지
407	2023년01월19일 11시49분12초	GET_AUTH_LOG_LIST	jek	200	OK	인증 로그 조회 성공
406	2023년01월19일 11시31분23초	GET_AUTH_LOG_LIST	jek	200	OK	인증 로그 조회 성공
405	2023년01월19일 11시17분48초	GET_USER_LIST	jek	200	OK	사용자 목록 조회 성공
404	2023년01월19일 11시17분46초	GET_GROUP_LIST	jek	200	OK	사용자 그룹 목록 조회 성공
403	2023년01월19일 11시17분32초	GET_AUTHPOLICY_LIST	jek	200	OK	인증 정책 목록 조회 성공
402	2023년01월19일 11시17분31초	GET_LCE_LIST	jek	200	OK	라이선스 목록 조회 성공
401	2023년01월19일 11시17분31초	GET_CLIENT_LIST	jek	200	OK	외부 연동 목록 조회 성공
400	2023년01월19일 11시17분13초	GET_OTP_LIST	jek	200	OK	OTP 목록 조회 성공
399	2023년01월19일 11시17분13초	GET_PROD_LIST	jek	200	OK	상품 목록 조회 성공
398	2023년01월19일 11시17분13초	GET_OTP_SUMMARY_STAT US	jek	200	OK	OTP 현황 요약 조회 성공

관리자 포털의 '개발자 가이드'를 통해 서비스 이용 방법에 대한 도움을 얻을 수 있습니다.



주요 관련 법령

MFA(2차 인증)도입 관련 법령



추가인증 도입 관련 법령

개인정보 보호법 제29조(안전조치의무)

개인정보처리자는 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 내부 관리계획 수립, 접속기록 보관 등 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하여야 한다.

개인정보의 안전성 확보 조치 기준 제5조(접근 권한의 관리)_(6항)

개인정보처리자는 권한 있는 개인정보취급자만이 개인정보처리시스템에 접근할 수 있도록 계정정보 또는 비밀번호를 일정 횟수 이상 잘못 입력한 경우 개인정보처리시스템에 대한 접근을 제한하는 등 필요한 기술적 조치를 하여야 한다.

개인정보의 안전성 확보 조치 기준 제6조(접근통제)

개인정보처리자는 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속하려는 경우 가상사설망(VPN: Virtual Private Network) 또는 전용선 등 안전한 접속수단을 적용하거나 안전한 인증수단을 적용하여야 한다.

개인정보의 기술적·관리적 보호조치 기준 제4조 4항(접근통제)

정보통신서비스 제공자 등은 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속이 필요한 경우에는 안전한 인증 수단을 적용하여야 한다.

주요 공공기관 추가인증 도입 배경

- 국정원 정보보안 관리 실태 평가
- (평가항목(5.2.1) 아이디, 패스워드 OTP 추가 인증 도입)
- 중요 정보시스템 접근 시 추가 인증을 통한 보안성 강화
- 외부 유지보수 및 용역업체, 프로젝트 인력 등에 의한 보안사고 및 업무과실 발생 시 책임소재 파악과 원인규명에 필요한 내부통제 및 감사체계 마련 필요
- 정보보호 컴플라이언스 준수 요구 강화
- 개인정보보호실태 점검 기준 준수 또는 보완 조치
- 외부메일 보안을 위한 2차 인증 도입



MFA(2차 인증)도입 관련 법령

개인정보의 안전성 확보 조치 기준 제5조(접근 권한의 관리)_ (6항)

개인정보처리자는 개인정보처리시스템에 권한 없는 자의 비정상적인 접근을 방지하기 위하여 계정정보 또는 비밀번호를 일정 횟수 이상 잘못 입력한 경우에는 개인정보처리시스템에 접근을 제한하는 등 기술적 조치를 하여야 한다.

해설

〈출처: 개인정보의 안전성 확보조치 기준 해설서 / 행정안전부 / 2019〉

- 계정정보 또는 비밀번호를 일정 횟수(예: 5회) 이상 잘못 입력한 경우 사용자 계정 잠금 등의 조치를 취하거나 계정정보, 비밀번호 입력과 동시에 추가적인 인증 수단(인증서, OTP 등)을 적용하여 정당한 접근 권한 자임을 확인하는 등의 조치를 취하는 것을 말한다

개인정보의 안전성 확보 조치 기준 제6조(접근통제)

개인정보처리자는 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속하려는 경우 가상사설망(VPN: Virtual Private Network) 또는 전용선 등 안전한 접속수단을 적용하거나 안전한 인증수단을 적용하여야 한다.

해설

〈출처: 개인정보의 안전성 확보조치 기준 해설서 / 행정안전부 / 2019〉

- 접속수단의 예시: 가상사설망(VPN), 전용선 등
- 인증수단의 예시: 인증서(PKI), 보안토큰, 일회용 비밀번호(OTP) 등

인증수단만을 적용하는 경우, 통신 보안을 위한 암호화 기술의 추가 적용이 필요할 수 있으므로 보안성 강화를 위해 안전한 접속수단을 권고한다.

MFA(2차 인증)도입 관련 고시

행정절차법 제46조 기반 교육부의 '평가인정 학습과정 운영지침 일부개정 고시(안)'

현행

Ⅲ. 출석 및 휴강 등

1. 출석 관리

...

나. 원격수업기관 경우

- ... 2) 범용 공인인증서를 포함하여 대리출석을 차단할 수 있는 로그인 장치를 마련·적용하여야 함.

...

Ⅳ. 시험 및 성적 부여

...

2. 시험출제, 채점방법 등

...

- 6) 범용 공인인증서를 포함하여 시험부정행위 방지대책 및 본인이 아닌 타인이 대리출석·시험을 치를 수 있는 가능성을 차단하는 장치를 마련·적용하여야 함.

개정안

Ⅲ. 출석 및 휴강 등

1. 출석 관리

...

나. 원격수업기관 경우

- ... 2) 대리출석을 차단할 수 있는 로그인 장치를 마련·적용하여야 함.(예: 생체인식, OTP, PIN, SMS인증, PKI 등)

...

Ⅳ. 시험 및 성적 부여

...

2. 시험출제, 채점방법 등

...

- 6) 시험부정행위 방지대책 및 본인이 아닌 타인이 대리출석·시험을 치를 수 있는 가능성을 차단하는 장치를 마련·적용하여야 함.(예: 생체인식, OTP, PIN, SMS인증, PKI 등)

Reference

01. KICA MFA Reference

KICA MFA Reference

기업

							SHIN & KIM 법무법인 세종		

KICA MFA Reference

공사/공공기관

KICA MFA Reference

전자금융거래용

해외



미국 일본 영국 인도 인도네시아 베트남 카자흐스탄 우즈베키스탄 싱가포르 터키 독일 홍콩 호주 멕시코 미얀마 필리핀

감사합니다.