ENTRUST

Best Practices – Preparing for Post Quantum Computing

Crypto Agility Checklist and FAQs

It’s hard to prepare for post quantum (PQ) when no one is sure what algorithms will be standardized or when it will be instituted.

Organizations need to start thinking about it though, because migrating to PQ will be difficult. One of the key reasons to start thinking about PQ early is to see how algorithms with different size, performance, and throughput characteristics perform in your IT environment. When you start testing new algorithms, you can determine what breaks when PQ is introduced into your IT environment.

Here are things you can do now in preparation for PQ:

Cryptographic inventory

The first step in planning for PQ is to gain a full understanding of your cryptographic inventory, which includes getting a complete picture of what you have and understanding how easy it will be to switch. There will likely be multiple algorithms in use that will react differently when new algorithms are applied.

❒ Find all algorithms that are in use:
- o certificates
- o applications
- o protocols
- o networks
- o support
- o systems

❒ Identify what key sizes are being utilized:
- o in certificates
- o in applications
- o in protocols

❒ Know how algorithms used in your IT environment are determined.
- o Are there limitations? For example, find out whether algorithms are hardcoded into applications with a maximum key size.
- o Are protocols set up to use only certain algorithms?

❒ Determine what will be required to migrate to new algorithms.

Post Quantum Computing Best Practices Checklist

IT vendor preparedness

Vendor conversations are a critical next step toward understanding how your technology providers are thinking about PQ and what steps they are taking toward crypto agility. PQ readiness relies heavily on whether or not your IT vendors are doing a good job at PQ implementation. Delays or poor planning on database, buffer, system, memory, or support updates, for example, will impact the software you rely on. Your assessment in how well your IT vendors are prepared for PQ will help you make critical decisions on whether you feel confident transitioning to PQ with that vendor or whether you move to something else to mitigate risk.

Here are some questions to ask your vendors:

❒ Are you thinking about PQ?

❒ What are your thoughts around crypto agility?

❒ Are you thinking about how to migrate to new algorithms? Do you have plans to test new algorithms and the impact of migrations?

❒ Do you plan to develop proof of concepts or test implementations for us to demo and experiment with? (It's important to know that your vendors are thinking about it. It could take a few years before you can expect to have something available to demo.)

FAQs

How is Entrust preparing for PQ?

Entrust has taken a leading role in PQ by collaborating with other organizations to propose new IETF X.509 certificate formats that place traditional algorithms like RSA and ECC side-by-side with new PQ algorithms. We are also closely following the work of organizations like the National Institute of Standards and Technology (NIST), which has a project underway to develop algorithms that are resistant to quantum computing and eventually will standardize on them. We want to help companies sustain their IT ecosystem to reduce replacements, maintain system uptime, and avoid costly changes caused by a lack of preparation.

- Entrust is also taking the lead by working with these agencies and organizations to stay in front of quantum computing.
- We offer Platinum Services customers access to a next-level vulnerability scanning solution. It evaluates crypto against standard and quantum policies.

How do you do a cryptographic inventory?

We can help with this. An advanced Discovery tool is included for Entrust Platinum Services customers.

Are implementations available for testing?

You can test open-source implementations and approved proof of concepts, but don't deploy anything until NIST announces the standardized algorithms and approved implementations are available. The purpose of testing is to identify any bottlenecks or blockers in your environment.

Learn more at
entrust.com

ENTRUST

U.S. Toll-Free Phone: 888 690 2424
International Phone: +1 952 933 1223
info@entrust.com