Prepare for a Post-Quantum World With Entrust Solutions

The challenge of post-quantum (PQ)

Quantum computers exist today, and the technology behind them continues to advance at a rapid rate. Although the exact timeline is unknown, it's expected that within the decade quantum computing will disrupt encryption-based cryptographic defenses, ultimately ending the golden age of cryptography as we know it.

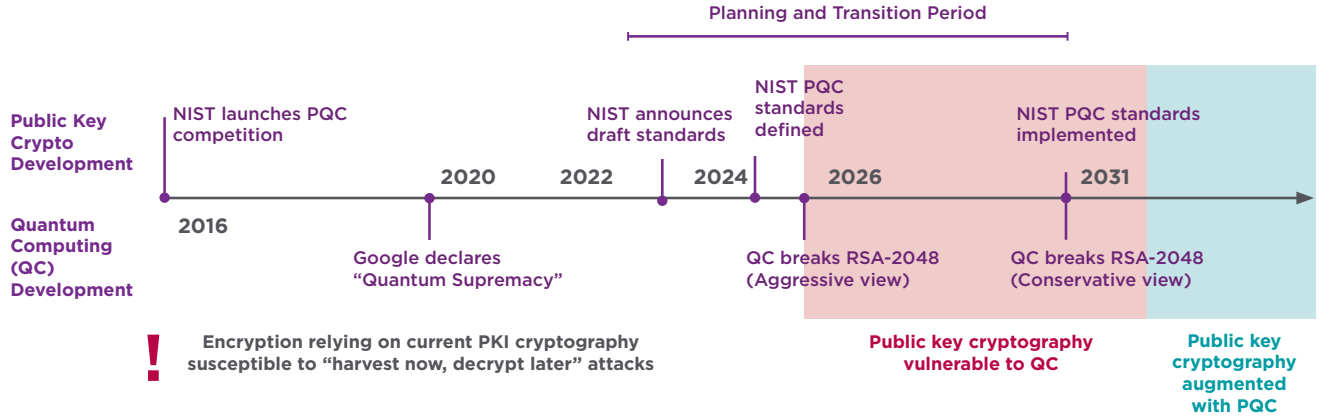
The time to prepare is now

Quantum computers are well-suited to solving certain types of problems in a fraction of the time required by classic computers. Prime number factoring is the hardness problem underlying the security of RSA encryption, and this will become feasible with quantum computers. The same is true of elliptic curve cryptography (ECC).

With so much of our data and communications security relying on these public key algorithms, organizations need to start looking for their post-quantum preparedness strategies.

The transition to quantum-safe algorithms is not just another cryptographic refresh cycle. It will be more involved and will take several years, so it's important that organizations start looking at this now.

Quantum Threat Timeline



Learn more about our post-quantum cryptography (PQC) solutions at entrust.com

Entrust PQC Solutions

> **The transition to post-quantum encryption algorithms is as much dependent on the development of such algorithms as it is on their adoption. While the former is already ongoing, planning for the latter remains in its infancy. We must prepare for it now to protect the confidentiality of data that already exists today and remains sensitive in the future.**
>
> - Alejandro Mayorkas, U.S. Secretary of Homeland Security

What organizations should be doing today

1. **Inventory Your Data:** It's important to understand where your valuable and/or long-life data resides, as well as the related data flows. Once you have that catalog and inventory, you'll know where your highest concerns are and therefore, where to start.

2. **Inventory Your Cryptographic Assets:** Know what cryptographic assets and algorithms you have in your environment and where they reside. It's also important to ensure compliance, control, and automation of these assets.

3. **Build a Cryptographic Agility Strategy and Roadmap:** Cryptographic agility will be critical for the PQC transition. And because these are not mature sets of algorithms, post-transition agility will be key, too. It's also important for organizations to identify areas of risk relating to cryptography including process, people, and technology.

4. **Test and Plan the Migration:** As the NIST PQC standards continue to evolve, organizations can begin testing within their applications. Work with your vendors and ensure they have a plan and roadmap to support PQ.

Learn more about our post-quantum cryptography (PQC) solutions at entrust.com

Entrust PQC Solutions

Entrust solutions for post-quantum preparedness

Entrust has a leading role in creating the post-quantum cryptography (PQC) standards that are the future of data protection. Through innovation and investment in our portfolio, we are designing solutions for today and tomorrow, ensuring a secure connected world.

PQC readiness assessment

As part of the Entrust Cryptographic Center of Excellence consulting portfolio, this tool:

- Evaluates your cryptographic agility maturity and identifies your readiness to manage the introduction of PQC algorithms
- Provides actionable recommendations to remediate identified risks in cryptographic systems, ultimately helping you prepare to manage the challenges of PQ
- Provides a roadmap to achieve cryptographic agility and make the transition to PQC

Entrust PKI as a Service for PQ

This cloud-based offering:

- Provides you with composite and pure quantum certificate authority hierarchies
- Allows you to issue hybrid or composite certificates combining classical and quantum-safe algorithms
- Gives you the ability to test multi-certificates or composite certificates with their applications
- Supports the NIST PQ draft standard algorithms

Entrust nShield PQ SDK

- This offering – in conjunction with Entrust CodeSafe – provides a software development suite of cryptographic functions based on NIST's PQ cryptography algorithms identified for standardization, which can run within the FIPS 140-2 Level 3 physical boundary of an Entrust nShield Hardware Security Module (HSM)
- Supports a range of PQ cryptographic operations including key generation, key signing, digital signature, encryption, decryption, and key exchange
- Enables developers to:
  - test PQ algorithms
  - invoke cryptographic operations via Java calls
  - execute code within a secure test environment

Learn more about our post-quantum cryptography (PQC) solutions at entrust.com

For more information

888.690.2424
+1 952 933 1223
sales@entrust.com
entrust.com

ABOUT ENTRUST CORPORATION

Entrust keeps the world moving safely by enabling strong identities, secure payments, and protected data. We offer an unmatched breadth of solutions that are critical to the future of secure enterprises, governments, the people they serve, and the data and transactions associated with them. With our experts serving customers in more than 150 countries and a network of global partners, it's no wonder the world's most trusted organizations trust us.

Learn more at
entrust.com

ENTRUST

Global Headquarters
1187 Park Place, Minneapolis, MN 55379
U.S. Toll-Free Phone: 888 690 2424
International Phone: +1 952 933 1223