MBQ

POST-QUANTUM SECURITY · ABU DHABI

Security that outlasts today's cryptography.

MBQ builds post-quantum security infrastructure for records and critical systems. Designed and built in Abu Dhabi, on published international standards.

4	18	100+	100,000
engines, built and tested	product families, from records to devices	products built and tested	test cases per product, with two independently written verifiers that must agree

THE PROBLEM

A signature has an expiry date.

Today's digital signatures rest on mathematics that quantum computers are expected to break. Under the transition plan of the US National Institute of Standards and Technology (NIST IR 8547), quantum-vulnerable public-key algorithms are deprecated after 2030 and disallowed after 2035.

A 25-year mortgage signed today runs to 2051. A title deed has no end date. Whoever can forge a signature later can produce a false record and date it to today.

HOW IT WORKS

Seal	Each record is signed with two post-quantum signatures from different mathematical families.
Log	The seal is entered in a witnessed, append-only log, so a later change or a backdated entry shows.
Check	Anyone who holds the issuer's public key can check a record offline, on their own machine. Your records never leave your environment.
Renew	As algorithms age, the protection is renewed under their successors. The original is never touched.

STANDARDS

FIPS 203	ML-KEM, key establishment
FIPS 204	ML-DSA, signatures on every sealed record
FIPS 205	SLH-DSA, the second signature, from a different mathematical family
IETF	The record format is published as an Internet-Draft, draft-alhemeiri-wathiqa-pqc-ers

THE ENGINES

Four engines, all built.

Core engine	Seal, log, check and renew, for whatever it protects.
Crypto-Agility	Applications take their algorithms from a sealed policy, and every use is recorded.
Sovereign PKI	A post-quantum certificate authority, with every certificate entered in a public log.
Legacy Tunnel	A hybrid post-quantum tunnel in front of a private-sector system that cannot itself be changed.

PRODUCTS

Records (Wathīqa)	Seals official records and renews their protection.
Lupibex	Firmware signing for long-lived devices.
Software Signing	Signed, logged software releases.
Time	Proof a record existed by a given moment.
Credentials	Credentials checkable offline.
Provenance	Where an image or file came from.

The full product guide is available on request.

Stated plainly. The software passes the official NIST test vectors for these standards. Independent laboratory testing of the algorithms is being arranged. The products are working software, built and tested on synthetic data.

Demonstrations by appointment.

It runs offline on a laptop and takes a few minutes.

hello@mbquantum.ae
mbquantum.ae
MBQ · company in formation · Abu Dhabi, United Arab Emirates
November 2026