

Becoming Quantum Ready

*Quantum won't break your future.
It will break your past. What ready means
today, and how to get there.*



BROUGHT TO YOU BY



Executive Summary

What it means today, who is exposed, and how a ministry gets there.

Every vendor has a quantum roadmap.
Few can say what ready means today.

What is changing. Quantum computers will break the maths behind most encryption: RSA and elliptic curves. That includes every login, digital signature, and sealed record relying on them. The fix exists. In August 2024 NIST published three post quantum standards. They are software updates for any server or phone. Hash-based systems are not affected, which becomes vital later.

Why it is urgent now. Encrypted data is being recorded today to be opened later. The part less discussed is that when the maths breaks, old signatures do not just become readable. They become disputable. A land title signed today must still prove itself in 2050. Records cannot be re-signed after the maths breaks. Only before.

Who is most exposed. In order: long-lived signed records like land titles and identity credentials; network traffic being recorded now, such as mobile money and tax filings; and core systems procured this year on old cryptography with fifteen-year lifespans.

The clock. The US requires post quantum key exchange on high value systems by end 2030 and signatures by end 2031. EU member states start national transitions by end 2026. A platform procured in 2026 will be in service on both dates. Africa's quantum investment was 10.7 million dollars in 2025 against 245 billion globally. Procurement choices will close that gap, not research budgets.

What ready means:

- Protect what must exist.
- Transmit less worth stealing.
- Say plainly what is not done yet.

What a ministry can do this year. Inventory what is signed and what is stored. Buy crypto-agile, so the algorithm can be swapped from one place without the vendor. Ask every vendor which layers are post-quantum today, and which are not.

As of October 2026, nobody can promise quantum safe. This report shows what ready looks like: what breaks, who is exposed, and what a ministry should ask before it signs.

The Lock · Quantum breaks the lock, not the seal.



Most encryption today rests on two mathematical problems: factoring large numbers (RSA) and elliptic curves, which sign most internet traffic. Both are hard for normal computers and easy for a large enough quantum computer. Shor's algorithm proved this in 1994. The physical machine does not exist at that scale yet, but the maths has been settled for thirty years.

Not everything breaks. Hash functions, the one-way fingerprints that seal records and chain ledgers, are weakened rather than broken. A quantum computer makes them cheaper to attack, not trivial. Doubling the hash length restores the security margin. This makes a tamper-evident ledger among the most quantum-durable assets in a government stack. Keep this in mind for page 8.

The fix is already published. In August 2024 NIST released three post quantum standards: FIPS 203 (ML-KEM) for exchanging keys, FIPS 204 (ML-DSA) for signatures, and FIPS 205 (SLH-DSA), a fallback signature scheme built on hashes if the first is ever compromised.

Three things about these standards matter to a buyer.

First, they are software. They require a server update, a phone update, or a firmware update on a key store. No new hardware or satellite links are required.

Second, they form the global reference. NIST standards become the default baseline for banks, browsers, and governments. Chrome, Cloudflare, and Apple already run ML-KEM in hybrid mode, pairing old and new algorithms.

Third, they come with an end date for legacy systems. NIST's draft transition plan **deprecates the weakest RSA and elliptic curve settings after 2030, and disallows all of them after 2035.**

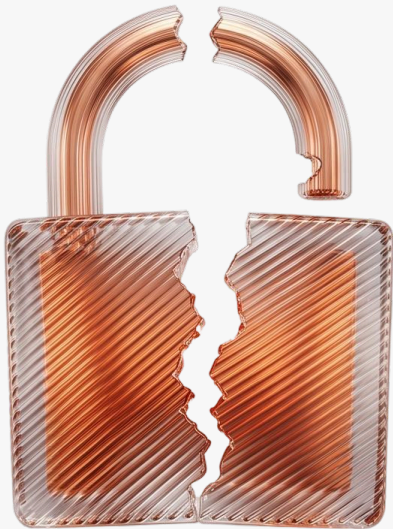
Quantum does not break the seal on a record. It breaks the lock on the key, and the pen that signed it.



"There is no need to wait for future standards."
— Dustin Moody, NIST, 13 Aug 2024

The Lock · Quantum breaks
the lock, not the seal.

Breaks



RSA

elliptic curves

Diffie-Hellman

logins, signatures, certificates

Replace: ML-KEM, ML-DSA.

Holds



hash functions

hash-chained ledgers

hash-based signatures

Keep, lengthen.

The Clock · The deadlines are set. The machine is not needed to meet them.

Nobody knows when a quantum computer large enough will arrive. Governments stopped waiting for that answer and set hard dates on the cryptography instead.

United States. Executive Order 14412, signed 22 June 2026, requires federal high-value systems to use post quantum key establishment by 31 December 2030 and post quantum signatures by 31 December 2031. NIST's draft transition plan goes further for everyone else: the weakest RSA and elliptic curve settings are deprecated after 2030, and all classical options are disallowed after 2035.

A smaller date, often misread. On 21 September 2026 NIST moved remaining FIPS 140-2 certificates to its historical list. This is not a post quantum deadline. It retires an older generation of cryptography certifications. Vendors citing 140-2 validation are offering a retired standard.

European Union. The Coordinated Implementation Roadmap asks member states to start national transitions by end 2026, move high-risk systems by 2030, and cover as many systems as feasible by 2035.

Africa. Investment is concentrated elsewhere. African quantum investment reached 10.7 million dollars in 2025, against 245 billion globally. Procurement decisions will determine how that gap is handled, not research budgets.

Read these dates against one more number. A national platform procured in 2026 typically has a working life of ten to fifteen years. It will be in active service on every date listed above.

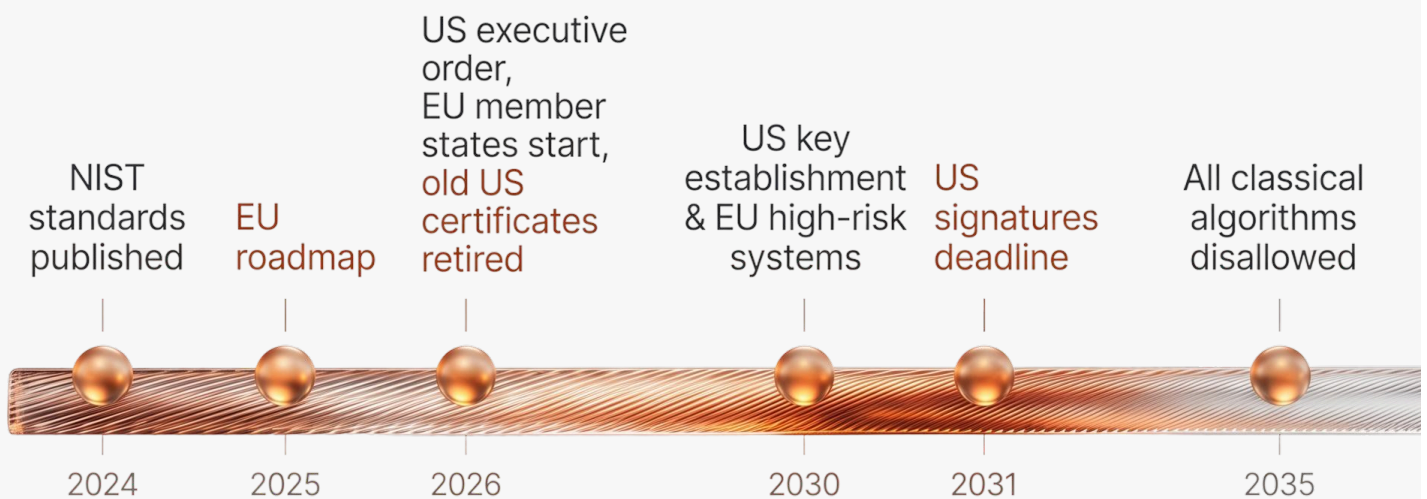
The question for a ministry is not whether a quantum computer arrives before 2035. It is whether a system bought this year can update its cryptography before then, and who holds the authority to make that change.

Quantum does not break the seal on a record. It breaks the lock on the key, and the pen that signed it.



Post-quantum key establishment by 31 December 2030. Post-quantum signatures by 31 December 2031.

The Clock · The deadlines are set. The machine is not needed to meet them.



A platform procured in 2026, still in service.

The Risk · Quantum won't break your future. It will break your past.

Quantum capability exposes governments in two distinct ways. The first gets most of the attention, but the second carries far greater long term impact.

Harvest now, decrypt later. An adversary does not need a quantum computer today to cause damage. They only need storage. Encrypted network traffic is intercepted today, stored, and held until a suitable machine can open it. Citizen identity files, tax records, medical histories, and diplomatic traffic are all targets. The exposure window opens the day the data moves over the wire, not the day the quantum computer turns on.

Forge later. A signature proves that a document came from an authorized source and remains unaltered. When the maths behind that signature breaks, the signature loses its binding power. Old signatures do not simply become readable. They become reproducible. Anyone with access to the computer can generate valid signatures under the ministry's identity for land titles, court orders, birth certificates, or software updates. Every historic record becomes disputable.

You cannot patch a broken historical signature after the fact. A document signed with compromised maths cannot be rescued by a software update. The only fix is re-signing it with post quantum algorithms while the classical maths still holds, preserving an unbroken chain of authority. That window is limited.

The three clocks. Calculate exposure by looking at three numbers together: how long the record must stay valid, how long system migration takes, and how long until a large quantum computer exists. If the first two numbers combined exceed the third, the record is already exposed. For a land title that must remain valid for fifty years, the record lifespan alone settles the question.

Registries do not need to predict when quantum computers will arrive. They need to know what they signed this year, and whether they can re-sign those records themselves.

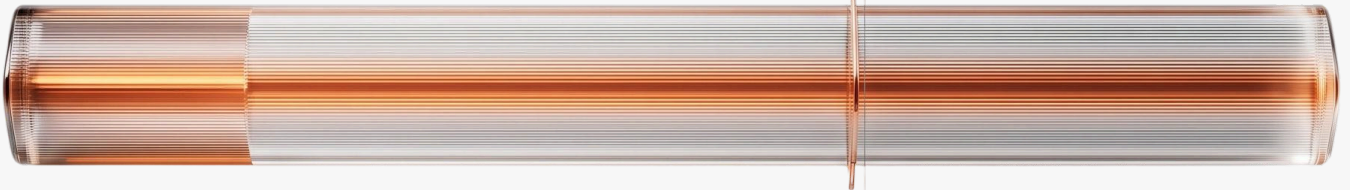


Old signatures do not become readable. They become reproducible.

The Risk · Quantum won't break your future. It will break your past.

Record life, 50 years
land title identity credential

After this point,
old signatures can
be reproduced.



Re-sign window

Algorithm life 2035

Who is Exposed · The longer a record must last, the sooner it is at risk.

Prioritize systems by how long data must stay valid, and how much traffic relies on legacy algorithms.

- 1. Long-lived signed records.** Land titles, civil status, identity credentials, court orders, and academic certificates. These records stay valid for decades. Signed once, they are expected to hold authority indefinitely. These represent the primary targets for signature reproduction. They require re-signing before legacy maths breaks, managed by a signing authority the state controls.
- 2. Traffic recorded today.** Mobile money, tax filings, healthcare data, and routine network communications. These are the primary targets for current data capture. Confidentiality requirements extend from several years to decades. Sub-Saharan Africa conducts a larger share of its economy over mobile money than any other region. Every transaction relies on signatures and encryption that face depreciation within ten years.
- 3. Systems procured this year.** A national system purchased in 2026 on classical cryptography, lacking a native migration mechanism, will remain in service long past the expiration of its underlying security. The procurement decision creates the exposure.

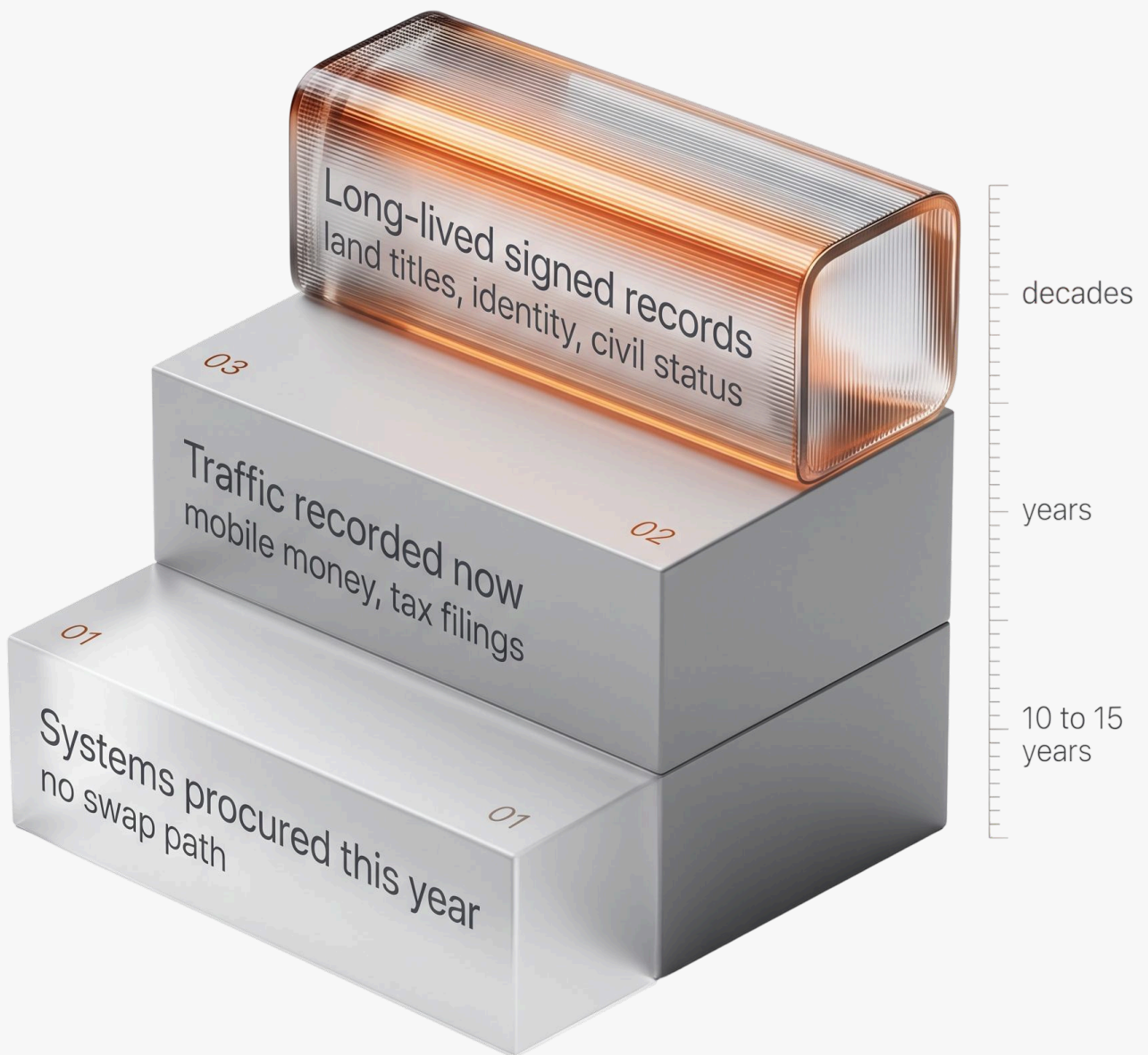
Africa faces three specific pressures. First, registries are undergoing active digitization today, meaning foundational digital signatures on land and identity records are being established right now. Second, mobile money operates as the primary banking network rather than an auxiliary service. Third, quantum funding sits elsewhere, with 10.7 million dollars allocated locally against 245 billion globally. The region will purchase its post quantum architecture from external suppliers. The central question is whether it buys software it can manage independently.

Bank regulators, land registries, and identity authorities share a common problem. They issue records that must hold legal weight in 2050, evaluated by people who were not alive when those records were created.



**Signed once. Trusted forever.
That is the problem.**

Who is Exposed · The longer a record must last, the sooner it is at risk.



Possible Features · Three ways a ministry can meet 2035.

Every government will arrive at 2035 through one of three operational approaches. Only one leaves the ministry in control of its data.

Path One: Wait for the vendor. Maintain current systems. Request a post quantum upgrade from the vendor as deadlines approach. The vendor dictates the price, schedule, and scope. Records signed during the waiting period rely on algorithms scheduled for deprecation. If the vendor shuts down or drops support, the path to an upgrade disappears.

Path Two: Add external protection later. Place a post quantum encryption layer in front of a classical system. Network transport gets wrapped, but the underlying signatures and stored records remain unchanged. This addresses current data interception without solving historic signature reproduction. Every added proxy adds complexity for future maintainers.

Path Three: Build crypto-agile software today. Decouple algorithm selection behind a clean interface. Keep signing keys in hardware the state controls. Run classical and post quantum algorithms together during transition periods, matching standard browser implementations. When NIST updates its standards, update system configuration rather than replacing the platform. Re-sign historic archives on a schedule set by the ministry, using keys the ministry holds.

Path three requires higher initial procurement focus, but lowers ongoing costs over time. It ensures that taking delivery of a system includes the tools required to keep it secure.

The unstated option is avoiding a decision entirely. That behaves exactly like path one, without explicit planning.



**Change the configuration,
not the platform.**

Possible Features · Three ways a ministry can meet 2035.

	Wait for the vendor	Bolt on later	Build crypto-agile
fixes harvest now	✗ No, wait and see	✗ No, too late	✓ Yes, immediate protection
fixes forge later	✗ No, leaves future risk	✓ Yes, eventually secures data	✓ Yes, secures from day one
who sets the date	✗ The vendor's roadmap	✓ Your integration team	✓ You control the timeline
who holds the keys	✗ Locked in by vendor	✗ Third-party or joint	✓ Full internal ownership
survives vendor exit	✗ No, high vendor dependency	✗ No, relies on system	✓ Yes, vendor agnostic

What ready looks like · Done, in transition, and the honesty to say which is which.

Quantum readiness applies to individual components, not complete platforms. Systems consist of application logic, credential issuance, key storage, data at rest, audit ledgers, and transport. Each layer either runs post quantum cryptography today, or it does not. A vendor who cannot detail readiness layer by layer is not prepared. A vendor claiming complete post quantum security is misleading you.

Protect what must exist. Keys, signatures, and long term archives require immediate priority. In AlphaX Identity and Registry services, post quantum algorithms run today across the application, credential, key management, and data at rest layers. Implementations use NIST standards: ML-KEM for key exchange, alongside ML-DSA and SLH-DSA for signatures. Keys reside in hardware security modules under client control, supported by managed rotation. Primitive algorithms sit behind an abstraction layer, allowing deployment without re-engineering core platform code. Future updates can occur through simple configuration changes.

Transmit less worth stealing. The effective countermeasure to data capture is avoiding data transmission. Zero knowledge proofs allow a system to verify specific attributes without taking custody of the underlying data, covering age, residency, statutory rights, or property ownership. Our identity and registry platforms verify claims rather than collecting raw records. Selective disclosure, pairwise identifiers, and local biometric matching limit centralized data accumulation.

Say plainly what is not done yet. Two layers of our stack remain in transition due to broader industry constraints. First, the ledger. Our rollup relies on Ethereum components, where base protocol cryptography is not yet post quantum. We align with the Ethereum Foundation's open post quantum roadmap, targeting Layer 1 upgrades by 2029 to replace validator signatures with hash-based schemes. Our chain layer inherits that upgrade path. The underlying hash-chained ledger history remains durable against quantum attacks today. Second, transport. Current deployments run standard TLS on network links. Post quantum hybrid TLS exists in broader software ecosystems, and we will enable it as sovereign customer networking environments stabilize. Payloads moving across those connections are already protected by application layer algorithms and zero knowledge design.

That defines readiness in October 2026. Four layers operational. Two named, dated, and undergoing migration.



L1 protocol upgrades could be completed by 2029, with full execution-layer migration taking additional years beyond that.

What ready looks like · Done, in transition, and the honesty to say which is which.

■ In production □ In transition

Application

Credential

Ledger (rollup)

Est. Q3 2026

Key management

Data at rest

Transport (TLS)

Est. Q4 2026

Disclosure

Four layers done. Two named, in transition.

Questions to ask any vendor .

If they cannot answer in one line, they are not ready.

Use these questions in any procurement conversation, including ours. Each warrants a clear, single-line answer. Extended explanations indicate technical gaps.

Readiness Questions

1. Which layers of your system run post quantum cryptography today? Name them explicitly.
2. Which layers do not? Name them, and state the target deployment date.
3. Which NIST algorithms do you run, and where? Specify ML-KEM, ML-DSA, SLH-DSA, or custom alternatives.
4. Who holds administrative control of the signing keys? The ministry, the vendor, or an external party?
5. When NIST updates its standard algorithms, what action is required on our side? A configuration edit, or a software rebuild?
6. Can we re-sign our document archive independently of your software? What tools are required, and how long does execution take?
7. How much citizen data moves across your networks unnecessarily? What attributes do you verify without transmitting raw records?
8. If our contract ends, what assets stay under ministry control?

Six concrete answers alongside two clear target dates show genuine progress. Complete claims of full readiness do not match reality in October 2026.



If you leave, what
leaves with you?

Records outlive algorithms . Handed over means upgradeable.

A land title signed this year must maintain its legal validity in 2050. The mathematical algorithm that signed it will be deprecated long before then. The record must outlast the maths.

That sums up digital sovereignty. A ministry that cannot update its cryptography does not control its records. It leases them.

Quantum readiness is an operational trait of a system, not a static certificate. Algorithms are declared in a central configuration, keys remain under state custody, archives can be re-signed on the state's schedule, and pending components are documented with dates.

Two actions every ministry can start this quarter:

- 1 Inventory
- 2 Mandate crypto-agile signatures.

We build national digital infrastructure and hand it over completely. Handed over means upgradeable by the owner. Otherwise, it is simply a lease.

Sovereignty is built, not declared.



A ministry that cannot change its own
cryptography does not own its records.
It rents them.

The Takeaway.

Start with an inventory. Sign the next record crypto-agile.

Nobody can promise quantum safe in October 2026, and nobody needs to. Two things are within any ministry's reach this quarter. List what is signed, what is stored, and how long each must stay valid. Then sign every new record with an algorithm chosen behind an interface, with keys in hardware the state controls. Old records can be re-signed in batches. New ones should stop adding to the pile. Everything else follows from those two.

