CERTLABZ CERTIFICATION BOARD

CPQS-001

Certified Post-Quantum Cryptography Specialist (CPQS)

Exam Objectives CPQS-001

About the exam

Item	Detail
Level	Advanced
Number of questions	120. A performance-based exam: each form can carry up to 5 to 12 performance-based questions alongside the multiple-choice questions.
Delivery model	Computer adaptive in 3 stages of 42, 39, 39 questions. Your score on each stage selects the difficulty of the next, so no two candidates sit the same paper.
Time limit	180 minutes
Scoring	You need a score of 700 out of 900 to pass. Results are reported on a scale of 100 to 900, and 700 corresponds to answering 72% of the exam correctly. Harder questions carry more weight, so a score means the same thing on any route. Multiple-response items and PBQs are scored all or nothing.
Delivery	Online, fully proctored (webcam, microphone and screen).
Prerequisites	No formal prerequisite. Candidates do best with two years in security or infrastructure work, working knowledge of TLS and PKI, and 50 to 80 hours of study.
Retakes	No waiting period after a failed first attempt. Candidates pay the exam price each time they attempt the exam. See the CertLabz Certification Retake Policy at certlabz.com/certification-retake-policy.html
Validity	3 years. Renew with 75 CEUs per cycle and the $55 annual continuing-education fee, or by passing the current exam.
Language	English
Exam voucher	$199 for one sitting, valid 12 months. Bundles add the study guide ebook and the All Access plan.

Domain weights

Domain	Questions

D1 Cryptographic Foundations and the Quantum Threat (15%)

	18
D2 Post-Quantum Algorithms and Standards (20%)	24
D3 Cryptographic Inventory and Risk Assessment (15%)	18
D4 Migration Planning and Crypto Agility (20%)	24
D5 Protocols and Implementation (18%)	22
D6 Governance, Compliance and Assurance (12%)	14
Total (100%)	**120**

Objectives by domain

Each objective may appear as knowledge, a scenario to judge, a circuit to trace or assemble, or a number to compute. Each form can carry up to 5 to 12 performance-based questions: drag-and-drop matching, sequencing and table completion, drawn fresh each attempt. The exam does not test any vendor's SDK syntax.

D1 Cryptographic Foundations and the Quantum Threat — 15% — 18 questions

D1.1 Symmetric and asymmetric primitives, hashes, MACs, KEMs and signatures
D1.2 Security levels, key sizes and the meaning of 128-bit security
D1.3 Shor against RSA, finite-field and elliptic-curve Diffie-Hellman
D1.4 Grover against symmetric keys and hashes, and why AES-256 holds
D1.5 Harvest-now-decrypt-later and the confidentiality lifetime of data
D1.6 Mosca's inequality: migration time, shelf life and the threat horizon

D2 Post-Quantum Algorithms and Standards — 20% — 24 questions

D2.1 FIPS 203 ML-KEM: parameter sets, key and ciphertext sizes, encaps and decaps
D2.2 FIPS 204 ML-DSA and FIPS 205 SLH-DSA: parameter sets, signature sizes and trade-offs
D2.3 FN-DSA (Falcon), HQC and the reasons for a backup KEM
D2.4 Stateful hash-based signatures: LMS and XMSS under SP 800-208
D2.5 Lattice, hash and code-based hardness assumptions in plain terms
D2.6 Implementation risk: side channels, implicit rejection, randomness and constant time

D3 Cryptographic Inventory and Risk Assessment — 15% — 18 questions

D3.1 Discovering cryptography in code, configuration, certificates, HSMs, firmware and third parties
D3.2 Cryptographic bills of materials and automated discovery tools
D3.3 Classifying assets by data shelf life, exposure and algorithm
D3.4 Risk scoring and prioritization of what to migrate first
D3.5 Dependencies on vendors, protocols and certificate authorities
D3.6 Maintaining the inventory as a living record

D4 Migration Planning and Crypto Agility — 20% — 24 questions

D4.1 Phased migration roadmaps and hybrid transition strategies
D4.2 Crypto agility in design: algorithm negotiation, configuration and abstraction
D4.3 Key management, rotation and HSM readiness for larger keys
D4.4 Testing, performance budgets and rollback plans
D4.5 Long-lived signatures, archives and re-signing strategies
D4.6 Vendor engagement, procurement language and supply-chain requirements

D5 Protocols and Implementation — 18% — 22 questions

D5.1 Hybrid key exchange in TLS 1.3 and its handshake cost
D5.2 SSH, IKEv2 and VPN migration
D5.3 X.509 certificates, PKI, certificate chains and composite signatures
D5.4 Code, firmware and document signing with post-quantum schemes
D5.5 Libraries, language runtimes and interoperability testing
D5.6 Messaging, secure boot and constrained devices

D6 Governance, Compliance and Assurance — 12% — 14 questions

D6.1 NIST IR 8547 deprecation and disallowance timelines
D6.2 CNSA 2.0, NSM-10 and OMB requirements for United States national systems and agencies
D6.3 FIPS 140-3, CAVP validation and what a validated module actually proves
D6.4 European and international roadmaps and sector regulation
D6.5 Policy, standards and metrics for a migration program
D6.6 QKD, QRNG and other claims a specialist must evaluate

Continuing education

Renewal	Requirement
Validity	3 years from the date of issue
CEUs required per cycle	75
Annual CE fee	$55
Alternative to CEUs	Pass the current version of the exam before the expiry date

Qualifying activities

Activity	CEUs
CertLabz labs, PBQs, courses and SkillTracker assessments	1 CEU per hour, up to 25 per cycle
Other industry certifications earned or renewed	10 to 25 each, depending on level
Conferences, webinars and training	1 CEU per hour, up to 20 per cycle
Cryptography or security work experience	3 per year, up to 9 per cycle
Teaching, mentoring, publishing or open-source contributions	Up to 15 per cycle
College courses in cryptography, mathematics, security or computing	10 per completed course

CertLabz Certification Retake Policy

- **No waiting period after a failed first attempt:** If you fail your first attempt at any CertLabz certification examination, CertLabz does not require any waiting period between the first and second attempt.
- **Once you pass, you cannot resit the same exam code:** A candidate who has passed an exam and achieved a certification cannot take that exam again under the same exam code without prior consent from CertLabz. You will need to wait until a new series of the exam is published before attempting to recertify by examination.
- **Beta examinations, one attempt only:** A CertLabz beta examination may be taken one time by each candidate.
- **Violations invalidate the attempt:** A test found to be in violation of this policy will be invalidated, and the candidate may be subject to a suspension period. Repeat violators will be permanently banned from the CertLabz Certification Program.
- **Every attempt is paid for:** Candidates must pay the exam price each time they attempt the exam. CertLabz does not offer free retests or discounts on retakes.

Published by the CertLabz Certification Board, a division of CertLabz LLC. Objectives document CPQS-001.
https://certlabz.com/certifications/certified-post-quantum-cryptography-specialist.html