Q-Shield proof report

Evidence for an auditor, not a certification.

EXAMPLE DATA. Alder Biosciences is a made-up company and no scan was run: its servers' answers were written by hand and judged by Q-Shield's own code. Signed with a demo key, not one of EpochCore's report keys.

Engagement: example-alder-2026-11-03
Generated at: 2026-11-07T16:40:11Z
Profile: mid_market

1. Signature check

Both signatures verified against the key file given: demo-keys-not-epochcore.json.

Ed25519, key 7B93DFD4897D6E1E: valid
ML-DSA-87, key 31EE547A2E8849B0: valid

2. Audit result

The audit failed against profile mid_market: 4 finding(s) fail its rules.

6 meet the rules, 4 fail, 8 are due (allowed today, migrate by a date), 0 are unknown.

Findings in this report: 23 (18 judged by the audit; 5 web server software checks get no verdict). Audit results: 18. The counts add up to 18, the number of judged findings.

6 of 9 readable key exchanges are post-quantum hybrid (what each server would pick); 0 unknown, not counted. (Audit field kex_coverage_pct: 66.7.)

Audit result recorded: failed

Policy basis (profile mid_market)

NIST IR 8547 (final, October 2026): RSA and ECC deprecated after 2030, disallowed after 2035

Digest

SHA-256 of the RFC 8785 canonical report without its signatures field.

`24d63c61afbff6e75f175c4a59aca0444afe94308f07227464dea17946ddb89c`

Signature keys

```
SHA-256 of that key file: 7377570a0b5bf6bb9bf8ce8f7df26745f420d6f4b59b7fc3d40587566b5de0cc
Ed25519   key id 7B93DFD4897D6E1E
ML-DSA-87   key id 31EE547A2E8849B0
```

EpochCore publishes its public keys at epochcoreqcs.com/qshield-keys. This report does not fetch them: compare the key ids and the SHA-256 above with that page.

ML-DSA signing randomness: random bytes from the signer's computer only; no IBM job recorded.

That is the signer's own statement, inside the signed report. It cannot be checked from the signature.

The two signatures cover the digest above, which is computed from the report file. Checking them (steps in the appendix) shows that the digest was signed by the private keys matching the public keys above. To check that a report file has this digest, run `node src/cli.mjs verify <report file>` from the Q-Shield prove/ folder, or compute SHA-256 over its RFC 8785 canonical form without the signatures field. It says nothing about hosts that were not scanned.

Findings and audit verdicts

Each key-exchange result shows the group the server would select for a modern client; the probe does not complete a handshake. Unknown means the probe failed: it is never counted as safe or exposed. Verdicts are the audit's, for profile mid_market; due means allowed today, migrate by a date. Recorded exposure says what the finding's hndl_exposed and quantum_vulnerable fields record; the probe's own reason text is not printed; it is in the signed report file.

Asset	Check	Observed	Traffic exposed	Audit verdict	Recorded exposure
www.alder.example:443	tls_kex	X25519MLKEM768	no	meets the rule	Recorded traffic not exposed by this check. Algorithm not recorded as quantum-vulnerable.
www.alder.example:443	tls_cert	{"tls_version":"TLSv1.3","cipher":"TLS_AES_256_GCM_SHA384","cert_key":"EC-secp256r1","cert_signature_algorithm":"ecdsa-with-SHA256","rsa_key_transport":false,"not_after":"2027-01-29T08:15:42+00:00","issuer":"CN=Example Edge CA E1,O=Example Trust,C=US","issuer_key_id":"5a1b9c0e7d2f4a6b8c3d1e0f9a7b5c4d3e2f1a0b","distrusted_issuer":null}	no	due	Recorded traffic not exposed by this check. Certificate (key or signature) recorded as quantum-vulnerable.
www.alder.example:443	web_software	{"status":200,"server":"cloudflare","x_powered_by":null,"software":[],"known_exploited":[]}	not applicable	no verdict (no known-exploited match)	Names no software version. Not a quantum finding.
mail.alder.example:587	tls_kex	X25519	yes	fails	Recorded as exposed to harvest-now-decrypt-later. Algorithm recorded as quantum-vulnerable.
mail.alder.example:587	tls_cert	{"tls_version":"TLSv1.3","cipher":"TLS_AES_256_GCM_SHA384","cert_key":"RSA-2048","cert_signature_algorithm":"sha256WithRSAEncryption","rsa_key_transport":false,"not_after":"2027-02-14T23:59:59+00:00","starttls":"smtp","issuer":"CN=Example Issuing CA R3,O=Example Trust,C=US","issuer_key_id":"c47e2a9b1d0f8e6c5b4a3928170615f4e3d2c1b0","distrusted_issuer":null}	no	due	Recorded traffic not exposed by this check. Certificate (key or signature) recorded as quantum-vulnerable.
vpn.alder.example:443	tls_kex	X25519	yes	fails	Recorded as exposed to harvest-now-decrypt-later. Algorithm recorded as quantum-vulnerable.
vpn.alder.example:443	tls_cert	{"tls_version":"TLSv1.3","cipher":"TLS_AES_256_GCM_SHA384","cert_key":"EC-secp384r1","cert_signature_algorithm":"ecdsa-with-SHA384","rsa_key_transport":false,"not_after":"2027-03-02T12:00:00+00:00","issuer":"CN=Example Edge CA E1,O=Example Trust,C=US","issuer_key_id":"5a1b9c0e7d2f4a6b8c3d1e0f9a7b5c4d3e2f1a0b","distrusted_issuer":null}	no	due	Recorded traffic not exposed by this check. Certificate (key or signature) recorded as quantum-vulnerable.

EXAMPLE DATA, NOT A SCAN

Asset	Check	Observed	Traffic exposed	Audit verdict	Recorded exposure
vpn.alder.example:443	web_software	{"status":200,"server":null,"x_powered_by":null,"software":[],"known_exploited":[]}	not applicable	no verdict (no known-exploited match)	Names no software version. Not a quantum finding.
db.alder.example:5432	tls_kex	secp256r1	yes	fails	Recorded as exposed to harvest-now-decrypt-later. Algorithm recorded as quantum-vulnerable.
db.alder.example:5432	tls_cert	{"tls_version":"TLSv1.3","cipher":"TLS_AES_256_GCM_SHA384","cert_key":"RSA-2048","cert_signature_algorithm":"sha256WithRSAEncryption","rsa_key_transport":false,"not_after":"2027-05-20T23:59:59+00:00","starttls":"postgresql","issuer":"CN=Example Issuing CA R3,O=Example Trust,C=US","issuer_key_id":"c47e2a9b1d0f8e6c5b4a3928170615f4e3d2c1b0","distrusted_issuer":null}	no	due	Recorded traffic not exposed by this check. Certificate (key or signature) recorded as quantum-vulnerable.
git.alder.example:22	ssh_kex	mlkem768x25519-sha256	no	meets the rule	Recorded traffic not exposed by this check. Algorithm not recorded as quantum-vulnerable.
portal.alder.example:443	tls_kex	X25519MLKEM768	no	meets the rule	Recorded traffic not exposed by this check. Algorithm not recorded as quantum-vulnerable.
portal.alder.example:443	tls_cert	{"tls_version":"TLSv1.3","cipher":"TLS_AES_128_GCM_SHA256","cert_key":"RSA-2048","cert_signature_algorithm":"sha256WithRSAEncryption","rsa_key_transport":false,"not_after":"2027-04-11T23:59:59+00:00","issuer":"CN=Example Issuing CA R3,O=Example Trust,C=US","issuer_key_id":"c47e2a9b1d0f8e6c5b4a3928170615f4e3d2c1b0","distrusted_issuer":null}	no	due	Recorded traffic not exposed by this check. Certificate (key or signature) recorded as quantum-vulnerable.
portal.alder.example:443	web_software	{"status":200,"server":"nginx","x_powered_by":null,"software":[],"known_exploited":[]}	not applicable	no verdict (no known-exploited match)	Names no software version. Not a quantum finding.
intranet.alder.example:443	tls_kex	X25519MLKEM768	no	meets the rule	Recorded traffic not exposed by this check. Algorithm not recorded as quantum-vulnerable.

EXAMPLE DATA, NOT A SCAN

Asset	Check	Observed	Traffic exposed	Audit verdict	Recorded exposure
intranet.alder.example:443	tls_cert	{"tls_version":"TLSv1.3","cipher":"TLS_AES_256_GCM_SHA384","cert_key":"EC-secp256r1","cert_signature_algorithm":"ecdsa-with-SHA256","rsa_key_transport":false,"not_after":"2027-01-08T10:30:00+00:00","issuer":"CN=Example Edge CA E1,O=Example Trust,C=US","issuer_key_id":"5a1b9c0e7d2f4a6b8c3d1e0f9a7b5c4d3e2f1a0b","distrusted_issuer":null}	no	due	Recorded traffic not exposed by this check. Certificate (key or signature) recorded as quantum-vulnerable.
intranet.alder.example:443	web_software	{"status":200,"server":"Apache/2.4.49","x_powered_by":null,"software":[{"product":"Apache","version":"2.4.49","header":"server"}],"known_exploited":[{"product":"Apache HTTP Server","cve":"CVE-2021-41773","name":"path traversal and file disclosure","affected":[["2.4.49","2.4.49"]],"fixed":"2.4.50","kev_date_added":"2021-11-03","condition":"files outside the document root not protected by \"Require all denied\"","source":"https://httpd.apache.org/security/vulnerabilities_24.html#CVE-2021-41773","version":"2.4.49"},{"product":"Apache HTTP Server","cve":"CVE-2021-42013","name":"path traversal and remote code execution","affected":[["2.4.49","2.4.50"]],"fixed":"2.4.51","kev_date_added":"2021-11-03","condition":"files outside the document root not protected by \"Require all denied\"","source":"https://httpd.apache.org/security/vulnerabilities_24.html#CVE-2021-42013","version":"2.4.49"},{"product":"Apache HTTP Server","cve":"CVE-2024-38475","name":"mod_rewrite improper escaping of output","affected":[["2.4.0","2.4.59"]],"fixed":"2.4.60","kev_date_added":"2025-05-01","condition":"mod_rewrite rules whose substitution starts with a path on the server","source":"https://httpd.apache.org/security/vulnerabilities_24.html#CVE-2024-38475","version":"2.4.49"}]}	not applicable	fails	Announces Apache 2.4.49: a version in the range of CVE-2021-41773, CVE-2021-42013, CVE-2024-38475, on CISA's Known Exploited Vulnerabilities list. Not a quantum finding.
sso.alder.example:443	tls_kex	X25519MLKEM768	no	meets the rule	Recorded traffic not exposed by this check. Algorithm not recorded as quantum-vulnerable.

Asset	Check	Observed	Traffic exposed	Audit verdict	Recorded exposure
sso.alder.example:443	tls_cert	{"tls_version":"TLSv1.3","cipher":"TLS_AES_256_GCM_SHA384","cert_key":"EC-secp256r1","cert_signature_algorithm":"ecdsa-with-SHA256","rsa_key_transport":false,"not_after":"2027-02-27T09:00:00+00:00","issuer":"CN=Example Edge CA E1,O=Example Trust,C=US","issuer_key_id":"5a1b9c0e7d2f4a6b8c3d1e0f9a7b5c4d3e2f1a0b","distrusted_issuer":null}	no	due	Recorded traffic not exposed by this check. Certificate (key or signature) recorded as quantum-vulnerable.
sso.alder.example:443	web_software	{"status":200,"server":null,"x_powered_by":null,"software":[],"known_exploited":[]}	not applicable	no verdict (no known-exploited match)	Names no software version. Not a quantum finding.
api.alder.example:443	tls_kex	X25519MLKEM768	no	meets the rule	Recorded traffic not exposed by this check. Algorithm not recorded as quantum-vulnerable.
api.alder.example:443	tls_cert	{"tls_version":"TLSv1.3","cipher":"TLS_AES_128_GCM_SHA256","cert_key":"EC-secp256r1","cert_signature_algorithm":"ecdsa-with-SHA256","rsa_key_transport":false,"not_after":"2027-03-19T16:45:00+00:00","issuer":"CN=Example Edge CA E1,O=Example Trust,C=US","issuer_key_id":"5a1b9c0e7d2f4a6b8c3d1e0f9a7b5c4d3e2f1a0b","distrusted_issuer":null}	no	due	Recorded traffic not exposed by this check. Certificate (key or signature) recorded as quantum-vulnerable.
api.alder.example:443	web_software	{"status":200,"server":"nginx","x_powered_by":null,"software":[],"known_exploited":[]}	not applicable	no verdict (no known-exploited match)	Names no software version. Not a quantum finding.

Triage

Profile: mid market. Method: baseline score. Model: none.

Rank	Asset	Check	Why, and plan
1	intranet.alder.example:443	web_software	intranet wiki: announces Apache HTTP Server 2.4.49, in the range of known-exploited CVE-2021-41773, CVE-2021-42013, CVE-2024-38475 (CISA KEV); internal data kept 5 years. Target: Apache HTTP Server 2.4.60; deadline 2026-11-03 (on CISA's Known Exploited Vulnerabilities list: CVE-2021-41773 since 2021-11-03, CVE-2021-42013 since 2021-11-03, CVE-2024-38475 since 2025-05-01) Steps: 1. Upgrade Apache HTTP Server from 2.4.49: CVE-2021-41773 is fixed in 2.4.50; CVE-2021-42013 is fixed in 2.4.51; CVE-2024-38475 is fixed in 2.4.60 2. If it is a distribution build, check its changelog first: distributions often backport a fix without changing the version shown 3. Re-scan to confirm the version the server announces Front page: Server header: Apache/2.4.49, which names Apache HTTP Server.

EXAMPLE DATA, NOT A SCAN

Rank	Asset	Check	Why, and plan
2	db.alder.example:5432	tls_kex	clinical records (PostgreSQL): traffic recorded today is exposed; regulated data kept 25 years, still secret at 3 of 3 plausible quantum break years. Target: X25519MLKEM768; deadline 2027-11-03 (if a quantum break came as early as 2029, traffic recorded today would still need to be secret then; policy date: NIST IR 8547 (final, October 2026): quantum-vulnerable key establishment deprecated after 2030) Steps: 1. Enable X25519MLKEM768 on the TLS terminator (OpenSSL 3.5+, BoringSSL or Go 1.24+ builds) 2. Re-scan to confirm the negotiated group
3	mail.alder.example:587	tls_kex	mail (SMTP): traffic recorded today is exposed; confidential data kept 10 years, still secret at 3 of 3 plausible quantum break years. Target: X25519MLKEM768; deadline 2027-11-03 (if a quantum break came as early as 2029, traffic recorded today would still need to be secret then; policy date: NIST IR 8547 (final, October 2026): quantum-vulnerable key establishment deprecated after 2030) Steps: 1. Enable X25519MLKEM768 on the TLS terminator (OpenSSL 3.5+, BoringSSL or Go 1.24+ builds) 2. Re-scan to confirm the negotiated group
4	vpn.alder.example:443	tls_kex	remote access (VPN): traffic recorded today is exposed; confidential data kept 10 years, still secret at 3 of 3 plausible quantum break years. Target: X25519MLKEM768; deadline 2027-11-03 (if a quantum break came as early as 2029, traffic recorded today would still need to be secret then; policy date: NIST IR 8547 (final, October 2026): quantum-vulnerable key establishment deprecated after 2030) Steps: 1. Enable X25519MLKEM768 on the TLS terminator (OpenSSL 3.5+, BoringSSL or Go 1.24+ builds) 2. Re-scan to confirm the negotiated group Front page: no Server header in the front page's response.
5	api.alder.example:443	tls_cert	lab-results API: certificate can be forged once a quantum computer exists (not a risk to recorded traffic); regulated data kept 25 years. Target: ML-DSA-65; deadline 2035-12-31 (NIST IR 8547 (final, October 2026): RSA and ECC signatures disallowed after 2035) Steps: 1. Inventory which clients must accept a post-quantum certificate on this endpoint 2. The CA/Browser Forum's rules for publicly trusted certificates do not allow ML-DSA yet (its ML-DSA ballot was still in draft at the 2026-07-30 Server Certificate Working Group meeting, cabforum.org), and Chrome said on 2026-02-27 it has no immediate plan to trust post-quantum X.509 certificates (blog.google/security, 'Cultivating a robust and efficient quantum-safe HTTPS') 3. Move to an ML-DSA-65 certificate once a CA can issue it and those clients accept it; keep the classical one until then 4. Re-scan to confirm the certificate's key and signature Front page: Server header: nginx, which names nginx.
6	db.alder.example:5432	tls_cert	clinical records (PostgreSQL): certificate can be forged once a quantum computer exists (not a risk to recorded traffic); regulated data kept 25 years. Target: ML-DSA-65; deadline 2035-12-31 (NIST IR 8547 (final, October 2026): RSA and ECC signatures disallowed after 2035) Steps: 1. Inventory which clients must accept a post-quantum certificate on this endpoint 2. The CA/Browser Forum's rules for publicly trusted certificates do not allow ML-DSA yet (its ML-DSA ballot was still in draft at the 2026-07-30 Server Certificate Working Group meeting, cabforum.org), and Chrome said on 2026-02-27 it has no immediate plan to trust post-quantum X.509 certificates (blog.google/security, 'Cultivating a robust and efficient quantum-safe HTTPS') 3. Move to an ML-DSA-65 certificate once a CA can issue it and those clients accept it; keep the classical one until then 4. Re-scan to confirm the certificate's key and signature
7	mail.alder.example:587	tls_cert	mail (SMTP): certificate can be forged once a quantum computer exists (not a risk to recorded traffic); confidential data kept 10 years. Target: ML-DSA-65; deadline 2035-12-31 (NIST IR 8547 (final, October 2026): RSA and ECC signatures disallowed after 2035) Steps: 1. Inventory which clients must accept a post-quantum certificate on this endpoint 2. The CA/Browser Forum's rules for publicly trusted certificates do not allow ML-DSA yet (its ML-DSA ballot was still in draft at the 2026-07-30 Server Certificate Working Group meeting, cabforum.org), and Chrome said on 2026-02-27 it has no immediate plan to trust post-quantum X.509 certificates (blog.google/security, 'Cultivating a robust and efficient quantum-safe HTTPS') 3. Move to an ML-DSA-65 certificate once a CA can issue it and those clients accept it; keep the classical one until then 4. Re-scan to confirm the certificate's key and signature

EXAMPLE DATA, NOT A SCAN

Rank	Asset	Check	Why, and plan
8	portal.alder.example:443	tls_cert	partner portal: certificate can be forged once a quantum computer exists (not a risk to recorded traffic); confidential data kept 7 years. Target: ML-DSA-65; deadline 2035-12-31 (NIST IR 8547 (final, October 2026): RSA and ECC signatures disallowed after 2035) Steps: 1. Inventory which clients must accept a post-quantum certificate on this endpoint 2. The CA/Browser Forum's rules for publicly trusted certificates do not allow ML-DSA yet (its ML-DSA ballot was still in draft at the 2026-07-30 Server Certificate Working Group meeting, cabforum.org), and Chrome said on 2026-02-27 it has no immediate plan to trust post-quantum X.509 certificates (blog.google/security, 'Cultivating a robust and efficient quantum-safe HTTPS') 3. Move to an ML-DSA-65 certificate once a CA can issue it and those clients accept it; keep the classical one until then 4. Re-scan to confirm the certificate's key and signature Front page: Server header: nginx, which names nginx.
9	sso.alder.example:443	tls_cert	single sign-on: certificate can be forged once a quantum computer exists (not a risk to recorded traffic); confidential data kept 7 years. Target: ML-DSA-65; deadline 2035-12-31 (NIST IR 8547 (final, October 2026): RSA and ECC signatures disallowed after 2035) Steps: 1. Inventory which clients must accept a post-quantum certificate on this endpoint 2. The CA/Browser Forum's rules for publicly trusted certificates do not allow ML-DSA yet (its ML-DSA ballot was still in draft at the 2026-07-30 Server Certificate Working Group meeting, cabforum.org), and Chrome said on 2026-02-27 it has no immediate plan to trust post-quantum X.509 certificates (blog.google/security, 'Cultivating a robust and efficient quantum-safe HTTPS') 3. Move to an ML-DSA-65 certificate once a CA can issue it and those clients accept it; keep the classical one until then 4. Re-scan to confirm the certificate's key and signature Front page: no Server header in the front page's response.
10	vpn.alder.example:443	tls_cert	remote access (VPN): certificate can be forged once a quantum computer exists (not a risk to recorded traffic); confidential data kept 10 years. Target: ML-DSA-65; deadline 2035-12-31 (NIST IR 8547 (final, October 2026): RSA and ECC signatures disallowed after 2035) Steps: 1. Inventory which clients must accept a post-quantum certificate on this endpoint 2. The CA/Browser Forum's rules for publicly trusted certificates do not allow ML-DSA yet (its ML-DSA ballot was still in draft at the 2026-07-30 Server Certificate Working Group meeting, cabforum.org), and Chrome said on 2026-02-27 it has no immediate plan to trust post-quantum X.509 certificates (blog.google/security, 'Cultivating a robust and efficient quantum-safe HTTPS') 3. Move to an ML-DSA-65 certificate once a CA can issue it and those clients accept it; keep the classical one until then 4. Re-scan to confirm the certificate's key and signature Front page: no Server header in the front page's response.
11	intranet.alder.example:443	tls_cert	intranet wiki: certificate can be forged once a quantum computer exists (not a risk to recorded traffic); internal data kept 5 years. Target: ML-DSA-65; deadline 2035-12-31 (NIST IR 8547 (final, October 2026): RSA and ECC signatures disallowed after 2035) Steps: 1. Inventory which clients must accept a post-quantum certificate on this endpoint 2. The CA/Browser Forum's rules for publicly trusted certificates do not allow ML-DSA yet (its ML-DSA ballot was still in draft at the 2026-07-30 Server Certificate Working Group meeting, cabforum.org), and Chrome said on 2026-02-27 it has no immediate plan to trust post-quantum X.509 certificates (blog.google/security, 'Cultivating a robust and efficient quantum-safe HTTPS') 3. Move to an ML-DSA-65 certificate once a CA can issue it and those clients accept it; keep the classical one until then 4. Re-scan to confirm the certificate's key and signature Front page: Server header: Apache/2.4.49, which names Apache HTTP Server.

Rank	Asset	Check	Why, and plan
12	www.alder.example:443	tls_cert	public website: certificate can be forged once a quantum computer exists (not a risk to recorded traffic); public data kept 1 year. Target: ML-DSA-65; deadline 2035-12-31 (NIST IR 8547 (final, October 2026): RSA and ECC signatures disallowed after 2035) Steps: 1. This host's front page names Cloudflare in its Server header (Server header: cloudflare). If Cloudflare's edge terminates TLS here, the certificate visitors see is the one on Cloudflare's edge, and Cloudflare lists post-quantum signatures for visitors as planned via Merkle Tree Certificates (developers.cloudflare.com/ssl/post-quantum-cryptography/pqc-cloudflare-products, read 2026-11-03) 2. The CA/Browser Forum's rules for publicly trusted certificates do not allow ML-DSA yet (its ML-DSA ballot was still in draft at the 2026-07-30 Server Certificate Working Group meeting, cabforum.org), and Chrome said on 2026-02-27 it has no immediate plan to trust post-quantum X.509 certificates (blog.google/security, 'Cultivating a robust and efficient quantum-safe HTTPS') 3. No certificate you could install today changes this: keep the classical certificate and re-scan when Cloudflare offers post-quantum authentication to visitors Front page: Server header: cloudflare, which names Cloudflare.

6 finding(s) were not ranked: the plan lists no step for them.

Symmetric ciphers (Grover's search, on paper)

Grover's search is the quantum attack on symmetric keys. It is a note, not part of the score or the rank. The sentence is the PDF's own, built from the recorded fields; the report's own note text is in the signed report file.

Asset	Cipher suite	Hash	Logical qubits	AES-256 (CNSA 2.0)	Recorded
www.alder.example:443	TLS_AES_256_GCM_SHA384	SHA-384	6681	yes	AES-256: 128 bits against Grover's search on paper.
mail.alder.example:587	TLS_AES_256_GCM_SHA384	SHA-384	6681	yes	AES-256: 128 bits against Grover's search on paper.
vpn.alder.example:443	TLS_AES_256_GCM_SHA384	SHA-384	6681	yes	AES-256: 128 bits against Grover's search on paper.
db.alder.example:5432	TLS_AES_256_GCM_SHA384	SHA-384	6681	yes	AES-256: 128 bits against Grover's search on paper.
portal.alder.example:443	TLS_AES_128_GCM_SHA256	SHA-256	2953	no	AES-128: 64 bits against Grover's search on paper.
intranet.alder.example:443	TLS_AES_256_GCM_SHA384	SHA-384	6681	yes	AES-256: 128 bits against Grover's search on paper.
sso.alder.example:443	TLS_AES_256_GCM_SHA384	SHA-384	6681	yes	AES-256: 128 bits against Grover's search on paper.
api.alder.example:443	TLS_AES_128_GCM_SHA256	SHA-256	2953	no	AES-128: 64 bits against Grover's search on paper.

Migrations

not in this report

Appendix: check the signatures without Q-Shield

What you need: a terminal (bash or zsh) and OpenSSL 3.5 or newer. Check with: openssl version

macOS ships LibreSSL, which cannot do this: install OpenSSL 3.5 or newer and use that one.

1. Open a terminal in an empty folder. Paste each block below, one at a time and in order. Each file is made by one block; the longer signature files by several blocks marked "part 1 of N".

digest (SHA-256 of the RFC 8785 canonical report without "signatures"):
24d63c61afbff6e75f175c4a59aca0444afe94308f07227464dea17946ddb89c
message.bin is "qshield-proof-report-v1:" followed by that digest.

message.bin (88 bytes)

```
printf '%s' 'qshield-proof-report-v1:24d63c61afbff6e75f175c4a59aca0444afe94308f07227464dea17946ddb89c' > message.bin
```


EXAMPLE DATA, NOT A SCAN

ed25519.pub.der (44 bytes)

```
cat > ed25519.pub.der.b64 <<'EOF'
MCowBQYDK2VwAyEAiS0DisQdj8H4jAawxOOMVx3ka9l5BEPbouUhnXdJ1rM=
EOF
openssl base64 -d -in ed25519.pub.der.b64 -out ed25519.pub.der
```

ed25519.sig (64 bytes)

```
cat > ed25519.sig.b64 <<'EOF'
GJjdYqcWbcz00fnboNM5ETAHT9fougXxsCuk2ORxvI/fybH4kbJA3uzlpGrjoWj5724ZKl62eADh
gmiappBVDQ==
EOF
openssl base64 -d -in ed25519.sig.b64 -out ed25519.sig
```

ml-dsa-87.pub.der (2614 bytes), part 1 of 2

```
cat > ml-dsa-87.pub.der.b64 <<'EOF'
MIIKMjALBglghkgBZQMEAxMDggohADthAMCeJygtjT4rtXiHu/Fzfmmb6pnFz4V0jyYfQxsDG9Sm
GbIsCfK6SuHSd4dVH7yRS2aixCJyyCuBQueV4vpkLfzv3y5pOkR+nhPOMmh5gBOIR/Psviye4L32
nMWaopnhcqL6MSsMTQDonbRGioKHDReDTxMNywf23CEdwn+7KPiv1MeREzwUGYi0sL9RS7y7Rpkm
g0NOOhYa8pi0dx/pghxKwkCdCDWoZdfzsV9C5d1tI2AzfcaxL4dUsZmEzRKezPQ97zpzFYlEf9L+
TTPL9Ir9ooQkDpby3l1gmHlkkwwEXN+hXHUt9rId41yGfMpwkp4a43IhG2bTehGK05txHYtLqDgI
OHosh4XRuNodGEpiNJbvKfjXWnoS6FBQhwmdCkCycXYZX+3RIdMfomOsjRw9kGTjgo4PeRc8yXhX
awac9NJ4E/LOydd5IBE2A40uAcIpnTYJ5PzdFWhHwOkJOEYG6saH4Jl6CySxFwb4sWMFaL9JReol
U0r6s04NzMrFH0b5G8mkZtIO13d/+kZXqJSvjDxN++opZtiJtbKH44xxa3rq9AtoSBDPmw+5hujv
ctgmHnL9XvF/rw0ln4i7M767HbfN25Z5czgsS4Jjmb/DMZvl9r4POS3qsN8njJQ7TOK4sVPNhDPY
4oGn9xCPPqiqzUEfEwyrD+ppNftSAqggT22P/JOcwqcljHmAakAg3OfdTE6TIMzcpjD9vD7nznwK
flTEN+nHfkHf9oy0twhSbK9u5vicDFzFww2/64BovFCImEY4TFI/fh8w6niWZvNMf3yhcFTXXY4K
LrmTCIsrq8Z5zsATXrun49TYIrmMU+WQb0haX/t7qu/tqiqgfT1Axi223aI4y8bLi59s22pkN+Cr
ZA6DQUxbaJNP0RkGkKOsbfDJ0pTAUsaWfIwnBrUInHCRqqu/ohuBQYB4mS+QpyFYdqm2o/2Y0EWj
0h3+S4MGcZNzUuDMKap7uj7j9/Nb71OrB283zn8JhFcXrUKAcGJykBaxbRyoLX4uOT3q5Z431mOT
ubyhzXCCLBOkEUuG6GWYHpCcLrcjuV9DbCrT+CNkE35A64LznfTX2VAgIXQIbtP+I7/NqSVnAjSl
WgljBwVq9QdK1gxHmpTRUuNLuCaCQRGjFRAeVMPTQV1+J9iDal0tIjYmuO2e/M7j6Z/VIT4YTTdl
qEScXrcEShDRH5RBxOOefCw0ds8OO59lfwcJF60XWHbkASrPPcpUzq6H6B5uNH87z+FuNkk0Hw4z
fYY4HcM8Xj1oxns4nSRrOVptueiKklgogub5gd2q9RVgQi1hEIWBRqfDcj0IAA3+ipNgo19L25U2
DaujkjOla2y/Pc/6yy3JzW4xOyk8etEF70oEoST4W692lkiUMBUvGGl78RXMoNutTQ6Jz5hT7dkq
sLuVQbeDlxsmdtjOe1SJfE9oOVogD0LJ+qJANmZ4dBYgmLmjxYh+4shYSpmQwSTARA72/xBGd5NR
gHlu+owZyEibRm2qR4hbrwp7rpQixnNamRleRGN1v/k9Fg+DjdnEt4kLCOfIeYXMoghH7ONe2+en
2/l1sEj8b5hDCruqIHg/txoNkySCsPa5Ed8psDP2Kv8w4/1o/P/AR4jRo8OWpC1pmaaM+dFF1k/3
r10cbIbobavKoubwaoyYtv/B/xUKGPmFFZGS0VtveTirXOTdye+DKBMHKjtozxFnm/xvMgqnE6wF
C7Zs9/dwr/jrvvjBEsVlxcU1PNQ8E+k2dYyAVyHsWLQRt0Y6aHNyxRbRU+St876nH8Apti4GvpfF
6QtNR4xrZ5zcI3iwCWC5gRYQMVKhroetUHTjSx4OjN1TUM55LI7B87HlRst9Ihkku805sGgMeA09
UuUiGCzG12QSpodbrEGFcVoBxRIcgQ6Oz+WNLwjguQ4D7VK/R3gzFVseIcrQ1OC76LAg+HByYGZe
Dmv7t7k1KYHpe3nXDoAqADxRNvPuLXAg8j82qj5feU+rsuu3V7rWbzEDO+BqprfG3oRmFfGI3Gqi
YlDxvjooQjNDI89fao0P1+WKrPwfvFdWsy12JBOmZNPOo7cOJ9DXDVrffG8PPaFhR09R4SZ/5P4b
PqGrQS0Prh9kxBpf0rvzyXzT1c0rCLDqDgUQqSz6FDWty5twkEUXKRfTkXuonoyog4aZBAvgwrG9
/dOr1yP8Nw1H5xxxhGtq/85McH3WOOnzufO0WS3Wiz1zVRr4VUPSNkPVF4tK4zZ87ZozDY+5TbAf
sMDaix9bKqYqfVRkwIwrZYfEdKwfcG3dyld8XSRcGwUPlcNQ4ihs130JdZ8og2e9g3MIbZ35k1if
lmxMQ4nRh/MsdMg6i/vavHi7aCIYG9Y+d1guebWRHGKmv0KC3xw/i41n62QbWa5AUgcbNsaQmXOQ
Nigkbu8inVeJDZsccanEmjDfZNh2aXxFmlW7U7wPc55fMUY9Sd1mf4VBFvtcO3bcn5uUKcRTdAbr
laCuXUpdoGREmFaFLtp3Udwm0IBWg0SubxVlsQdovXgsX3BH/FtJOrukdQMw3uApDcSAOZEBp8ie
xcqTbh1MYEdinDmgg/3qXQ8/TUQ5vPnVWr8aLwuGtw9n2CKM9xg1pRdC2uJsQcX/oLIKdiD9+faH
EEnw6yfD3YWDouumrGnpR6/2jnNhzQnUQFpq+G9T3KBjq76YD2pWbYv93/kXadtZykYcg/xo3cIC
DIS3RW0i37iL1jiVzWaeM4ke1lGWqCXfz1LxRIFVq1GkGh6jKx8TPlFRu6ZaiVIwE79LttMofLLS
3tKiazecNl1ZsWb5UkoYToiwtdwLMOWIYYz+o1oePx+Bn2+zBqPf8yybt2tFMoZiH4+ryZ9U/Na1
WlgXM1SBlhPEshsmjXXQAatEEzt/yQu5NjN9BgZL8MxjriBeEm3rY9RDpd3Io88j4M59areh1LjN
GhlmHihwV1527vRJXRVH+GUBsmSmR/ordtjp/irictZnxv6WzUHNdR5YHNVOHH+gkH7mO4htY1Kq
EOF
```

ml-dsa-87.pub.der (2614 bytes), part 2 of 2

```
cat >> ml-dsa-87.pub.der.b64 <<'EOF'
pAlVwK+0IdA5PBukF1UalaR1pCvy0Uej+FpOuBkb7akioEknKzwLGAt5LKORSwRv/DPGR+5oX7da
QvjFMVvgQm4PZrJ+DnrUihp8K0LONNDIWbdfZHXaMwftenh+iA1mlbQwOw1Tj6DQM19YksqaXDmm
lHiagimQM8pTAa1Y8/0vBemAAXtSe9+D6E5IPUf6fWGUkkpLuAkwWH1ez2loLjtIyu/mku4EhP7b
6OpcU5M5cKK3evCrHMm06ppetKmATdMRkwgMkbs7jPiyjqnxwIIV8x74Zj+YPLU2XqvlaQr4SWVV
nmyRj2BEqSpTcq8qIhPzyccVICJQEqG2fmnfiU2sG5JSz/cK42HeOI6l8MAURQAtSPiy2vQPTAEL
czU24PHFImADwjrINxYHuxPBenqymjc3aDjOirwnjBtPSZFCD5y+p77BycfqWv7fgg==
EOF
openssl base64 -d -in ml-dsa-87.pub.der.b64 -out ml-dsa-87.pub.der
```

ml-dsa-87.sig (4627 bytes), part 1 of 3

```
cat > ml-dsa-87.sig.b64 <<'EOF'
eg16xh83l6Tvh/hKiM7sg147VZU0mUZ3iJenVaJxP00uKGMCD4MvW/psaDd+JeUoLi3PQn3lQbwk
Q1EEoxkBTkiB8sFgI0bP/ry63MkTDcVIIxYnSsw7nEpTGeeDZtkNNNH6XNrNsed95QQZEZjGMhFd
JvjQxQb1UFZcMwLzp7XJExj6brs3bzS8+uYv/OTMQOIKoSYSsdHRZT+8+5xU9XVR6Y7ywtABsQOA
fODpinO9Rry85rxHfZgNN2w5+m0hbrSk3rrBPfgKald85hVMJv5SIaKXpW23MCBrIiehrUNYpDA2
R2Ut5gnCeXSw+JXWLDt059Bf+ciHtiVZfzfIoWlYi5XVA5tg6GvNcIRsFPFVyjM5EY1egSX0eihH
EfR4LWGvgzD0yBh4Jdnxbg+gow5itQqbdLAdFL0Xp1Q9Ux7pea0HkZncFLd4x9qMi859lGH2OEeU
n2dY5j7cuzXLLJfkI5qhEADEQpL71WZjLdFGv4E+rrAi7D2A3B7jmYKVd0NQjAOmvO6rzMHAO3S/
ypBTMjhGBhbFpzNnHZ2DDVf2UnupL81FRKDg21XTeTsUQWe6wDZomNPrFMRxQKES+xPqk0cdT7oE
z2obM/vQg/3lAYM+MOVMUTEtG48nbk0KYf1sCYvzJ7AcYLwKKP4B7fI4xL/acdrnbxk2T0aWFVy2
zbHGnw3SzWwqPn8R0t08BzU1lxJH+XA8gK1Ls9uEQiIqdYc59UMxx6gkVLhvepJ2yztgpmQZJpAE
cxqzU1khsEE4BtMsKZNvGaYab9Y6Dzm0T3KtqjswJ/stBniCostr5m0iI7r+dkOJ9t/eP/bG595u
NGeX8lVlERzgv1xIZ0L2h5L7lTnLOSHoB2OwIMfPWxNJigXz55US8hOqwHH9G/TCF8G1UA2800cT
ZIVaDF1FiEmpagVO4Z67I7vIGi6HDmCuQoi7DkTX/3I56CRAXHmI57F+mK/FKbw4QK93ymvT4XuR
37HgXSZSCfRxLO19pcNOBcIJ0kaAq7KDq6kBGXTIopwdobH5EMeSqSbfHwhGb3fn2M3lmm7kFm7q
d8cEH7fhAb6JBPPnUeE8+Ry0PbDsZG+Rzwjx5wh8u59lnqtMFCZpoKmhQUIXKH/KBme1Iougb7Cb
qvIC3fTkjCTwTGJeFDXnmEMUM1IhEQa1lF6vz5jLszIfkS5HBqRPc5o1nK2E9rYlrzKtzDbcC4dC
KK3LwJY+BPhMbuhKaRjnP3jlrlilossYjB9Fe1G/iwo9NSdWB8/zpeSBKwISdTyKth001Qsf458P
7spRwrisarv1JlUU3XSvVDBJmM+dT0qfHqLn/pYF8AIpganGHT3nOo/wPPpV3W64R3tZYIW1zDxx
dZbd9UiZei6ShMTQXkkuRHcbZITxjM1s9pvoIBzQOIQYfRORgJkFdnTCCKa6WinIHD213ohOZXXG
OQhkr7BKP4/kMLH1B9kBZU0WkVhadkMhYVnTOkm7bcbGHuakHyx8+dYGvAwdvttfU40X7oSLmk7e
fnalPgpi8YUSIxMx7qrVbNf+3FUzgzptDOpYdOkF5BtUr5lRvVW1UAjZwbinR0St3ZUXMwauqjut
XpGk66RUI4X48mvxim1R1NxiRWajd1Sy3JcDJZuHhQMl8jJAmxqE+BTg3j2+oJNwweZp5tjHb9or
mICCVdN3Z3ZG9fVvNIg/ykWLU/2D1G8QGHi8N0HTs1Ondp5Wl+KsrBOndHJUfVd/ZQzyHoaLvQoY
TGt3BwAu9vZFXxMec9WfODzHEcyyH8ybqGuUZuD7S7Xnc1/gVp2GWeFsWbXnjO0h1JWdf8Fvqony
1sYzwXOjAyMTeXYtJ1MSryqYV/O+xffCoHXewAruN+nWQeDtTnF/IqGXCvYey42ydCavSFv4FMzr
X7oi0BZkTYTKqsUjighO6XaiGHYgGoFczB5kUPqE4Twty5bg115TnzC27CjN/5di1kCNOdMByDqq
Iz/332oB8R4lCwj+po93kCGpcCTzXI4zHVEdcOYqJDmLvvGxC7ifuhM3Fg3pLEmOmeEGCJp57Iuz
soW022jH1vDK5sx6O8kcfqDQaNsQC17uMuU3z/RhqO90bC7zltv9upKnjN2QAYrYBMhUGhj3Xi6I
6Ulf9jBN297Plf56NbBMhy/Cg0+rowtGGbEzzydpGV+TCYCbBogEPs0HgYGnaafD59pdqUUM+rAV
vZJ7Xuug/jjB+x028e2Rpq0eoiY6EL7I25sxE+VewF8l69NBHJkEDYe4137/qmg6eVpjV8zrztC/
BqUZk0luVAg6juNSdXTg2LtvaU6gLIibhDXV936BKzyidxojfw/CWK10y/5dwxmZ6hcUxIIt14HT
X0G+SIDDiWiIZLiwtIMeK7ti3NAcCDex6ZHo2YONBV73U/VvsczvLwsARLc+o0QVB1AzG0Vtrwn6
Y5QqPPBQnwjK6O91WHmRicTCWDFuo2LGBT+6j719VT3SWNcSPmqSutIX/J+b16ydIhTq1btOzJs6
7ymNH3sXEv9LcviFvtiCq5BLVCHHWA1rArqj61D93i+am2XYIdqdMg6GAtI12u85SSPj6iGefwd8
thd1O7U3HfVt1SivXKl/rPlp0+IGqwMO87EXV6waipLEB9zx8armfl2fsmXxPvDFtZej05zsQNFd
3LRaqKSKHaSV1XBS1tSjvwV+lbcqVDH+A/tbRW6CA5N+0vtFBSx+4J7jEJrRQcN8LI8GAEYC+UkC
2jhu+8hW28mQ2/rCxP/48VUDWT8tun73u0syvZI653S9b05PnCzBF0cGr83O2tTMvTODDu5GSeZK
KCNYUtco5eJXr4wBmOGhqJLfq5A7omH0syElAE1AAALpBC+FWmd/GHi4iJed9vxta5CkK/JXWprX
BtSBbqtt7EELjBFp+G5skXoSZnrIuLUUXZN571Zm07xupuSj+aX3o+/3ATvn2RrlKkaOiuc7DsYE
WHsw3HSBin/TDWdC2So/n4s+eCGYcaBAlwNXLEmWJaQtGeM6GdhHjMQwZcts2x4F8jaK7RccMZiD
EOF
```


EXAMPLE DATA, NOT A SCAN

ml-dsa-87.sig (4627 bytes), part 2 of 3

```
cat >> ml-dsa-87.sig.b64 <<'EOF'
itqr2GbKE1Fh5MN6pxzgOtxE10lWWVtfPCgXqdkfeU1tgrP3LgFS4yJqfI2zZM+TNeqAw2/4BItB
DO48qDbm3JodX+INpV+JphjA44Q/7Ha696nx3W3CPsNZBHe10OwAePv4M4t+kjCj77HeSZMY4dBe
0XqZV88CH8rIlx0rEpd1xfnqBDR4Mpkub77TddiMObJc6O9wEMZH5ZZn3nhy6NgD18m0pHs5UK1R
ox4VlD6636E/siX812eGGlqh3ExmeKusFuzSZynDNeQjNOpS/92mGCyBRCMxgnJGwp2S3vVxnxax
EV7taoJcDUEyQzuVd+hZ15Qfzkawhj17X1M1QTP4bRGAxTZLPjXzUhYZkelfnYfcGVYJjjUxuXDB
IRR2kYxHjGlfMD2PnRTg/Z8jr9rPNHC4QZi3BJhLv/xumsKOyk6ukUtNuVXPOo5lJ5Lit89YZC2U
aOXUwoePZGDr40NLpEaiIZo76pc1RU34CDvMrge51bLRu7YSRECHlTkN/OnMW5LHVSNLZTKq0cjK
lTRLMz/hGDuQuQGE9Gd2XKIAvnOd6vtJmxMRuwmjQiIi6482PS4Bk/0TF1Ex3UKHfnWJduNAiDMW
zW0oAP8LQTENakcfN1rSNt7rD/95DElpHMmvrEebvFFM7fO++04AbynAzSOERGHIYSQY/2Rk7oPM
jzHILcYd2Kw3cAzRETBeGDbFjdLAvbQhMMqERcJXAU8PKh9OpL69ajzWD6eII1/2TrRc1RM60F5K
n8W6lpTDOTz0jEqxVuiha94tsFv+NEam7C7FNwa2HMCMZ2czFutygsuOBClVgYxtqaK6uAOnCOMg
Zu2c/lKt3hkqmP+5g1sb+CtkCJrFof30HdPpzkqlOAPXkDcfoGzxJ6TOitkmkOikqzmrgnYliODX
6f6EbxplZHEFJsYBjpT1/NPWyfaCRilhy5LBW9uStiYOpFkM5BxpG4IQPHrrzzlXpFGUVzgvtQ6I
Y0NDak323oh+hTeWwyc7kB73XO5wH0yBD7RnyhcMnL1IgiljRfFJ+ndFRL9GdM1DbQR20Obs2NX8
yrjzl9euSYskDNUhvH+cmff41OYzYaKA0vBTcETcwcIJUJKsR8ioo140prFGvNFy5j7VJGPJP5yE
gBGxUcMuYI0gr9VOEZBtnAw5zUskepDIzz8/1E/g6xDQLUrE6lKxSMz7jJORGyS/6oKhCpfHcSst
NZNhuaQ0GQBDGHfeQXowcwP2AqE76aBMN9jo93wTmsAoWkWjjrNbixMbttiblZCv4kamOhxg9KNA
20lrM4wocMCrtanZe17abU2YJxLmvmU8A8zq83qH4y00U18D7ZA6820cJoxG+4QkcI3TFPPk5BCK
y28KoUI7u8pcAnhvbY4AsF0ZdZqUe00In76Wq2sakepuQ+6MBDAxp7Lh3iIRNTe5feyisn5T7ItL
/+TZHlYUOueDT3Kth8NXoqcVQsVlMwrRpE6LTs9RWG9/ydEvhR4Y/I1fgO7Tc2klAUCS6imjX4gY
vBgAyutJ7gapqIYnnTfZ2JLgFJ5ZFEMrxWidmpelR5k/oBg7mm/gaxF862+DHSBji/GN3T5vF8LP
1PDdzM1HM1rVkJVQDk8FDOqdFczIo/7hHVs0Ag9trYnpCzQoQoJHyWCHXon3gCzzfjRqOZZbq/0s
BSM0RPGxQipUo8vsgelHe4u4vbkyN2bOLMKWNDhzrUsC5Ma+BLJDN6ZgxkBo5S7MHh2LWayFuv04
72cdNXLzcruPvNUIlIjugrbqs9fb/Xyd2TQvildQ0g/g0DWBzTOmXyMMAgtzNYlcH1igRs/t3R+6
PtOFlMC5k5Bo6V7aeydH1nhxPILNPJJIOeH0vcj11zbQ4v1t95mUbwbCsejhdTc73NSKN1n6SGKV
BoGzQ//TYYprBt7grz7Gn0fDtoarAS6VyCMjb2U+vkN2UMyIIrZfguMfuS0NgIocXJp0Q9ymE/2m
s0Mbughbk5Fvji8NEgfqx+PcBn5ataFAIIgRDDrj3v48pNzHtnEe38H5vWiBuwGy+oiBhfjlC77o
90jFZgYDU3Dws/OFUFigPrNa1Cz5O07Xaawzu5EaL+bAX9pI1+WxQ7R6bu6bugKG0UZ+ME4rq1rQ
aD2Ch0gLrPS5VkSyFkd7q0rQqeGWvRAz2z0YjGRx/wRpLPYU2EwBPdlkWR4JCWBk1MtV4lgbeiJQ
SjZaH/ZAlkKN+ykW2BeA3mEy9cj8tWeE/clkILFKcrW0x4fN4wDO2jLEg1bb77ifuf9+qiLqNBiZ
BTibf+WvkAqZevwVKOCamz1lehEQR7YHabpUK1EdbR3dmA+StW3SHGPKH7vTRdNhkDAg6DhTxkH6
4/sDgpGIgYc3Mer+ERCGfNBfHfFXOMIgR4lPH6Qo+bi+JOwpaQOlb9je37uEJM3KjR5H2TJHRW/c
ELxIxeUyejrsC8v/kQGveQ+hyB224UjVopbTwSh7zyq2G4bqF53h9+MfCcCByKHody+q5En1ET9B
70EwUWKT+X8p18nlXNSwOScP3f7jf5QYMSh131lKK08Lkv4Inv5wz0NXSDRGPxLFxdbuhTOncXIz
VIp8TjtoN+oy80DxJdQIruhGeKA7TodbiVXfRvCiVfBhAojDYzueTqEawtilQjL/nhnoH9pkoAXl
HJvruznlKuBSmuo7KWfFqHnENg7wXMa5aWnVGNidQPj5DpwSrW15U5eQ7SiVdFK/21mB55B0AI1v
9p0ZZadmACETXDAeMblIs3lGEX0QAMAbRjlRXlKm4BVTJqIHtK/bg2QWyTjxNmUYV9WHVYxnQahd
lMpSNz8dJlAx4mRqprQeHl5RPMc7biJzfmxtse/HQ7l8K03m8Z2r1EIR8hR1vPLK3rNollDNrErk
Qonb4a3JmFw5FEmu4UD5VEgYGsHLBp/rfoHAl4m+FUsaMpjvmhi8aNuCvwb9o/nrWEMFP5Qx8yUd
LLRi9F2uabUjYdGgM93UJMOBpru6AyeRLCrIlq2+/ZcPpqwN6Swv1R8TI1N1sbTKH3mquubx/Qkv
EOF
```

ml-dsa-87.sig (4627 bytes), part 3 of 3

```
cat >> ml-dsa-87.sig.b64 <<'EOF'
NFZylKWyxQU0SEt5e7AKm6rE2AtEi56j2eEkhusoQmVzfZGqy/kAAAAAAAAAAAAAAAAAAAAAAAA
AAAHDhceIyotNg==
EOF
openssl base64 -d -in ml-dsa-87.sig.b64 -out ml-dsa-87.sig
```

2. Check that each file has the size shown above (a pasting mistake changes it):

```
wc -c message.bin ed25519.pub.der ed25519.sig ml-dsa-87.pub.der ml-dsa-87.sig
```

Expected byte counts: 88 message.bin, 44 ed25519.pub.der, 64 ed25519.sig, 2614 ml-dsa-87.pub.der, 4627 ml-dsa-87.sig

3. Run in this folder; each line must print "Signature Verified Successfully":

```
openssl pkeyutl -verify -pubin -keyform DER -inkey ed25519.pub.der -rawin -in message.bin -sigfile ed25519.sig
openssl pkeyutl -verify -pubin -keyform DER -inkey ml-dsa-87.pub.der -rawin -in message.bin -sigfile ml-dsa-87.sig
```

4. Compare the key ids printed on page 1 with the keys EpochCore publishes at epochcoreqcs.com/qshield-keys