The records we are writing now

Version 0.1 · revised 4 September 2026 · this version as a PDF

> Drafted with AI assistance, then checked and revised by the author. The judgements and the errors are the author's.

Status of these claims

What this publication does not claim, and what is outstanding against it in the register.

Nothing outstanding in the register. Every claim in this publication has its evidence recorded, and no question against it is parked. That is a statement about this publication on the date shown above, generated from the register rather than asserted, and it will change when the register does.

Why post-quantum migration protects the future and abandons the past, and what closes the gap.

The half of the problem everyone is working on

Quantum computing will break the public key algorithms that secure most digital signatures. This is understood, it is on standards roadmaps, and New Zealand government guidance has carried it since January 2022: the Information Security Manual directs agencies to inventory their cryptographically protected assets and plan migration to post-quantum standards. Version 3.9 states plainly that quantum developments can undermine all widely used public key algorithms for digital signatures.

Every vendor will tell you they are migrating. Most of them will be telling the truth.

The half almost nobody is working on

Migration protects records signed **from the migration onward**. It does nothing whatever for records signed before it.

Those records do not become insecure. They become **forgeable** — and forgeable backwards. Once the algorithm that signed a 2026 record can be broken, anyone can produce a document that appears to have been signed by the same party, with the same key, saying something entirely different. There is no way to tell the genuine record from the fabricated one, because the property that distinguished them was the signature, and the signature no longer distinguishes anything.

The same manual notes this consequence in a single line that deserves considerably more attention than it has had: historical and archived data may be at risk.

Consider what that means for a record that has to last. A trust deed. A clinical note. A land or title record. A board minute. A whakapapa record. A consent given in 2026 and relied on in 2046. Each was signed to establish what it says and when it was written. After the transition, the signature establishes neither.

Why this cannot be fixed later

The obvious response is to re-sign everything with a stronger algorithm before the transition. For some records this works. For most it does not, and for the ones that matter most it never does.

Re-signing requires the authority of the original signer. The person who signed the 2026 consent may have died. The company may have been wound up. The board may have dissolved. The organisation may no longer hold the key, or may no longer exist. **A record you cannot re-sign is a record that becomes unprovable, and nothing about that moment announces itself.**

This is why it is a decision now rather than a decision later. It is the same shape as the argument about AI training: where the harm cannot be undone, remedies after the fact are decoration, and only a constraint applied beforehand does any work.

What actually survives the transition

Not the signature. The **timestamp** — provided it has two properties that are usually missing.

It must be issued by a party independent of the signer. An organisation attesting to the age of its own records has proved nothing to anyone. Independence is the entire source of a timestamp's evidentiary value, which is why timestamping is infrastructure rather than a feature.

There is a sharper version of this, and it is worth making against our own arrangements rather than someone else's. In most systems the signing key belongs to the *supplier*, not to the organisation whose record it is. What a third party can verify without the supplier's cooperation is therefore a supplier's signature. That retires the story *we wrote it last week and back-dated it*. It does not retire collusion: if supplier and organisation were both lying, the archive is worth their joint word. The timestamp is the part that holds regardless, because the authority is outside both of them.

The same asymmetry decides what survives the quantum transition. A signature whose independence rested on the supplier's honesty was always the weaker component. When the algorithm behind it breaks, it stops being a component at all.

It must be renewed before the algorithms beneath it weaken. A timestamp chain, re-anchored under fresh algorithms while the previous ones are still sound, carries evidentiary weight forward across the boundary. Each renewal attests to the validity of the chain beneath it at a time when that chain was still verifiable.

Done this way, a record does not break at the transition. Its evidentiary value accretes, and what would have been a fragile object — one that shatters, irreversibly — becomes something closer to a durable one that can be repaired.

What New Zealand is missing

A timestamp authority that is independent, durable across decades, and recognised in evidence here.

We do not have one. Organisations that timestamp at all use foreign authorities, which is better than nothing and carries an obvious question about what happens if that service withdraws or its jurisdiction changes. Organisations that timestamp their own records have a log, not evidence.

This is a small piece of infrastructure by any measure. It receives hashes and returns signed tokens; it holds no records and sees no content. The difficult parts are institutional rather than technical: key custody, a published renewal policy, continuity of the operator across a span longer than most institutions plan for, and standing in a New Zealand court.

And the mandate already exists. The Public Records Act 2005 mandates Archives New Zealand for the preservation of the digital record of government. More pointedly, its own Archives 2057 strategy states that in future it may not be necessary for all records of endur-

ing value to be transferred to the archive, and that technology will provide methods of assuring authenticity and trustworthiness of records whether archived or in current use.

Assuring the authenticity of a record held by someone else, by a custodian a relying party has no reason to trust, is exactly what an independent timestamp authority does. The strategy names the requirement. Nothing published names the mechanism.

What Archives NZ does publish on digital authenticity concerns format migration, emulation and checksums. Those address obsolescence and accidental corruption. A checksum tells you a file has not changed since you took the checksum; it tells you nothing about when the file was made, and nothing a third party can rely on. That is a different problem from the one described here, well solved, and orthogonal to it.

GCSB holds the cryptographic standards role. DIA holds the digital mandate. An existing mandate can be extended; a new institution need not be created.

What we are asking for, and what we are not

Asking: that someone with the standing to do it establishes this, and soon enough to matter for the records being written now. We would like to help design it and can prototype the requirement so that the property can be observed rather than argued about.

Not asking: to operate it. We are structurally disqualified and we say so plainly. A timestamp authority derives its whole value from independence of the parties relying on it, and an operator that timestamps its own records — or its customers' records, on its own authority — has recreated the problem it claimed to solve.

That disqualification is not modesty. It is the same principle that runs through everything else we have published: an assurance you cannot verify is not an assurance, and the party with an interest in the answer should not be the party providing it.

Sources: New Zealand Information Security Manual v3.5 (January 2022) and v3.9 (November 2025), nzism.gcsb.govt.nz; GCSB, gcsb.govt.nz. Retrieved 20 August 2026 — verify before citing.

Related: The supplier's signature sets out the record, integrity-check and attestation distinction in detail, including what the mechanism does not settle. The tokens described there come from an ordinary authority and are not qualified under eIDAS; what weight a New Zealand tribunal would give such a token is a question for a lawyer here, and this piece offers no opinion on it.

Published under CC BY 4.0. Applying or citing this does not imply endorsement of any conclusion drawn from it.

Cite this version

```
The records we are writing now, version 0.1 (September 2026).
agenticgovernance.digital/downloads/records-we-are-writing-now-v0-1.pdf
```

Licensed CC BY 4.0. Reuse is free, including commercially, provided the author is credited and the reuse does not suggest that the author endorses it. This link is frozen at version 0.1; /records-we-are-writing-now always shows the current one.

PREVIOUS
F · What it costs

Series contents

NEXT
H · Nine changes government could make