

POST-QUANTUM CRYPTOGRAPHY

# Vendor Readiness Questionnaire

*Twenty questions about one named product, answered with evidence.*

Part of the QuantumGate Post-Quantum Vendor Assessment Toolkit

October 2026 · Free to use and adapt with attribution

This toolkit supports preliminary supplier assessment and migration planning. It does not certify vendor readiness, verify security claims, or replace technical assessment, contractual review, or applicable regulatory requirements. Organizations in the United Arab Emirates should confirm the requirements that apply to them with the UAE Cyber Security Council and the National Cryptography Center, together with any sector requirements.

# How to complete this questionnaire

This questionnaire establishes what a named product supports today, what is planned, and what customers will have to do. Responses are used for supplier due diligence and migration planning.

|                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|---------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Scope                     | Answer for the single product, version, and deployment named in the profile section. Where capability differs between versions, configurations, or deployment models, say so in the Detail field rather than answering for the product line as a whole.                                                                                                                                                                                                                                      |
| Which questions to answer | The organization that sent this questionnaire states the questions it requires in the box at the foot of this page. Where that field names a subset, answer those and leave the rest. Where it is blank, answer all twenty.                                                                                                                                                                                                                                                                  |
| How to answer             | The response type is shown beside each question number. Questions with options take a selection, an Evidence field for the document, release note, report, or certificate that supports the answer, and a Detail field for the specifics: product versions, parameter sets, configurations, limitations, and dates. Some questions list several items and take one selection per row, because the answer can differ between them. Information requests take a written response and evidence. |
| Longer answers            | Where a Detail field is too small, write See attachment and return the fuller answer in a separate document, with each section labelled by question number.                                                                                                                                                                                                                                                                                                                                  |
| If you cannot answer      | Within the questions you were asked, select or write Unknown rather than leaving a field blank. Where a question does not apply, select Not applicable and state why in Detail.                                                                                                                                                                                                                                                                                                              |
| Status of claims          | A response is a statement by the vendor. It is not treated as independent verification, and material claims may be checked against public validation records or in technical discussion.                                                                                                                                                                                                                                                                                                     |
| Where responses go        | Completed questionnaires go to the organization that sent it. QuantumGate publishes this template and does not receive, collect, or review responses.                                                                                                                                                                                                                                                                                                                                        |
| Credit                    | This template was produced by QuantumGate. It is informed by published guidance from the Australian Signals Directorate and the AUSCERT Cyber Leaders Network. The questions are original and may be adapted with attribution.                                                                                                                                                                                                                                                               |

COMPLETED BY THE REQUESTING ORGANIZATION

| Requesting organization | Questions required                | Response deadline |
|-------------------------|-----------------------------------|-------------------|
|                         | Leave blank to request all twenty |                   |
|                         |                                   |                   |

# The four response types

|             |                                                                                                                            |
|-------------|----------------------------------------------------------------------------------------------------------------------------|
| Capability  | Does the product do this today?<br>Available · Limited · In development · Planned · Not planned · Unknown · Not applicable |
| Process     | Does this exist, and is it complete?<br>Yes · Partial · No · Unknown · Not applicable                                      |
| Cost        | What does the change cost?<br>Additional cost · Included · Not determined · Not applicable                                 |
| Information | A written response, with supporting evidence. No options.                                                                  |

WHAT THE CAPABILITY OPTIONS MEAN

|                |                                                                                 |
|----------------|---------------------------------------------------------------------------------|
| Available      | In production and usable by customers today.                                    |
| Limited        | Available only in some versions, configurations, regions, or deployment models. |
| In development | Implementation underway, with a target release.                                 |
| Planned        | On the roadmap. No implementation work started.                                 |
| Not planned    | No current intention to implement.                                              |
| Unknown        | Cannot be answered at this time.                                                |
| Not applicable | Does not apply to this product. State why.                                      |

COMPLETE THIS SECTION FIRST

## Vendor and product profile

The rest of the questionnaire applies to the product named here.

|                                                                                                         |  |
|---------------------------------------------------------------------------------------------------------|--|
| <b>Vendor legal name</b>                                                                                |  |
| <b>Product or service assessed</b>                                                                      |  |
| <b>Version, release, or model</b>                                                                       |  |
| <b>Deployment model</b><br>SaaS, private cloud, on premises, hybrid, operational technology             |  |
| <b>Region or environment in scope</b>                                                                   |  |
| <b>Product function</b><br>For example network, identity, PKI, HSM, application, device                 |  |
| <b>Commercial contact</b><br>Name, role, email                                                          |  |
| <b>Technical contact</b><br>Name, role, email                                                           |  |
| <b>Role accountable for the migration program</b><br>Job title and department, not an individual's name |  |
| <b>Date of response</b>                                                                                 |  |
| <b>Date supporting evidence was last updated</b>                                                        |  |
| <b>Confidentiality of this response</b><br>Any restriction on how it may be shared                      |  |

# Cryptographic visibility and dependencies

*Establish where cryptography sits in the product and how easily it can be changed.*

## Q1

PROCESS

### Cryptographic inventory

Can you provide a current inventory of the cryptographic algorithms, protocols, libraries, and certificates used by this product?

**Please provide** A cryptographic bill of materials or equivalent inventory, dated, stating what it covers and what it excludes.

ANSWER

☐ Yes    ☐ Partial    ☐ No    ☐ Unknown    ☐ Not applicable

EVIDENCE

DETAIL

## Q2

INFORMATION

### Where public key cryptography is used

Where does this product use public key cryptography, and for what?

**Please provide** Key establishment, authentication, digital signatures, software and firmware signing, certificate validation, and traffic between internal components.

RESPONSE

EVIDENCE

---

### Q3

INFORMATION

#### Third party dependencies

Which third party libraries, hardware components, cloud services, or suppliers could affect your migration timeline?

**Please provide** Component names, affected versions, the owner of each dependency, and known constraints on upgrading them.

RESPONSE

EVIDENCE

---

### Q4

PROCESS

#### Upgrade path

Can the cryptography in this product be changed without replacing hardware or the platform?

**Please provide** The update mechanism, any algorithms fixed in code or silicon, hardware roots of trust, firmware constraints, and the service life of affected equipment.

ANSWER

☐ Yes   ☐ Partial   ☐ No   ☐ Unknown   ☐ Not applicable

EVIDENCE

DETAIL

---

### Q5

INFORMATION

#### Products that cannot be upgraded

Where this product, or components of it, cannot be upgraded to post-quantum cryptography in place, what do you commit to for affected customers?

**Please provide** The affected components, the options you will offer, such as replacement, a migration path, or compensating controls, the timeline for each, and how existing deployments are supported in the meantime.

RESPONSE

EVIDENCE

# Risk assessment and governance

Find out whether the vendor understands its exposure and has made someone accountable.

Q6

PROCESS

Risk assessment

Have you assessed this product's exposure to a cryptographically relevant quantum computer?

**Please provide** Assessment date, scope, findings, remediation priorities, and review frequency.

ANSWER

☐ Yes    ☐ Partial    ☐ No    ☐ Unknown    ☐ Not applicable

EVIDENCE

DETAIL

Q7

INFORMATION

Long-lived data confidentiality

How have you assessed the risk that encrypted customer information collected today could be decrypted in the future by a cryptographically relevant quantum computer?

**Please provide** The data flows you have evaluated, the cryptographic mechanisms protecting each, how long that data must remain confidential, and the mitigations or migration plans that apply.

RESPONSE

EVIDENCE

---

**Q8**

INFORMATION

**Accountability and governance**

Which role and department are accountable for your migration program, and how is progress governed?

**Please provide** The accountable role and department, the approved plan, the review cycle, and how progress is reported.

RESPONSE

EVIDENCE

## SECTION C · Q9–Q13

**Standards and technical capability**

*Establish what the product can do today, as distinct from what is being announced.*

---

**Q9**

CAPABILITY

**Algorithm support**

Which standardized post-quantum algorithms does this product support today, and for which functions? Give a status for each algorithm, and name the exact parameter sets.

**Please provide** For each algorithm: product version, function, parameter set, and limitations. State separately any planned support for algorithms still in standardization, including FN-DSA, and any national algorithms required in your markets.

**ML-KEM**

☐ Available   ☐ Limited   ☐ In development   ☐ Planned   ☐ Not planned   ☐ Unknown  
☐ Not applicable

**ML-DSA**

☐ Available   ☐ Limited   ☐ In development   ☐ Planned   ☐ Not planned   ☐ Unknown  
☐ Not applicable

**SLH-DSA**

☐ Available   ☐ Limited   ☐ In development   ☐ Planned   ☐ Not planned   ☐ Unknown  
☐ Not applicable

EVIDENCE

DETAIL

---

## Q10

### CAPABILITY

### Production availability

For each algorithm you named in Q9, what is its release status for production use today? Answer for each one separately.

**Please provide** The release channel for each capability named in Q9: general availability, limited release, beta, or demonstration. Include the configuration instructions, the support terms that apply in production, and any restriction by edition, tier, or region.

#### ML-KEM

☐ Generally available   ☐ Limited release   ☐ Beta   ☐ Demonstration   ☐ Not available

#### ML-DSA

☐ Generally available   ☐ Limited release   ☐ Beta   ☐ Demonstration   ☐ Not available

#### SLH-DSA

☐ Generally available   ☐ Limited release   ☐ Beta   ☐ Demonstration   ☐ Not available

### EVIDENCE

### DETAIL

---

## Q11

### CAPABILITY

### Hybrid and post-quantum only modes

Does this product support a hybrid mode combining a traditional algorithm with a post-quantum algorithm, and does it support a post-quantum only mode? Answer for each mode separately.

**Please provide** Supported combinations, protocols, endpoints, and deployment modes; interoperability results; and whether you position hybrid as a transitional step or a long-term option.

#### Hybrid mode

☐ Available   ☐ Limited   ☐ In development   ☐ Planned   ☐ Not planned   ☐ Unknown

#### Post-quantum only mode

☐ Available   ☐ Limited   ☐ In development   ☐ Planned   ☐ Not planned   ☐ Unknown

### EVIDENCE

### DETAIL

---

## Q12

EVIDENCE

### Validation and interoperability

Which of the following can you provide, and what is in progress? Each kind of evidence proves something different, so answer for each one separately.

**Please provide** Algorithm test results, validated module certificate numbers with the module version and scope, third party assessments, and protocol interoperability reports. These give different assurances and are not interchangeable, and not every implementation requires the same certification, so label which is which and state where one does not apply. Include validations under way with their current stage.

Algorithm  
test results

☐ Provided    ☐ In progress    ☐ Not available    ☐ Not applicable

Validated  
module  
certificate

☐ Provided    ☐ In progress    ☐ Not available    ☐ Not applicable

Third party  
assessment

☐ Provided    ☐ In progress    ☐ Not available    ☐ Not applicable

Interoperability  
report

☐ Provided    ☐ In progress    ☐ Not available    ☐ Not applicable

EVIDENCE

DETAIL

---

## Q13

CAPABILITY

### Crypto-agility

How can cryptographic algorithms be changed as standards and requirements change?

**Please provide** How algorithms are selected and changed, key and certificate lifecycle handling, the update procedure, backward compatibility, and rollback.

STATUS

☐ Available    ☐ Limited    ☐ In development    ☐ Planned    ☐ Not planned    ☐ Unknown  
☐ Not applicable

EVIDENCE

DETAIL

# Migration plan and customer impact

Understand what the vendor will deliver, when, and what you will have to do.

## Q14

PROCESS

### Product roadmap

Can you provide a migration roadmap for this product with dated milestones?

**Please provide** Planned releases, target dates for general availability, dependencies, testing milestones, and decisions still open.

ANSWER

☐ Yes    ☐ Partial    ☐ No    ☐ Unknown    ☐ Not applicable

EVIDENCE

DETAIL

## Q15

INFORMATION

### Changes required

What changes will be required in the product, and in the customer's environment?

**Please provide** Software updates, operating system requirements, certificate and PKI changes, HSM implications, hardware replacement, API changes, and network changes. Separate what you change from what the customer changes.

RESPONSE

EVIDENCE

---

## Q16

DOCUMENTATION

### Deployment and testing

Which of the following exist today for the post-quantum capabilities in this product, and can be shared during the assessment?

**Please provide** Implementation guide, prerequisites, test plan, deployment steps, and rollback procedure. State which of these exist today.

Enablement  
steps

☐ Available now    ☐ Planned    ☐ Not available

Test guidance

☐ Available now    ☐ Planned    ☐ Not available

Rollback  
procedure

☐ Available now    ☐ Planned    ☐ Not available

EVIDENCE

DETAIL

---

## Q17

CAPABILITY

### Interoperability during transition

How will this product interoperate with systems that have not migrated?

**Please provide** Supported transitional configurations and their limits, protection against downgrade, and the plan for retiring traditional mechanisms.

STATUS

☐ Available    ☐ Limited    ☐ In development    ☐ Planned    ☐ Not planned    ☐ Unknown  
☐ Not applicable

EVIDENCE

DETAIL

## Cost and support

*Understand the cost of the change and the support available during it.*

### Q18

COST

#### Cost

Will the post-quantum capabilities in this product require additional licensing or hardware?

**Please provide** What is covered by the current agreement, what is chargeable, and what hardware is required. State where this is not yet decided.

ANSWER

☐ Additional cost   ☐ Included   ☐ Not determined   ☐ Not applicable

EVIDENCE

DETAIL

### Q19

INFORMATION

#### Documentation and support

What documentation, technical support, and migration assistance will you provide?

**Please provide** Migration guides, support arrangements during the migration, training material, and escalation contacts.

RESPONSE

EVIDENCE

### Q20

INFORMATION

#### Notification

How will you notify customers of changes to algorithms, of vulnerabilities, and of changes to migration timelines?

**Please provide** Notification channels, the security advisory process, and notice periods for material changes.

RESPONSE

EVIDENCE

## Questions by supplier type

Complete all applicable blocks, since a product can fall into more than one category. These questions are in addition to those above.

---

**Cloud and software as a service**

Which service endpoints support post-quantum key establishment? Does support vary by region or service tier? Which parts remain the customer's responsibility?

---

**Network and connectivity**

Which key establishment mechanisms and protocol versions are supported? Can both ends negotiate a supported configuration? What is the effect on throughput and latency?

---

**PKI, certificates, and hardware security modules**

Which keys, certificates, signature mechanisms, and interfaces support post-quantum algorithms? What changes are needed in certificate authority hierarchies and certificate lifecycle tooling?

---

**Software and applications**

Which cryptographic libraries are embedded, and at what versions? How will existing integrations and APIs be updated and tested?

---

**Operational technology and connected devices**

Can firmware and trust anchors be updated in the field? Is hardware replacement required? How will devices with long service lives be handled?

---

**Managed service providers**

Which cryptographic controls do you operate directly, and which are inherited from your own technology suppliers? How do you assess those suppliers?

---

# Declaration

The respondent confirms that these responses describe the product versions named in the profile section as at the date of response, distinguish capabilities available today from those planned, and disclose known material limitations.

|            |  |
|------------|--|
| Name       |  |
| Role       |  |
| Department |  |
| Date       |  |
| Signature  |  |

A typed name in the signature field is accepted. Where your organization requires a handwritten or digital signature, print this page, sign it, and return it with the rest of the response.

SOURCES AND FURTHER READING

|                                                         |                                                                                                                                  |
|---------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------|
| <u>Australian Signals Directorate</u>                   | Post-quantum questions to ask your vendors. Vendor questions for post-quantum readiness, with a quick reference list. July 2026. |
| <u>AUSCERT Cyber Leaders Network</u>                    | Navigating the Quantum Horizon. Executive briefing, vendor questionnaire, and audit template.                                    |
| <u>PKI Consortium</u>                                   | Post-Quantum Cryptography Maturity Model. Product level maturity levels, with self assessment and third party assessment paths.  |
| <u>NIST National Cybersecurity Center of Excellence</u> | Migration to Post-Quantum Cryptography. Practical migration guidance and demonstration reports.                                  |

This toolkit supports preliminary supplier assessment and migration planning. It does not certify vendor readiness, verify security claims, or replace technical assessment, contractual review, or applicable regulatory requirements. Organizations in the United Arab Emirates should confirm the requirements that apply to them with the UAE Cyber Security Council and the National Cryptography Center, together with any sector requirements.