



QShield 2.0 – The National Cryptographic Assessment & Assurance Framework

Know your cryptography. Govern your trust. Secure your future.

Every nation knows where its borders are. Almost nobody knows where every cryptographic key and algorithm actually lives, or whether it will survive the quantum era. NCAAF, built on QShield 2.0, is the sovereign platform that answers that question, and keeps answering it every day.

QShield 2.0 | Capability Layers

Discover

Every cryptographic asset, found automatically, across the entire estate

Assess

Every asset scored against quantum and classical risk, so priorities are clear

Assure

Continuous validation, not once a year, every day



QShield 2.0 | FIVE MODULES

Quantum Entropy

Pull randomness from physics to create keys that cannot be reversed-engineered, guessed, or replicated



Quantum Readiness Risk Assessment

Finds cryptographic assets, classifies exposure, prioritizes migration, and provides ongoing assurance



Quantum PKI

Issues certificates and manages identity to maintain security even as signing algorithms change



Quantum Vault

Securely stores keys, secrets, and long-lived confidential records protected against future decryption



AI Security

Provides cryptographic assurance for AI models, training pipelines, and autonomous agent identity



QShield 2.0 Module Details

1. Quantum Entropy

What it is: true random number generation from quantum physical processes, not a software algorithm pretending to be random.

Why a buyer needs it: every key is only as strong as the randomness that created it. Software-based randomness is a documented, well-known attack surface; predictable entropy produces keys that can eventually be guessed or reproduced. Auditors and regulators increasingly ask for certified true randomness specifically, not just "a random number generator" on a spec sheet.

2. Quantum Readiness Risk Assessment

What it is: automated discovery of every cryptographic asset, certificates, keys, algorithms, across an organisation's full estate, with each one scored for quantum and classical risk.

Why a buyer needs it: most organisations cannot currently produce an accurate inventory of where their own cryptography lives, especially inside legacy systems and third-party software. Before any migration deadline, a buyer needs to know what exists and what to fix first, not spend months on a manual audit that's out of date the day it finishes.

3. Quantum PKI

What it is: Certificate infrastructure that issues and manages certificates and digital identity, engineered to keep working as the signing algorithm now needs to move to post-quantum standards.

Why a buyer needs it: a full internal PKI rip-and-replace is expensive and operationally risky; it breaks trust chains and causes outages. A buyer needs an internal PKI that upgrades gradually, in place, rather than one that forces a system-wide cutover the day the algorithm changes.

4. Quantum Vault

What it is: hardware-anchored, secure custody for cryptographic keys and other long-lived confidential data.

Why a buyer needs it: secrets that must stay confidential for decades- state records, financial history, medical data is exactly the data most exposed to harvest now, decrypt-later attacks, where it's stolen encrypted today and decrypted once a quantum computer can do it. A buyer needs key custody that assumes today's protection has to outlast today's algorithms, not just this year's threat model.

5. AI Security

What it is: the same discovery, scoring, and continuous assurance model extended to AI models, training pipelines, and autonomous agents.

Why a buyer needs it: AI systems now hold sensitive data and make consequential decisions, often without the governance applied to traditional IT. A buyer adopting AI at scale needs one framework covering both classical and AI-era trust, rather than running two disconnected security programmes that don't talk to each other.

Who It's For



Government and Public sector



Defence and National Security



Critical Infrastructure



AI and technology providers



Banking and Financial Services

Without visibility, there is no governance.

Without governance, there is no trust.

Without trust, digital sovereignty cannot endure.

Industry Facts

Quantum computing is no longer just an emerging technology. Our latest Quantum Technology Monitor report shows that over 300 global companies are adopting it, fueling a multibillion-dollar market.

- Quantum Monitor, Mckinsey 2026

FAQ

What is QShield 2.0?

QNu Labs' advanced full-stack crypto-agile, sovereign post-quantum cryptography platform. It's the foundation every QNu framework runs on, built so algorithms can change as standards evolve without rebuilding what's above them.

How is QShield 2.0 different from QShield?

QShield was already QNu's cryptoagile foundation, entropy, PKI, and vault working together as one platform. What it didn't have was a way to turn that foundation into a national assurance capability, continuous discovery, risk scoring, and assurance across an entire estate. QShield 2.0 adds that layer. NCAAF is built on it and couldn't have existed on the original QShield alone.

What is the difference between QShield 2.0 and NCAAF?

QShield 2.0 is the platform. NCAAF is the sovereign framework built on top of it, giving a nation or enterprise one way to discover, assess, and assure its cryptographic posture.

How is this different from a quantum key management system (QKMS)?

A QKMS generates, stores, and rotates keys. QShield 2.0 and NCAAF cover the full picture: entropy, ongoing risk assessment, certificate and identity management, key custody, and AI security, on one platform.

Can this run fully on-premises or air-gapped for government and defence use?

Yes. Sovereign deployment, on-premises or air-gapped, is a core design principle, not an add-on.

What is crypto agility and why does it matter?

The ability to change a cryptographic algorithm without rebuilding what depends on it. Standards will keep changing as quantum computing advances; rebuilding the cryptography layer each time isn't realistic.

Who typically uses QShield 2.0 and NCAAF?

Government agencies, defence and national security bodies, critical infrastructure operators, banks, and technology providers who need a national cryptographic assurance framework they control themselves.

Accelerating World's Quantum-safe Future

Join the Quantum Revolution

Whether you're securing critical national infrastructure, protecting financial systems, or future-proofing enterprise networks – QNu Labs is your partner in quantum security.

India

USA

Australia

Global