

Open Bicycle Digital Identity (OBDI) Industry Specification

Version 0.3 — Pilot Draft

Author: Jacob Bayless

Status: Recommended open specification for implementation, testing, and public comment

Date: September 21, 2026

Prepared for: Municipalities, public agencies, land managers, manufacturers, and the broader e-bike ecosystem

Abstract

This specification defines an open, vendor-neutral method for associating a physical electric bicycle with a durable digital identity through Near Field Communication (NFC), a visually scannable code, and an authoritative web record. It is designed to support an achievable pilot using commercially available NFC stickers while remaining suitable for voluntary adoption by bicycle manufacturers, drive-system manufacturers, municipalities, public agencies, land managers, and other jurisdictions.

OBDI separates the identity of a bicycle from any particular regulatory classification, access policy, certification, or program. An OBDI-compatible tag identifies the bicycle; online services publish authoritative facts and current credentials associated with it. A single bicycle may have both a manufacturer-installed OBDI tag and one or more aftermarket program tags. All may resolve to the same canonical bicycle record and current eligibility information.

Version 0.3 intentionally defines a low-cost Minimum Viable Profile using commercially available NFC tags encoded with an HTTPS URI. It also reserves a path to manufacturer-installed, cryptographically authenticated tags without making advanced hardware a prerequisite for a pilot.

1. Purpose and scope

The Open Bicycle Digital Identity (OBDI) specification enables a person or field official to tap or scan a bicycle and retrieve an authoritative, privacy-preserving record describing that bicycle and any participating credentials associated with it.

This specification defines:

- the relationship among a physical bicycle, its canonical identity, one or more tag identifiers, and external credentials;
- the minimum NFC, QR, URI, resolver, web-response, and data requirements for an interoperable pilot;
- requirements for aftermarket and manufacturer-installed tags;
- a conformance framework for tags, resolvers, registries, and verification clients;
- security, privacy, lifecycle, and accessibility requirements; and
- a staged path from a low-cost pilot to authenticated factory implementations.

This specification does **not** define an e-bike class, decide which classes are permitted in a place, replace manufacturer or owner attestations, create a government-issued vehicle identifier, or require public disclosure of a bicycle serial number or owner information. Legal classifications and access decisions remain functions of applicable law and the responsible municipality, agency, or land manager. OBDI makes those decisions easier to implement by providing consistent identity, configuration, provenance, and credential data.

2. Design principles

1. **The bicycle is the subject.** OBDI identifies a physical bicycle, not its owner and not a subscription.
2. **The tag is a pointer, not the record.** Mutable status and certification data remain online.
3. **Identity and credentials are separate.** A permanent OBDI identity may support multiple present or future classification, eligibility, and access credentials.
4. **Multiple identifiers may describe one bicycle.** A manufacturer tag, an aftermarket tag, a QR code, and a mobile account may all resolve to one canonical bicycle record.
5. **A general-purpose phone must work.** The Minimum Viable Profile requires no specialized reader or installed app.
6. **Public verification must preserve privacy.** Verification does not expose owner personally identifiable information.
7. **Status is current, revocable, and time-bounded.** A tag must never contain an immutable claim that a bicycle is permanently compliant.
8. **Open web standards come first.** OBDI builds on NFC Forum NDEF and URI records, HTTPS, JSON, and established resolver patterns.

9. **Jurisdictions are policy layers, not identity boundaries.** The same bicycle identity can support different class definitions and access rules adopted by municipalities, agencies, and land managers.
10. **The pilot must be buildable now.** Advanced cryptographic tags are recommended for later profiles but are not required for Phase 1.

3. Conventions and terminology

The key words **MUST**, **MUST NOT**, **REQUIRED**, **SHALL**, **SHALL NOT**, **SHOULD**, **SHOULD NOT**, **RECOMMENDED**, **NOT RECOMMENDED**, **MAY**, and **OPTIONAL** are to be interpreted as described in RFC 2119 and RFC 8174 when, and only when, they appear in all capitals.

Term	Meaning
Bicycle	The physical e-bike that is the subject of an OBDI record.
Canonical Bicycle ID	An immutable internal identifier assigned by a participating registry. It is not a manufacturer serial number, NFC chip UID, or credential number.
OBDI Identifier	A globally unique, non-guessable identifier carried in an OBDI URI or resolved from a participating source.
OBDI Tag	An NFC data carrier conforming to this specification, whether installed by a manufacturer or applied after sale.
Tag UID	A hardware identifier supplied by some NFC chips. A UID alone is not an OBDI Identifier.
Resolver	An HTTPS service that accepts an OBDI URI and returns a human verification view and, when requested, a machine-readable representation.

Registry	A system maintaining canonical bicycle records, identifier mappings, provenance, and credential links.
Credential	A program- or jurisdiction-specific, revocable assertion associated with a bicycle, such as eligibility for a defined e-bike class or access policy.
Verification Client	A browser, law-enforcement application, manufacturer application, or other tool that reads and verifies OBDI information.
Manufacturer Record	An authoritative or delegated record describing a bicycle's factory identity and original configuration.
Program Tag	An aftermarket NFC/QR tag issued by a participating program and associated with a tag record and canonical bicycle record.
Public Verification View	A mobile-first page revealing current credential status and enough bicycle attributes for field comparison without owner PII.

4. Reference architecture

OBDI uses a many-identifiers-to-one-bicycle model:

Entry point	Identifies	Resolution outcome
Manufacturer-installed NFC	Manufacturer or delegated OBDI record	Canonical bicycle identity, factory data, participating credentials

Agency or program NFC	Program tag assignment	Same canonical bicycle and current applicable eligibility status
Printed QR on tag	Same HTTPS URI as the adjacent NFC tag	Same result as tapping the tag
QR in owner account	Time-safe public verification URI for the bicycle or credential	Same current public verification view
Enforcement or partner app	OBDI identifier or recognized manufacturer identifier	Machine-readable bicycle and credential response

An OBDI Registry SHALL NOT use an NFC chip UID, manufacturer serial number, manufacturer OBDI identifier, program tag identifier, or credential identifier as the database primary key for a bicycle. It SHALL maintain an immutable Canonical Bicycle ID and associate zero or more external and physical identifiers with that record.

An implementation SHALL support more than one active or historical identifier for a bicycle. It SHALL NOT assume that only one NFC tag exists on a bicycle.

5. Conformance profiles

5.1 Profile P1 — Minimum Viable OBDI Tag

Profile P1 is the REQUIRED profile for the initial pilot. It is suitable for low-cost, tamper-evident NFC stickers and may also be implemented by manufacturers.

A conforming P1 tag:

- MUST be readable by common NFC-capable smartphones without a dedicated application;
- MUST present one NFC Forum NDEF URI record containing an absolute HTTPS URI;
- MUST use a tag with sufficient user memory for the complete encoded NDEF message;
- MUST be permanently write-locked after successful encoding and quality assurance;
- MUST NOT store owner PII, legal status, fee status, attestation status, a complete serial number, or mutable credential claims on the tag;

- MUST have an adjacent human-visible identifier;
- SHOULD have an adjacent QR code encoding the same HTTPS URI;
- SHOULD be tamper-evident or destructible when removed if applied after sale; and
- MUST resolve to a service satisfying Section 8.

5.2 Profile P2 — Manufacturer-Installed Durable OBDI Tag

Profile P2 adds durability, lifecycle, and factory-provisioning requirements. A conforming P2 implementation MUST satisfy P1 except where a stronger P2 requirement supersedes it, and:

- MUST be permanently installed in or on the frame, motor, or another durable bicycle component;
- MUST be located so an ordinary phone or documented field reader can reliably read it;
- MUST remain readable after ordinary bicycle use, washing, vibration, weather exposure, and expected service;
- MUST be associated at manufacture with the specific physical bicycle and the manufacturer's authoritative identity record;
- MUST provide a visible tap target or durable marking indicating the read location, unless the installation location is an established industry convention;
- MUST NOT require disclosure of owner identity to perform a public lookup; and
- SHOULD use an authenticated tag as described in P3 when economically and operationally feasible.

Embedding a tag in carbon layup or inside a motor is conforming only when radio performance remains reliable through the surrounding materials and the tap location is discoverable.

5.3 Profile P3 — Authenticated OBDI Tag

Profile P3 is a future security profile for manufacturer and high-assurance uses. P3 MUST satisfy P2 and SHALL use a cryptographic mechanism that permits the resolver or verification client to distinguish a genuine tag interaction from a copied static URI.

The P3 authentication scheme:

- MUST use publicly documented algorithms and protocol behavior;
- MUST use per-tag key material or an equivalently strong anti-cloning mechanism;
- MUST permit key rotation, compromise handling, and revocation;
- MUST bind the authentication result to the OBDI Identifier;
- MUST fail safely to an explicit **Identity authentication unavailable or failed** result rather than displaying a verified state; and

- SHOULD support dynamic, tap-specific authentication data while preserving a stable public bicycle URI.

No particular commercial chip is mandated by version 0.3. A future implementation profile should identify tested interoperable hardware and define cryptographic test vectors.

6. NFC data carrier requirements

6.1 Standards foundation

An OBDI tag SHALL use NFC Forum-compatible NDEF encoding. Profile P1 SHOULD use an NFC Forum Type 2 Tag or Type 4 Tag implementation commonly readable by consumer phones. Other NFC Forum tag types MAY be used if they satisfy all conformance tests.

The NDEF message MUST contain a URI Record Type Definition record whose resolved value is the OBDI HTTPS URI. Implementations MAY include additional records only if the first actionable user experience remains the OBDI URI and common phones continue to open it predictably.

6.2 Tag capacity

The implementer SHALL calculate capacity using the final NDEF message, including record overhead, not merely the visible URI length. For the pilot, the provisioned tag SHOULD provide at least 144 bytes of usable NDEF memory. A larger capacity SHOULD be selected when the production hostname or path causes the encoded message to approach capacity.

6.3 Locking and provisioning

The issuer SHALL:

1. assign the tag identifier in the registry;
2. encode the final production HTTPS URI;
3. read the tag using an independent verification operation;
4. verify that NFC and printed QR resolve to the intended tag record;
5. permanently lock the NDEF data area against rewriting; and
6. record the provisioning result, tag technology, batch, and timestamp.

A tag that cannot be verified or locked MUST NOT be issued as conforming.

6.4 NFC chip UID

The NFC chip UID MAY be recorded privately as operational metadata when legally and technically appropriate. It MUST NOT serve as the sole public OBDI Identifier because UID behavior, length, privacy characteristics, and clone resistance vary among products. Public resolution MUST be based on the encoded OBDI URI and identifier.

7. Identifier and URI requirements

7.1 Identifier properties

An OBDI Identifier MUST:

- be unique within the issuing namespace;
- be generated with at least 128 bits of cryptographically secure randomness, or provide equivalent resistance to enumeration;
- contain no embedded owner, bicycle, serial-number, manufacturer, product, payment, or jurisdiction information;
- be treated as case-sensitive unless the issuing namespace explicitly defines a normalized alphabet; and
- remain stable for the useful life of the identifier record.

Version 0.3 RECOMMENDS a 128-bit random value encoded as unpadded base64url or a comparably compact, URL-safe representation.

Example identifier for illustration only:

F7xj4Kf0pQ9m2Vw8tN3aRg

7.2 URI form

The tag MUST encode an absolute HTTPS URI controlled by the issuer or its delegated resolver.

The recommended form is:

`https://{resolver-domain}/e/{opaque-id}`

Example:

`https://id.example.org/e/F7xj4Kf0pQ9m2Vw8tN3aRg`

The production resolver hostname and path SHALL be selected and published before pilot provisioning. The example domain above MUST NOT be used in production.

The URI:

- MUST use HTTPS;
- MUST NOT contain an owner name, email address, serial number, credential state, or other sensitive data;
- SHOULD be short enough for economical tag capacity and robust QR printing;
- MUST remain resolvable even if the credential is expired, revoked, transferred, replaced, or absent;
- MUST return a clear terminal or historical state rather than an ambiguous 404 when the identifier was validly issued; and
- SHOULD be governed by a durable-domain and service-continuity policy.

7.3 GS1 compatibility

A manufacturer using GS1 identifiers MAY expose an OBDI-compatible service through a GS1 Digital Link URI and conformant resolver. Such an implementation MUST still provide a stable bicycle-level identity, must not expose owner PII, and must support discovery or mapping to participating credential services.

OBDI does not allocate GS1 identifiers or claim that a non-GS1 OBDI URI is a GS1 Digital Link. Where GS1 identifiers are used, the manufacturer is responsible for GS1 conformance and identifier licensing.

8. Resolver requirements

8.1 Human-readable response

A direct browser request to an OBDI URI MUST return a mobile-first public page. When a bicycle has a participating classification or access credential, the page SHOULD display, in this order:

1. **Credential state:** Active, Expired, Suspended, Revoked, Transferred, Replaced, or Not Enrolled;
2. **Eligibility assertion:** the applicable e-bike class or access category, with the responsible authority, ruleset name, and ruleset version;
3. **Currentness:** attestation-through date and fee-through date, or a combined valid-through date;
4. **Bicycle match attributes:** manufacturer, model, model year if known, primary color, frame size if known, and a representative bicycle photo when supplied;
5. **Identity and provenance:** masked public identifier, verification method, and issuer; and

6. **Field guidance:** a concise statement explaining whether the displayed credential is currently valid and that visual matching does not prove absence of later modification.

Owner name, email, address, payment information, full serial number, and private enforcement evidence **MUST NOT** appear in the public view.

8.2 Machine-readable response

The resolver **MUST** provide a machine-readable JSON representation through HTTP content negotiation using `Accept: application/json` or through a documented stable API link discoverable from the human response.

The P1 JSON response **SHOULD** use the following top-level structure:

```
{
  "specification": "https://OBDI.example/spec/0.3",
  "recordType": "OBDIBicycle",
  "canonicalBicycleId": "public-or-pairwise-bicycle-reference",
  "identity": {
    "status": "linked",
    "authentication": "static-uri",
    "issuer": "https://registry.example.org"
  },
  "bicycle": {
    "manufacturer": "Example Cycles",
    "model": "Trail One",
    "modelYear": 2027,
    "color": "dark green",
    "frameSize": "L"
  },
  "credentials": [
    {
      "type": "AgencyAccessCredential",
      "issuer": "https://agency.example.gov",
      "jurisdiction": "US-CA-EXAMPLE",
      "status": "active",
      "classification": "class-1-only",
      "ruleset": "Example-Trail-Ebike-Policy",
      "rulesetVersion": "2026-01",
      "attestedThrough": "2027-09-16",
      "verificationMethod": "owner-attested"
    }
  ],
  "updatedAt": "2026-09-16T20:15:00Z"
}
```

The example vocabulary is provisional. Production implementations **MUST** publish a JSON Schema and field dictionary before claiming API interoperability.

8.3 Status semantics

Status	Required public meaning
Active	Required attestation and fees are current; no suspension or revocation is in effect.
Expired	A required time-bounded condition is no longer current.
Suspended	Use is temporarily invalid pending review or action.
Revoked	The issuer has invalidated the credential.
Transferred	The former owner relationship ended and required successor action is incomplete or recorded elsewhere.
Replaced	This tag or identifier has been superseded; the page may direct to the current record without concealing replacement history.
Not Enrolled	The bicycle identity is recognized, but no current credential from the named program exists.
Unknown	The identifier cannot be established as issued by the resolver. This MUST NOT be styled as valid.

A resolver MUST derive state from authoritative server-side records at request time. A cached response MUST have a documented maximum age appropriate to enforcement use and MUST NOT continue displaying Active after a known suspension or revocation.

8.4 Discovery of credentials

A manufacturer-controlled resolver is not required to become an agency or access-program website. It MAY show the manufacturer's normal product page, but an OBDI-conforming machine response MUST provide either:

- the current participating credential summary; or
- a documented, machine-discoverable bicycle identifier that an authorized verification client can query against the applicable participating registry.

The mapping SHALL be established through a privacy-preserving API or registry linkage. It MUST NOT require an enforcement agent to manually transcribe a full manufacturer serial number.

8.5 Municipal and agency class selection

OBDI is designed to let a responsible authority apply its own policy without creating a new bicycle identity system. A municipality, public agency, or land manager MAY publish a versioned ruleset defining which e-bike class or classes are eligible on a facility, trail, route, or network. A participating resolver MAY evaluate the bicycle's structured configuration facts and current attestations against that ruleset and return a concise eligibility result.

The authority's ruleset SHOULD identify:

- the legal or policy source defining each eligible class;
- the jurisdiction and facilities to which the rule applies;
- the effective date and ruleset version;
- the technical attributes evaluated, including assist behavior, cutoff speed, throttle capability, motor rating, and selectable operating modes where relevant;
- the accepted sources of evidence and required current-owner attestations;
- expiration, renewal, inspection, suspension, and revocation conditions; and
- a contact or appeal path for disputed results.

The resolver MUST distinguish the bicycle's manufacturer-reported configuration from the authority's eligibility decision. It MUST NOT present a local access result as a universal legal classification. The same bicycle MAY be eligible under one agency's ruleset and ineligible or unevaluated under another.

9. QR and visual marking requirements

An aftermarket program tag SHOULD print a QR code encoding exactly the same HTTPS URI as its NFC NDEF record. A manufacturer tag SHOULD provide either an equivalent QR code or a clear means to locate and use the NFC tap point.

The physical label SHOULD include:

- the issuing program or OBDI mark, as applicable;
- a plain-language **Tap or scan to verify** instruction;
- a human-readable short tag reference suitable for customer support;
- a QR quiet zone and contrast adequate for outdoor mobile scanning; and
- no printed owner PII or complete bicycle serial number.

The owner portal SHALL provide a digital QR code from the **My Bikes** view that leads to the same current public verification result. It MAY use a different presentation token, but that token MUST map to the same canonical bicycle record and MUST NOT expose account authentication data.

10. Bicycle and identifier data model

The registry MUST represent the following as distinct objects:

Object	Minimum purpose
Bicycle	Canonical record for the physical bicycle.
Identifier	One manufacturer, tag, QR, serial, or partner identifier linked to the bicycle.
Tag	Physical carrier, provisioning state, technology, batch, placement, and replacement history.
Manufacturer Product	Make, brand, model, year, market configuration, and original technical specifications.

Credential	Program-specific assertion, ruleset, validity, method, and status.
Attestation	Dated owner assertion, terms version, and renewal history.
Account Relationship	Private relationship between a user and bicycle, with role and effective dates.
Enforcement Case	Private report, evidence, review, decision, appeal, and audit trail.

The Identifier object SHOULD contain: identifier type, normalized value or secure hash as appropriate, issuing authority, status, effective dates, provenance, confidence, and the Canonical Bicycle ID to which it is linked.

The system MUST preserve identifier and credential history. Relinking, merging, replacement, transfer, suspension, and revocation events MUST be auditable.

11. Minimum public bicycle attributes

The following attributes SHOULD be available for field comparison when known and lawful to display:

- manufacturer or brand;
- model;
- model year or year range;
- primary color;
- frame size;
- bicycle category or frame style;
- representative or owner-supplied bicycle image; and
- masked identifier suffix.

A public record MUST NOT imply that color, size, or photograph alone establishes identity or technical compliance. These attributes are practical anti-transfer checks supporting a field official's judgment.

12. Manufacturer provisioning and interoperability

A manufacturer implementation SHOULD establish the following chain:

Physical bicycle → permanent OBDI tag → manufacturer bicycle record → canonical or mapped bicycle identity → credentials

At provisioning, the manufacturer SHOULD record:

- its bicycle-level identifier and serial number;
- tag identifier and, for authenticated tags, authentication-key reference;
- brand, model, variant, model year, market, and frame attributes;
- original drive-system configuration;
- original motor nominal rating and applicable maximum rating fields;
- pedal-assist behavior, assist cutoff, throttle capability, and selectable operating modes;
- firmware or configuration provenance where relevant;
- manufacturing and provisioning timestamps; and
- data source and responsible authority.

Manufacturer technical claims SHALL describe original configuration. They SHALL NOT by themselves assert that a bicycle remains unmodified after sale. Municipalities, agencies, land managers, and participating programs may combine manufacturer provenance with a continuing owner attestation, inspection result, and enforcement status when determining current classification or access eligibility.

Manufacturers SHOULD provide one of the following integration paths:

1. a bicycle lookup API accepting a privacy-preserving identifier;
2. a signed batch feed of eligible bicycles and configurations;
3. a conformant resolver that exposes the required machine-readable facts; or
4. a delegated registry relationship.

Manufacturer APIs SHOULD be documented using the OpenAPI Specification and MUST define authentication, authorization, rate limits, error behavior, provenance, update semantics, and data-retention expectations.

13. Municipal and Agency Pilot Profile

13.1 Phase 1 objective

Phase 1 SHALL demonstrate that a small group of owners can enroll bicycles, receive and apply NFC/QR tags, and enable field officials to retrieve current, privacy-preserving identity and classification information. The pilot SHOULD allow a participating municipality, agency, or land manager to define which e-bike class or classes qualify under its own adopted ruleset without changing the bicycle's underlying OBDI identity.

13.2 Recommended pilot tag

The pilot SHOULD procure commercially available NFC Forum-compatible, NDEF-capable adhesive tags with:

- at least 144 bytes of usable NDEF memory;
- permanent write-lock capability;
- outdoor-rated adhesive and face material appropriate to bicycle frames;
- destructible or visibly tamper-evident construction when removal is attempted;
- a production print area supporting the issuer or OBDI mark, QR, short reference, and tap instruction; and
- supplier lot traceability.

The pilot SHOULD test at least two tag constructions on representative aluminum, steel, and carbon bicycle locations. Conventional tags placed directly on metal may be unreadable; on-metal construction or an insulating spacer MAY be required. Radio and adhesive testing MUST precede bulk purchase.

13.3 Pilot placement

The pilot operator SHALL publish one preferred and one alternate placement location. Placement SHOULD be:

- readily reachable by enforcement agent's phone;
- visually associated with the bicycle described by the record;
- difficult to remove without damage;
- protected from abrasion, drivetrain contamination, and routine service; and
- compatible with carbon, metal, paint, and clear-coat limitations stated by the tag supplier and bicycle manufacturer.

13.4 Pilot issuance workflow

1. Owner creates or signs into an account.

2. Owner enters bicycle make, model, model year if known, serial number, color, size, and a photograph.
3. Owner selects or is assigned the participating municipality, agency, land manager, or access program whose ruleset will be evaluated.
4. System evaluates manufacturer facts and owner-supplied information against the applicable versioned ruleset.
5. When required, the owner attests that the bicycle currently remains configured within the selected class and has not been modified to operate outside that class definition.
6. The system automatically issues the applicable classification or access credential unless a defined risk rule requires exception review.
7. A provisioned P1 tag is assigned to the canonical bicycle record and distributed.
8. Owner applies and activates the tag, confirming placement and bicycle match.
9. NFC, printed QR, and an optional owner-account QR display the same current public verification result.

Fees, if any, are implementation policy and are outside the OBDI technical standard.

13.5 Pilot operational controls

The pilot operator **MUST** support tag inventory, assignment, activation, non-delivery, damage, replacement, suspected transfer, suspension, revocation, reinstatement, and audit history. A replacement tag **MUST** link to the same canonical bicycle record; the former tag **MUST** resolve to **Replaced** rather than silently becoming unknown.

14. Security requirements

14.1 Threat model

The implementation **SHALL** address at least:

- enumeration of identifiers;
- cloning of a static NFC URI or QR code;
- physical transfer of an aftermarket sticker;
- rewriting an unlocked tag;
- linking public lookups to owner identity;
- unauthorized merging or relinking of bicycle records;
- stale Active results after revocation;
- forged manufacturer or credential-provider responses;
- account takeover and unauthorized transfer; and

- denial of service during field verification.

14.2 P1 security posture

P1 provides a convenient link and tamper evidence; it does not provide cryptographic proof of physical tag originality. The public view **SHOULD** disclose **Static tag — visual bicycle match required** or equivalent language where relevant.

P1 mitigations **MUST** include opaque identifiers, HTTPS, permanent NDEF locking, tamper-evident construction, field-visible bicycle attributes, rate limiting, monitoring, and immediate server-side suspension or revocation.

14.3 Registry and API security

Private APIs **MUST** use authenticated and authorized connections. Administrative actions affecting identity linkage or credential status **MUST** require strong authentication and **MUST** produce an append-only or equivalently protected audit event. Sensitive identifiers **SHOULD** be encrypted or cryptographically hashed where the use case permits.

Public endpoints **SHOULD** limit bulk harvesting while preserving ordinary field access. Logs **MUST** follow a documented retention policy and **MUST NOT** be repurposed to track rider location or movement.

15. Privacy requirements

OBDI implementations **MUST** apply data minimization and purpose limitation.

The public verification surface **MUST NOT** reveal:

- owner name, username, email, phone, address, or payment details;
- full manufacturer serial number;
- precise owner or bicycle location;
- enforcement evidence or reporter identity;
- account history; or
- any data unnecessary to verify the bicycle and credential.

The operator **MUST** publish a privacy notice describing data collected, purposes, public fields, retention, sharing, owner rights, and security contacts. Transfer of ownership **MUST** sever the former owner's private account access while preserving the bicycle's non-personal identity and required audit history.

Public identifier design SHOULD reduce cross-service correlation. A registry MAY expose pairwise or service-specific public references while maintaining the canonical mapping privately.

16. Accessibility and field usability

Human verification pages MUST conform to WCAG 2.2 Level AA or the current adopted accessibility requirement of the implementing organization. Status MUST be conveyed through text and iconography, not color alone.

The field page SHOULD load quickly on a constrained mobile connection, use large touch targets, avoid requiring sign-in for ordinary public verification, and render the credential state before secondary details. The design SHOULD provide a printable or cached operational fallback, while making the age of cached data conspicuous.

17. Lifecycle requirements

An OBDI implementation MUST support these lifecycle events:

- unassigned tag;
- provisioned tag;
- assigned but not activated;
- active identifier;
- damaged or lost tag;
- replacement;
- ownership transfer;
- bicycle retirement or destruction;
- suspected compromise or clone;
- identifier merge or correction;
- credential expiration, suspension, revocation, reinstatement, and cancellation; and
- resolver or registry migration.

The permanent bicycle identity SHOULD survive ordinary changes of ownership, credential participation, and resolver presentation. A credential's continuing validity MUST NOT be inferred merely because the identity remains resolvable.

18. HTTP and service behavior

Resolvers **MUST** use valid publicly trusted TLS certificates and **SHOULD** support current secure HTTP versions. They **MUST NOT** require cookies, advertising identifiers, or third-party tracking for public verification.

Responses **SHOULD** use explicit cache controls. Active status responses used for enforcement **SHOULD** be short-lived. Revoked, suspended, and replaced states **SHOULD** propagate without avoidable delay.

The service **SHOULD** provide operational monitoring, backups, incident response, and a durable-domain transition plan. If a resolver domain changes, the original domain **SHOULD** continue resolving or redirecting for the expected life of issued tags.

19. Conformance tests

A P1 implementation is conforming only if all applicable tests pass.

ID	Test	Pass condition
P1-01	Consumer-phone read	Supported iOS and Android phones read the tag without a dedicated app.
P1-02	NDEF validation	Tag contains a valid NDEF URI record resolving to the registered HTTPS URI.
P1-03	Write protection	Issued tag cannot be rewritten through ordinary NFC tools.
P1-04	NFC/QR equivalence	NFC and adjacent QR lead to the same tag or bicycle record and credential state.

P1-05	Identifier entropy	Identifier generation meets the 128-bit or equivalent requirement.
P1-06	Privacy	Public view and URI expose no prohibited PII or full serial number.
P1-07	Multiple identifiers	Two identifiers assigned to one test bicycle resolve to the same canonical record.
P1-08	Revocation	Active changes to Revoked within the documented propagation target.
P1-09	Replacement	Old tag shows Replaced and new tag shows the correct current record.
P1-10	Unknown handling	Random or malformed identifiers never display a valid state.
P1-11	Content negotiation	Browser receives HTML and documented machine request receives JSON.
P1-12	Field match	Public view contains the configured make, model, color, and size/photo fields.

P1-13	Accessibility	Verification page passes the operator's WCAG 2.2 AA acceptance process.
P1-14	Material/radio test	Selected production tag reads reliably at designated placement locations.
P1-15	Auditability	Assignment, activation, replacement, suspension, and revocation produce auditable events.

The pilot acceptance plan SHOULD define device models, operating-system versions, read orientations, environmental conditions, sample size, and success threshold before testing begins.

20. Governance and versioning

This document is a recommended open industry specification, not an NFC Forum, GS1, W3C, ISO, SAE, or government standard. Claims of conformance SHALL identify the OBDI version and profile, for example:

OBDI 0.3 / P1

Changes SHALL use semantic versioning principles:

- patch revisions clarify without changing interoperability;
- minor revisions add backward-compatible capabilities; and
- major revisions may introduce incompatible requirements.

The specification steward SHOULD maintain a public issue tracker, change log, implementation registry, test artifacts, and a documented process for stakeholder proposals. Manufacturers, land managers, rider organizations, accessibility experts, privacy experts, tag vendors, drive-system suppliers, and enforcement practitioners SHOULD be represented in review.

21. Phase 1 implementation decisions

The following decisions are RECOMMENDED for immediate adoption so the pilot can proceed:

Decision	Phase 1 recommendation
Tag profile	OBDI 0.3 / P1
Carrier	NFC Forum-compatible NDEF adhesive tag, minimum 144-byte usable memory
Payload	One locked NDEF HTTPS URI record
Identifier	128-bit cryptographically random, base64url without padding
QR	Same HTTPS URI as NFC
Record authority	Participating OBDI Registry or delegated public-agency registry
Bicycle key	Separate immutable Canonical Bicycle ID
Public data	Issuer, classification or access status, ruleset, currentness, make/model/year/color/size/photo, masked reference
Private data	Owner PII, full serial, payment, enforcement evidence, account history
Issuance	Automated by default, exception review only

Security	Tamper-evident physical tag + opaque URI + visual bike match + server revocation
Manufacturer tags	Supported through identifier mapping; not required for pilot
Authenticated NFC	Deferred to P3 technical profile and field testing

22. Items to finalize before production procurement

The pilot team must approve and publish:

1. production program and resolver domain names;
2. stewardship and licensing terms for this specification;
3. final URI path and identifier alphabet;
4. JSON Schema and API field dictionary;
5. tag face artwork, dimensions, QR size, and human-readable reference format;
6. tested tag constructions and supplier requirements;
7. preferred and alternate frame placement instructions;
8. public verification vocabulary and exact status messages;
9. credential ruleset and owner attestation text;
10. revocation, appeal, replacement, transfer, and privacy policies;
11. conformance device matrix and pilot acceptance thresholds; and
12. durable-domain, uptime, backup, and incident-response ownership.

These are implementation selections within the architecture; they do not prevent publication of version 0.3 for public review.

Appendix A — Example identifier mapping

One physical bicycle may be represented as follows:

Record	Example value	Public?
--------	---------------	---------

Canonical Bicycle ID	bike_01K5...	No; internal primary identity
Manufacturer serial	WTUX12345678	No; masked in public view
Manufacturer OBDI	mfr:example:F82...	As permitted by issuer
Municipal program tag ID	F7xj4Kf0pQ9m2Vw8tN3aRg	Yes, through opaque URI
Replacement tag ID	c9Kp1Yt7bL4sQ2nM6xR0Vw	Yes, after assignment
Agency access credential	access_01K5...	Masked or pairwise public reference

All identifiers map to the Canonical Bicycle ID. Credential and attestation state are evaluated separately.

Appendix B — Example field-verification result

AGENCY E-BIKE ELIGIBILITY — ACTIVE

Eligible classification: Class 1 only

Issuer: Example Regional Parks Agency

Ruleset: Example Natural-Surface Trail E-Bike Policy v2027.1

Attestation current through: September 16, 2027

Bicycle

Example Cycles Trail One · 2027 · Dark green · Large

Photo: displayed when supplied

Reference: •••3aRg

Verification basis

Original configuration: manufacturer/model verified

Current configuration: owner attested

Tag security: static P1 tag; visually match this record to the bicycle

No owner identity is displayed.

Appendix C — Standards and references

1. NFC Forum, [Specifications](#): NDEF, URI Record Type Definition, Tag Type specifications, and related technical specifications.
2. NFC Forum, [NFC Digital Product Passport Candidate Technical Specification](#).
3. GS1, [GS1 Digital Link Standard: URI Syntax](#).
4. GS1, [GS1-Conformant Resolver Standard](#).
5. IETF, [RFC 3986, Uniform Resource Identifier \(URI\): Generic Syntax](#).
6. IETF, [RFC 2119](#) and [RFC 8174](#), *Key words for use in RFCs to Indicate Requirement Levels*.
7. OpenAPI Initiative, [OpenAPI Specification](#).
8. W3C, [Web Content Accessibility Guidelines \(WCAG\) 2.2](#).
9. W3C, [Verifiable Credentials Data Model v2.0](#) — informative future option for portable, cryptographically verifiable credentials; not required by OBDI 0.3/P1.

Appendix D — Publication notice

Version 0.3 is intended for pilot implementation and public comment. It standardizes the identity and resolution layer while leaving e-bike class definitions, access eligibility, fees, attestations, enforcement policy, and legal recognition to participating municipalities, agencies, land managers, programs, and jurisdictions.

OBDI is a geographically and programmatically neutral technical framework. It can make class-specific policies easier to administer because an agency can evaluate consistent manufacturer facts and current attestations against its own versioned ruleset. Adoption of OBDI does not itself classify a bicycle, grant access, or imply endorsement by a manufacturer, land manager, government agency, or standards organization.