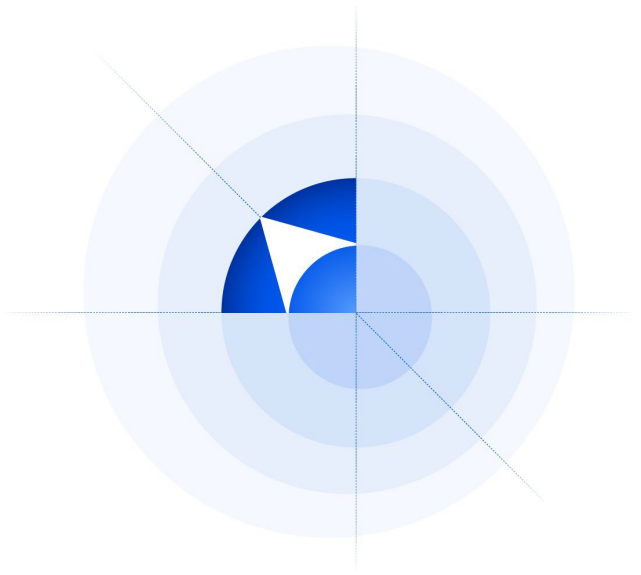
ITCEN

Insight Report

양자 컴퓨터 시대의 보안

산업계가 PQC에 주목하는 이유

양자컴퓨터의 상용화가 현실로 다가오면서, 기존 암호체계는 더 이상 안전하지 않습니다.
이 변화에 대응하기 위해, 모든 산업계가 '양자내성암호(PQC)' 도입을 서두르고 있습니다.



June 2025

Inspire with Technology

최신 IT 트렌드와 비즈니스 인사이트, 실전 노하우까지 !
아이티센그룹 홈페이지에서 깊이 있는 분석 자료로 만나 보세요.

ITCEN

양자 컴퓨터 시대의 보안

산업계가 PQC에 주목하는 이유

목차

01	PQC, IT 업계의 공통 관심사가 되다	3
02	NIST가 표준화를 서두른 이유	4
03	ITCEN PNS의 EdgeQWallet이란?	5
04	차세대 'ZERO-Trust' 전략의 핵심, iEnXectionPQC	7
05	마치며	8

01. PQC, IT 업계의 공통 관심사가 되다

최근 IT 업계 전반에서 인프라에 양자내성암호(PQC, Post-Quantum Cryptography)를 지원하려는 움직임이 본격화되고 있습니다. 주요 하드웨어 보안 모듈(HSM) 제조사들은 펌웨어 업그레이드를 통해 PQC 알고리즘을 지원하고 있고, Red Hat Enterprise Linux 10 등의 운영체제도 PQC 지원을 공식화했습니다. 네트워크 통신 프로토콜에도 PQC 도입이 활발히 이뤄지고 있으며, 일부 웹 서비스에는 이미 하이브리드 PQC 방식이 적용됐습니다. 오픈 소스 생태계에서도 OpenSSL, NSS 등 주요 암호 라이브러리에 PQC 알고리즘이 추가되고 있습니다.

이처럼 업계가 발 빠르게 양자컴퓨팅 시대에 대비할 수 있게 된 배경에는 미국 국립 표준기술연구소(NIST)의 표준화 노력이 자리하고 있습니다. NIST는 2024년 8월 첫 PQC 표준 (FIPS 203,204,205)을 공식 발표하며, 산업계가 빠르게 대응할 수 있도록 표준화 작업을 가속화했습니다.

ⓒ ITCEN GLOBAL

02. NIST[1]가 표준화를 서두르는 이유

NIST는 왜 이토록 표준화를 서둘렀을까요? 그 이유는 두 가지로 요약할 수 있습니다.

① 기존 암호화 기술의 무력화

첫째, 양자컴퓨터가 기존 암호화 기술을 무력화할 수 있기 때문입니다. 현재 인터넷 보안과 디지털 서명 등에 널리 쓰이는 공개키 암호(RSA, ECC 등)는 큰 수의 소인수분해 및 이산대수 문제의 어려움에 기반하지만, 쇼어(Shor) 알고리즘을 사용하는 양자컴퓨터는 이 문제를 기존 컴퓨터보다 훨씬 빠르게 풀 수 있습니다. 또한 그로버(Grover) 알고리즘은 AES 같은 대칭키 암호의 보안을 약화시킬 수 있습니다. 이런 이유로 양자컴퓨팅 시대의 도래는 기존 공개키 암호의 근본적인 취약성을 드러내며, 새로운 암호체계로의 전환을 요구하고 있습니다.

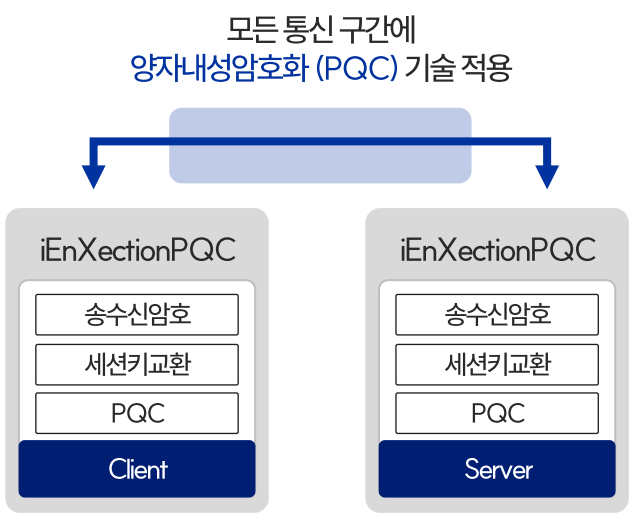
② HNDL(Harvest Now, Decrypt Later) 공격의 위험

두 번째 이유는 HNDL(Harvest Now, Decrypt Later) 공격의 위험 때문입니다. 이는 '지금 암호화된 데이터를 수집해 두었다가, 미래에 양자컴퓨터가 상용화되어 해독(복호화)이 가능한 시점에 해독한다'라는 새로운 공격 방식입니다. HNDL 공격이 실제로 감행되었는지는 구체적으로 확인되지 않았지만, 보안 업계에서는 이 공격이 매우 은밀하고 장기적으로 이루어질 수 있다는 점에 공감하고 있습니다. 특히 장기적 가치가 있는 정보, 예를 들어 의료기록이나 국가 기밀, 암호화폐 지갑 정보 등이 주요 표적이 될 수 있습니다. 모순적이게도, 기업이 HIPAA, GDPR 등 각종 규제를 준수하며 특별히 신경 쓰는 데이터일수록 오히려 공격자에게는 가치 있는 표식이 될 수 있습니다. 즉 보안통신 세션과 프로토콜 등의 데이터가 기존 방식으로 암호화되어 있다면, 언젠가 해독될 위험이 있는 것입니다.

1) NIST : 국립표준기술연구소

03. ITCEN PNS의 EdgeQWallet 이란?

EdgeQWallet(엣지큐월렛)은 양자 컴퓨터 시대에도 안전성을 확보할 수 있는 양자내성암호(Post-Quantum Cryptography, PQC) 기술을 적용한 전자지갑입니다. 디지털 자산의 안전한 보관 및 관리를 위한 혁신적인 MPC (다자간 컴퓨팅) 기술을 적용한 보안 솔루션 제품군이죠. 내부, 외부의 어떠한 위협에도 원천적으로 안전한 수탁 기술을 바탕으로, 디지털 자산의 키를 여러 조각으로 분산 저장해 단일 취약점(SPoF, Single Point of Failure)을 제거하고, 각 파티 간의 모든 통신에는 양자내성암호(PQC) 기술을 적용하였습니다. 이를 통해 기관 투자자부터 일반 개인 사용자까지 모든 유형의 고객을 위한 맞춤형 디지털 자산 지갑 솔루션을 제공합니다. EdgeQWallet의 제품군은 다음과 같이 구성되어 있습니다.



ⓒ ITCEN PNS

① EdgeQ-Vault - 사업자용 MPC 기반 분산 안전 금고

STO(증권형 토큰 발행)와 같이 높은 수준의 보안과 신뢰가 요구되는 사업자를 위해 설계된 최상위 보안 솔루션입니다. EdgeQ-Vault는 MPC 기술을 통해 개인 키를 여러 개의 조각으로 암호화하여 분산 저장함으로써, 단일 지점의 해킹이나 내부자 공격으로부터 자산을 원천적으로 보호합니다. 이는 특정 개인이나 서버가 단독으로 자산에 접근하는 것을 불가능하게 만들어, 최고 수준의 보안을 보장합니다. 사업자의 운영 정책에 따라 출금 한도, 승인 절차 등 다양한 보안 정책을 유연하게 설정하고 관리할 수 있습니다.

03. ITCEN PNS의 EdgeQWallet 이란?

② EdgeQ-pWallet – 개인용 MPC 복구 안전 지갑

개인 사용자가 더욱 안전하고 편리하게 디지털 자산을 관리할 수 있도록 지원하는 개인용 지갑 솔루션입니다. 기존 지갑의 가장 큰 문제점이었던 개인 키 분실의 위험을 MPC 기술을 통해 해결했습니다. 사용자가 개인 키를 분실하더라도 사전에 지정된 복구 절차를 통해 안전하게 자산을 복구할 수 있어, 더 이상 니모닉 구문이나 개인 키를 종이에 적어 보관하는 불안함에서 벗어날 수 있습니다. 복잡한 기술에 대한 이해 없이도 누구나 쉽고 편리하게 사용할 수 있도록 직관적으로 설계되었습니다.

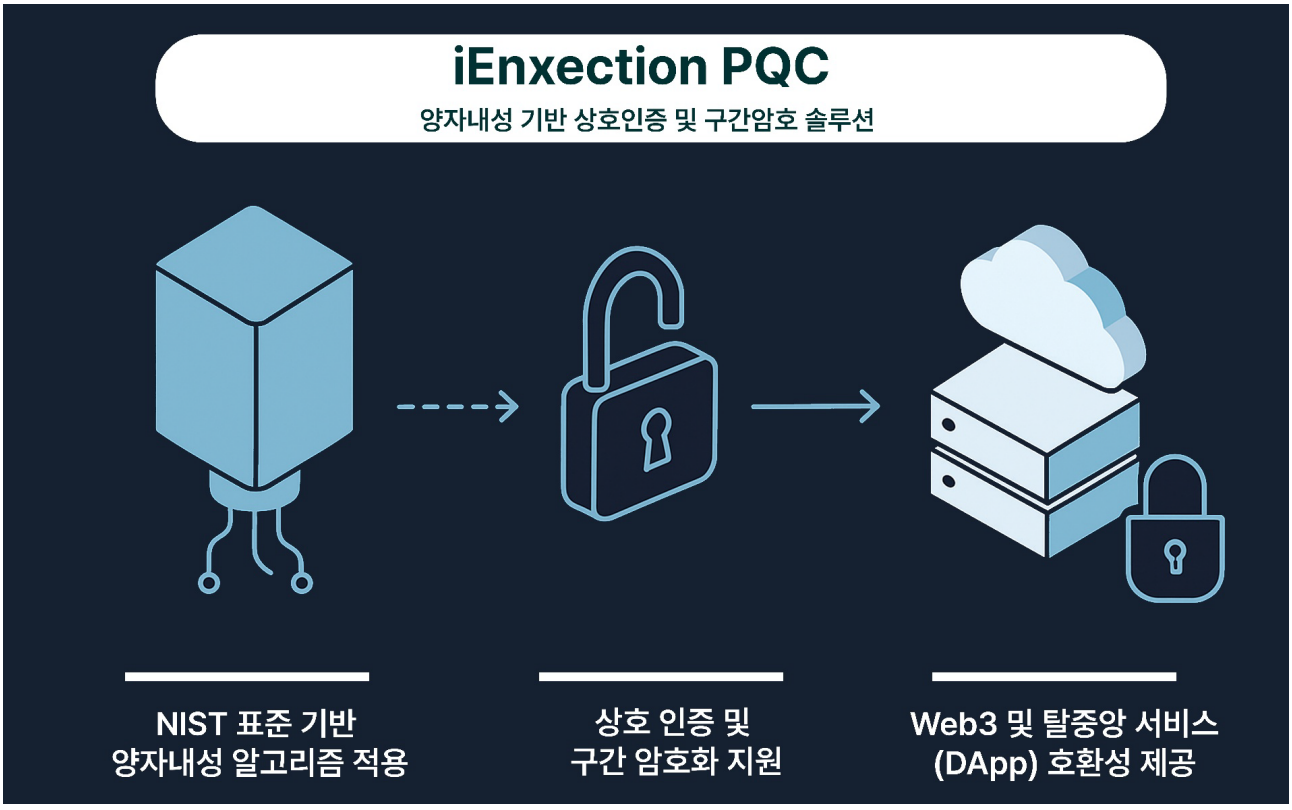
③ EdgeQ-CWallet – 기업용 MPC 다자 공동 지갑

개인 사용자가 더욱 안전하고 편리하게 디지털 자산을 관리할 수 있도록 지원하는 개인용 지갑 솔루션입니다. 기존 지갑의 가장 큰 문제점이었던 개인 키 분실의 위험을 MPC 기술을 통해 해결했습니다. 사용자가 개인 키를 분실하더라도 사전에 지정된 복구 절차를 통해 안전하게 자산을 복구할 수 있어, 더 이상 니모닉 구문이나 개인 키를 종이에 적어 보관하는 불안함에서 벗어날 수 있습니다. 복잡한 기술에 대한 이해 없이도 누구나 쉽고 편리하게 사용할 수 있도록 직관적으로 설계되었습니다.

04. 차세대 'ZERO-Trust' 전략의 핵심, iEnXectionPQC

iEnXectionPQC(아이인젝션PQC)는 제로트러스트(Zero-Trust) 환경에서 요구되는 강력한 인증 체계와 데이터 보호 메커니즘을 구현하는 미래형 보안 솔루션으로, 올해 KISA가 주관하는 '2025년 제로트러스트 도입 시범 사업'에 참여해 국내 주요 은행의 금융망을 대상으로 실증 사업을 추진하고 있습니다. 이 프로젝트는 기존 금융 네트워크를 교체하는 대신 그 위에 PQC 기반 보안 계층을 덧씌우는 '오버레이' 방식으로 진행되는데, iEnXectionPQC는 은행의 국내외 지점과 본사 간 통신망에 PQC 기반 인증 및 암호화 체계를 적용하는 핵심 역할을 맡습니다.

또한 iEnXectionPQC는 한국형 암호모듈 검증(KCMVP)을 획득한 기술력을 바탕으로, 미국 NIST 표준 PQC 알고리즘과 한국형 PQC 알고리즘(KpqC)를 모두 지원하는 데이터 및 통신 보안 솔루션으로 이미 다양한 분야에서 실전 검증을 마쳤습니다.



05. 마치며

이상으로 양자내성암호 기술 PQC의 등장 배경과 IT 업계의 움직임, 그리고 ITCEN PNS가 EdgeQWallet과 iEnXectionPQC로 PQC 시대를 어떻게 열어가고 있는지 알아보았습니다. 산업계가 PQC에 집중하는 것은 단순한 기술 교체가 아닌 디지털 신뢰 체계 재정립을 위한 필수 과제입니다. 양자컴퓨팅 시대의 보안 위협에 선제적으로 대응할 수 있는 차세대 전자지갑이자, 블록체인 디지털 금융 혁신의 핵심 인프라로서 기업의 보안을 강화해 줄 EdgeQWallet과 iEnXectionPQC! 더 자세한 내용이 궁금하시면 언제든 연락 주시기 바랍니다.

최신 IT 트렌드와 비즈니스 인사이트, 실전 노하우까지 !
아이티센그룹 홈페이지에서 깊이 있는 분석 자료로 만나 보세요.