ARCHIVED SAMPLE — NOT A LIVE MEASUREMENT · For format preview only. Live signed attestations ($5.00 USDC via x402) contain a fresh scan and live Ed25519 JWS signatures.

Quantum Aether · Post-Quantum TLS Attestation

Auditor-Ready Transport Evidence Bundle (NIS2 / DORA Supporting Observation)

Attestation ID: `qa_att_archived_sample`
Issued (UTC): 2026-11-03T08:58:57Z
Receipt JTI: `qa_rcpt_archived_sample`

Grade B · FAIL **github.com:443**

Post-Quantum Key Exchange: NO (Classical Only) | **Negotiated Group:** `x25519` | **TLS:** `TLSv1.3`

1. Observed Transport & Endpoints

Public IP	Family	TLS Version	Key Exchange Group	Status
20.26.156.215	-	TLSv1.3	x25519	observed_classical

2. Certificate & Cryptographic Fingerprints

Subject / Issuer	github.com / Sectigo Limited
Public Key	ECDSA-256 (secp256r1)
Validity & Chain	Valid: True · Chain valid: None · Hostname match: None · Expires: 2027-01-27T23:59:59+00:00 (85d)
Leaf SHA-256	-
SPKI SHA-256	-
Legacy TLS (≤1.1)	None

3. CycloneDX 1.6 Cryptographic Bill of Materials (CBOM Summary)

Serial: `urn:uuid:9d497eae-cb1e-4857-b5e8-b72827d4c1dc` · Full CycloneDX 1.6 JSON included in the machine-readable bundle.

Ref	Asset Name	Type	Quantum Security Level
`protocol-tls`	TLSv1.3	protocol	-
`kx-x25519`	X25519	algorithm	NIST Level 0
`cipher-tls_aes_128_gcm_sha256`	TLS_AES_128_GCM_SHA256	algorithm	NIST Level 1
`cert-key`	ECDSA-256	algorithm	NIST Level 0
`certificate`	github.com	certificate	-

4. Methodology & Explicit Measurement Limits

Vantage & Probe: Single external vantage point (eu-central), public HTTPS port 443. Active TLS 1.3 ClientHello offering hybrid post-quantum group X25519MLKEM768 (ML-KEM, FIPS 203). A single HelloRetryRequest is answered as modern browsers do; only a failed retry is recorded as undetermined.

- External observation from one vantage point at issued_at; CDN routing, time, or IP family can change results.
- Port 443 public endpoint only; may not reflect an origin server behind a CDN or TLS-terminating proxy.
- Measures transport key exchange and leaf certificate posture only; does NOT assess application security, HSTS, or internal infrastructure.

- Supporting measurement evidence (e.g. NIS2 Art. 21 / DORA Art. 9 transport controls), NOT a legal compliance certification or cryptographic audit.

5. Offline Cryptographic Verification (Ed25519 JWS)

JWKS Endpoint	`https://ather-quantum.com/.well-known/jwks.json` (Ed25519 / EdDSA, RFC 7515)
Policy Document	`https://ather-quantum.com/policies/qa-pqc-transport/1.0`
CLI Verification	`python3 tools/qa_verify.py --receipt receipt.json --expect-host github.com:443 --jwks-url https://ather-quantum.com/.well-known/jwks.json`

```
SAMPLE_ONLY.NOT_A_LIVE_SIGNATURE.RUN_LIVE_ATTESTATION_FOR_REAL_ED25519_JWS
```

Issued by Quantum Aether (https://ather-quantum.com) at 2026-11-03T08:58:57Z. External technical observation only — not a legal compliance certification or full cryptographic audit. Verify the Ed25519 signatures offline against https://ather-quantum.com/.well-known/jwks.json and match the PDF SHA-256 digest in the signed JSON bundle.