Quantum SafeGuard

양자내성암호화(PQC)가 적용된 PKI기반의 전자서명 솔루션

Overview

양자내성암호화(PQC)가 적용된 PKI기반의 전자서명 솔루션으로 NIST가 표준으로 선정한 양자내성 알고리즘(ML-DSA)을 화이트박스 암호화 기술에 적용하였습니다.

Strengths

양자내성알고리즘(PQC) FIPS인증 표준 ML-DSA적용

NIST에서 표준으로 지정한 알고리즘을 사용하여 양자컴퓨터의 위협에도 안전합니다.

화이트박스기반의 Quantm SafeBOX적용

키 생성, 보관을 안전한 저장 장소에서 작업을 수행하여 탈취가 불가능합니다.

완벽한 호환성

저장매체 단일소스를 통해 OS에 관계없이 개발 및 유지보수가 용이하며, 스마트폰 OS, 버전, 제조사 별 차이 없는 단일 단말 Lib제공합니다.

뛰어난 확장성

공공, 그룹 통합 인증 등 연계서비스로 이용 채널 확대가 가능합니다. 또한 DID, 전자지갑, 실명증표 등 다양한 서비스로 확장이 가능합니다.

Key Features

양자내성 암호화 기술 적용	양자내성암호화(PQC) 기술을 적용하여 양자컴퓨터에 의한 개인키 유추가 불가능합니다.
NIST 표준 규격 - FIPS204 준용	FIPS 204는 양자 컴퓨터 시대에 대비한 디지털 서명 보안 표준으로, CRYSTALS-Dilithium 알고리즘을 기반으로 합니다. 현재 ML-DSA로 알려진 이 알고리즘은 격자 구조를 활용해 양자 컴퓨터의 위협에 대응하도록 설계되었습니다.
화이트박스 기반의 SE를 적용한 솔루션	화이트박스 암호화 기술기반 일반 어플리케이션과 소프트웨어적으로 분리된 모바일 기기 내 특수 보안 공간에서 양자내성 알고리즘을 적용하여 인증 서비스를 안전하게 실행합니다.
가장 유연하고 손쉬운 시스템 전환	양자 컴퓨터 공격에 위협받는 기존 RSA/ECC 알고리즘 사용환경을 양자 내성을 지원하는 ML-DSA 알고리즘으로 전환할 수 있는 유연하고 편리한 방법을 제공합니다.

Advantages

다양한 경험을 통한 축척된 전문성

다양한 프로젝트를 성공적으로 수행해 왔습니다. 이러한 경험을 통해 **폭넓은 도메인 지식을 축적**하였으며, 복잡하고 까다로운 요구사항에도 최적의 솔루션을 제공합니다. 우리와 함께 라면 업계 최고 수준의 전문성을 경험할 수 있습니다.

높은 완성도의 솔루션 제공

수많은 케이스를 통해 **검증된 기술력을 보유**하고 있습니다. 이미 구현된 시스템을 활용하여 커스터 마이징을 최소화하고, 빠르고 안정적인 서비스를 제공합니다. 이를 통해 고객은 시간을 절약하고 비즈니스 성과를 극대화할 수 있습니다.

검증된 보안과 신뢰

보안을 최우선으로 하며, 보안 사고 0건의 기록을 유지하고 있습니다. **검증된 보안 기술과 철저한 관리**를 통해 고객의 데이터를 안전하게 보호하며, 안심하고 서비스를 이용할 수 있는 환경을 제공합니다.

고객 중심의 철학

"고객의 성공이 우리의 성공"이라는 신념을 바탕으로 모든 프로젝트를 진행합니다. 고객의 니즈를 깊이 이해하고, 최상의 결과를 창출하기 위해 노력합니다. 이는 단순한 파트너십을 넘어 고객의 지속적인 성공을 위한 동반자로서의 역할을 의미합니다.

Reference

다양한 프로젝트 경험과 지식을 바탕으로 최적의 솔루션과 업계 최고 수준의 전문성을 제공합니다.

신한은행, 농협은행, 국민은행, IBK기업은행, 하나은행, 케이뱅크, 제주은행, KB증권

신한투자증권, 한국투자증권, 메리츠증권, 대신증권, IBK투자증권, 삼성증권, 한화투자증권, NH투자증권

한국포스증권, 상상인증권, 유안타증권, 삼성선물, 신한카드, 에큐온저축은행, SBI저축은행, 대신저축은행