Quantum SafeOTP

양자내성암호화(PQC)가 적용된 OTP 솔루션

ATON LIFE INNOVATOR GROUP

Overview

양자컴퓨팅 시대에도 안전한 차세대 OTP 솔루션 NIST 표준 알고리즘 ML-KEM(FIPS 203)을 적용해 양자컴퓨터 환경에서도 안전한 키 교환이 가능합니다. 기존 시스템에 손쉽게 적용할 수 있으며, 미래 보안 위협에도 선제적으로 대응할 수 있습니다.

Strengths

양자컴퓨팅 환경에서도 안전한 키 교환

기존 공개키 암호방식이 무력화되는 양자 환경에서도 안전하게 키를 교환할 수 있습니다. 양자 내성 알고리즘 기반으로 장기적인 보안성을 보장합니다.

화이트박스기반의 Quantm SafeBox 적용

화이트박스 암호화 기술이 적용된 보안 매체는 OTP 생성과 키 보관을 안전한 저장 영역에서 수행하여, 외부로의 탈취를 원천적으로 차단합니다.

복잡한 인프라 없이 간편한 도입 가능

OTP 시스템이 처음인 기업도 쉽게 적용할 수 있도록, 별도의 고가 장비나 복잡한 구축 과정 없이 빠르게 도입할 수 있도록 설계되었습니다.

경량화된 연산 구조로 높은 성능 유지

PQC 알고리즘 특성상 연산 복잡도가 증가할 수 있으나, 최적화된 구현을 통해 기존 OTP 수준의 처리 성능과 응답 속도를 유지하고 모바일 및 다양한 환경에서 실시간 인증 처리가 가능합니다.

Key Features

양자내성 알고리즘 기반 키 교환	NIST 표준 ML-KEM(FIPS 203) 알고리즘을 적용하여, 인증 과정에서 양자컴퓨팅 환경에서도 안전한 키교환이 가능합니다. 기존 대비 보안성이 뛰어나며, 장기적으로 안정적인 인증 기반을 제공 합니다.
QRNG 기반 일회용 비밀번호(OTP) 생성 및 검증 선택 사항	고전적 난수 생성 방식이 아닌 양자 난수 생성기(QRNG)를 활용하여, 예측이 불가능한 진정한 무작위성을 가진 OTP를 생성합니다. 서버는 생성된 OTP를 실시간으로 검증하며, 모바일 앱이나 웹 환경을 통해 안전한 인증을 제공합니다. QRNG를 통해 기존 방식보다 더욱 강화된 보안 수준을 확보할 수 있습니다.
다양한 환경과 유연한 연동 지원	웹, 모바일, VPN, 업무 시스템 등 다양한 환경에 연동 가능하며, API 및 표준 프로토콜을 통해 기존 인증 시스템과 유연하게 통합할 수 있습니다.

Quantum SafeGuard

양자내성암호화(PQC)가 적용된 PKI기반의 전자서명 솔루션

ATON LIFE INNOVATOR GROUP

Overview

양자컴퓨팅 시대에도 안전한 차세대 전자서명 솔루션 NIST 표준 알고리즘 ML-DSA(FIPS 204)를 기반으로, 화이트박스 암호화 기술과 결합한 PQC 전자서명 솔루션입니다. 양자컴퓨팅 환경에서도 안전하게 서명키를 보호하며, 강화된 보안성과 미래 대응력을 동시에 확보할 수 있습니다.

Strengths

양자 환경에서도 안전한 전자서명 제공

NIST 표준 알고리즘 ML-DSA(FIPS 204)를 적용하여, 양자컴퓨터의 계산 능력으로도 서명 위·변조가 사실상 불가능합니다. 무결성 확보가 필수적인 업무에 최적화되어 있습니다.

화이트박스기반의 Quantm SafeBox 적용

서명키를 소프트웨어 내부에서도 노출되지 않도록 보호하는 화이트박스 암호화 기술을 적용해, 단말 탈취나 악성코드 위협으로부터 키 유출을 방지합니다.

완벽한 호환성으로 안정적인 서비스 구현

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

환경 변화에 유연하게 대응하는 확장성

공공, 그룹 통합 인증 등 연계서비스로 이용 채널 확대에 용이합니다. 또한 DID, 전자지갑, 실명증표 등 다양한 서비스로 확장 가능 합니다.

Key Features

양자내성 알고리즘 기반 전자서명 생성 및 검증	NIST 표준 ML-DSA(FIPS 204) 알고리즘을 적용하여, 전자문서에 대한 무결성과 본인 서명 여부를 검증합니다. 기존의 RSA/ECDSA 대비 향후 양자 위협에 대응하는 미래형 서명 기술입니다.
화이트박스 암호화 기반 서명키 보호	화이트박스 암호화 기술기반 일반 어플리케이션과 소프트웨어적으로 분리된 모바일 기기 내 특수 보안 공간에서 인증 서비스를 안전하게 실행 합니다. 암호화 장치 내부를 해킹 하더라도 Private Key 유추 불가능합니다.
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.

미래 보안 위협에 대한 **선제적 대응**

양자컴퓨터 상용화를 대비한 양자내성암호화알고리즘(PQC) 도입은 기업의 장기 보안 전략의 핵심입니다.
지금 도입함으로써 규제 변화, 고객 신뢰, 글로벌 보안 트렌드에 선제적으로 대응할 수 있습니다.

QUANTUM SAFEOTP

QUANTUM SAFEGUARD

ATON LIFE INNOVATOR GROUP

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

ATON LIFE INNOVATOR GROUP
서울시 영등포구 여의대로 108, 파크원타워1 26층
Tel 02-786-4273 **e-mail** leedh@atoncorp.com **www.atoncorp.com**