Defend Devices Against Quantum Threats

Future-Proof Your Device Encryption with TrustCore SDK

Overview

Quantum computing is advancing rapidly, posing a significant threat to traditional cryptographic methods like RSA and ECC. To address this, NIST has developed Post-Quantum Cryptography (PQC) algorithms to protect against quantum attacks. DigiCert® TrustCore SDK — a C SDK for embedded systems — integrates these NIST-approved algorithms, providing quantum-safe cryptographic solutions to safeguard data and maintain security into the future.

PQC-Ready Capabilities

TrustCore SDK incorporates the latest NIST-approved PQC algorithms to offer comprehensive quantum-safe encryption and signing:

ML-KEM (FIPS 203): Lattice-based key encapsulation for secure key exchanges.

ML-DSA (FIPS 204): Efficient digital signatures to ensure transaction integrity.

SLH-DSA (FIPS 205): Stateless hash-based signatures for long-term asset protection.

TLS 1.3 Integration: Enables secure network traffic using ML-KEM and ML-DSA for post-quantum key exchange and authentication.

Implementation Guidance

Transition Strategy: TrustCore SDK simplifies the adoption of PQC with clear integration paths and comprehensive documentation.

Compatability: Easily incorporate new PQC algorithms alongside into your applications alongside existing RSA and ECC algorithms.

Testing and Validation: Comprehensive validation tools and guidance to verify PQC implementations, with support for FIPS 140-3 certification requirements.

Next Steps

1. **Discover:** Inventory your current cryptographic usage and generate a Crypto Bill of Materials (CBOM) using open-source tools.
2. **Implement:** Leverage TrustCore SDK's APIs for easy PQC integration.
3. **Test:** Use provided resources to validate performance, security, and regulatory compliance.
4. **Deploy:** Transition to quantum-safe security with confidence, ensuring future-proof data protection.

Open Source Access

TrustCore SDK is available under the AGPL v3 license, offering transparent access to the code for evaluation and integration. Commercial licensing options are available for production use.

Conclusion

TrustCore SDK equips your organization with the tools needed to secure data in the quantum era. By integrating NIST-approved PQC algorithms, TrustCore SDK ensures your cryptographic infrastructure remains resilient, adaptable, and ready for future challenges, allowing you to protect your data while maintaining operational continuity.

Get started today

Scan the QR code to learn more:

To get started with TrustCore SDK, contact your DigiCert account manager or email sales@digicert.com

digicert®