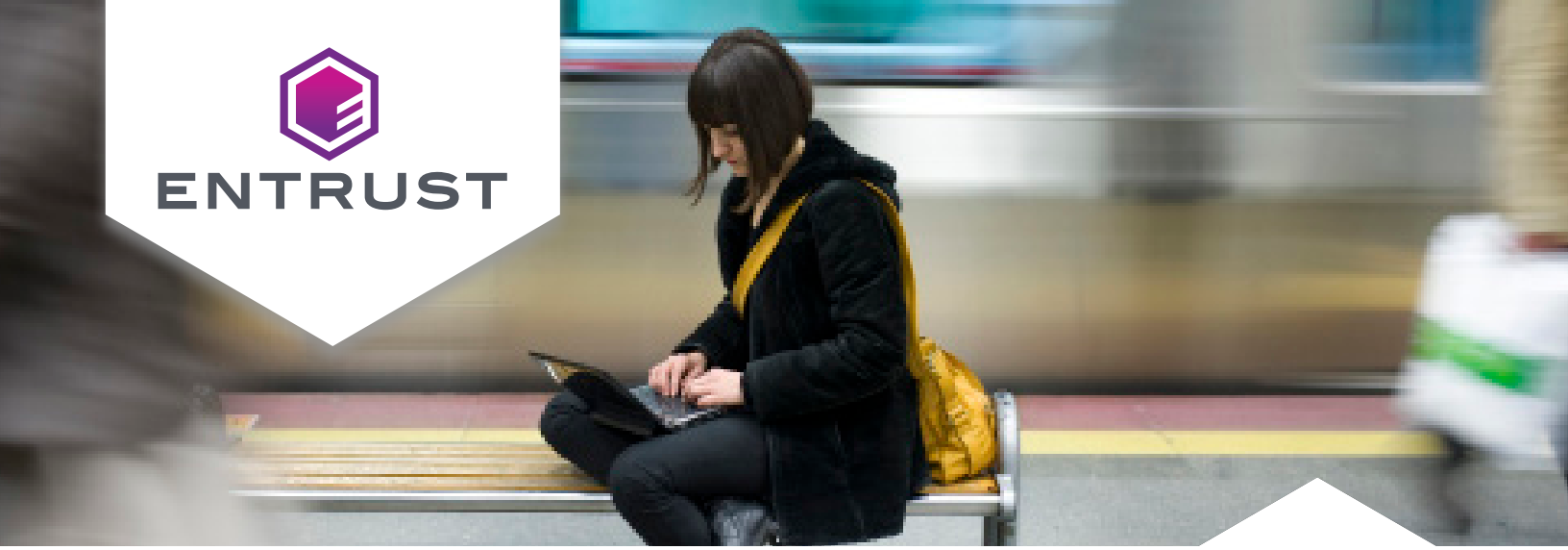


Prepare for a Post-Quantum World with Entrust Solutions

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.

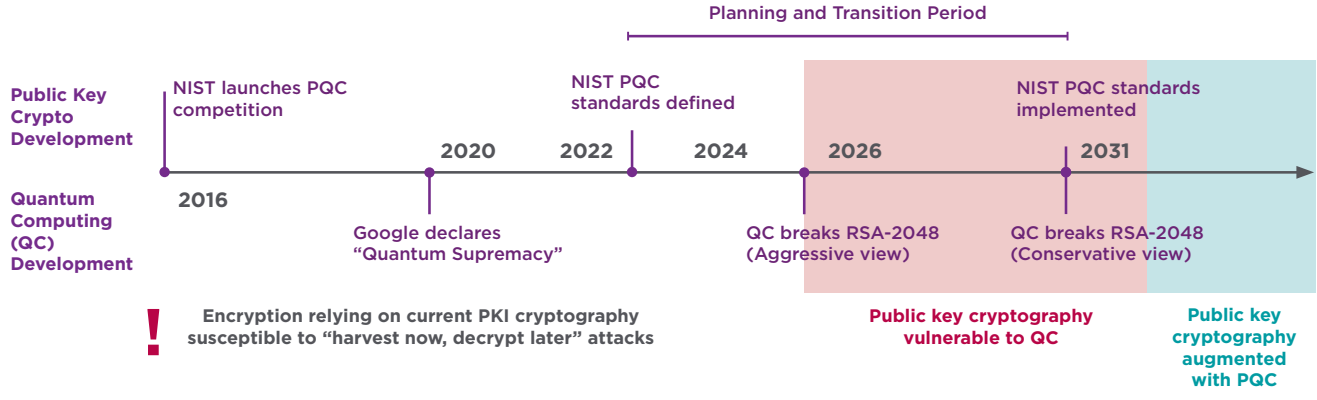
The time to prepare is now

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 solutions for post-quantum cryptography 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:** Consider the shelf life of your data and how far into the future it will need to be protected.
2. **Inventory Your Cryptographic Assets:** Know what cryptographic assets and algorithms you have and where they reside.
3. **Figure Out Your Timeline to Transition:** Flag this as an issue now, knowing the migration to post-quantum cryptography could take several years.
4. **Plan the Migration:** Talk to your vendors too and make sure they have a plan and roadmap to support PQ.

Entrust solutions for post-quantum preparedness

Entrust has a leading role in creating the post-quantum cryptography 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:

- Identifies your readiness to manage the introduction of PQ 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 the required level of cryptographic agility

Learn more about our solutions for post-quantum cryptography at entrust.com

Entrust PQC Solutions

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 finalist algorithms

ENTRUST NSHIELD PQ SOFTWARE DEVELOPMENT KIT (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, encrypt, decrypt, sign, verify, and key exchange
- Enables developers to:
  - test PQ algorithms
  - invoke cryptographic operations via Java calls
  - execute code within a secure test environment

ENTRUST QUANTUM JAVA TOOLKIT

This pluggable Java toolkit:

- Provides a way for you to integrate quantum-safe algorithms into your digital certificate-generation workflows
- Allows you to start building secure applications with PQ cryptography
- Supports:
  - composite certificate draft standards
  - traditional single algorithm certificates
  - NIST post-quantum development

Learn more about our solutions for post-quantum cryptography 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 trusted experiences for identities, payments, and digital infrastructure. We offer an unmatched breadth of solutions that are critical to enabling trust for multi-cloud deployments, mobile identities, hybrid work, machine identity, electronic signatures, encryption, and more. With more than 2,800 colleagues, a network of global partners, and customers in over 150 countries, it's no wonder the world's most entrusted 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