Solution Brief

Thales Luna 포스트-퀀텀 암호화(PQC) 기능 모듈(FM)

Luna 하드웨어 보안 모듈(HSM)에서 시작되는 퀀텀-세이프 암호화 민첩성의 혁신적 변화

cpl.thalesgroup.com

THALES
Building a future we can all trust

THALES
Building a future we can all trust

문제

오늘날 디지털 환경은 특히 다음과 같은 IT 영역에서 신뢰를 구축하고 보장하려면 공개키 인프라(PKI)가 필요합니다.

- 소프트웨어 및 펌웨어 무결성과 정품 인증을 보장하는 코드 서명 기술
- 신뢰성을 보장하는 문서 서명 기술
- 주요 인터넷 통신 프로토콜(TLS, IPSEC, S/MIME 등)
- 정보 권한 관리 솔루션

하지만 새로운 기술이 끊임없이 개발되면서 각 기술마다 크든 작든 영향을 미치기 마련입니다. 양자 컴퓨팅은 새롭게 개발 중인 기술 중 하나이지만 앞으로 현재 사용되고 있는 모든 공개키 암호화 보안을 위협할 것으로 예상됩니다. 또한 현재 대칭형 암호화의 보안 강도를 취약하게 만들어 더욱 긴 키를 사용해야 하는 상황을 초래할 수도 있습니다.

양자 방지 암호화를 준비하지 않는다면 지금까지 네트워크를 통해 전송했거나, 앞으로 전송할 모든 데이터가 도청 또는 공개에 취약할 수 밖에 없습니다. 이미 고객들이 사용하고 있는 디바이스들도 멀웨어 공격에 취약해질 것이고, 오늘날 일상적인 상호작용에 없어서는 안 될 개인의 디지털 아이덴티티 역시 해당 디바이스와 연결되어 위험에 노출될 것입니다.

과제:

1.상당한 시간이 걸리는 암호화 민첩성의 변화

기업들이 암호화 메커니즘을 업데이트하려면 신중하게 준비해야 할 뿐만 아니라 업데이트 과정에서 검증까지 필요하기 때문에 오랜 시간이 걸립니다예를 들어, DES, SHA-1 또는 RSA 1024비트 키 사용을 중단하는 데 어려움이 있었습니다.. 기업들은 새로운 포스트-퀀텀 메커니즘이 주요 인프라 구성 요소마다 빠짐없이 지원되는지 확인해야 합니다. 더욱이 기업 규모가 클수록 데이터가 각 로케이션에, 혹은 클라우드/온프레미스로 구성된 하이브리드 환경에 상주하다 보니 업그레이드 프로세스가 뒤얽혀 인프라가 더욱 복잡할 때가 많습니다. 이러한 과제를 해결하려면 양자 컴퓨팅이 시작되기전에 새롭게 배포되는 메커니즘을 테스트할 수 있는 준비를 마쳐야 합니다. 지금 암호화 민첩성 전략을 수립하여 필요할 때 더욱 빠르고 안전하게 전환할 수 있도록 해야 합니다.

2.커넥티드 디바이스 보호

표준 퀀텀-세이프 보안 기술을 사용해 커넥티드 디바이스를 보호하는 일은 현재는 물론이고 미래에도 매우 중요합니다. 커넥티드 디바이스를 안전하게 보호하려면 다면적 접근 방식이 필요하지만 빈틈없는 보안을 위해 한 가지 중요한 방안은 키변조를 방지 하는 HSM에 저장하여 신뢰의 루트를 적용하는 것입니다.

오늘날 RSA나 ECC와 같은 비대칭 알고리즘은 디지털 서명에 사용되지만, 양자 위협에 취약합니다. 다행스럽게도 오늘날 퀀텀-세이프를 대체할 수 있는 기술들이 존재하지만 이러한 기술들로 대체하려면 구현에 관련된 문제들을 새롭게 고민해야 합니다.

솔루션

Luna HSM 포스트-퀀텀 암호화(PQC) 기능 모듈(FM)은 라운드 3 NIST 최종 후보에 들어가 오늘날 코드 서명이나 그 밖에 PKI가 필요한 사용 사례에 활용되고 있는 퀀텀-세이프 암호화 메커니즘 사용이 가능합니다. PQC FM은 PCIe HSM과 Network HSM에 설치할 수 있으며, 설치를 위해 하드웨어를 변경하거나 업그레이드할 필요도 없습니다. 이 시스템은 SP 800-208 요구 사항을 준수하며, 상태 비저장 및 상태 저장 키 유형 모두에 대한 키 관리 기능을 포함합니다.

주요 이점

- PQ 세이프 코드 서명을 배포하여 오늘날 소중한 디바이스를 안전하게 보호합니다. 이를 통해 향후 비용이 많이 드는 리콜이나 물리적 업데이트 없이 디바이스를 양자 위협에서 지킬 수 있습니다.
- 변조 방지 HSM을 사용해 양자 내성 키를 안전하게 생성하고 관리할 수 있는 이점을 제공합니다.
- 상태 저장 해시 기반 서명이든, 상태 비저장 해시 기반 서명이든 상관없이 표준 퀀텀-세이프 공개키 암호화를 사용해 디지털 서명을 원활하게 생성합니다.
- 광범위한 탈레스 기술 파트너와 협력해 퀀텀-세이프 PKI, TLS 또는 VPN을 설정하여 암호화 민첩성을 검증합니다.

협력을 통한 보안 강화: 지금 암호화 민첩성을 검증하십시오

탈레스는 공개/비공개 파트너와 협력하여 퀀텀-세이프 암호화를 비롯한 퀀텀-세이프 프로토콜 및 표준 도입 여부를 검증하고 있습니다. 또한 오늘날 보안 환경에서 탈레스 제품의 기능 최적화를 보장하려는 헌신적 노력의 일환으로 주요 파트너와 함께 Thales Luna PQC FM 통합을 검증하고 있습니다.

Luna HSM PQC FM의 특징:

- 퀀텀-세이프 디지털 서명 알고리즘의 미래 경쟁력을 확보하여 오늘날 오랜 기간 사용되는 디바이스들을 대상으로 알고리즘을 표준화함으로써 다음과 같이 먼 미래까지 안전하고 믿을 수 있는 소프트웨어/펌웨어 업데이트를 구현할 수 있습니다.
  - HSS(Hierarchical Signature System) IETF RFC 8554, XMSS(eXtended Merkle Signature System) IETF RFC 8391 등 IETF에서 표준으로 채택한 상태 저장 해시 기반 서명을 사용합니다.

- 문서 서명이나 코드 서명 같은 아이덴티티 사용 사례에서 양자 위협에 맞설 수 있는 암호화 민첩성을 제공하는 HSS와 XMSS는 모두 IETF에서 표준으로 채택되어 SP 800-208로 NIST의 승인을 받았으며, NSA(CNSA 2.0)에서 권장하고 있습니다.

- 다음과 같이 NIST에서 표준으로 채택되어 키 교환, 암호화, 디지털 서명에 퀀텀-세이프 메커니즘을 제공하는 상태 비저장 퀀텀 세이프 암호화 메커니즘을 검증합니다.
  - Falcon, SPHINCS+, Crystal-Kyber, Crystal-Dilithium

무료 PQC 암호화 민첩성 위험 진단 도구

탈레스의 무료 PQC 암호화 민첩성 위험 진단 도구는 기업이 포스트-퀀텀 위협에 노출되어 있는지 더욱 정밀하게 살펴보고, 어디까지 대응해야 하는지, 그리고 포스트 퀀텀에 대비하기 위해 지금 무엇을 해야 하는지 이해하는 데 효과적이므로 반드시 사용해보시기 바랍니다.

탈레스 소개

개인정보를 중요시하는 사람들은 데이터 보안을 위하여 탈레스의 솔루션을 사용합니다. 기업은 데이터 보안과 관련된 결정적인 순간에 직면하곤 합니다. 탈레스를 사용하면 이러한 순간(암호화 전략 구축, 클라우드 이전, 규정 준수 요건 충족)에도 끊임없는 디지털 혁신이 가능합니다.

결단이 필요한 순간을 위한 결정적인 솔루션