솔루션 개요

포스트 퀀텀에 대비하기 위한 암호화 민첩성

cpl.thalesgroup.com

THALES
Building a future we can all trust

THALES
Building a future we can all trust

양자의 위협에 대비하십시오

기존 암호화 기법은 양자 컴퓨터에 취약하기 때문에 이제 데이터를 보호할 수 있는 대책을 강구해야 합니다. Harvest Now, Decrypt Later(HNDL) 공격, 즉 암호화된 데이터를 수집하여 저장한 후 나중에 양자 컴퓨터를 사용해 복호화하는 사이버 공격이 이미 일어나고 있기 때문입니다.

이제 신뢰할 수 있는 환경에서 PQC 대비 암호화를 테스트하여 양자 컴퓨팅이 인프라 보안에 어떤 영향을 미칠 수 있는지 파악한 후 유연하고 민첩한 계획을 수립함으로써 포스트-퀀텀 암호화(PQC)를 준비해야 합니다.

NIST는 올해 몇 가지 PQC 알고리즘을 발표하여 표준으로 채택할 예정입니다. 기업은 여기에서 원하는 알고리즘을 선택하여 양자 컴퓨팅 공격을 방어할 수 있습니다. NIST가 PQC 알고리즘을 공식적으로 표준화하면 전 세계 관리 기구들은 NIST PQC 표준화 프로세스에 따라 규정 준수 의무화를 공표합니다. 의무화가 공표되면 다양한 규정 준수 지침이 제정되어 기업들도 서둘러 지침을 이행할 수밖에 없습니다.

기본적인 암호화 민첩성 아키텍처를 기반으로 PQC를 위한 네트워크 암호화 솔루션을 사용하여 전송 데이터를 보호

지금 PQC가 중요한 이유

현재 사용되는 암호화 기법을 PQC로 전환하려면 시간이 오래 걸리기 때문에 지금부터 최상의 전략을 **준비해야 합니다**. 누구보다 앞서 시작한다면 PQC로 가는 여정에서 기업과 고객의 피해를 최소화하고, 비용을 절감하고, 위험을 줄이고, 비즈니스 연속성을 유지할 수 있습니다. 또한 NIST를 비롯한 기타 산업 PQC 규정이 발표되더라도 기업들은 유리한 위치에서 발빠르게 해당 규정들을 따를 수 있습니다. 양자 공격은 HNDL의 형태로 이미 발생하고 있습니다. 따라서 지금은 더욱 긴 대칭 키, 즉 대역외 키를 사용하는 등 중간 솔루션부터 시작하는 것이 바람직합니다. 그러면 오늘날 HNDL에서 기업을 보호할 뿐만 아니라 포스트 퀀텀 암호화 구현에 철저히 대비할 수 있습니다.

QR 코드를 스캔하여
HSE PQC 스타터 키트를
요청하십시오

PQC 스타터 키트로 시작하는 첫 걸음

Thales High Speed Encryptors(HSE)와 함께 제공되는 PQC 스타터 키트는 기업이 테스트 환경을 구축하여 양자 관련 대책을 빠르고 안전하게 테스트할 수 있는 저가형 솔루션입니다. PQC 랩에서는 포스트-퀀텀 암호화와 엔트로피를 사용해 애플리케이션 실행, 데이터 전송 등을 시뮬레이션할 수 있기 때문에 아키텍처의 유효성 검증에 효과적입니다. 지금부터 준비하여 펌웨어 알고리즘이 완성되었을 때도 비즈니스를 원활하게 운영할 수 있도록 계획을 세우십시오.

손쉬운 퀀텀-세이프 테스트 환경 설정:

- ✓ **NIST 포스트-퀀텀 알고리즘 사전 구현**
- ✓ **대역외 키 관리 제공, NIST가 KDF 방법 승인**
- ✓ **옵션으로 ETSI eQKD v14.01을 통한 양자 키 분배 선택 가능**
- ✓ **옵션으로 QRNG(양자 난수 생성) 또는 외부 엔트로피 소스 (BYOE—Bring your own encryption) 선택 가능**

HSE PQC 스타터 키트의 구성

스타터 키트는 완전한 기능을 갖춰 프로덕션 환경에도 배포할 수 있는 HSE로 구성되어 기존 네트워크에 한층 더 강력한 보안과 향상된 성능을 제공합니다.

- **Thales HSE 포트폴리오에서 선택할 수 있는 3가지 HSE 네트워크 암호화 어플라이언스**
  - **CN4010/CN4020**: 최대 1Gbps 네트워크 암호화 어플라이언스, 인증된 고성능, CNI, SCADA, 음성/영상 등 원격 위치에 최적화된 소형 폼팩터
  - **CN6010**: 1 및 10 Gbps 네트워크 암호화 어플라이언스, 랙 마운트 가능, 완전한 이중화로 안정적인 설계, 프라이빗 네트워크 및 데이터 센터에 최적화
  - **CN6140**: 최대 4x10Gbps 네트워크 암호화 어플라이언스, 규모에 따른 독립 암호화 채널 4개 제공, 높은 확장성과 멀티링크 네트워크 지원
- **CM7 네트워크 관리자 – 암호화 관리 플랫폼(고객 포털에서 다운로드 가능)**
- **유용한 추가 서비스**
  - 전원 코드(CN6000 시리즈 모델)
  - 트랜시버(특히 CN6000 및 CN4020 유닛에 적합)
  - 유지보수 및 지원
  - 원격 설치 및 구성

cpl.thalesgroup.com
문의 – 서울특별시 용산구 독서당대로 98 6층 탈레스코리아 82.2.3278.8202 https://cpl.thalesgroup.com/ko/contact-us