MOHAWK NATION
OF GRAND RIVER
SECRETARIAT

BOOK XXVI OF THE REGISTER'S BOOKS

The Developer and Auditor Book

The Register's records and data dictionary; its open interfaces; the Ledger checked from outside; the audit and the standards it follows.

One of the National Books of the Mohawk Nation of Grand River.

First edition · October 2026

The Developer and Auditor Book

Book XXVI of the Register’s books

Edition	First edition, October 2026
Mohawk Publication Number (MPN)	_____ — entered when the Register issues it
Published by	The Mohawk Nation of Grand River Secretariat · Grand River Territory, Ohsweken
To cite it	The Developer and Auditor Book, Mohawk Nation of Grand River Secretariat, 2026, and its MPN
Copyright	© Mohawk’s Printer for Grand River, 2026, for the Mohawk Nation of Grand River. Reproduction as the Nation’s law allows (Book XXXI)
Version and date	1.0 — 26 October 2026
Status	For publication. Rules marked “proposed” take effect only when adopted by Gazette
Classification	Public
Approved by	The Secretary-General, on publication; the approval entered in the Gazette
Changes	First edition. Each later change is listed here, with its version, date and Gazette entry
A genuine copy	Its SHA-256 fingerprint is listed in the Catalogue of the Register’s books, and on the Nation’s Ledger. A copy whose fingerprint differs is not the published edition
Written	In plain language, to ISO 24495-1. Generated from the Register’s own definitions, so it says what the Register does

CONTENTS

Contents

For developers and auditors 5

The records, and the data dictionary 7

Reading the Register 9

The Ledger, checked from outside 11

Changing the schema 13

Protecting the open interfaces 15

The audit, and how we compare 17

How we compare 18

Questions an expert or critic would ask 18

SECTION 1

For developers and auditors

What this book covers, and the rules that hold everywhere.

Interface names and fields marked “illustrative” show the form; the Register’s published schema is the authority.

Its colour: **Slate**

SCOPE

This book is for those who build on the Register, and for those who audit it. It describes the Register’s records, how they join, the interfaces through which they are read, the Ledger that makes them tamper-evident, and how an auditor checks all of it from outside, without trusting the Nation’s word.

Rule	Everywhere
One identifier	Every record has one Three-Block Record Code: FAMILY-YYMMDD-NNNNNN. No second scheme
Dates and times	ISO 8601; times in UTC
Names	In parts: first, middle, LAST
Fingerprints	SHA-256, over the record in canonical JSON (RFC 8785)
Tamper-evidence	Every record entered on the Ledger; each entry carries the fingerprint of the one before

SECTION 2

The records, and the data dictionary

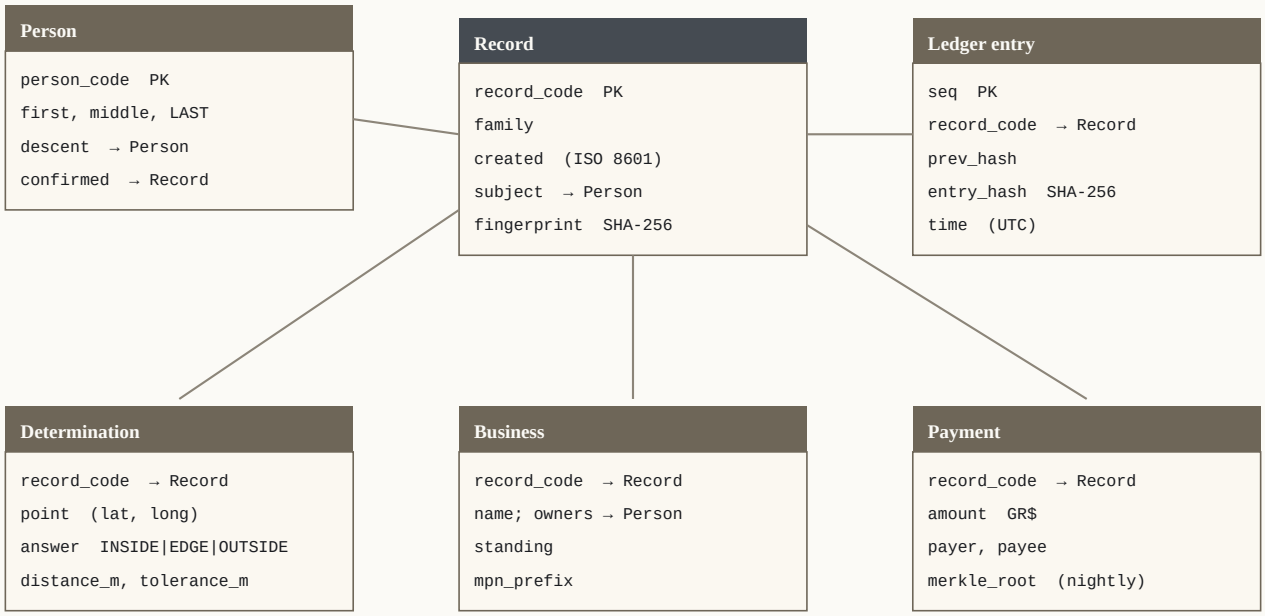
The core records, field by field.

Interface names and fields marked “illustrative” show the form; the Register’s published schema is the authority.

Its colour: **Slate**

DATA MODEL

How to read the drawing: each box is one kind of record, with its fields; “PK” marks the field that identifies it, and an arrow (→) a field that points to another record. Every record shares one Record, at the centre, and every Record is entered on the Ledger, on the right.



Every record has one Record Code, and every Record is entered on the Ledger. Illustrative; the published schema is the authority.

Field	Type	Meaning
record_code	string, 20 characters	FAMILY-YYMMDD-NNNNNN; unique; never reused
family	string, 6 characters	The kind of record, e.g. REG001, BUS001, MPN001
created	ISO 8601 date-time, UTC	When the record was made
fingerprint	hex, 64 characters	SHA-256 of the record in canonical JSON
first, middle, last	strings	A person’s name in its parts; LAST held in capitals
answer	INSIDE | EDGE | OUTSIDE	A determination’s answer for a place
distance_m, tolerance_m	decimal metres	The distance to the six-mile line, and the survey’s tolerance
standing	enumerated	A business’s or credential’s current standing
seq	integer	The Ledger entry’s place in the chain
prev_hash, entry_hash	hex, 64 characters	The fingerprint of the entry before; this entry’s own
merkle_root	hex, 64 characters	The root of the night’s payment tree, entered on the Ledger

SECTION 3

Reading the Register

The open interfaces, and what they return.

Interface names and fields marked “illustrative” show the form; the Register’s published schema is the authority.

Its colour: **Slate**

INTERFACES

Interface	Returns
/verify/ (page) — by Record Code or scan	A document’s current standing: genuine and in force, suspended, revoked, or unknown
/wp-json/mngr/v1/open/sixmiles	The Tract’s determinations: for a point, INSIDE, EDGE or OUTSIDE, with distance and tolerance
The Ledger, by sequence (illustrative)	Each entry: its sequence, Record Code, previous fingerprint and own fingerprint
The Nation’s public keys (illustrative)	The keys that sign documents and Ledger roots, for partners to pin

A worked call (illustration)	
Asked	The open six-miles interface, for a point near Ohsweken
Returned	answer: INSIDE; distance_m: 2140; tolerance_m: the survey standard’s; and the Record Code of the determination
Checked	The determination’s Record Code at /verify/; its entry on the Ledger

Standard	For
OpenAPI 3.1	Describing each interface
JSON Schema 2020-12	Describing each record
RFC 8785 (JSON Canonicalization Scheme)	Fingerprinting records the same way everywhere

SECTION 4

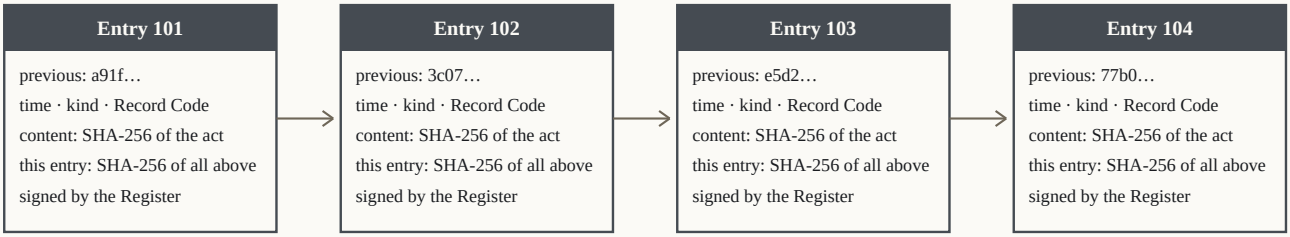
The Ledger, checked from outside

How an auditor proves the record has not been changed.

Its colour: **Slate**

THE LEDGER

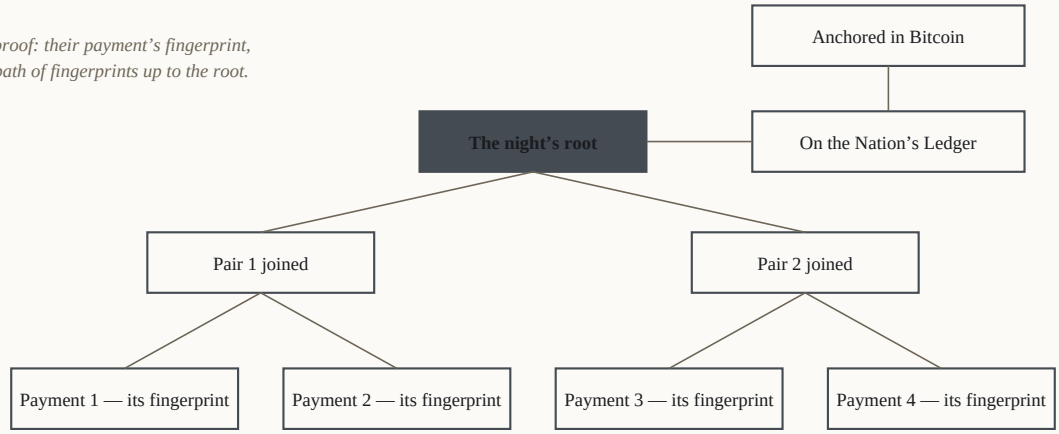
Read the drawing below left to right. Each box is an entry on the Ledger, and each carries the fingerprint of the one before it — so changing any entry breaks every entry after it.



Change one entry and its fingerprint changes — and so does every one after it. The daily anchor in Bitcoin fixes the latest.

Read the drawing below from the bottom up. Each payment of the night is a leaf; each pair is joined into one fingerprint above it, until a single root remains. The root is written on the Ledger, so a change to any payment would show.

A customer’s proof: their payment’s fingerprint, and the short path of fingerprints up to the root.



	Step
1	Take the Ledger’s entries in order, from the first or from a checkpoint the auditor trusts
2	For each entry, recompute the fingerprint from the previous fingerprint and the record’s own; it must match the entry
3	For a sample of records, recompute each record’s fingerprint from the record itself; it must match the Ledger
4	For a sample of nights, rebuild the payment tree from the payments; its root must match the Ledger
5	Report: entries checked, any mismatch by sequence number, and the sample drawn

RULE An auditor never needs the Nation’s word: every check is a recomputation from public data. A single mismatch is reported by its sequence number, and the Nation answers it in writing.

SECTION 5

Changing the schema

Versions, compatibility, and how a change is published.

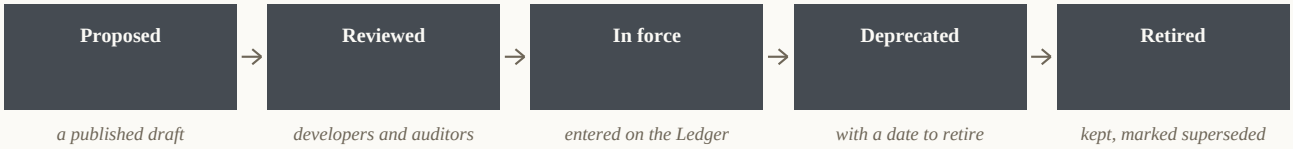
Interface names and fields marked “illustrative” show the form; the Register’s published schema is the authority.

Its colour: **Slate**

VERSIONS

The records will change as the Nation’s work does. A change must never break the past: every record already written stays valid, and keeps its fingerprint. So each change is numbered, published first, and entered on the Ledger when it takes effect.

How to read the diagram: follow a change left to right through its five stages — proposed in public, reviewed, in force, deprecated with a date, and retired but kept. Beneath each is who acts.



Change	Version number	What it means for existing records
Correcting a description	Patch: 1.2.0 → 1.2.1	Nothing: no record changes
A new, optional field	Minor: 1.2.1 → 1.3.0	Old records stay valid and unchanged
Removing a field, or changing what one means	Major: 1.3.0 → 2.0.0	A new version of that family; old records keep the old version, named in each

A worked change: adding a language field to a publication	Result
The proposal	Add “language” (en, moh, or both) to the publication record; optional
The number	A minor change: 1.2.1 → 1.3.0
Old records	Valid; fingerprints unchanged; the field is simply absent
New records	Carry the field, and name the schema version they were written under
The Ledger	Records the new schema’s own fingerprint on the day it takes effect

Standard	For
Semantic Versioning 2.0.0	Numbering a change so its effect is plain from the number
JSON Schema 2020-12	Describing each version of each record
OpenAPI 3.1	Describing each version of each interface

RULE A record is fingerprinted as it was written, under the schema version it names. A later schema never reaches back and changes it.

SECTION 6

Protecting the open interfaces

What guards them, and how to report a weakness.

Interface names and fields marked “illustrative” show the form; the Register’s published schema is the authority.

Its colour: **Slate**

SECURITY

The open interfaces are read-only and carry no personal records: they return standings, determinations and fingerprints, and nothing else. They are still guarded, because anything public is tried by someone.

Protection	How	Standard
Read-only	The open interfaces can read; they cannot write	—
Nothing personal	Only standings, fingerprints and determinations, never a person’s record (Book XIII)	Privacy by design
Rate limits	A caller that asks too often is told to wait: HTTP 429, with a Retry-After header	RFC 6585; RFC 9110
Encrypted in transit	TLS 1.2 or later on every interface	RFC 8446 (TLS 1.3)
Keys that can be pinned	Partners pin the Nation’s public keys and check signatures themselves	Book XXV
A short memory (proposed)	Requests counted; nothing identifying kept beyond 30 days	—

The OWASP API Security Top 10 (2023) — four of its risks	How the Register answers
Broken object-level authorization	Open interfaces return only what is public; private records are not reachable by them at all
Unrestricted resource consumption	Rate limits, and a cap on the size of every answer
Security misconfiguration	Reviewed every year, and after every change of version
Improper inventory management	Every interface is in the OpenAPI document; none is live without being listed

Anyone who finds a weakness can say so. The Nation publishes a security.txt file at /.well-known/security.txt, as RFC 9116 describes, saying where to send a report.

	Step
1	Send the report to the address in security.txt, with the interface, what was seen and how to see it again
2	The Nation acknowledges it within three days (proposed)
3	The Nation fixes it, or explains in writing why it will not, within 30 days (proposed)
4	The finder is credited, if they wish
5	A serious weakness, once fixed, is noted in the Gazette, so every partner knows

RULE Reporting a weakness in good faith is never treated as an attack. The Nation answers in writing, and says what it did.

SECTION 7

The audit, and how we compare

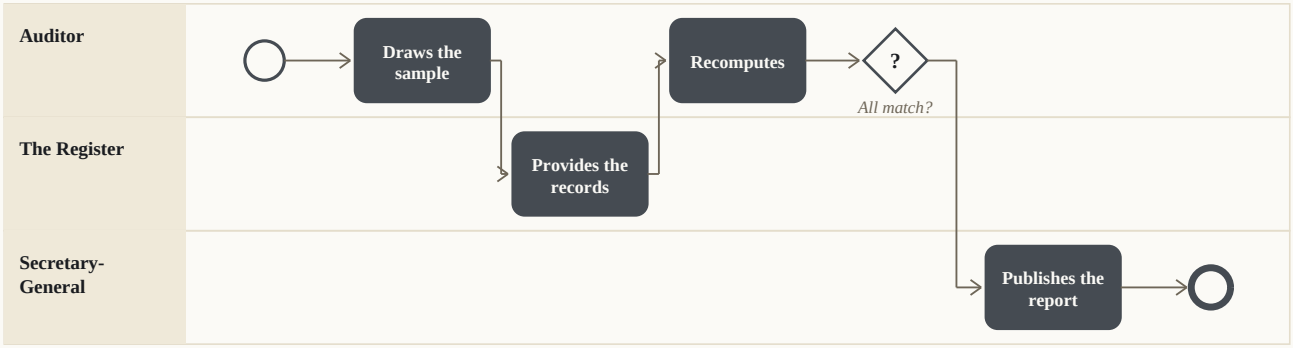
Who audits, how often, and against what.

The audit cycle is proposed: for the Nation to adopt by its Gazette.

Its colour: **Slate**

AUDIT

How to read the diagram: each row is one party — the auditor, the Register, and the Secretary-General. Follow an audit left to right; the diamond is the auditor's test: do the recomputed fingerprints all match?



Standard	For
ISO 19011:2018 — auditing management systems	How the audit is planned, sampled and reported
ISO/IEC 27001:2022	The security of the Register's systems
SOC 2 (Trust Services Criteria)	Security, availability and integrity, reported independently

How we compare

Benchmark	What they do	What the Nation does
Certificate Transparency (RFC 9162)	Public, append-only logs anyone can audit	The Ledger: append-only, checkable by recomputation
Estonia's KSI blockchain for state records	Each record's integrity proven by hash	Each record fingerprinted and chained
Open-data APIs of national registers	Published interfaces and schemas	Open interfaces, OpenAPI and JSON Schema

Questions an expert or critic would ask

Can the Nation rewrite its own Ledger?
Not without breaking every fingerprint after the change — which any auditor would find by recomputation.

What does the auditor see of people's private records?
Only fingerprints and the sample the audit needs, under the privacy rules of Book XIII.

How often is it audited?
Yearly by an independent auditor (proposed), and at any time by anyone through the public checks.

Is the schema fixed?
Changes are versioned, published and entered on the Ledger; old records keep their fingerprints.