POST-QUANTUM CRYPTOGRAPHY

Protect Today & Future-Proof Your Business Against Quantum Threats

ENTRUST

SECURING A WORLD IN MOTION

The State of Post-Quantum Cryptography

Quantum computing promises transformative breakthroughs for science, industry, and society. Yet it also presents one of the most urgent security challenges organizations have ever faced. The public key algorithms that secure today's digital ecosystem – most notably RSA and elliptic curve cryptography (ECC) – will be vulnerable once large-scale quantum computers are realized. A single quantum-capable adversary could retroactively decrypt previously captured data, undermine digital identities, and disrupt the cryptographic foundations organizations rely on to operate securely.

To meet this challenge, global standards bodies and regulators are moving quickly. NIST has selected its first suite of post-quantum cryptography (PQC) algorithms and is continuing preparations for developing additional standards for future candidate algorithms. At the same time, government and industry mandates are accelerating timelines for organizations to identify where RSA and ECC are used, reduce risk, and prepare for PQC migration.

As a result, organizations must begin a structured post-quantum readiness journey. This starts with gaining visibility into where cryptography is deployed across the enterprise – understanding which systems, applications, certificates, and keys rely on RSA or ECC. Next comes assessing the risk and prioritizing migration efforts based on sensitivity, exposure, and operational impact. Teams can then evaluate post-quantum algorithms, develop hybrid and transition architectures, and plan for updates to PKI, applications, and infrastructure. While full migration will take years, early discovery, assessment, and planning are essential to minimizing disruption and ensuring a smooth transition to quantum-safe cryptography.

What's at Stake if Organizations Stall

While large-scale quantum computers are still emerging, the risk to today's encrypted data is immediate. Adversaries can harvest sensitive data now and decrypt it later once quantum capabilities mature – exposing long-lived data, identities, and systems assumed to be secure.

- Long-lived data exposure from "harvest now, decrypt later" attacks
- Certificate and identity failures that could disrupt access and services
- Rushed, high-cost migrations driven by regulatory or industry mandates
- Erosion of customer trust, operational resilience, and regulatory confidence

The Deadlines to Prepare Are Approaching

2025 NSA (CNSA 2.0) requires software, firmware, and browsers to prefer and support quantum-safe algorithms

2030 NIST deprecating classical asymmetric algorithms like RSA

2033 NSA (CNSA 2.0) requires exclusive use of quantum-safe algorithms for software, firmware, and browsers

2035 NIST disallowing classical asymmetric algorithms

Entrust: PQ-Ready Solutions Today, to Secure Against Tomorrow

Our post-quantum ready solutions help organizations identify and transition their cryptographic assets with confidence. Our PQ-ready PKI empowers you to act now, issuing hybrid and pure PQC certificates backed by HSMs that support all standardized NIST algorithms. With complete visibility into your cryptographic landscape and automated workflows for discovery, assessment, and rollout, you can begin your quantum transition today without disruption. Entrust helps you build resilience, maintain compliance, and safeguard data that needs to remain secure for decades.

Accelerate your transition to quantum-safe cryptography with Entrust and:

- **Gain visibility** into where quantum-vulnerable cryptography exists
- **Reduce migration risk** through hybrid and quantum-ready architectures
- **Protect roots of trust** with high-assurance hardware
- **Automate cryptographic lifecycle management** to reduce manual error, accelerate remediation, and enforce consistent policy
- **Build crypto-agility** to adapt as standards and threats evolve

PQ-Ready HSM

Entrust nShield HSMs are NIST-validated for post-quantum algorithms – including ML-DSA, ML-KEM, and SLH-DSA – delivering production-ready, quantum-safe cryptography in tamper-resistant hardware. With native PQ support in firmware, organizations can begin testing and deploying quantum-safe digital signatures and key exchanges. The nShield 5's crypto-agile FPGA architecture accelerates these algorithms, helping minimize performance impacts. This makes nShield HSMs a future-proof root of trust – enabling secure key generation, storage, and operations today and into the post-quantum era.

Cryptographic Security Platform

The Entrust Cryptographic Security Platform (CSP) helps organizations prepare for the post-quantum era by unifying key, certificate, and secrets management across their entire environment and enforcing consistent crypto policy at scale. With centralized visibility and built-in crypto-agility – including support for emerging NIST-approved PQ algorithms – CSP lets organizations assess their current posture, reduce quantum-related risk, and transition seamlessly to quantum-safe encryption and PKI.

PQ-Ready PKI

Entrust post-quantum ready PKI brings future-proof trust to digital identities by integrating NIST-approved quantum-safe algorithms into certificate issuance and validation, with support for both pure PQC and composite certificates to enable smooth, crypto-agile migration. It allows organizations to introduce quantum-safe roots, intermediates, and end-entity certificates, while enforcing strong policy control and lifecycle automation. With Entrust PQ-ready PKI, teams can modernize their infrastructure, reduce quantum-related risk, and transition confidently to a secure, hybrid, and post-quantum future.

PQC Readiness Assessment

The Entrust PQC Readiness Assessment helps organizations understand their cryptographic posture and prepare for the transition to post-quantum cryptography. Delivered through the Cryptographic Center of Excellence, the assessment evaluates crypto-agility maturity, maps where PQ-vulnerable algorithms and dependencies exist, and identifies gaps that could impede migration. It provides clear, actionable recommendations and a tailored roadmap so organizations can remediate risks, strengthen agility, and confidently plan their move to quantum-safe cryptography.

Turning Readiness into Resilience

Organizations that begin their post-quantum journey today position themselves to achieve:

- Reduced long-term data exposure
- Fewer emergency-driven migrations
- Improved regulatory and audit readiness
- Greater operational resilience and continuity
- Sustained customer and stakeholder trust

Moving Forward with Confidence

Post-quantum readiness is a journey, not a single upgrade. With Entrust, organizations can take measured, confident steps today – protecting critical assets now – while building a foundation of trust that endures through the quantum era and beyond.

Reach out today for your PQC Assessment.

ABOUT ENTRUST

Entrust fights fraud and cyber threats with identity-centric security that protects people, devices, and data. Our comprehensive solutions help organizations secure every step of the identity lifecycle, from verifying identity at onboarding to securing connections and fighting fraud in everyday transactions. Ongoing monitoring supports compliance and safeguards keys, secrets, and certificates. With a foundation of identity-centric security, our customers can transact and grow with confidence. Entrust has a global partner network and supports customers in over 150 countries.

For more information, visit www.entrust.com.

entrust.com Toll-Free: 888.690.2424 | International: +1.952.933.1223 | sales@entrust.com

ENTRUST
SECURING A WORLD IN MOTION