# DCVaaS Multi-Brand SEO Safety Spec v1.0

## 0) Scope

Applies to the DCVaaS portfolio running **3 independent brands/domains** on **shared codebase/infrastructure**:

- KeylessSSL (developer intent)
- DelegatedSSL (agency/MSP intent)
- AutoCertify (SMB “panic fix” intent)

Goal: **rank independently** without triggering:

- dedup/canonical folding (WebMirror + shingles)
- “similar neighbor” crowding suppression
- site/topic dilution (siteFocusScore/siteRadius)
- cross-domain relationship poisoning (`spam_siblings`)
- engagement-driven demotions (NavBoost clicks)

This spec is grounded in the leaked-doc forensic findings (feature existence + intended measurement), not weights.

---

## 1) Non-negotiable Principles (the rules we do not break)

### P1 — Each domain must maintain a tight topical footprint

Why: site-level topical cohesion signals exist (`siteFocusScore`, `siteRadius`) and site-wide authority exists (`siteAuthority`).

**Implementation rules**

- KeylessSSL content: ACME/DNS-01/API/security automation only.
- DelegatedSSL content: reseller/white-label/client management/ops only.
- AutoCertify content: “Not Secure” fixes, platform guides, wizards, SMB education only.
- If a topic doesn’t clearly belong to ONE brand, we either:
  - rewrite it from that brand’s persona angle **so it truly becomes brand-native**, or
  - don’t publish it on that brand.

### P2 — No page-level duplication across brands

Why: near-duplicate detection systems based on shingles/fingerprints exist (`IndexingConverterShingleFingerprint`, `ShingleInfoPerDocData`) and WebMirror manages canonical/duplicate resolution.

**Forbidden**

- Copy/paste landing pages (features/pricing/about/how-it-works) with only logo swaps.
- Same blog post on multiple domains with light rewrites.

**Allowed**

- Same underlying *concept* across brands **only if** content is rewritten so the **token sequence + structure + intent** materially differs (not synonyms).

## P3 — Cross-domain links must be sparse and contextual

Why: relationship/poisoning features exist (`UrlPoisoningData`, `spam_siblings`) and outlink spam scoring concepts exist.

**Forbidden**

- Sitewide footer “family of brands” cross-links.
- Blogrolls / “our other brands” blocks across every page.

**Allowed**

- Contextual link where it solves a user problem (example: AutoCertify → DelegatedSSL “Manage this for clients?”).
- Maximum **1 cross-brand link per page**, and only on pages where it’s genuinely relevant.

## P4 — We must optimize for click satisfaction, not just rankings

Why: NavBoost exists and tracks good/bad/long clicks, including “unsquashed” metrics; scopes include URL/subdomain/root domain.

**Rule**

- Every indexed page must match query intent cleanly and deliver the answer fast (avoid pogo/bounce patterns that create “bad clicks”).

## P5 — Expect “new domain drag”

Why: `hostAge` is described as used to “sandbox fresh spam in serving time.”

**Rule**

- Plan brand launches with patience + link building + brand demand. No panic pivots after 2 weeks.

---

# 2) Indexing Architecture Rules (marketing vs app)

## A) Marketing vs App split

- **Marketing site (indexable):** `/`, `/pricing`, `/features`, `/blog`, `/docs` (brand-dependent)
- **App/portal (not indexable):** login, dashboard, wizards, authenticated routes

Reason: removing app routes from index prevents low-value/duplicate app structure from entering dedup/canonical systems and reduces accidental thin indexation risk. This aligns with your earlier platform strategy.

**Implementation**

- Host app on dedicated subdomains per brand:
  - `app.keylessssl…`
  - `portal.delegatedssl…`
  - `wizard.autocertify…`
- Apply `X-Robots-Tag: noindex, nofollow` at the edge for **all app subdomains**.

## B) Robots and sitemaps must be tenant-isolated

Reason: the multi-tenant strategy already called out mixed sitemaps/robots as a critical failure mode.

**Rules**

- `robots.txt` is generated per hostname.
- `sitemap.xml` is generated per hostname and contains **only URLs for that domain**.
- Separate Google Search Console properties + sitemap submission per domain.

---

# 3) Canonical & Redirect Policy (WebMirror-proofing)

Why: WebMirror is the canonicalization/duplication manager. If we’re sloppy, Google will choose for us.

### A) Canonical tags

#### Default

- Every indexable page must output a **self-referencing canonical** matching current hostname and path.

#### Absolute ban

- No accidental cross-domain canonicals (this is how you “donate” Brand A to Brand B).

#### Exceptions

- If we *intentionally* publish identical content (rare), pick one canonical domain and accept the other two will not rank for it.

### B) Host canonicalization (www/non-www)

- Choose one style per domain (recommend: non-www).
- 301 redirect all alternates to the chosen canonical host.

### C) Parameter handling

- Canonical URL must strip tracking params (`utm_*`, `gclid`, etc.).
- Ensure internal links never include params.

---

## 4) Page Template Divergence Requirements (to avoid “similar neighbor” clustering)

Reality: the reports tie crowding to “similar neighbors” and vector/crowding configs.
Also, duplication systems exist at the shingle/fingerprint layer.

Even if “DOM sameness penalty” isn’t 100% proven by the leak, **we don’t gamble**. We enforce structural divergence because it reduces dedup/crowding risk.

### Required layout differences by brand

#### KeylessSSL

- Docs-first IA (sidebar nav, code blocks, API refs, quickstart).
- Technical schema types where relevant (SoftwareApplication, TechArticle).

#### DelegatedSSL

- SaaS/enterprise IA (top nav, case studies, ROI calculators, security/compliance blocks).
- CaseStudy / Organization markup emphasis.

**AutoCertify**

- Wizard/diagnostic IA (single-column, step-by-step flows, “check my SSL” tools).
- FAQPage/HowTo markup emphasis.

**Engineering requirement**

- Separate layout components per brand (not just CSS theme tokens).
- Different section ordering and CTA structures per brand on key pages.

---

# 5) Cross-Domain Linking Policy (anti-poisoning)

Why: `UrlPoisoningData` tracks `spam_siblings`; outlink spam scoring appears in the analysis.

## Allowed cross-brand links

- Only on pages where the other brand is the correct “next step.”
- No more than **1 cross-brand link per page**.
- Anchor text must match target content (Anchor mismatch demotion exists).

## Forbidden link patterns

- Reciprocal sitewide links.
- “Partner network” blocks repeated across many pages.
- Mass cross-linking blog posts across brands.

## Operational kill switch

If we suspect poisoning:

- Temporarily remove cross-links
- Add `rel="nofollow"` to remaining cross-brand links until resolved

---

# 6) Content Publishing Rules (Shingle/Fingerprint safe)

Why: shingles/fingerprints are explicitly called out as near-duplicate detection infrastructure.

### A) Brand-specific editorial constraints

- Every article must be written as if the other two brands do not exist.
- Each article must use persona-native vocabulary (dev jargon vs ops jargon vs SMB language).

### B) “Shared topic” handling (47-day renewals, DCV, CNAME)

If the topic must appear on all three sites:

- Write **three different outlines** (not three versions of the same outline).
- Change:
  - intro problem framing
  - headings
  - examples
  - tool/screenshots
  - CTA goal

### C) Legal pages

Legal pages don’t need to rank.
Choose one:

1. Make them unique per brand (preferred)
2. Publish identical but set `noindex` on them across all brands

---

## 7) Performance & Noisy-Neighbor Controls (protect engagement + CWV)

Bad performance kills clicks; clicks feed re-ranking.
Your scaling blueprint already details the real risk: AutoCertify spikes stealing capacity and dragging the others down.

### Required controls

- Edge cache marketing pages aggressively (ISR/SSG where possible)
- WAF + bot controls + rate limiting on diagnostic endpoints (“check my SSL”, scans)
- Queue background work (DCV polling, renewals, scans) — never run long operations in web requests
- DB pooling + per-tenant quotas (max concurrent jobs, scan frequency, batch limits)

### Optional isolation (recommended)

- **Separate deployments per brand, same repo** to isolate compute burst limits while keeping one codebase.

---

## 8) Automated QA Gates (this is how we prevent “oops we shipped a doorway cluster”)

### A) Pre-deploy SEO smoke test (must pass for every release)

For each hostname (3 marketing + 3 app subdomains), test top routes:

**Marketing host assertions**

- Status 200
- `<title>` includes correct brand name
- `<meta name="description">` brand-unique
- `<link rel="canonical">` matches host + path (no params)
- `robots` allows indexing for marketing pages

**App host assertions**

- `X-Robots-Tag` includes `noindex`
- No marketing sitemap served on app host

**Sitemap assertions**

- Every `<loc>` URL in sitemap matches requesting hostname (no cross-domain contamination)

### B) Duplicate-content tripwire (weekly)

Run a similarity scan for:

- homepage
- pricing
- features
- top 20 blog posts per brand

If similarity exceeds threshold → block publish + rewrite. (We’re proactively avoiding shingle/fingerprint collisions.)

## 9) Monitoring & Alarms (so we see the punch before it lands)

### Search Console (per domain)

Watch:

- “Duplicate, Google chose different canonical”
- Index coverage drops
- Queries where CTR tanks after a release (possible NavBoost pain)

### Performance (per domain)

Track:

- p95 TTFB
- error rate
- CWV field data
- bot traffic share

(Again: engagement is a ranking weapon in this architecture.)

# The bottom line

This isn’t “SEO best practices.” This is **feature-aware defense**:

- **siteAuthority/siteFocusScore/siteRadius** → keep each domain topically pure.
- **NavBoost** → match intent and prevent pogo/bad clicks.
- **WebMirror + shingles** → no duplicates, canonicals must be correct.
- **Crowding “similar neighbors”** → enforce real semantic + structural separation.
- **UrlPoisoningData/spam_siblings** → don’t build a detectable link network.