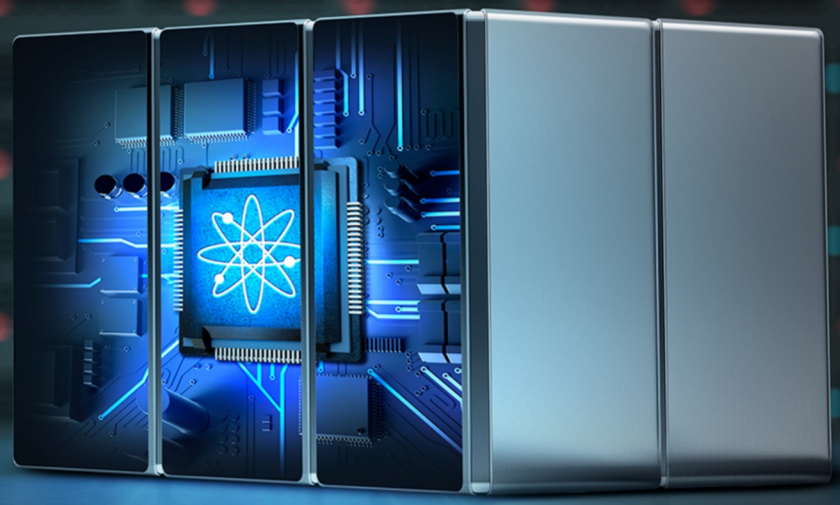
UCUBE

Q-SIGN

QUANTUM SECURITY PLATFORM



양자 보안 전자서명 & 통합인증 솔루션

QRNG · PQC · Hybrid Crypto · Q-KMS 기술을 결합하여
현재와 미래의 보안 위협에 완벽하게 대응합니다.

Quantum Safe Identity

Next Gen SSO & Signing

왜 지금 **Q-Sign**인가?

양자 위협의 현실화 (HNDL)

공격자들은 현재의 암호화된 데이터를 탈취하여 저장한 후, 미래의 양자 컴퓨터로 복호화하는 **'Harvest Now, Decrypt Later'** 공격을 감행하고 있습니다. 장기 보존이 필요한 중요 데이터는 이미 위험에 노출되어 있습니다.

기존 암호체계의 한계

기존 공개키 암호(RSA/ECC 등)는 양자 알고리즘에 취약함에 따라 미국 NIST와 국가정보원은 **PQC (양자내성암호)**로의 즉각적인 전환을 권고하고 있습니다.

Q-Sign 양자보안 솔루션

Q-Sign은 **QRNG(양자난수)**와 **PQC**를 결합하여 완벽한 무결성을 보장하며, 오픈소스 기반 아키텍처로 유연한 확장성과 합리적인 TCO를 제공합니다.

- Quantum-Safe Security Platform
- NIST PQC Standards Compliant

⚠ 인증 시스템 관련 주요 해킹 사례

UCUBE

최근 5년간(2021~2025) 발생한 주요 인증 시스템 관련 침해 사고 사례

사건		주요 공격 방식	비고
2021	공급망 공격 **SolarWinds 침해 사고**	• 침입 후 **통합인증(SSO) 서명키 탈취** • 정식 발급된 것처럼 보이는 위조 "SSO 토큰" 생성 (Golden SAML)	통합인증(SSO) 신뢰 관계 악용 시초
2022	사회공학 **Uber SSO 침해사건**	• 소셜 엔지니어링 + 지문인식 등 다중인증(MFA) **피로도(Fatigue) 공격** • 사내 Okta SSO 관리자 계정 장악 및 내부 시스템 접근	지문인식 등 다중인증(MFA) 우회 기법 진화
2023	관리자 탈취 **Okta 고객지원 계정 해킹**	• Okta 지원 직원 계정 탈취 → 내부 지원 포털 접근 • 고객 업로드 파일 내 **통합인증 토큰, 브라우저 세션 캡쳐** 가능	지원 프로세스 취약점
2024	토큰 위조 **Microsoft Entra ID 토큰 위조 공격**	• OIDC 토큰을 임의로 위조 (Fake JWT) • SSO 기반으로 정부, 기관의 클라우드 리소스 접근 시도	실제 사건은 아님 (연구 결과)
2025	계정 탈취 **Western Sydney Univ. SSO 계정 침해**	• SSO(IdP) 계정 침탈 및 무단 접근 • 내부 학적, 등록 시스템 및 민감 정보 접근	대학/교육 분야 타겟
	대규모 유출 **Oracle Cloud (OCI) SSO/LDAP 유출 주장**	• Login.oraclecloud.com 인증 엔드포인트 취약점 이용 주장 • 저장된 자격정보 파일(**JKS, KeyStore, 비밀번호 hash** 등) 탈취	클라우드 인프라 타격

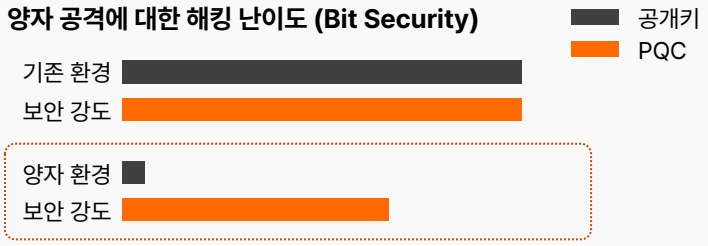
Q-Sign의 핵심 기술

Q-Sign은 양자 난수 생성(QRNG)과 양자 내성 암호(PQC)를 결합하여,
현재의 보안 위협뿐만 아니라 미래의 양자 컴퓨팅 공격에도 대응하는 강력한 보안 플랫폼을 제공합니다.

또한 AI 기반의 지능형 보안 분석과 통합 모니터링 체계를 더해, 더욱 안전하고 효율적인 차세대 인증 환경을 구축합니다.

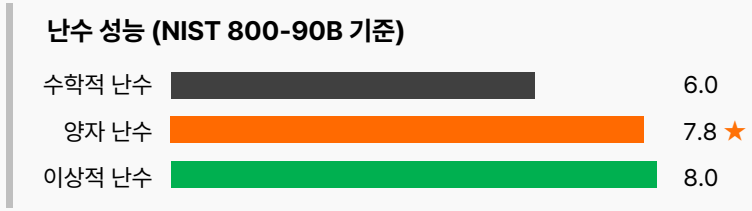
01 PQC (양자내성암호)

NIST 표준 알고리즘(ML-KEM, ML-DSA)을 적용하여
양자 컴퓨터의 무차별 대입 공격에도 안전한 전자서명 및
키 교환 메커니즘을 보장합니다.



02 QRNG (양자난수생성)

물리적 양자 현상에 기반한 순수 난수를 생성하여 예측 불가능한
고품질의 암호 키와 Nonce를 제공함으로써 근본적인 보안성을
확보합니다.

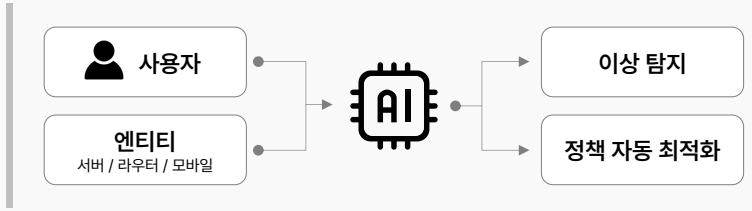


03 Hybrid Crypto

기존 공개키 암호(RSA/ECC 등)와 PQC를 이중으로 적용하는
하이브리드 방식을 채택하여, 레거시 시스템과의 호환성을 유지하며
단계적인 보안 강화를 실현합니다.

04 AI 보안 분석

인공지능 기반 기술(UEBA, 사용자 및 엔티티 행동 분석)을 적용하여
비정상 행위를 실시간으로 탐지하고, 사용자의 이용 내역을 분석하여,
권한 정책을 자동으로 최적화하여 내부 위협을 선제적으로 차단합니다.



Q-Sign 플랫폼

Q-Sign 플랫폼의 4대 핵심 모듈 및 기능 구조

외부 요청 처리 및 트래픽 관리
[APISIX]

API 정책 엔진 및
보안정책 기반 접근
제어

PQC 기반 통합인증
[Q-SSO]

글로벌 표준 인증 프로토콜
(OIDC/OAuth/SAML)
기반 인증 및 통합 로그인

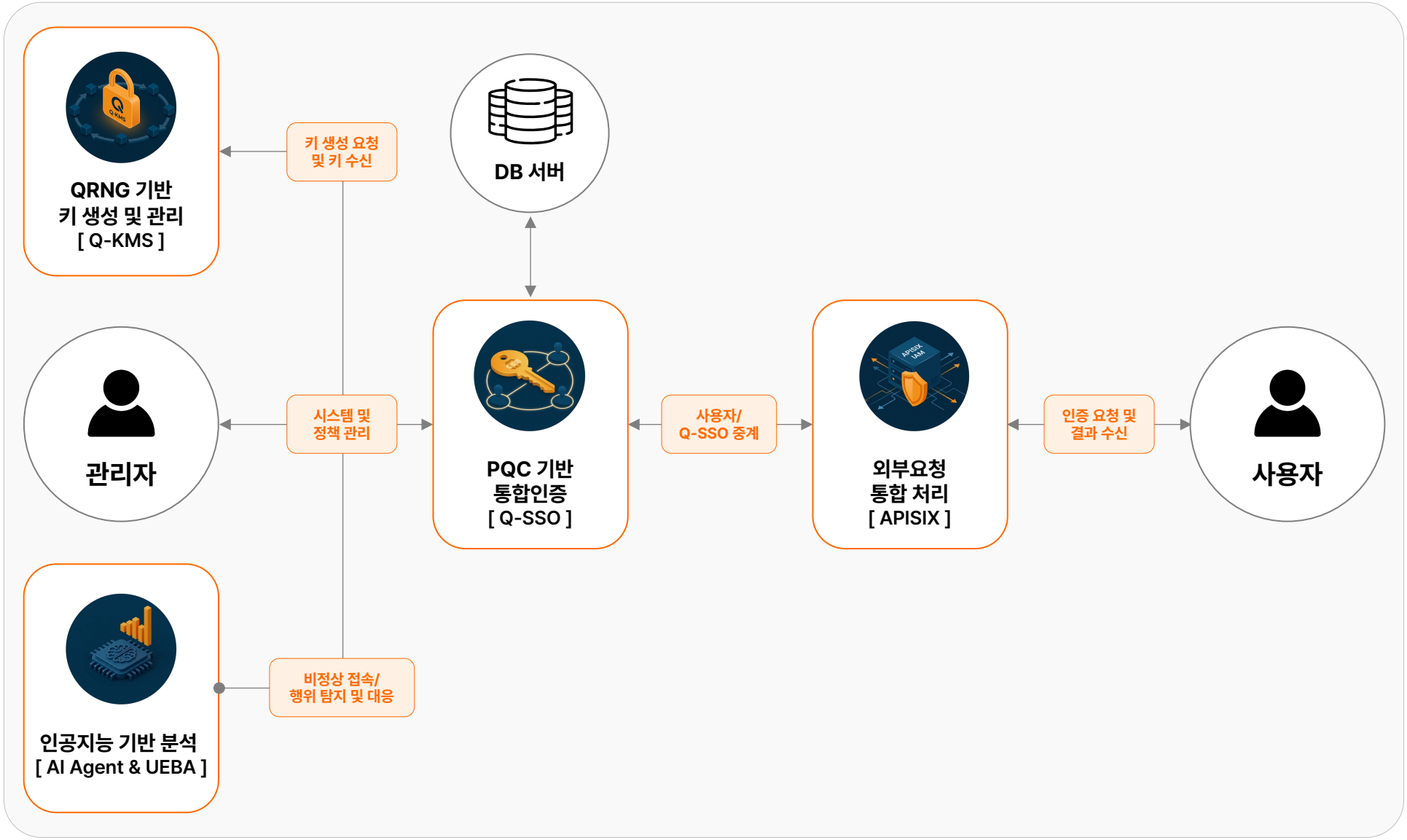
QRNG 기반 키 생성 및 관리
[Q-KMS]

양자 키 수명주기 관리
및 보안정책 자동화

인공지능 기반 분석
[AI Agent & UEBA]

UEBA 이상 징후 탐지
및 권한 자동 분석

Q-Sign 플랫폼 운용


QRNG 기반
키 생성 및 관리
[Q-KMS]
키 생성 요청
및 키 수신
DB 서버
관리자
시스템 및
정책 관리
PQC 기반
통합인증
[Q-SSO]
사용자/
Q-SSO 중계
외부요청
통합 처리
[APISIX]
인증 요청 및
결과 수신
사용자
인공지능 기반 분석
[AI Agent & UEBA]
비정상 접속/
행위 탐지 및 대응

Q-Sign 플랫폼 구성 요소별 기능

APISIX

고성능, 낮은 지연 시간, 핫 리로딩 지원으로 무중단
운영 환경을 제공하는 차세대 API Gateway 솔루션

- 동적 라우팅 및 업스트림
- 플러그인 시스템 (Lua/Wasm)
- 탁월한 관측가능성
- 강력한 보안 기능
- Admin API 및 대시보드
- 데이터/제어 평면 분리

Q-SSO

한 번의 로그인으로 연동된 모든 서비스에 접근 가능한
통합 인증 환경 제공

- Realm 정책 설정
- 사용자 및 접근 제어
- Client (애플리케이션) 관리
- 시스템 운영 및 유지보수

AI Agent & UEBA

UEBA(사용자/엔티티 행동 분석) 기술로
이상 행동 탐지 및 내부자 위협 조기 발견

- ML 모델 관리
- 탐지 정확도 지표
- False Positive 최소화
- 학습 데이터 관리
- 자동화된 대응

Q-KMS

Q-RNG 기반의 암호키 생성과 OpenSSL 3.0 PQC
정책을 통해 양자 내성 암호 키를 안전하게 관리하고 공급

- Q-RNG 기반 키 생성
- PQC 기반 인증서 정책
- 키 분배 및 생명주기
- 시스템 연동 및 PQC 정책

Q-Sign 플랫폼 시스템 구성

Q-Sign 플랫폼의 4대 핵심 모듈 및 기능 구조

Q-SSO 소프트웨어

- 한번의 로그인으로 연동된 서비스에 로그인 지원
- 사용자 접근 제어
- Client 관리
- 시스템 운영 및 유지보수

Q-KMS 소프트웨어

- 암호키 생성 및 관리 지원
- 양자 난수 생성 및 PQC 기반 암호키 분배

AI-Monitoring

- 인공지능 기반 사용자, 엔티티 (서버, 라우터 등) 사용 패턴 분석 및 비정상 행위 탐지

APISIX 소프트웨어

- 외부 요청 처리 및 트래픽 관리
- 외부 접근 제어 및 보안감사

Q-SIGN 하드웨어

- CPU
  : 인텔 제온 3.2Hz
- RAM : 64GB
- Storage
  : 2TB/12TB
- 통시접속 처리 수
  : 1,000 ~ 2,000tps
  (HSM 기준)

NIST
Post-Quantum Cryptography Standards

PQC 알고리즘

- PQC 알고리즘 지원
- NIST 검증 표준
- ML-KEM, ML-DSA
- HW 가속 고속 처리

QRNG

- 양자 난수 시드 생성
- PQC 알고리즘 HW 가속
- PQC 기반 SSL 지원

PERFORMANCE METRICS

UCUBE

PQC 도입의 현실적 장벽

- Key/Cert Size: 기존 대비 3~5배 증가
- Complexity: 격자 기반 연산의 과부하
- Latency: SW 처리 시 성능 급격히 저하

HW 가속의 필요성

- Key/Cert Size: 기존 대비 3~5배 증가
- Complexity: 격자 기반 연산의 과부하
- Latency: SW 처리 시 성능 급격히 저하

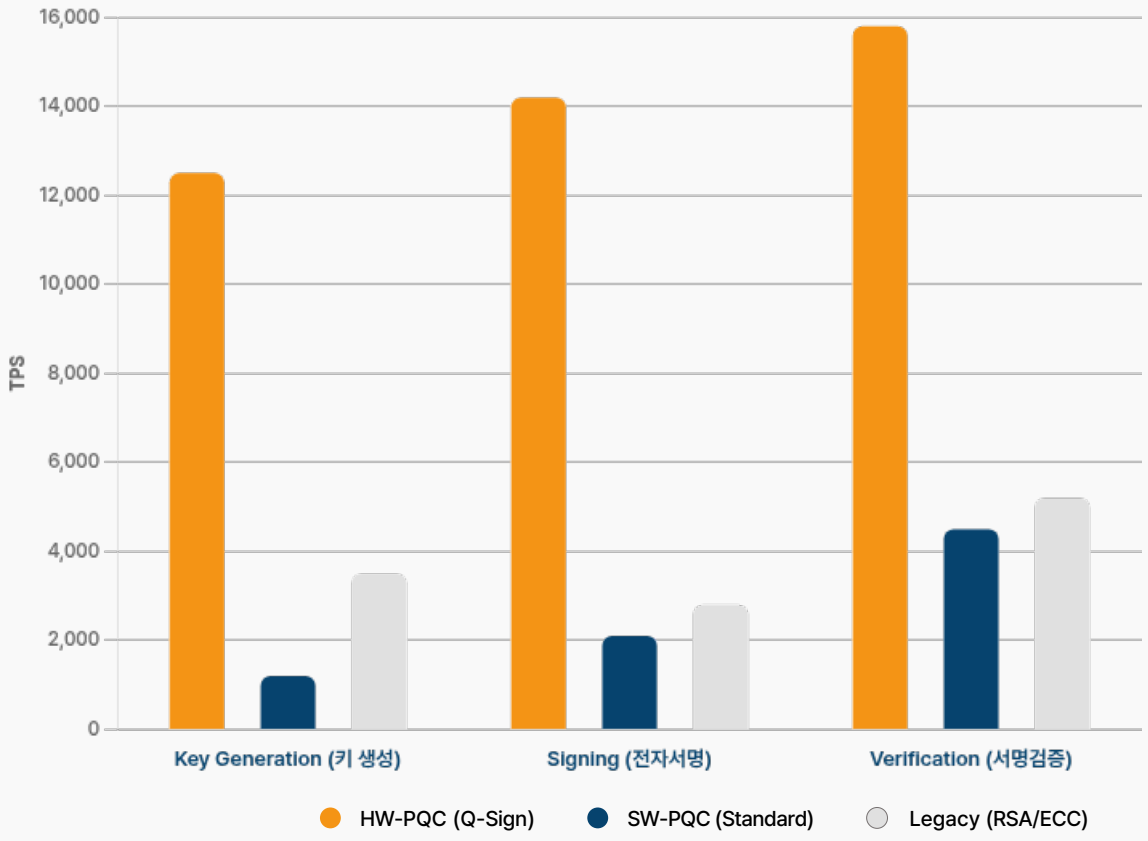
MAX THROUGHPUT (TPS)

15,000+

FPGA HW-PQC Acceleration

Cryptographic Operation Throughput

Higher is better (Transactions Per Second)



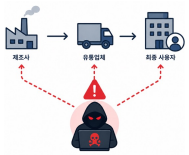
Q-Sign 도입 프로세스

성공적인 Q-Sign 도입을 위한 5단계 전략 (5-Step Strategy)

01	02	03	04	05
진단 및 분석	**전략 설계**	**검증 및 POC**	**구축 및 이행**	**운영 및 최적화**
DIAGNOSIS	DESIGN	VERIFICATION	IMPLEMENTATION	OPERATION
- 중요 데이터 자산 식별	- 하이브리드 암호 전환 로드맵 수립	- 레거시 시스템 호환성 테스트	- 단계적 마이그레이션 실행	- 실시간 보안 모니터링 가동
- 현행 암호체계 취약점 분석	- 키 수명주기 관리 (Q- KMS) 정책 정의	- PQC 성능 벤치마킹 수행	- Q-Sign 솔루션 본 구축	- 주기적 암호 키 회전 수행
- PQC 전환 규제 준수 격차 진단	- 최적의 통합 인증 아키텍처 설계	- 파일럿 서비스 적용 검증	- 운영자 기술 이전 및 교육	- 보안 정책 튜닝 및 최적화
- 우선순위 도출	- 기존 시스템 연동 방안 수립	- 운영 안정성 사전 확보	- 무중단 시스템 전환 지원	- 지속적 컴플라이언스 대응

Q-Sign 보안 공격 대응

토큰위조
정상 토큰처럼 위조된 토큰을 생성하여 공격



공급망 공격
소프트웨어 공급업체 등을 침투하여 고객에 악성코드를 전파하는 공격

사회공학
사람을 속여 인증정보나 중요 정보를 획득하는 공격

관리자 탈취
관리자 계정 또는 권한을 탈취 후 시스템 전체를 공격

사용자 탈취
악성코드 등을 통해 일반 사용자 계정을 탈취하는 공격

탐지 및 방어 / 대응

Q-SSO

- 사용자별 이용 영역 제한
- 계정 중앙 통합 관리
- 토큰 발급(QRNG, PQC) 및 수명 관리

Q-KMS

- 암호키/서명키(QRNG) 생성 및 관리
- 암호키/서명키 분배(PQC)
- 암호키/서명키 보관 (HSM)

AI Agent & UEBA

- 비정상 접근 패턴 분석 및 탐지
- 비정상 행동 분석 및 탐지
- 비정상 패턴 대응

AS-IS

기존 통합인증 시스템 (Legacy IDP)의 한계

양자 위협 취약

기존 RSA/ECC 기반 암호 체계에 의존하여, 양자 컴퓨터 등장 시,
모든암호화된 데이터와 인증 토큰이 무력화될 위험에 노출되어 있습니다.

높은 운영 비용

SaaS 기반의 사용자 수(User) 기준 과금 정책으로 인해 조직 규모가
커질수록 구독료가 기하급수적으로 증가하며 예산 예측이 어렵습니다.

벤더 종속성(Lock-in)

특정 글로벌 벤더의 기술 스택에 종속되어 커스터마이징이 제한적이며,
기업 고유의 비즈니스 로직이나 UI/UX 반영이 어렵습니다.

규정 준수 한계

해외 데이터 센터 저장으로 인한 데이터 주권 문제와 국내 금융권
망분리 규제 등 특수한 컴플라이언스 요건 대응에 한계가 있습니다.

TO-BE

UCUBE

Q-Sign 전환 후 차세대 인증 환경

양자 내성(Quantum Resistance)

NIST 표준 PQC(Kyber, Dilithium) 알고리즘을 적용하여
양자 컴퓨터 공격으로부터 서명키와 인증 토큰을 안전하게 보호합니다.

비용 최적화

온프레미스 또는 프라이빗 클라우드 구축을 통해 사용자 수 증가에 따른
추가 비용 없이 합리적인 TCO로 운영 가능합니다.

완벽한 독립성 및 커스터마이징

오픈소스(Keycloak) 기반의 유연한 아키텍처로 기업 환경에 맞춘
100% 커스터마이징과 독자적인 인증 로직 구현이 가능합니다.

국내 규정 완벽 준수

데이터의 국내 보관은 물론, 금융권 망분리 환경 지원, HSM 연동,
상세 감사 로그 등 국내 보안 규제를 완벽하게 준수합니다.

유연한 전환(Migration)

기존 사용자 DB와의 원활한 연동 및 단계적 마이그레이션 전략을
지원하여 서비스 중단 없는(Zero-downtime) 전환이 가능합니다.

AS-IS

개별 인증 시스템 운영의 문제점

사용자 불편 가중

기존 RSA/ECC 기반 암호 체계에 의존하여, 양자 컴퓨터 등장 시,
모든암호화된 데이터와 인증 토큰이 무력화될 위험에 노출되어 있습니다.

보안 취약점 노출

시스템별 보안 수준이 상이하여 취약점이 발생하며,
중앙화 된 모니터링 이 불가능합니다.

운영 비효율 및 복잡성

계정 생성 및 권한 부여가 수작업으로 이루어져 관리가 복잡하고
실수가 발생하기 쉽습니다.

비용 증가 및 중복 투자

각 시스템별로 별도의 인증 모듈 유지보수 인력과 비용이 발생하여
예산 낭비를 초래합니다.

TO-BE

UCUBE

Q-Sign 도입 후 통합 인증 혁신

단일 인증(SSO) 구현

한 번의 로그인으로 모든 연동 시스템에 안전하게 접근하여
사용자 편 의성을 극대화합니다.

통합 보안 및 가시성 확보

중앙화 된 보안 정책 적용과 실시간 접근 로그 감사로
전체적인 보안 수 준을 상향 평준화 합니다.

운영 효율성 극대화

통합 계정/권한 관리 및 자동화된 프로비저닝으로
관리 업무를 단순화 하고 정확성을 높입니다.

미래 대비 (PQC 적용)

양자내성암호(PQC) 기반의 암호화 기술 적용으로
미래의 양자 컴퓨팅 위협까지 선제적으로 방어합니다.

도입기관 (중소벤처기업부 산하 69개 기관)

기관명 (대분류)	기관명(중분류)
소상공인시장진흥공단	희망리턴패키지 협동조합활성화 소상공인스마트상점
신용보증재단중앙회	보증드림
소상공인시장진흥공단	소상공인 프렌차이즈 물류정보시스템 소상공인365 소상공인 정책자금 소상공인24 소상공인지식배움터
메인비즈협회	경영혁신마일리지넷 메인비즈넷
대중소기업농어업협력재단	상생누리 시스템 기술보호울타리
기술보증기금	K-TOP 탄소가치플랫폼 매출채권팩토링 소셜벤처 홈페이지 SmartTechBridge 기보디지털지점
KoDATA	중소기업현황정보시스템
(재)한국화학융합시험연구원	해외규격인증획득지원센터
(재)장애인기업종합지원센터	창업넷
(재)여성기업종합지원센터	여성기업 일자리허브 플랫폼
(사)벤처기업협회	벤처확인종합관리시스템
한국중소벤처기업유통원	한국중소벤처기업유통원 홈페이지 판판셀러 판판대로 공공구매종합정보망(SMPP)
한국벤처캐피탈협회	벤처투자종합포털 중소벤처기업 M&A 정보망
중소기업기술정보진흥원	중소기업기술개발종합과제관리시스템(SMTECH) 인공지능중소벤처 제조플랫폼(KAMP) 스마트공장 사업관리시스템 중소기업기술혁신센터

기관명 (대분류)	기관명(중분류)
한국창업보육협회	창업보육센터네트워크시스템
신용보증재단중앙회	재기지원 포털
이노비즈협회	이노비즈넷
중소기업중앙회	협업정보시스템 중소기업해외전시포탈
중소벤처기업부	참 괜찮은 강소기업
중소벤처기업연구원	중소기업수출지원센터 기업마당
중소벤처기업진흥공단	기업지원플러스(G4B) 내일채움공제 중진공디지털지점 고비즈코리아 비즈패스파인더 중소기업인력지원사업종합관리시스템 기업인력애로센터 일자리매칭플랫폼 비대면스마트진단시스템(K-doctor) ESG통합플랫폼 중속이버혁신플랫폼(혁신바우처) 청년창업사관학교 홈페이지 구조혁신지원사업 운영시스템 중소벤처기업 자산거래중개장터 중소기업재도전종합지원센터 도약(Jump-Up)프로그램 중소벤처기업-숲(SSUP)
창업진흥원	K-Startup 창업사업통합관리시스템(PMS) 창업에듀 창업공간플랫폼 창업기업확인시스템 온라인법인설립시스템 메이크홀(제조생산 종합플랫폼) 모두의창업 창조경제혁신센터 홈페이지
한국경영기술지도사회	비즈니스지원단

NEXT STEPS

양자 컴퓨팅 시대의 보안 위협에 대비하세요.
Q-Sign은 현재와 미래의 보안을 동시에 해결하는 가장 확실한 솔루션입니다.

지금 데모 시연을 요청하시거나, 귀사의 보안 환경 진단 워크숍을 신청해 보세요.
전문가 팀이 귀사 에 최적화된 양자 보안 전환 로드맵을 제시해 드립니다.

CONTACT US

(주)유큐브 U.CUBE
서울시 강남구 역삼로 220
T. 02-6925-0445 M. kangcs@u-cube.kr www.u-cube.kr