Post-quantum questions to ask your vendors

Quick-reference list

Use these questions, which align to the key phases of the Australian Signals Directorate's (ASD) LATICE framework, to assess vendor readiness for post-quantum cryptography (PQC).

Organisations are not expected to ask every question of every vendor. Instead, apply the questions based on the vendor's risk level, the degree of cryptographic control exercised by the vendor, data sensitivity and longevity, and the organisation's current stage of PQC transition.

Locate

- Do you maintain a current inventory of cryptographic dependencies, such as a cryptographic bill of materials or equivalent artefacts?
- Where is cryptography implemented?
- Is any cryptography hardcoded, fixed or hardware bound?
- Do third-party dependencies introduce cryptography?
- How is cryptography updated?
- Do your products rely on hardware roots of trust?
- How is firmware authenticity verified?
- Are firmware and boot processes updatable to support PQC signature schemes?

Assess

- Which customer data flows rely on traditional asymmetric cryptography?
- What data lifetime assumptions does your product or service make for the data it processes or stores, and how can customers configure or manage those lifetimes?
- Do you have a documented, product- or service-specific assessment of risks posed by a CRQC?
- Do you distinguish between signing, encryption and authentication risks?
- Can customers choose stronger cryptographic settings today?
- What authentication mechanisms rely on traditional asymmetric cryptography?

Triage

- Which products or services will be PQC-ready early enough to support customer rollout before the end of 2030?
- Which components require hardware replacement or re-architecture?
- Do you support post-quantum/traditional (PQ/T) hybrid modes as a temporary transition mechanism, and how and when will you transition to PQC-only?
- How do you consider customer risk when prioritising PQC transition activities?
- What internal governance arrangements oversee your PQC transitions?

Implement

- Which post-quantum cryptographic algorithms will you support, and when will support be generally available to customers?
- Is your PQC implementation production ready and available for customer use?
- How do you validate and maintain cryptographic libraries?
- How will key management, certificate sizes and lifecycle processes change under PQC?
- How do customers enable PQC in your product or service?
- Is PQC included in base licensing?

Communicate and educate

- How are customers notified of cryptographic changes?
- Do you provide customer-ready transition guides for PQC?
- How will traditional cryptography be deprecated, including any temporary use of PQ/T hybrid approaches?
- Are your support and engineering teams trained to support PQC?
- Does your roadmap align with ASD guidance and support PQC transition by the end of 2030?
- Do you contribute to or track relevant PQC standards bodies, and how does this influence your roadmap?