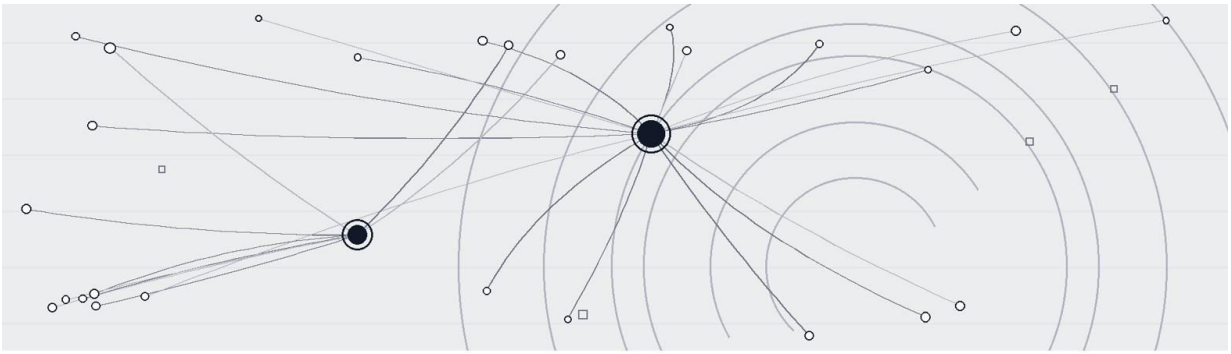
AUGUST 2026

APPLIED QUANTUM

THE APPLIED QUANTUM CCF INSTRUMENT SUPPLIER LINEAGE DISCLOSURE REQUEST



Implementation ancestry, firmware family, manufacturing origin and key generation design

Version 1.0-RC – August 2026

Steve Vaile and Marin Ivezic, Applied Quantum

Disclosure: Applied Quantum provides post-quantum migration advisory services. This work is published openly under CC BY 4.0 and is computable without engaging Applied Quantum.

COPYRIGHT AND LICENSE

© 2026 Steve Vaile and Marin Ivezic / Applied Quantum. This work is licensed under Creative Commons Attribution 4.0 International (CC BY 4.0). You are free to share and adapt this material for any purpose, including commercial use, provided you give appropriate credit to Steve Vaile, Marin Ivezic and Applied Quantum, link to the licence, and indicate any changes made.

Licence details: https://creativecommons.org/licenses/by/4.0/

The reference implementation and canonical test vectors publish separately under Apache-2.0 on the Applied Quantum GitHub. Neither licence reads onto the other.

DISCLAIMER

This document is provided as professional guidance based on the authors' and Applied Quantum's practitioner experience and publicly available standards, regulations and industry research. It does not constitute legal, regulatory, financial or compliance advice. Organisations should consult qualified legal counsel, auditors and regulatory authorities for guidance specific to their jurisdiction, sector and circumstances.

The regulatory instruments, certification records, standards and vendor capabilities referenced in this document reflect the state of the landscape as of August 2026, and that landscape moves. Readers should verify current status against primary sources (regulators and supervisory authorities, NIST, EMVCo and PCI SSC, the CycloneDX specification, public certification listings, vendor documentation) before making decisions.

References to specific vendors, products or tools are for illustrative purposes and do not constitute endorsement.

This is a v1.0 release candidate: v1.0 final publishes in November 2026 after a pilot cycle. Open items are public on the roadmap at CCFramework.org, and corrections are published as dated entries on its errata page.

ABOUT THIS DOCUMENT

Document type	CCF instrument – supplier disclosure request
Parent document	The Cryptographic Concentration Framework – Universal – v1.0-RC (August 2026)
Intended audience	Vendor-management and second-line teams dispatching the request, and supplier security-response functions answering it
Assumed knowledge	The Universal Framework’s reach semantics and evidence tiers
Scope	The Supplier Lineage Disclosure Request: attributed and anonymised response tiers, the three-state record, and the dispatch checklist including the pre-send certification-record check.

Status	Version 1.0-RC – release candidate; v1.0 final November 2026 after pilot

VERSION HISTORY

Version	Date	Changes
1.0-RC	August 2026	First public release, as a release candidate; drafted through four external review rounds and a family-wide line-edit pass.
1.0-RC	7 September 2026	Sections 2 and 3 aligned to the reach mechanism of Universal C.3 before dispatch; the retired double-computation wording removed from the supplier-facing text.
1.0-RC	8 September 2026	Response states aligned to the Profile enumeration: silence at the deadline is no-response; refusal and deflection are declined, with deflection recorded as the reason. Corroboration of a full response against a certification record is recorded separately from its E4 basis. Prose revised throughout. No figure changed.

HOW TO USE THIS DOCUMENT

This instrument is the supplier-facing request behind the framework's reach measurements. Dispatch follows the checklist in its usage notes, including the pre-send certification-record check. Responses, anonymised responses and named non-responses are recorded per its three-state model.

ACCOMPANYING RESOURCES

The framework family publishes at CCFramework.org: the Universal Framework, the Payments and Financial Services extensions, the payments whitepaper, the CBOM Conformance Statement, the Technical Companion and the instruments, together with the public roadmap, the errata and corrections page, the provenance survey and the frontier-census methodology.

Every canonical figure in the family comes from the reference implementation, with ten canonical test vectors that fix each one exactly. Both are open under Apache-2.0 on the Applied Quantum GitHub, and any implementation that reproduces the fixtures is conformant.

The Applied Quantum CBOM Profile, the input data contract, publishes at CBOMProfile.org. The Applied Quantum PQC Migration Framework, whose sector taxonomy the extensions follow, publishes at PQCFramework.org. Practitioner background and adjacent analysis sits on PostQuantum.com, as further reading rather than a normative source.

© 2026 Steve Vaile and Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

TABLE OF CONTENTS

© 2026 Steve Vaile and Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

Used in Phase 2 of the CCF Universal Framework v1.0-RC, and separately as a right-of-reply instrument for published research.

---

1. SCOPE AND USE

This instrument asks suppliers for information that an institution may be unable to establish from its own inventory: implementation origin, retained code, firmware family, manufacturing origin and generation design. Its output is an evidence record for layers 2, 4 and 6. It does not calculate concentration, assess every aspect of the supplier's security, or require publication of proprietary source code.

Assessment use. An institution sends this request to its own cryptographic suppliers to obtain the provenance required at layers 2, 4 and 6. These supplier-held facts cannot be established from internal data alone. The request is sent through third-party risk, with engineering support and reference to existing contractual information rights.

Research use. A researcher sends the same questions to a market's suppliers and publishes what each answered, together with the names of those that did not. The responses turn undisclosed fields into sourced original data. Asking suppliers directly and retaining their answers provides a fair basis for naming them in publication.

Attributed disclosure is preferred. A supplier that declines attribution may elect anonymised aggregate publication instead. Its answers enter the aggregate figures, labelled as anonymised, and no named row is published. A supplier taking neither option is recorded as a named non-response. Both uses send the same questions; only the framing paragraph and the escalation differ.

The request should identify exact products, versions and functions. A generic answer about a supplier's product range may be useful context but is not evidence of the implementation actually deployed. Where a supplier resells or integrates another party's component, the response should identify that relationship rather than imply that the visible supplier authored every cryptographic implementation.

2. CONFIDENTIALITY AND FAIR TREATMENT

The request asks for provenance metadata: implementation ancestry, firmware family, manufacturer origin, and entropy and generation design. It does not ask for keys, secrets, source code or exploit detail. Some provenance information may still be commercially or security-sensitive. Controlled disclosure is available under an NDA, through a redacted public entry backed by full private disclosure, or through attestation by an independent assessor. These forms are graded as disclosed.

© 2026 Steve Vaile and Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

Much of the requested information is already public. Published FIPS 140-3 non-proprietary security policies frequently name the upstream library. Entropy Source Validation certificates are publicly listed, and their public-use documents describe the noise source.

Where ancestry is undisclosed, the assessment includes the component in the upper bound of every known upstream from which it cannot be excluded. It reports the evidenced figure, the bound and the difference in reach points, attributing that difference to the absence of disclosure. The bounds must follow feasible relationships and the stated failure mechanism; they are not a penalty score or a claim that non-disclosure proves insecurity.

Research publication must distinguish full and partial disclosure, explicit refusal, a deflected answer, a pending request and no response. Confirm notice, intended use and factual-review arrangements before publishing named outcomes.

3. COVER TEXT

Cryptographic Provenance Disclosure Request

To: [supplier]

From: [institution / researcher]

Response requested by: [date, no less than 30 days]

Reference: [ref]

We are assessing cryptographic dependency concentration across [our estate / the sector], using the openly published Cryptographic Concentration Framework (ccframework.org). The assessment measures whether nominally independent suppliers share underlying cryptographic components, such that one defect could affect several at once.

The questions below ask for provenance metadata only. They do not ask for source code, architectural detail, vulnerability information, or any material that would assist an attacker. Several answers may already be public in your FIPS 140-3 security policy or entropy validation records.

How responses are used. Answers are recorded against your products in our assessment. Where a question is not answered, the assessment records the component as undisclosed and carries it inside the upper bound of every known upstream implementation it cannot be excluded from. Both the evidenced figure and the bound are reported, with the difference between them attributed to the absence of disclosure.

[*Research use only:* We publish the responses we receive and name every supplier that does not send one. Attributed disclosure is preferred. If you decline attribution, you may elect anonymised aggregate publication instead: your answers enter aggregate figures, labelled as anonymised, and no named entry appears. Declining both is recorded as a named non-response. You will receive the relevant extract for factual review no less than 14 days before publication.]

We are glad to discuss scope, confidentiality terms, or partial disclosure. Please direct questions to [contact] rather than declining on scope grounds without discussion.

© 2026 Steve Vaile and Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

4. QUESTION SET

Section A – Implementation ancestry

For each cryptographic implementation in the products listed at Annex 1.

A1. For each cryptographic implementation in this product – at minimum every key-establishment, signature and key-generation implementation in scope, including but not limited to ML-KEM, ML-DSA, SLH-DSA, RSA, ECDSA and ECDH – from which upstream codebase is the implementation derived? Name the project and version, and where obtainable the commit or content hash. Where the implementation is entirely your own, state that.

A2. Where derived, has the code diverged from its upstream? If so, in which primitives, and since when? Divergence evidence may take the form of commit or patch history, reproducible source comparison, engineering attestation identifying the rewritten primitives, or validated source provenance.

A3. Do any two products in Annex 1 share an implementation for the same algorithm?

A4. Which FIPS 140-3 or Common Criteria certificate covers the module containing this implementation? Provide the certificate number.

A5. Where an implementation is supplied to you by a third party rather than written by you, name the supplier.

Section B – Firmware family and manufacturing origin

For hardware products.

B1. To which firmware family does this product belong? Name every other product, under any brand, that shares that family.

B2. Is the hardware manufactured by your organisation, or by a third party? If by a third party, name the manufacturer.

B3. Is this product sold under any other brand or model designation?

B4. Where two products in Annex 1 appear distinct, do they share a firmware lineage, a manufacturer, or a cryptographic module?

Section C – Entropy and random number generation

C1. What entropy source design generates random values in this product? Describe the design class, not the implementation detail.

C2. Which deterministic random bit generator specification is used?

© 2026 Steve Vaile and Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

C3. Which NIST Entropy Source Validation certificate covers the design named at C1? Provide the number. Where validation is under another scheme, name it and the certificate.

C4. Is the entropy source your own design, or licensed or purchased from a third party? If the latter, name the source.

C5. What key generation design produces asymmetric key material in this product – the scheme for primes, nonces and derivation – and is that design your own or supplied? Name the supplier where supplied.

Section D – Roadmap and change

Optional and unscored. Section D is recorded separately whether it is answered or not, and never counts toward the response rate or the grading of Sections A to C. The binding form of D2 belongs in contracts and selection questionnaires, per Section 7, where a supplier commits more readily than at audit.

D1. Do you plan to change the upstream source of any implementation in Annex 1 within 24 months?

D2. Will you notify us of a change in implementation ancestry, firmware family, manufacturer or entropy design during the contract term?

5. GRADING AND RECORDING RESPONSES

Grade the **completeness of the answer** separately from the **basis of each claim**. A full engineering attestation can remain E4; a partial answer can contain one strongly verified fact. The grade must not act as a numerical discount on the assets using the supplier.

Grade	Response character	Evidence tier	Treatment
Full	Names the upstream project and version, or states own implementation with divergence detail	E4; corroboration against a certification record recorded as a separate attribute	Recorded as disclosed
Partial	Names a library but not a version or ancestry; answers some sections	E4 for what is answered; unanswered items undisclosed	Mixed record; follow up on the gap
Deflected	Cites certification,	E5 at best	**Recorded as**

© 2026 Steve Vaile and Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

Grade	Response character	Evidence tier	Treatment
	standards compliance, or "industry-standard implementations" without naming a source		**undisclosed.** Status `declined`, register reason "deflected".
Declined	States that the information will not be provided	–	Undisclosed, status `declined`
No response	Nothing by the deadline	–	Undisclosed, status `no-response` at the deadline

The response rate is full plus partial disclosures divided by requests issued, based on Sections A to C only. Section D is excluded. Each graded response is an input to the metric: full and partial disclosures create evidenced reach edges in Universal C.3.2 for the claims they establish; unanswered claims and other outcomes widen the applicable bounds.

A project name without the requested version and relevant derivation evidence is insufficient to resolve ancestry at the requested precision. The supplier statement itself may be E4, while an inferred lineage conclusion from that statement is E5 and remains qualified. Do not promote that inference to a fully established ancestry edge.

The Profile has no `deflected` enumeration value. Refusal and deflection are recorded as `declined`, with "deflected" retained in the disclosure register's reason field. Silence at the deadline is `no-response`. Preserve a deflected reply as a received response, not as supplier silence. Independently established provenance is not erased because the supplier's own answer is incomplete.

Anonymised research responses use the same grading scale and are capped at E4, with no corroboration attribute. Corroboration against a named certification record is unavailable without attribution. Label them as anonymised wherever they are used. Assessment use is unaffected.

A deflected response can appear to answer the request. A validation confirms that a module computes an algorithm correctly; it says nothing about ancestry. Accepting "FIPS-validated, industry-standard implementations" as disclosure records an unknown as a favourable value and is the most common route to an understated layer 2.

© 2026 Steve Vaile and Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

Corroborate full responses against the module's published security policy. Where the supplier names an upstream and the policy states the same, record corroboration as a separate attribute; the evidence basis remains E4. Where the records conflict, retain the discrepancy and raise it for resolution. A CMVP certificate number alone is not lineage evidence; relevant content in its associated documentation may be.

Pre-send check. Complete this check before dispatch.

Pull the supplier's own records before sending. For every supplier in scope, retrieve the CMVP certificate entries, the published FIPS 140-3 security policy and any Entropy Source Validation records before dispatch. Corroboration then starts on day one rather than at the deadline, and a deflected answer is met with the supplier's own published material.

Cite relevant passages in follow-up questions where they genuinely identify the scoped component. Do not assume every public security policy names an upstream or that certification necessarily resolves the question.

5.1 Usable-disclosure response rate

For the stated request population and as-of date, the response rate is:

`(requests with a full or partial usable disclosure for Sections A to C) / (requests issued)`.

Count each scoped request once. Follow-up emails are not new denominator entries, and one response covering several products is not several responses unless the original population was explicitly defined at product-request level. Report numerator, denominator, pending requests and due dates. A supplementary due-request rate can be useful, but it must be labelled separately from the issued-request denominator.

The rate is not the percentage of assets with known ancestry. Report asset-weighted provenance coverage or unresolved reach separately when useful. Optional roadmap answers do not convert a provenance non-answer into a usable disclosure.

6. ESCALATION

Assessment use. Record non-response at the deadline as `no-response` and report it. Escalate to third-party risk where contractual information rights exist, and to procurement for suppliers in an active renewal or selection cycle. The assessment proceeds with its stated bounds and limitations. A refusal to disclose publicly may still be resolved through confidential technical assurance; that route remains distinct from an assumption of independence.

The disclosure response rate across all suppliers is a reported figure. It distinguishes an institution unable to reach CCF-3 because suppliers refused disclosure from one that did

© 2026 Steve Vaile and Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

not issue the requests. The figure therefore accompanies the conformance claim where disclosure requests were issued.

Research use. An attributed answer appears in a named row; an anonymised answer appears only in the aggregate figures. A supplier taking neither option is listed by name as a non-response. A supplier that declined and one that never replied are recorded distinctly, with neither characterised beyond the fact. Preserve incomplete and deflected replies, the factual-review correspondence and the basis for the published outcome.

7. MAINTAINING THE CONTROL

Add Sections A to C to the standard cryptographic supplier questionnaire at selection. Use the questions during renewal as well, not only during an incident or annual assessment. Maintain a stable link between supplier answers, the products actually deployed and the services they support. Review the record when a relevant version, module, manufacturing arrangement or generation design changes.

Add D2 to contracts through the institution's legal and procurement process: notification of change in implementation ancestry, firmware family, manufacturer or entropy design. Define which changes require notification, the lead time, the evidence format and the treatment of urgent security updates. Requiring provenance should not delay a necessary security patch; the control should permit emergency action followed by the required evidence and assessment update.

ANNEX 1 – PRODUCTS IN SCOPE

Institution completes: product, model, version, deployment context, and the important business services each supports.

ANNEX 2 – STRUCTURED RESPONSE TEMPLATE

Suppliers may answer in prose, and a structured response maps directly into the Applied Quantum CBOM Profile without interpretation error. One record per implementation:

```
{
  "product": "", "model": "", "version": "",
  "implementations": [{
    "algorithm": "", "upstreamProject": "", "upstreamVersion": "",
    "commitOrHash": "", "ownImplementation": false,
    "divergence": { "since": "", "primitives": [], "evidence": "" },
    "thirdPartySupplier": "", "certificate": ""
  }],
  "hardware": { "firmwareFamily": "", "sharedFamilyProducts": [],
```

© 2026 Steve Vaile and Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.

```
    "manufacturer": "", "otherBrands": [] },
  "keyGeneration": { "entropySourceDesign": "", "drbgSpecification": "",
    "esvCertificate": "", "generationDesign": "", "designSupplier": "" },
  "roadmap": { "upstreamChangePlanned24m": false, "changeNotificationCommitted": false }
}
```

RESOLVED AT V1.0-RC

Three questions carried from v0.9 review, closed August 2026.

1. Section D stays in the assessment request, marked optional and unscored in Section 4. The binding form belongs at selection and in contracts, per Section 7.
2. Research use offers anonymised aggregate publication as an explicit second tier across Sections 1, 3, 5 and 6: attributed disclosure preferred, anonymised responses used in aggregate and capped at E4, and a supplier taking neither recorded as a named non-response.
3. Supplier certification records are pulled before dispatch, per Section 5, so corroboration starts on day one and a deflected answer is met with the supplier's own published material.

© 2026 Steve Vaile and Marin Ivezic / Applied Quantum. Licensed under CC BY 4.0.