B P P P Q C

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 di cult. One of the key reasons to start thinking about PQ early is to see how algorithms with di erent 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 di erently when new algorithms are applied.

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.