



ODNCA

FOUNDATION DOCUMENT · ODNCA-FD-001

The chain is the root.

ODNCA — ORDnet Decentralized Names Coordination Authority

This document is the official foundation of ODNCA: what the authority is, the standards and policies it stewards, how it is governed, and why none of it requires your trust. It condenses the twelve adopted ODNCA documents into one reference for partners, operators, registrars, and rights holders.

DOCUMENT	ODNCA-FD-001 · Foundation Document
VERSION · STATUS	v1.0 · Adopted · August 2026
ISSUED BY	ODNCA — ORDnet Decentralized Names Coordination Authority
NAMESPACE AT ISSUE	BSV / SNS · 651,483 canonical names
WEB	odnca.org · sns.ordnet.io · search.ordnet.io · whois.ordnet.io
CONTACT	info@odnca.org

Don't trust us — recompute us.

CONTENTS

§1	The authority	§7	Registration data (WHOIS)
§2	The namespace	§8	Policies: fair use, registrars, abuse
§3	Ownership & resolution	§9	Governance
§4	The Root Registry & TLDs	§10	The trust framework
§5	Registration (SNSP)	§11	The document library
§6	Data channels & URI schemes	§12	Participation

PREAMBLE

A ledger without agreed reading rules is only data. ODNCA exists to publish those rules for on-chain naming — the root rules, the standards, the conformance vectors, and the policies — so that any two parties reading the same chain arrive at the same names, the same owners, and the same answers.

ODNCA is an authority of an unusual kind: it has no power over the chain, claims none, and is designed so that its own existence is optional. Names cannot be seized, rules cannot be changed silently, and every answer any ODNCA service gives can be recomputed by anyone from public data. The authority's product is not control; it is *agreement* — published, versioned, signed, and anchored on the chain it describes.

The ecosystem this document describes is live: 651,483 canonical names indexed under frozen rules, a signed resolver, an operating registrar, on-chain state commitments with mintable ownership certificates, and a mail and content layer in production. This document is a summary; each section names the adopted document that governs it in full.

§1 · GOVERNED BY ODNCA-GOV-001, ODNCA-POL-001

The authority

ODNCA coordinates on-chain naming the only way a chain allows: by **recognition, not permission**. On the chain, claiming a name — even inventing a TLD — is permissionless, and ODNCA does not pretend otherwise. What ODNCA stewards is the **recognised set**: which namespaces, TLDs, registrars, and operators the coordinated ecosystem serves, under published rules that anyone can verify and any implementation can join by passing the conformance vectors.

LAYER	LIVES AT	ROLE
Fact layer	the indexer · search.ordnet.io	Indexes every claim, always. Knows what, by whom, when. Neutral by design.
Coordination layer	ODNCA · odnca.org	The recognised set: root rules, standards, vectors, policies, keys — published, signed, chain-anchored.
Service layer	registrars & operators	Commercial services on top: portals, premium features, content measures. Each operator's own policy, honestly labelled.

The separation is strict in both directions: the fact layer never censors, and the service layer never redefines validity. Even the founding registrar operates under the standard on identical terms — and is deliberately *stricter* than the standard requires, claiming no privileges under it.

§2 · GOVERNED BY ODNCA-STD-003 (SNS-NAME-1)

The namespace

The name standard documents deployed reality — the exact rules under which all 651,483 names were indexed — and therefore needs no transition regime. Two name shapes, made deliberately unmistakable:

NAMESPACE	SHAPE	EXAMPLE
SNS	name.tld — exactly one dot	alex.web3
OpNS	bare name — no dot, no TLD	alex

A valid SNS registration is a JSON inscription `{"p":"sns", "op":"reg", "name":"alex.web3"}` on an output of exactly one satoshi. The name is normalized (head-strip, trim, lowercase), must contain exactly one dot with no whitespace or control characters, and may be 1–2048 bytes of UTF-8 — permissive at the character level, strict at the structural level. Uniqueness is enforced on the lowercase canonical form; the raw form is retained for lookalike detection. First seen wins, among valid claims only. Registrar sales restrictions (such as the founding portal's letters-and-digits offering) are registrar policy, never chain validity.

§3 · GOVERNED BY ODNCA-STD-001

Ownership & resolution

Transfer is a chain fact, not a protocol operation. The name lives in a satoshi; spending the output that carries it moves the name. Any wallet that can move a sat can transfer a name — no registry approval, no special transaction. Conformant indexers track each name to its exact satoshi position, classify where it lands (held, in contract, or burned), and journal every transfer for reorg-safe rollback.

Resolution is signed and provable. One HTTP call turns `name.tld` or `mailbox@name.tld` into the current holder. Every answer is signed over a fixed field set including its expiry, and carries the name's origin and its **current outpost** — check that outpost unspent at any node and the answer is *proven* live, not trusted.

```
$ curl sns.ordnet.io/resolve/ordnet.web3
ok: true v: 1 name: ordnet.web3
holder_script: 76a914...88ac
origin: 367a0a1d..e3ee:0
current: dc54c20a..80ac:0
expires: +300s as_of_height: 960102
sig: ✓ secp256k1 · verified
```

Clients choose their trust level — each a strict superset of the last, and skipping levels is always the client's choice, never the protocol's requirement:

LEVEL	ADDS	WHAT IT BUYS
1 Trust	read JSON, pay the script	five-line integration
2 Verify	check the signature	caching-safe; every answer provable after the fact
3 Prove	check the outpost unspent	trust nobody — the chain confirms the holder

Honesty is wire-level: mailbox fallbacks are disclosed in the signed fields, fresh registrations answer `no_holder` during propagation instead of guessing, and errors are always readable JSON with a machine code.

§4 · GOVERNED BY ODNCA-STD-004, ODNCA-POL-001

The Root Registry & TLDs

A TLD's birth is a decision, not a discovery. Validity under a TLD begins at its published **activation height**: claims inscribed before activation are void, so nobody can squat a TLD before it exists. Each activation is inscribed on-chain as a signed activation record — the TLD's birth certificate — giving every TLD a registry-id of the form `bsv:<activation-txid>`. Namespaces themselves are identified by the hash of their frozen ruleset: a registry *is* its rules, so its rules are its fingerprint.

TLD	CATEGORY	MEANING
.web3 .bitcoin .crypto .blockchain .ordnet	Active	Open for registration through recognised registrars; resolved ecosystem-wide.
.bsv .bitcoinsv	Retired	Registration closed out of respect for the BSV Association's registration of these names. Existing names resolve forever — retirement never expropriates.
.1sat	Withheld	Deliberately untouched so the 1Sat Ordinals ecosystem retains the ability to issue it — although no registration of the term exists. Prior association and community stewardship count.

This is the fair-use policy in practice: registered rights are honoured, and so are moral claims. A withheld TLD activates only by, or with the consent of, the party for whom it is held. Where the same label exists elsewhere, the recognised entry is canonical for the coordinated ecosystem; the rest is acknowledged as chain fact and resolved nowhere in it.

§5 · GOVERNED BY ODNCA-STD-007 (SNSP)

Registration

Nobody needs permission to register: a raw conformant inscription is always a valid path, and the minimum viable registrar is a static page that produces one. SNSP is the protocol that makes a registrar's *assisted* path safe and fair:

```
GET /check → POST /claim/prepare → wallet inscribes the signed record → POST /claim/complete → chain → indexer → resolver
```

- **The claim lock:** one active claim per name, idempotent for the same wallet, expiring on abandonment — no races, no double-sell.
- **The signed claim record** binds the name *and* the destination wallet under the registrar's published issuer key — replay-proof by construction.
- **Direct flow:** for paid names, payment can ride as an output in the same transaction as the inscription — the transaction itself contains both the claim and the money, leaving no trust window.
- **Valid vs. verified**, deliberately separate: validity is the chain's (any conformant claim), verification is the registrar's (issuer-signed provenance). An unverified raw claim that is first still wins the name.

§6 · GOVERNED BY ODNCA-STD-005, ODNCA-STD-006

Data channels & URI schemes

There is no DNS-style record model — deliberately. A name has three data channels, and each channel's truth lives on the chain in its own native form; the records API is a reading window, not a management surface.

CHANNEL	THE ON-CHAIN TRUTH	READ VIA
Payment	the current outpoint of the name's satoshi	signed resolver answer (§3)
Mail	1-sat message inscriptions <i>owned by the recipient</i> — the inbox is literally the recipient's property; attachments are inscriptions referenced by outpoint; end-to-end encryption via the mailbox public key	the recipient's own wallet
Content	a 1Sat Ordinals inscription script in a sat; the name → content coupling (with subdomains and routes) points at an exact outpoint, holder-managed by wallet signature	ord://name.tld

SCHEME	MEANING
sns:alex.web3	the name — primary scheme for links, QR codes, deep links; action from context
ord://alex.web3	the content coupled to the name — a <i>mutable reference</i> , valid across content updates
ord://<txid>	that exact inscription — a <i>permanent reference</i> , immutable forever
ordns:	reserved for a future standard; accepted on input, never emitted

§7 • GOVERNED BY ODNCA-STD-008

Registration data (WHOIS)

One public, unauthenticated lookup — the same answer for everyone, exposing only what the chain and the published lists already make public. Four statuses: **available** (with honest pricing), **reserved** (never advertised as buyable), **flagged** (never denied to exist), **registered** (holder, content coupling, dates). Reverse lookup completes the surface: a wallet's names are as public as a name's wallet. An RDAP mapping is published for existing domain tooling — with two deliberate departures from web2: names do not expire, and there is no redaction layer, because the registrant is a public address on a public chain. Where WHOIS and the chain briefly differ, the chain is right — as always.

§8 • GOVERNED BY ODNCA-POL-001 • 002 • 003

Policies: fair use, registrars, abuse

Fair use (POL-001) — the TLD categories, the honoured rights, and the withheld .1sat — is summarised with the Root Registry in §4; its two absolutes bear repeating: retirement never expropriates, and a withheld TLD activates only by or with its party's consent.

Registrars (POL-002)

Recognition, the only lever an open chain allows: recognised registrars pass the conformance vectors, offer Active TLDs only, disclose fallbacks and lookalikes, label their own restrictions as their own, and never claim exclusivity. Losing recognition is the only sanction — chain access is untouched and untouchable.

Dispute & abuse (POL-003)

A name cannot be seized — enforcement is refusal of service, never removal of property, and the indexer indexes everything, always. Anyone may report a name by **signing a flag transaction**: complaints cost a signature and leave a paper trail. The central rule: **the crowd can warn, only review can block**.

TIER	TRIGGER	EFFECT
WARNING	automatic at the flag threshold, or applied pending review	pop-up disclosure, one click through; reversible, cheap if wrong — and it queues expedited review
BLOCKED	human review only — never a flag count; direct only for CSAM, active malware/phishing, court order	content replaced by the standard offline page; explicit blocked answer with reason code — never a fake not_registered

Everything reparable gets a cure period (default 7 days) before escalation. Bought flags cannot take anyone offline; at most they buy the target an expedited inspection — and clean content turns the attack into a public clearance. Every measure is published on a versioned, dated, **signed blocklist**: blocking in secret is censorship; blocking in public is moderation anyone can recompute. Measures are per-operator, under each operator's own law — a second independent operator is this policy's safety valve, not its threat.

§9 • GOVERNED BY ODNCA-GOV-001

Governance

Governance here is deliberately small: the chain settles ownership and the vectors settle conformance, so what remains is the genuinely human residue — recognising TLDs, adopting standards, applying the policies, stewarding the keys.

- **The Board.** ORDnet holds the founding seat. Seats are reserved for ecosystem stewards — in the first place the parties for whom TLDs are withheld or retired: the steward of the 1Sat Ordinals ecosystem and the BSV Association. An invitation stands until accepted or declined; declining costs nothing and closes no doors.
- **Decisions.** Sole-steward phase: the founding steward decides. Multi-seat: consensus sought, majority decides, founding seat breaks ties. Always: every decision is published with reasons and, where it changes recognised state, anchored on-chain. *A decision that is not published is not a decision.*
- **Standards changes** get a 14-day public review; vectors update in the same release. **TLD requests** get Board screening — patent and trademark search, collision check, and direct consultation of affected parties — a public comment window, and a decision within 30 days. Screening is a rights-and-fairness test, never an auction.

- **What no majority may decide:** no power over chain facts, no expropriation, no changing frozen math, no secret measures.

§10 · GOVERNED BY ODNCA-TF-001, ODNCA-STD-004 §6

The trust framework

Five principles run through every standard:

- The chain is the root.
- Central follows decentral.
- Trust is optional at every level.
- Honesty over convenience.
- Permissionless base, recognition on top.

Escrow, solved by construction. Web2 registries deposit data with escrow agents; here the chain *is* the deposit, the on-chain commitment chain is the receipt (periodic merkle roots, prev-linked, each binding the exact ruleset hash), and every holder can mint an offline-verifiable Certificate of Ownership as their own copy. The failure of any operator — including the founding one — loses convenience, never names.

WHAT FAILS	WHAT IS LOST
Registrar portal down	assisted convenience — the raw path remains
Resolver down	one endpoint — run your own from the rules
Registry database lost	extras until resync — rebuilt from the chain
A key compromised	nothing durable — rotation; stale lies fail the outpoint check
ODNCA disappears	a coordinator, not a registry — anyone recomputes and continues

The last row is the point: this ecosystem is designed so that its own authority is optional. *Don't trust us* — *recompute us* is not a slogan under the documents; it is the architecture in one line.

§11 · THE ADOPTED DOCUMENTS

The document library

DOCUMENT	TITLE	GOVERNS
ODNCA-STD-001	SNS Resolution Specification	claims, transfers, signed answers, verification levels
ODNCA-STD-002	Protocol Parameters Registry	living parameter lists: TLD sets, thresholds, timers, keys
ODNCA-STD-003	SNS-NAME-1 · Name Format	the name standard: form, normalization, characters, length
ODNCA-STD-004	The Root Registry	namespaces, TLD activation, commitments & certificates
ODNCA-STD-005	URI Schemes	sns:, ord://, the ordns: reservation
ODNCA-STD-006	Data Channels	payment, mail, content; state flow & custody rule
ODNCA-STD-007	SNSP · Registration Protocol	the assisted claim flow; valid vs. verified
ODNCA-STD-008	Registration Data (WHOIS)	the public lookup; RDAP mapping
ODNCA-POL-001	TLD Fair-Use Policy	categories, withholding, recognition of new TLDs
ODNCA-POL-002	Registrar Requirements	the permissionless base; recognition & conduct
ODNCA-POL-003	Dispute & Abuse Policy	flags, warning/block tiers, the public signed blacklist
ODNCA-GOV-001	Governance	the Board, procedures, and the limits on both

Companion framework: ODNCA-TF-001 · Trust Framework. All documents are published in full at odnca.org, versioned, with dated changelogs; conformance vector sets are published alongside the standards they freeze.

§12 · PARTICIPATION

Participation

YOU ARE	THE PATH
A wallet or application	Integrate resolution at any trust level — level 1 ships in an afternoon (sns.ordnet.io/skill.md).
A prospective registrar	The base is permissionless today; recognition and directory listing per ODNCA-POL-002 — run the vectors, match the answers.
A TLD requester	File per ODNCA-GOV-001 §6: screening on rights and fairness, public window, decision within 30 days.
A rights holder	The fair-use policy honours registered rights and prior association — as the withheld and retired TLDs attest. Consultation is direct: info@odnca.org .
An ecosystem steward	Board seats stand reserved per ODNCA-GOV-001 §2 — the invitation costs nothing and closes no doors.

ODNCA — ORDnet Decentralized Names Coordination Authority.

The rules are published. The vectors are frozen. The state is committed on-chain.

[Don't trust us — recompute us.](#)